Семинар 17-18. Группа перестановок. Кольцо целых чисел.

Пусть $N = \{1, 2, \ldots, n\}$, где $n > 1$. *Перестановкой* π называется взаимнооднозначное отображение $\pi\colon N \to N$. Множество всех перестановок из n элементов с операцией композиции называется *группой перестановок* S_n.

Рассмотрим табличный способ задания перестановки. Перестановка

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

означает, что 1 переходит в $\pi(1)$, 2 в $\pi(2)$ и т.д.

Для примера возьмем S_5. Например, перестановка

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

означает, что элемент первой строки переходит в элемент второй строки в том же столбце, т.е. 1 переходит в 3, 2 переходит в 1, 3 переходит в 2, 4 в 5, а 5 в 4. Заметим, что перестановка столбцов в записи таблицы не влияет на смысл перестановки. Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}.$$

Операция на множестве перестановок задается следующим образом:

$$\pi \circ \rho(x) = \rho(\pi(x)).$$

Рассмотрим несколько задач.

Задача 1. Найти произведение подстановок $\alpha \circ \beta$ и $\beta \circ \alpha$ в S_5 для перестановок

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}.$$

Решение: Будем выполнять преобразования слева направо. Имеем

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}$$

В результате перестановки α 1 переходит в 5, а в результате перестановки β 5 переходит в 3. Значит, в результате композиции перестановок 1 переходит в 3:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & & & & \end{pmatrix}.$$

Аналогично, 2 в результате α переходит в 1, а 1 в результате β в 4. Получим:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & & & \end{pmatrix}.$$

Заполняя таблицу далее аналогично, получим

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

Аналогично,

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}.$$

Обратной к перестановке

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

называется перестановка

$$\pi = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix},$$

которую перестановкой столбцов можно привести к стандартному виду.

Задача 2. Вычислить обратные перестановки для α и β:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}.$$

Решение: Меняя строки, имеем

$$\alpha^{-1} = \begin{pmatrix} 5 & 1 & 2 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Эту перестановку можно привести к стандартному виду

$$\begin{pmatrix} 5 & 1 & 2 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}.$$

Аналогично для β:

$$\beta^{-1} = \begin{pmatrix} 4 & 2 & 5 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}.$$

Циклической перестановкой (циклом) называется перестановка элементов $i_1, \dots, i_n$, переводящая i_1 в i_2, i_2 в i_3, i_{n-1} в i_n, а i_n в i_1, причем остальные элементы остаются на месте. Такая перестановка обозначается $\begin{pmatrix} i_1 & i_2 & \dots & i_n \end{pmatrix}$. Таким образом,

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_{n-1} & i_n \\ i_2 & i_3 & \dots & i_n & i_1 \end{pmatrix}$$

Заметим, что циклическая перестановка элементов в записи цикла не влияет на содержательный смысл перестановки, то есть

$$\begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} = \begin{pmatrix} i_2 & i_3 & \dots & i_n & i_1 \end{pmatrix}$$

Циклические перестановки называются *независимыми*, если в их записи использованы разные элементы. Например, циклические перестановки $\begin{pmatrix} 2 & 3 \end{pmatrix}$ и $\begin{pmatrix} 1 & 5 & 4 \end{pmatrix}$ являются независимыми, а $\begin{pmatrix} 1 & 3 & 4 \end{pmatrix}$ и $\begin{pmatrix} 2 & 4 & 5 \end{pmatrix}$ — нет.

Любую перестановку можно представить в виде произведения независимых циклов. Например,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 3 & 2 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix},$$

при этом циклическую перестановку из одного элемента (что соответствует переходу элемента в себя), можно обозначать $\big(\big)$ и вообще не указывать в произведении:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 3 & 2 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 3 & 2 \end{pmatrix}.$$

Кстати, именно таким образом, $\big(\big)$, обозначается тождественная перестановка. Тождественная перестановка соответвует переходу каждого элемента в себя и является нейтральным элементов группы перестановок.

