Вариант 1

#1

Размер кода не ясен, но должен быть больше 20…

#2

Двоичный код (3, 6) с образующим многочленом $g(x) = x^3 + x + 1$

Не является циклическим:

$\frac{x^6-1}{x^3+x+1} = x^3 + x + 1 + \frac{x^2}{x^3+x+1}$, так как не делится без остатка.

Значит он просто полиномиальный.

Кодирующая матрица (3x6) строится как сдвиг образующего многочлена [0, 0, 1, 0, 1, 1] влево, начиная с нижней строки и до верхней:

1	0	1	1	0	0
0	1	0	1	1	0
0	0	1	0	1	1

Построим множество кодовых слов:

0	0	[0,0,0,0,0,0]
1	$x^3 + x + 1$	[0,0,1,0,1,1]
x	$x^4 + x^2 + x$	[0,1,0,1,1,0]
$x + 1$	$x^4 + x^3 + x^2 + 1$	[0,1,1,1,0,1]
x^2	$x^5 + x^3 + x^2$	[1,0,1,1,0,0]
$x^2 + 1$	$x^5 + x^2 + x + 1$	[1,0,0,1,1,1]
$x^2 + x$	$x^5 + x^4 + x^3 + x$	[1,1,1,0,1,0]
$x^2 + x + 1$	$x^5 + x^4 + 1$	[1,1,0,0,0,1]

Найдем остатки от деления на $g(x)$:

1	1	[0,0,1]
x	x	[0,1,0]
x^2	x^2	[1,0,0]
x^3	$x + 1$	[0,1,1]
x^4	$x^2 + x$	[1,1,0]

x^5	$x^2 + x + 1$	[1,1,1]

Запишем проверочную матрицу, используя эти остатки (вертикально):

1	1	0	1	0	0
1	1	1	0	1	0
1	0	1	0	0	1

Транспонированная проверочная матрица должна выдавать нулевой вектор при умножении на правильное кодовое слово:

Например на $x^5 + x^4 + 1$.

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

В результате получается нулевой вектор по модулю 2.

Кодовые слова - векторы размера 6 с элементами из множества {0,1}. Их общее количество составляет 64, но при кодировании используются только 8 из них, которые образуют подгруппу. Построим смежные с ней классы, поэтапно прибавляя вектор из общей группы ко всем векторам данной подгруппы:

Итого имеется 8 смежных классов:

Номер класса	Что прибавляли	Состав класса
1	[0, 0, 0, 0, 0, 0] [0, 0, 1, 0, 1, 1] [0, 1, 0, 1, 1, 0] [0, 1, 1, 1, 0, 1] [1, 0, 0, 1, 1, 1] [1, 0, 1, 1, 0, 0] [1, 1, 0, 0, 0, 1] [1, 1, 1, 0, 1, 0]	[0, 0, 0, 0, 0, 0] [0, 0, 1, 0, 1, 1] [0, 1, 0, 1, 1, 0] [0, 1, 1, 1, 0, 1] [1, 0, 1, 1, 0, 0] [1, 0, 0, 1, 1, 1] [1, 1, 1, 0, 1, 0] [1, 1, 0, 0, 0, 1]
2	[0, 0, 0, 0, 0, 1]	[0, 0, 0, 0, 0, 1]

	[0, 0, 1, 0, 1, 0] [0, 1, 0, 1, 1, 1] [0, 1, 1, 1, 0, 0] [1, 0, 0, 1, 1, 0] [1, 0, 1, 1, 0, 1] [1, 1, 0, 0, 0, 0] [1, 1, 1, 0, 1, 1]	[0, 0, 1, 0, 1, 0] [0, 1, 0, 1, 1, 1] [0, 1, 1, 1, 0, 0] [1, 0, 1, 1, 0, 1] [1, 0, 0, 1, 1, 0] [1, 1, 1, 0, 1, 1] [1, 1, 0, 0, 0, 0]
3	[0, 0, 0, 0, 1, 0] [0, 0, 1, 0, 0, 1] [0, 1, 0, 1, 0, 0] [0, 1, 1, 1, 1, 1] [1, 0, 0, 1, 0, 1] [1, 0, 1, 1, 1, 0] [1, 1, 0, 0, 1, 1] [1, 1, 1, 0, 0, 0]	[0, 0, 0, 0, 1, 0] [0, 0, 1, 0, 0, 1] [0, 1, 0, 1, 0, 0] [0, 1, 1, 1, 1, 1] [1, 0, 1, 1, 1, 0] [1, 0, 0, 1, 0, 1] [1, 1, 1, 0, 0, 0] [1, 1, 0, 0, 1, 1]
4	[0, 0, 0, 0, 1, 1] [0, 0, 1, 0, 0, 0] [0, 1, 0, 1, 0, 1] [0, 1, 1, 1, 1, 0] [1, 0, 0, 1, 0, 0] [1, 0, 1, 1, 1, 1] [1, 1, 0, 0, 1, 0] [1, 1, 1, 0, 0, 1]	[0, 0, 0, 0, 1, 1] [0, 0, 1, 0, 0, 0] [0, 1, 0, 1, 0, 1] [0, 1, 1, 1, 1, 0] [1, 0, 1, 1, 1, 1] [1, 0, 0, 1, 0, 0] [1, 1, 1, 0, 0, 1] [1, 1, 0, 0, 1, 0]
5	[0, 0, 0, 1, 0, 0] [0, 0, 1, 1, 1, 1] [0, 1, 0, 0, 1, 0] [0, 1, 1, 0, 0, 1] [1, 0, 0, 0, 1, 1] [1, 0, 1, 0, 0, 0] [1, 1, 0, 1, 0, 1] [1, 1, 1, 1, 1, 0]	[0, 0, 0, 1, 0, 0] [0, 0, 1, 1, 1, 1] [0, 1, 0, 0, 1, 0] [0, 1, 1, 0, 0, 1] [1, 0, 1, 0, 0, 0] [1, 0, 0, 0, 1, 1] [1, 1, 1, 1, 1, 0] [1, 1, 0, 1, 0, 1]
6	[0, 0, 0, 1, 0, 1] [0, 0, 1, 1, 1, 0] [0, 1, 0, 0, 1, 1] [0, 1, 1, 0, 0, 0] [1, 0, 0, 0, 1, 0] [1, 0, 1, 0, 0, 1] [1, 1, 0, 1, 0, 0] [1, 1, 1, 1, 1, 1]	[0, 0, 0, 1, 0, 1] [0, 0, 1, 1, 1, 0] [0, 1, 0, 0, 1, 1] [0, 1, 1, 0, 0, 0] [1, 0, 1, 0, 0, 1] [1, 0, 0, 0, 1, 0] [1, 1, 1, 1, 1, 1] [1, 1, 0, 1, 0, 0]
7	[0, 0, 0, 1, 1, 0]	[0, 0, 0, 1, 1, 0]

	[0, 0, 1, 1, 0, 1] [0, 1, 0, 0, 0, 0] [0, 1, 1, 0, 1, 1] [1, 0, 0, 0, 0, 1] [1, 0, 1, 0, 1, 0] [1, 1, 0, 1, 1, 1] [1, 1, 1, 1, 0, 0]	[0, 0, 1, 1, 0, 1] [0, 1, 0, 0, 0, 0] [0, 1, 1, 0, 1, 1] [1, 0, 1, 0, 1, 0] [1, 0, 0, 0, 0, 1] [1, 1, 1, 1, 0, 0] [1, 1, 0, 1, 1, 1]
8	[0, 0, 0, 1, 1, 1] [0, 0, 1, 1, 0, 0] [0, 1, 0, 0, 0, 1] [0, 1, 1, 0, 1, 0] [1, 0, 0, 0, 0, 0] [1, 0, 1, 0, 1, 1] [1, 1, 0, 1, 1, 0] [1, 1, 1, 1, 0, 1]	[0, 0, 0, 1, 1, 1] [0, 0, 1, 1, 0, 0] [0, 1, 0, 0, 0, 1] [0, 1, 1, 0, 1, 0] [1, 0, 1, 0, 1, 1] [1, 0, 0, 0, 0, 0] [1, 1, 1, 1, 0, 1] [1, 1, 0, 1, 1, 0]