Задача 3. Записать перестановку, заданную в табличном виде в S_7,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix}$$

в виде произведения независимых циклов.

Решение: Первый цикл будем начинать с 1. При такой перестановке 1 переходит в 4. Значит,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 & \ldots \end{pmatrix} \ldots$$

Далее, 4 переходит в 1, а 1 — это начало цикла. Значит, на этом первый цикл можно закончить:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \ldots$$

Второй цикл начнем с любого элемента, не записанного в первом цикле, например, с 2. 2 при такой перестановке переходит в 3. Получим:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 & \ldots \end{pmatrix} \ldots$$

Однако 3 переходит в 2, а значит, второй цикл тоже можно закончить:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \ldots$$

Третий цикл начнем с элемента, который не используется в записи первых двух циклов, например, с 5. При этой перестановке 5 переходит в 7:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 5 & 7 & \ldots \end{pmatrix} \ldots$$

7 переходит в 6, а 6 — в 5. Помним, что 5 — это начало цикла. Значит, третий цикл также можно закончить:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 5 & 7 & 6 \end{pmatrix} \ldots$$

При этом не осталось элементов, которые были бы не использованы в одном из циклов, а значит, процесс можно закончить. Окончательно получим:

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

Задача 4. Записать перестановку, заданную в виде произведения независимых циклов в S_5, в табличном виде
$$\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4 & 5\end{pmatrix}.$$

Решение: Циклическая перестановка $\begin{pmatrix}1 & 2\end{pmatrix}$ означает, что 1 переходит в 2, а 2 — в 1. Запишем это:
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & & & \end{pmatrix}.$$
Далее, циклическая перестановка $\begin{pmatrix}3 & 4 & 5\end{pmatrix}$ означает, что 3 переходит в 4, 4 в 5, а 5 — в 3. Запишем и это:
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 4 & 5 & 3\end{pmatrix}$$

Задача 5. Записать перестановку, заданную в виде произведения независимых циклов в S_7, в табличном виде
$$\begin{pmatrix}1 & 3 & 2\end{pmatrix}\begin{pmatrix}7 & 6 & 5\end{pmatrix}.$$

Решение: Циклическая перестановка $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$ означает, что 1 переходит в 3, 3 в 2, а 2 — в 1. Запишем это:
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 1 & 2 & & & & \end{pmatrix}.$$
Далее, циклическая перестановка $\begin{pmatrix}7 & 6 & 5\end{pmatrix}$ означает, что 7 переходит в 6, 6 в 5, а 5 — в 7. Запишем и это:
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 1 & 2 & & 7 & 5 & 6\end{pmatrix}.$$
Осталось указать, что 4 при такой перестановке переходит в себя:
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 1 & 2 & 4 & 7 & 5 & 6\end{pmatrix}.$$

Для нахождения произведения перестановок, записанных в виде произведения независимых циклов, совершенно не обязательно записывать их в табличном виде. Достаточно только понимать, что стоит за каждой циклической перестановкой.

Задача 6. Вычислить произведение перестановок, заданных в S_5 в виде произведения независимых циклов:
$$\alpha = \begin{pmatrix}1 & 5 & 3 & 2\end{pmatrix}, \quad \beta = \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}$$

Решение: Начнем записывать полученное произведение, начиная с 1.
$$\alpha\circ\beta = \begin{pmatrix}1 & 5 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix} = \begin{pmatrix}1 & \ldots\end{pmatrix}\ldots$$
В результате первого цикла в записи произведения 1 переходит в 5, цикл $\begin{pmatrix}1 & 4\end{pmatrix}$ не содержит 5, а в результате последней перестановки 5 переходит в 3. Таким образом, в результате произведения 1 переходит в 3:
$$\alpha\circ\beta = \begin{pmatrix}\boxed{1} & \boxed{5} & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}\boxed{3} & \boxed{5}\end{pmatrix} = \begin{pmatrix}1 & 3 & \ldots\end{pmatrix}\ldots$$
Теперь смотрим, куда в результате перестановки переходит 3. В результате первого цикла 3 переходит в 2. Поскольку больше ни один цикл не содержит в своей записи 2, в результате всех остальных циклов 2 переходит в себя. Получим:
$$\alpha\circ\beta = \begin{pmatrix}1 & 5 & \boxed{3} & \boxed{2}\end{pmatrix}\begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix} = \begin{pmatrix}1 & 3 & 2 & \ldots\end{pmatrix}\ldots$$

Теперь смотрим, куда в результате перестановки переходит 2. В результате первого цикла 2 переходит в 1, а в результате второго цикла 1 переходит в 4. Получим, что в результате произведения циклов 2 переходит в 4. Имеем:

$$\alpha\circ\beta=\begin{pmatrix}\boxed{1} & 5 & 3 & \boxed{2}\end{pmatrix}\begin{pmatrix}\boxed{1} & \boxed{4}\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2 & 4 & \ldots\end{pmatrix}\ldots$$

Теперь смотрим, куда в результате перестановки переходит 4. В результате первого цикла 4 переходит в себя, поскольку первый цикл не содержит в своей записи 4. В результате второго цикла 4 переходит в 1. Значит, в результате произведения 4 переходит в 1. Поскольку 1 является первым элементом получаемого цикла, запись этого цикла можно закончить:

$$\alpha\circ\beta=\begin{pmatrix}1 & 5 & 3 & 2\end{pmatrix}\begin{pmatrix}\boxed{1} & \boxed{4}\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}\ldots$$

Новый цикл начинаем с элемента, который не участвует в записи первого цикла. Такой элемент всего один — 5. Значит, начинаем новый цикл с 5:

$$\alpha\circ\beta=\begin{pmatrix}1 & 5 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}\begin{pmatrix}5 & \ldots\end{pmatrix}$$

5 переходит в результате первого цикла в 3, а 3 в результате последнего цикла в 5. Следовательно, 5 переходит в себя при произведении. Значит, и второй цикл можно закончить. Окончательно получим:

$$\alpha\circ\beta=\begin{pmatrix}1 & \boxed{5} & \boxed{3} & 2\end{pmatrix}\begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}\boxed{3} & \boxed{5}\end{pmatrix}=\begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}\begin{pmatrix}5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}$$

Для циклической перестановки

$$\begin{pmatrix}i_1 & \ldots & i_k\end{pmatrix}$$

обратной является перестановка

$$\begin{pmatrix}i_k & \ldots & i_1\end{pmatrix},$$

которую можно получить, записав элементы цикла в обратном порядке.

Если перестановка задана в виде произведения циклов (не обязательно независимых)

$$\alpha=\begin{pmatrix}i_1 & \ldots & i_k\end{pmatrix}\ldots\begin{pmatrix}j_1 & \ldots & j_m\end{pmatrix},$$

то обратной к ней будет перестановка

$$\alpha^{-1}=\begin{pmatrix}j_m & \ldots & j_1\end{pmatrix}\ldots\begin{pmatrix}i_k & \ldots & i_1\end{pmatrix}.$$

Для получения такой перестановки надо записать в обратном порядке все циклы, участвующие в произведении, и обратить каждый цикл. Для обращения произведения независимых циклов не обязательно записывать циклы в обратном порядке. Например, обратной к перестановке

$$\alpha=\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4 & 5\end{pmatrix}$$

является перестановка

$$\alpha^{-1}=\begin{pmatrix}3 & 1\end{pmatrix}\begin{pmatrix}5 & 4 & 2\end{pmatrix}.$$

Заметим также, что обратным к циклу длины 2 является тот же цикл, поскольку

$$\begin{pmatrix}i_1 & i_2\end{pmatrix}=\begin{pmatrix}i_2 & i_1\end{pmatrix}.$$

Для решения уравнения в группе перестановок вида

$$\begin{pmatrix} i_1 & \dots & i_k \end{pmatrix} X = \begin{pmatrix} j_1 & \dots & j_m \end{pmatrix},$$