Наименьшее расстояние может быть найдено либо, сравнивая вектора из таблицы напрямую и считая число разных элементов, либо как наименьшее число ненулевых элементов в векторе среди всех векторов, кроме нулевого. **В данном случае это 3.**

Чтобы код мог обнаружить k ошибок, минимальное расстояние должно составлять k+1, в данном случае **код обнаруживает 2 ошибки**.

Чтобы код мог исправить k ошибок, минимальное расстояние должно составлять 2k + 1, в данном случае **код исправляет 1 ошибку**.

В многочлене $x^5 + x^2 + 1$ **имеется ошибка**, во-первых, имеется не нулевой остаток (x) от деления на $g(x)$, во-вторых, это вектора нету среди множества кодовых слов, в-третьих, при умножении на проверочную матрицу появляется ненулевой элемент по модулю 2:

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

Данную ошибку **можно исправить.**

Первый способ — это найти ближайшие правильные коды, минимально отличающиеся от полученного вектора, если такой правильный код один, то использовать его, в данном случае получим этот вектор:

$$x^5 + x^2 + x + 1$$

Второй способ заключается в подсчете количества ненулевых элементов в векторе остатка (x). В данном случае он 1 и не превышает число ошибок, проверяемых кодом, поэтому чтобы исправить можно сложить этот вектор с полученным сообщением ($x^5 + x^2 + 1$ и x), тогда получим аналогичный результат.

#3

Группа должна состоять из чисел, взаимно простых с 27, т. е. не кратных 3:

$$Z_{27}^* = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$$

Найдем порождающий элемент напрямую, перебирая все числа:

1 - не подходит

$$1$$

2 - **подходит**:

$$2 \to 4 \to 8 \to 16 \to 5 \to 10 \to 20 \to 13 \to 26 \to 25 \to 23 \to 19 \to 11 \to 22 \to 17 \to 7 \to 14 \to 1$$

4 - не подходит:

$$4 \to 16 \to 10 \to 13 \to 25 \to 19 \to 22 \to 7 \to 1$$

5 - **подходит**:

$$5 \to 25 \to 17 \to 4 \to 20 \to 19 \to 14 \to 16 \to 26 \to 22 \to 2 \to 10 \to 23 \to 7 \to 8 \to 13 \to 11 \to 1$$

7 **–** не подходит

$$7 \to 22 \to 19 \to 25 \to 13 \to 10 \to 16 \to 4 \to 1$$

8 - не подходит:

$$8 \to 10 \to 26 \to 19 \to 17 \to 1$$

10 - не подходит:

$$10 \to 19 \to 1$$

11 - **подходит**:

$$11 \to 13 \to 8 \to 7 \to 23 \to 10 \to 2 \to 22 \to 26 \to 16 \to 14 \to 19 \to 20 \to 4 \to 17 \to 25 \to 5 \to 1$$

13 - не подходит:

$$13 \to 7 \to 10 \to 22 \to 16 \to 19 \to 4 \to 25 \to 1$$

14 - **подходит:**

$$14 \to 7 \to 17 \to 22 \to 11 \to 19 \to 23 \to 25 \to 26 \to 13 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

16 - не подходит:

$$16 \to 13 \to 19 \to 7 \to 4 \to 10 \to 25 \to 22 \to 1$$

17 - не подходит:

$$17 \to 19 \to 26 \to 10 \to 8 \to 1$$

19 - не подходит:

$$19 \to 10 \to 1$$

20 - **подходит**:

$$20 \to 22 \to 8 \to 25 \to 14 \to 10 \to 11 \to 4 \to 26 \to 7 \to 5 \to 19 \to 2 \to 13 \to 17 \to 16 \to 23 \to 1$$