нужно выразить X из уравнения, домножив обе части уравнения на обратную к перестановке $\begin{pmatrix} i_1 & \dots & i_k \end{pmatrix}$ слева:

$$X = \begin{pmatrix} i_k & \dots & i_1 \end{pmatrix} \begin{pmatrix} j_1 & \dots & j_m \end{pmatrix}.$$

Аналогично, для решения уравнения вида

$$X \begin{pmatrix} i_1 & \dots & i_k \end{pmatrix} = \begin{pmatrix} j_1 & \dots & j_m \end{pmatrix},$$

нужно выразить X из уравнения, домножив обе части уравнения на обратную к перестановке $\begin{pmatrix} i_1 & \dots & i_k \end{pmatrix}$ справа:

$$X = \begin{pmatrix} j_1 & \dots & j_m \end{pmatrix} \begin{pmatrix} i_k & \dots & i_1 \end{pmatrix}.$$

Эти же соображения позволят нам решать более сложные уравнения в группе перестановок.

Задача 7. Решить уравнение в группе перестановок S_7:

$$\begin{pmatrix} 6 & 4 & 7 & 5 & 3 & 1 & 2 \end{pmatrix} X \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \end{pmatrix} \begin{pmatrix} 4 & 6 & 5 & 7 & 2 & 3 & 1 \end{pmatrix}$$

Решение: Выразив X из уравнения, получим

$$X = \begin{pmatrix} 2 & 1 & 3 & 5 & 7 & 4 & 6 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \end{pmatrix} \begin{pmatrix} 4 & 6 & 5 & 7 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}.$$

Для получения решения достаточно выполнить умножение циклов. Окончательно получаем:

$$X = \begin{pmatrix} 1 & 6 & 2 & 4 & 7 & 3 & 5 \end{pmatrix}.$$

Задача 8. Решить уравнение в группе перестановок S_7:

$$\begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} 2 & 7 & 3 \end{pmatrix} X \begin{pmatrix} 1 & 6 & 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix}$$

Решение: Коэффициент перед (и после) X представляет собой произведение двух зависимых циклов. Имеем

$$\left(\begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} 2 & 7 & 3 \end{pmatrix}\right)^{-1} = \begin{pmatrix} 3 & 7 & 2 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix},$$

$$\left(\begin{pmatrix} 1 & 6 & 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 & 7 \end{pmatrix}\right)^{-1} = \begin{pmatrix} 7 & 4 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 & 6 & 1 \end{pmatrix}.$$

Таким образом, выразив X из уравнения, получим

$$X = \begin{pmatrix} 3 & 7 & 2 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix} \begin{pmatrix} 7 & 4 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 & 6 & 1 \end{pmatrix}.$$

Для получения решения достаточно выполнить умножение циклов. Окончательно получаем:

$$X = \begin{pmatrix} 1 & 7 & 2 & 5 & 3 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix}.$$

Проверка

$$\begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} 2 & 7 & 3 \end{pmatrix} \begin{pmatrix} 1 & 7 & 2 & 5 & 3 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 6 & 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix}$$

подтверждает правильность решения уравнения.

Порядок и четность перестановки

Напомню, что порядок элемента a группы определяется как наименьшее натуральное число k, такое, что $a^k = e$. Для цикла длины k порядок равен k. Порядок произведения независимых циклов определяется как НОК[1]$(k_1, \dots, k_\tau)$, где k_i — длина i-того цикла в

[1]Наименьшее общее кратное.

произведении. Таким образом, для того, чтобы определить порядок перестановки, нужно записать ее в виде произведения независимых циклов.

Задача 9. Определить порядок перестановки

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix}.$$

Решение: Воспользовавшись результатом решения задачи 3, имеем

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

Полученная перестановка содержит 2 цикла длины 2 и один цикл длины 3. Таким образом,

$$\mathrm{ord}(\tau) = \text{НОК}(2, 2, 3) = 6.$$

Инверсией перестановки π называется пара индексов (i, j) такая, что $1 \le i < j \le n$ и $\pi(i) > \pi(j)$. Если число инверсий четно, то перестановка называется *четной*, иначе — *нечетной*.

Задача 10. Найти все инверсии и определить четность перестановки

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

Решение: Инверсии образуют пары индексов $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$. Например, пара $(1,4)$ является инверсией, поскольку $\tau(1) = 3$, $\tau(4) = 1$, а $3 > 1$. Число инверсий нечетное, а значит, перестановка нечетная.

Чтобы определить четность перестановки, не обязательно искать все инверсии. Другим способом нахождения четности перестановки является представление перестановки в виде произведения транспозиций. *Транспозицией* называется цикл длины 2. Одним из способов разложения цикла в произведение транспозиций является следующий:

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \end{pmatrix} = \begin{pmatrix} i_{k-1} & i_k \end{pmatrix} \begin{pmatrix} i_{k-2} & i_{k-1} \end{pmatrix} \dots \begin{pmatrix} i_2 & i_3 \end{pmatrix} \begin{pmatrix} i_1 & i_2 \end{pmatrix}$$

Если число транспозиций четно, то перестановка четная, иначе — нечетная. Этот способ разложения на транспозиции не единственный, но при использовании любого способа число четность перестановок оказывается постоянным. Верна формула

$$\mathrm{sgn}(\tau) = (-1)^k,$$

где k — число транспозиций в разложении на транспозиции перестановки τ. Если $\mathrm{sgn}(\tau) = 1$, то перестановка τ четная, иначе — нечетная.

Таким образом, четность циклической перестановки можно определить по следующей формуле:

$$\mathrm{sgn}(\tau) = (-1)^{k-1},$$

где k — длина циклической перестановки.

Если перестановка разложена на произведение независимых циклов, то четность перестановки можно определить по следующей формуле:

$$\mathrm{sgn}\,\sigma = (-1)^{k_1 - 1} \cdot \ldots \cdot (-1)^{k_r - 1}$$

где k_i — длина i-того цикла в разложении σ, r — число циклических перестановок в разложении σ.

Задача 11. Определить четность и порядок перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 3 & 2 & 6 & 9 & 7 & 8 \end{pmatrix}.$$

Решение: Представим перестановку в виде произведения независимых циклов:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 3 & 2 & 6 & 9 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 7 & 9 & 8 \end{pmatrix}.$$

Пусть

$$\sigma_1 = \begin{pmatrix} 1 & 5 & 2 & 4 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 7 & 9 & 8 \end{pmatrix}.$$

Определим порядок перестановки. Длины циклов σ_1, σ_2 равны 5 и 3 соответственно, поэтому

$$\operatorname{ord}(\sigma_1) = 5, \quad \operatorname{ord}(\sigma_1) = 3,$$

а значит,

$$\operatorname{ord}(\sigma) = \text{НОК}(5, 3) = 15.$$

Определим четность перестановки. Длины циклов σ_1, σ_2 равны 5 и 3 соответственно, поэтому

$$\operatorname{sgn}(\sigma_1) = (-1)^{(5-1)} = 1, \quad \operatorname{sgn}(\sigma_2) = (-1)^{(3-1)} = 1,$$

а значит,

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma_1) \operatorname{sgn}(\sigma_2) = 1 \cdot 1 = 1.$$

Значит, перестановка σ четная.

Понятие порядка позволяет вычислять степени различных перестановок. В самом деле, если порядок элемента a равен k, то

$$a^{mk} = e, \quad \forall m \in \mathbb{Z}.$$

Произведение независимых циклов коммутативно. Это дает еще один бонус записи перестановки в виде произведения независимых циклов, поскольку степень перестановки можно вычислять по формуле

$$\sigma^m = \sigma_1^m \circ \cdots \circ \sigma_r^m,$$

где σ_i — независимые циклы в разложении перестановки σ.