22 - не подходит:

$$22 \to 25 \to 10 \to 4 \to 7 \to 19 \to 13 \to 16 \to 1$$

23 - **подходит**:

$$23 \to 16 \to 17 \to 13 \to 2 \to 19 \to 5 \to 7 \to 26 \to 4 \to 11 \to 10 \to 14 \to 25 \to 8 \to 22 \to 20 \to 1$$

25 - не подходит:

$$25 \to 4 \to 19 \to 16 \to 22 \to 10 \to 7 \to 13 \to 1$$

26 - не подходит

$$26 \to 1$$

Итого: $\{2,\ 5,\ 11,\ 14,\ 20,\ 23\}$ – порождающие элементы

#4

(не совпадает формула в 4-й части алгоритма: формула по лекции дает дробную степень, брал формулу из интернета)

Посчитать символ Якоби:

$$\left(\frac{221}{539}\right)$$

По определению:

Символ Лежандра:

$$\left(\frac{a}{p}\right) = 0,\ a\, mod\, p = 0$$

$$\left(\frac{a}{p}\right) = 1,\ a \text{ квадратичный вычет по модулю } p$$

$$\left(\frac{a}{p}\right) = -1,\ a \text{ квадратичный невычет по модулю } p$$

Разложим 539:

$$539 = 7 \cdot 7 \cdot 11$$

$$\left(\frac{221}{539}\right) = \left(\frac{221}{7}\right) \cdot \left(\frac{221}{7}\right) \cdot \left(\frac{221}{11}\right)$$

$$\left(\frac{221}{7}\right) = \left(\frac{4}{7}\right) = 1$$

$$\left(\frac{221}{11}\right) = \left(\frac{1}{11}\right) = 1$$

Получаем, что $\left(\frac{221}{539}\right) = 1 \cdot 1 \cdot 1 = 1$

По алгоритму: $J(221,\ 539)$

1.1) $221 < 539$

1.2) 221 не делится на 4

1.3) 221 не делится на 2

1.4) $(-1)^{\frac{221-1}{2} \cdot \frac{539-1}{2}} \cdot J(539,\ 221)$

$$(-1)^{110 \cdot 269} \cdot J(539,\ 221) = J(539,\ 221)$$

2.1) $539 > 221 \to J(97,\ 221)$

3.1) $97 < 221$

3.2) 97 не делится на 4

3.3) 97 не делится на 2

3.4) $(-1)^{\frac{97-1}{2} \cdot \frac{221-1}{2}} J(221,\ 97)$

$$(-1)^{48 \cdot 110} J(221,\ 97) = J(221,\ 97)$$

4.1) $221 > 97 \to J(27,\ 97)$

5.1) $27 < 97$

5.2) 27 не делится на 4

5.3) 27 не делится на 2

5.4) $J(27,\ 97) = (-1)^{\frac{27-1}{2}\cdot\frac{97-1}{2}} J(97,\ 27)$

$$(-1)^{13\cdot 48} J(97,\ 27) = J(97,\ 27)$$

6.1) $97 > 27 \rightarrow J(16,27)$

7.1) $16 < 27$

7.2) 16 делится на $4\ \rightarrow\ J(4,\ 27)$

8.1) $4 < 27$

8.2) 4 делится на $4\ \rightarrow\ J(1,\ 27)$

$$J\left(\frac{1}{m}\right) = 1$$

Т. к. при рекурсивных вызовах знак не менялся → $J(221,\ 539) = J(1,\ 27) = 1$

#5

Алгоритм Соловея-Штрассена работает с числами: $[2,\ n-1]$

В данной задаче это $[2,\ 20]$

Число является составным по алгоритму в двух случаях:

1) Если $\text{НОД}(a,\ n) > 1$, тогда подойдут: $\{3,\ 6,\ 7,\ 9,\ 12,\ 14,\ 15,\ 18\}$

$$3\colon \text{НОД}(3,21) = 3$$
$$6\colon \text{НОД}(6,21) = 3$$
$$7\colon \text{НОД}(7,21) = 7$$
$$9\colon \text{НОД}(9,21) = 3$$
$$12\colon \text{НОД}(12,21) = 3$$
$$14\colon \text{НОД}(14,21) = 7$$
$$15\colon \text{НОД}(15,21) = 3$$
$$18\colon \text{НОД}(18,21) = 3$$

2) Если $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} (mod\, n)$

$$\left(\frac{a}{21}\right) = \left(\frac{a}{3}\right) \cdot \left(\frac{a}{7}\right) - \text{по определению}$$
$$a^{\frac{21-1}{2}} = a^{10}$$

Квадратичные вычеты 3: $\{0,\ 1\}$

Квадратичные вычеты 7: $\{0,\ 1,\ 2,\ 4\}$

a = 2:

$$\left(\frac{2}{21}\right) = -1$$
$$2^{10} mod\ 21 = 16$$

a = 3:

$$\left(\frac{3}{21}\right) = 0$$
$$3^{10} mod\ 21 = 18$$

a = 4:

$$\left(\frac{4}{21}\right) = 1$$
$$4^{10}\ mod\ 21 = 4$$

a = 5:

$$\left(\frac{5}{21}\right) = 1$$
$$5^{10}\ mod\ 21 = 16$$

a = 6:

$$\left(\frac{6}{21}\right) = 0$$
$$6^{10}\ mod\ 21 = 15$$

a = 7:

$$\left(\frac{7}{21}\right) = 0$$
$$7^{10}\ mod\ 21 = 7$$

a = 8:

$$\left(\frac{8}{21}\right) = -1$$
$$8^{10}\ mod\ 21 = 1$$

a = 9:

$$\left(\frac{9}{21}\right) = 0$$
$$9^{10}\, mod\, 21 = 9$$

a = 10:

$$\left(\frac{10}{21}\right) = -1$$
$$10^{10}\, mod\, 21 = 4$$

a = 11:

$$\left(\frac{11}{21}\right) = -1$$
$$11^{10}\, mod\, 21 = 4$$

a = 12:

$$\left(\frac{12}{21}\right) = 0$$
$$12^{10}\, mod\, 21 = 9$$

a = 13:

$$\left(\frac{13}{21}\right) = -1$$
$$13^{10}\, mod\, 21 = 1$$

a = 14:

$$\left(\frac{14}{21}\right) = 0$$
$$14^{10}\, mod\, 21 = 7$$

a = 15:

$$\left(\frac{15}{21}\right) = 0$$
$$15^{10}\, mod\, 21 = 15$$

a = 16:

$$\left(\frac{16}{21}\right) = 1$$
$$16^{10}\, mod\, 21 = 16$$

a = 17:

$$\left(\frac{17}{21}\right) = 1$$
$$17^{10}\, mod\, 21 = 4$$

a = 18:

$$\left(\frac{18}{21}\right) = 0$$
$$17^{10}\, mod\, 21 = 18$$

a = 19:

$$\left(\frac{19}{21}\right) = -1$$
$$19^{10}\, mod\, 21 = 16$$

a = 20:

$$\left(\frac{20}{21}\right) = 1$$
$$20^{10}\, mod\, 21 = 1$$

Таким образом, по второму критерию подходит только ***20***

#6

$$y^2 = x^3 + 4x + 4,\ Z_5$$

Построим вообще все точки их никак не больше 25:

	0	1	2	3	4
y^2	0	1	4	4	1
$x^3 + 4x + 4$	4	4	0	3	4

Найдем такие пары (x, y), где выполняется равенство $y^2 = x^3 + 4x + 4$:

$$\{(0,2), (0,3), (1,2), (1,3), (2,0), (4,2), (4,3)\}$$

Проверим, что это множество является абелевой группой (по доказанному на лекции операция сложения коммутативна и ассоциативна, нейтральный элемент - бесконечно удаленная точка, остается проверить наличие противоположно элемента и замкнутости множества относительно операции сложения):

1) **Проверим наличие противоположного элемента и добавим нейтральный элемент - бесконечно удаленную точку** Θ **:**

$$(0,2) + (0,3) = \Theta$$

$$(1,2) + (1,3) = \Theta$$

$$(2,0) + (2,0) = \Theta$$

$$(4,2) + (4,3) = \Theta$$

Таким образом, для каждого элемента имеется противоположный элемент, также есть нейтральный.

2) **Проверим замыкание множества, относительно операции сложения:**

Попарно просуммируем множество точек (различных) по правилу:

При разных точках (не учитывая противоположные):

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \, mod\, 5$$

$$y_3 = y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_3 - x_1) \, mod\, 5$$

При одинаковых (не учитывая противоположные):

$$\lambda = \frac{3x_1^2 + 4}{2y_1} mod\, 5$$

$$x_3 = \lambda^2 - x_1 - x_1 \, mod\, 5$$

$$y_3 = \lambda(x_1 - x_3) - y_1 mod\, 5$$

Обозначим Θ , как null

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

(0, 2) + (0, 3) = null

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

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

(0, 2) + (2, 0) = (4, 2)

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

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

$(0, 3) + (0, 2) = \text{null}$

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

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

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

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

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

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

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

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

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

$(1, 2) + (1, 3) = \text{null}$

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

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

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

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

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

$(1, 3) + (1, 2) = \text{null}$

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

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

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

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

$(2, 0) + (0, 2) = (4, 2)$

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

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

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

(2, 0) + (2, 0) = null

(2, 0) + (4, 2) = (0, 2)

(2, 0) + (4, 3) = (0, 3)

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

(4, 2) + (0, 3) = (2, 0)

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

(4, 2) + (1, 3) = (4, 3)

(4, 2) + (2, 0) = (0, 2)

(4, 2) + (4, 2) = (1, 2)

(4, 2) + (4, 3) = null

(4, 3) + (0, 2) = (2, 0)

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

(4, 3) + (1, 2) = (4, 2)

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

(4, 3) + (2, 0) = (0, 3)

(4, 3) + (4, 2) = null

(4, 3) + (4, 3) = (1, 3)

Новых точек получено не было, следовательно множество является замкнутым, значит была построена группа: $\{(0,2),(0,3),(1,2),(1,3),(2,0),(4,2),(4,3),\Theta\}$

3) Определим является ли она циклической:

Проверим какая точка является порождающей:

(0, 2) - **порождающая**

$$(0,2) \to (1,2) \to (4,3) \to (2,0) \to (4,2) \to (1,3) \to (0,3) \to \Theta$$

(0, 3) - **порождающая**

$$(0,3) \to (1,3) \to (4,2) \to (2,0) \to (4,3) \to (1,2) \to (0,2) \to \Theta$$

(1, 2) - не порождающая

$$(1,2) \to (2,0) \to (1,3) \to \Theta$$

(1, 3) - не порождающая

$$(1,3) \to (2,0) \to (1,2) \to \Theta$$

(2, 0) - не порождающая

$$(2,0) \to \Theta$$

(4, 2) - **порождающая**

$$(4,2) \to (1,2) \to (0,3) \to (2,0) \to (0,2) \to (1,3) \to (4,3) \to \Theta$$

(4, 3) - **порождающая**

$$(4,3) \to (1,3) \to (0,2) \to (2,0) \to (0,3) \to (1,2) \to (4,2) \to \Theta$$

Θ - не порождающая

$\{(0,2), (0,3), (4,2), (4,3)\}$ - **порождающие точки,** они есть, значит группа **циклическая**