Задача 12. Вычислить α^{515} для перестановки

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

Решение: Запишем перестановку в виде произведения независимых циклов:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}.$$

Поскольку циклы являются независимыми, можно вычислить степень перестановки следующим образом:

$$\alpha^m = \alpha_1^m \circ \alpha_2^m.$$

Пусть

$$\alpha_1 = \begin{pmatrix}1 & 3 & 5\end{pmatrix}, \quad \alpha_2 = \begin{pmatrix}2 & 4\end{pmatrix}.$$

Порядки этих циклов равны

$$\operatorname{ord}(\alpha_1) = 3, \quad \operatorname{ord}(\alpha_2) = 2.$$

Вычислим α_1^{515}. Поскольку

$$515 = 513 + 2 = 3 \cdot 171 + 2,$$

то

$$\alpha_1^{515} = \alpha_1^{513} \circ \alpha_1^2 = (\alpha_1^3)^{171} \circ \alpha_1^2 = \alpha_1^2.$$

Вычисление α_1^2 дает

$$\alpha_1^2 = \begin{pmatrix}1 & 3 & 5\end{pmatrix}^2 = \begin{pmatrix}1 & 5 & 3\end{pmatrix}.$$

Заметим, что вычислить α_1^{515} можно иначе. Представим число 515 как

$$515 = 516 - 1 = 3 \cdot 172 - 1,$$

и получим

$$\alpha_1^{515} = \alpha_1^{516} \circ \alpha_1^{-1} = (\alpha_1^3)^{172} \circ \alpha_1^{-1} = \alpha_1^{-1} = \begin{pmatrix}5 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 5 & 3\end{pmatrix}.$$

Вычислим α_2^{515}. Поскольку

$$515 = 514 + 1 = 2 \cdot 257 + 1,$$

то

$$\alpha_2^{515} = \alpha_2^{514} \circ \alpha_2^1 = (\alpha_2^2)^{257} \circ \alpha_2 = \alpha_2 = \begin{pmatrix}2 & 4\end{pmatrix}.$$

Таким образом,

$$\alpha^{515} = \alpha_1^{515} \circ \alpha_2^{515} = \begin{pmatrix}1 & 5 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}.$$

Задача 13. Вычислить α^{418} для перестановки

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 10 & 1 & 8 & 2 & 5 & 3 & 9 & 7 & 6 & 4\end{pmatrix}.$$

Решение: Представим перестановку в виде произведения независимых циклов:

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 10 & 1 & 8 & 2 & 5 & 3 & 9 & 7 & 6 & 4\end{pmatrix} = \begin{pmatrix}1 & 10 & 4 & 2\end{pmatrix}\begin{pmatrix}3 & 8 & 7 & 9 & 6\end{pmatrix}.$$

Пусть

$$\alpha_1 = \begin{pmatrix}1 & 10 & 4 & 2\end{pmatrix}, \quad \alpha_2 = \begin{pmatrix}3 & 8 & 7 & 9 & 6\end{pmatrix}.$$

Таким образом,

$$\operatorname{ord}(\alpha_1) = 4, \quad \operatorname{ord}(\alpha_2) = 5.$$

Вычислим α_1^{418}. Будем считать, что

$$418 = 416 + 2 = 4 \cdot 104 + 2.$$

Таким образом,

$$\alpha_1^{418} = \alpha_1^{416} \circ \alpha_1^2 = (\alpha_1^4)^{104} \circ \alpha_1^2 = \alpha_1^2.$$

Имеем
$$\alpha_1^2 = \begin{pmatrix}1 & 10 & 4 & 2\end{pmatrix}^2 = \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 10\end{pmatrix}.$$

Вычислим α_2^{418}. Будем считать, что
$$418 = 415 + 3 = 5 \cdot 83 + 3.$$

Таким образом,
$$\alpha_2^{418} = \alpha_2^{415} \circ \alpha_2^3 = (\alpha_2^5)^{83} \circ \alpha_2^3 = \alpha_2^3.$$

Имеем
$$\alpha_2^3 = \begin{pmatrix}3 & 8 & 7 & 9 & 6\end{pmatrix}^3 = \begin{pmatrix}3 & 9 & 8 & 6 & 7\end{pmatrix}.$$

В итоге получим
$$\alpha^{418} = \alpha_1^{418}\alpha_2^{418} = \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 10\end{pmatrix}\begin{pmatrix}3 & 9 & 8 & 6 & 7\end{pmatrix}.$$

Несколько теоретических задач

Задача 14. Содержит ли группа перестановок S_{10} элемент порядка 7? Порядка 16? Порядка 21? Порядка 30? Порядка 40? Ответ обосновать.

Решение:
1. *Порядка 7.* Да, например, цикл длины 7.
2. *Порядка 16.* Нет. Элемент такого порядка нельзя получить без цикла длины 16, но такой цикл не принадлежит S_{10}.
3. *Порядка 21.* Да, например, произведение независимых циклов длин 3 и 7, поскольку $\text{НОК}(3,7) = 21$.
4. *Порядка 30.* Да, например, произведение независимых циклов длин 2, 3 и 5, поскольку $\text{НОК}(2,3,5) = 30$.
5. *Порядка 40.* Нет. $\text{НОК}(5,8) = 40$, при этом 5 и 8 — наименьшие числа a и b, которые удовлетворяют условию $\text{НОК}(a,b) = 40$. При этом для составления двух независимых циклов длин 5 и 8 понадобится 13 чисел.

Задача 15. Изоморфна ли группа перестановок S_4 группе симметрий правильного 12-угольника D_{12}?

Решение: Порядки этих групп равны:
$$|S_4| = 4! = 24, \quad |D_{12}| = 2 \cdot 12 = 24.$$

Однако группы не изоморфны. При изоморфизме порядки всех элементов групп должны совпадать, однако в нашем случае это не так: в группе D_{12} есть элемент порядка 12 (например, поворот относительно центра на угол $\frac{360^\circ}{12} = 30^\circ$), а в группе S_4 такого элемента нет (в самом деле, $12 = \text{НОК}(3,4)$, а в группе S_4 недостаточно элементов для образования двух независимых циклов длин 3 и 4).

Задача 16. В группе перестановок S_9 найти подгруппу, порожденную транспозициями $\sigma = \begin{pmatrix}2 & 5\end{pmatrix}$ и $\tau = \begin{pmatrix}5 & 8\end{pmatrix}$. Какой из следующих групп изоморфна эта группа: $\mathbb{Z}_5$, $\mathbb{Z}_6$, S_3?

Решение: Вычислим все элементы такой подгруппы. Обратные к элементам σ и τ равны σ и τ соответственно. Квадраты этих перестановок равны $()$, то есть тождественной перестановке. Вычислим произведения $\sigma \circ \tau$ и $\tau \circ \sigma$:
$$\sigma \circ \tau = \begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}5 & 8\end{pmatrix} = \begin{pmatrix}2 & 8 & 5\end{pmatrix},$$

$$\tau \circ \sigma = \begin{pmatrix}5 & 8\end{pmatrix}\begin{pmatrix}2 & 5\end{pmatrix} = \begin{pmatrix}2 & 5 & 8\end{pmatrix}.$$

Таким образом, перестановки $\begin{pmatrix}2 & 8 & 5\end{pmatrix}$ и $\begin{pmatrix}2 & 5 & 8\end{pmatrix}$ также являются элементами этой группы. Вычислим произведения элементов σ и τ с этим элементами:

$$\begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}2 & 8 & 5\end{pmatrix} = \begin{pmatrix}5 & 8\end{pmatrix},$$

$$\begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}2 & 5 & 8\end{pmatrix} = \begin{pmatrix}2 & 8\end{pmatrix},$$
$$\begin{pmatrix}5 & 8\end{pmatrix}\begin{pmatrix}2 & 8 & 5\end{pmatrix} = \begin{pmatrix}2 & 8\end{pmatrix},$$
$$\begin{pmatrix}5 & 8\end{pmatrix}\begin{pmatrix}2 & 5 & 8\end{pmatrix} = \begin{pmatrix}2 & 5\end{pmatrix}.$$

Получили одну новую перестановку: $\begin{pmatrix}2 & 8\end{pmatrix}$. Можно вычислить также произведения этой перестановки с другими перестановками этой группы, но новых перестановок не появится. Таким образом, группа, порожденная транспозициями σ и τ, содержит 6 элементов:

$$\Big\{(), \quad \begin{pmatrix}2 & 5\end{pmatrix}, \quad \begin{pmatrix}5 & 8\end{pmatrix}, \quad \begin{pmatrix}2 & 8\end{pmatrix}, \quad \begin{pmatrix}2 & 5 & 8\end{pmatrix}, \quad \begin{pmatrix}2 & 8 & 5\end{pmatrix}\Big\}.$$

Теперь выясним, какой из групп $\mathbb{Z}_5$, $\mathbb{Z}_6$, S_3 изоморфна следующая подгруппа. Очевидно, что она не изоморфна $\mathbb{Z}_5$, поскольку эти группы содержат разное число элементов. Эта группа не изоморфна $\mathbb{Z}_6$, поскольку группа $\mathbb{Z}_6$ содержит элемент порядка 6 (например, 1), а рассматриваемая подгруппа — нет. Таким образом, рассматриваемая подгруппа может быть симметрична S_3. Для доказательства достаточно построить изоморфизм (установить взаимно однозначное соответствие) этих групп. Будем полагать

$$\begin{aligned}
()_9 \quad &\longleftrightarrow \quad ()_3, \\
\begin{pmatrix}2 & 5\end{pmatrix}_9 \quad &\longleftrightarrow \quad \begin{pmatrix}1 & 2\end{pmatrix}_3, \\
\begin{pmatrix}5 & 8\end{pmatrix}_9 \quad &\longleftrightarrow \quad \begin{pmatrix}2 & 3\end{pmatrix}_3, \\
\begin{pmatrix}2 & 8\end{pmatrix}_9 \quad &\longleftrightarrow \quad \begin{pmatrix}1 & 3\end{pmatrix}_3, \\
\begin{pmatrix}2 & 5 & 8\end{pmatrix}_9 \quad &\longleftrightarrow \quad \begin{pmatrix}1 & 2 & 3\end{pmatrix}_3, \\
\begin{pmatrix}2 & 8 & 5\end{pmatrix}_9 \quad &\longleftrightarrow \quad \begin{pmatrix}1 & 3 & 2\end{pmatrix}_3.
\end{aligned}$$

Для установления такого соответствия поможет вычисление порядков элементов группы. Взаимно однозначное соответствие нужно устанавливать между элементами равных порядков.

Задача 17. В группе перестановок S_7 найти подгруппу, порожденную транспозицией $\sigma = \begin{pmatrix}2 & 3\end{pmatrix}$ и циклом $\tau = \begin{pmatrix}1 & 6 & 7\end{pmatrix}$. Какой из следующих групп изоморфна эта группа: V_4, $\mathbb{Z}_6$, S_3?

Решение: Вычислим все элементы такой подгруппы. Квадрат цикла $\tau = \begin{pmatrix}1 & 6 & 7\end{pmatrix}$ равен $\tau^2 = \begin{pmatrix}1 & 7 & 6\end{pmatrix}$, а квадрат транспозиции $\sigma = \begin{pmatrix}2 & 3\end{pmatrix}$ равен $()$, то есть тождественной перестановке. Поскольку две порождающие перестановки являются независимыми циклами, всеми элементами этой группы будут являться следующие перестановки:

$$\Big\{(), \quad \begin{pmatrix}2 & 3\end{pmatrix}, \quad \begin{pmatrix}1 & 6 & 7\end{pmatrix}, \quad \begin{pmatrix}1 & 7 & 6\end{pmatrix}, \quad \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 7 & 6\end{pmatrix}, \quad \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 6 & 7\end{pmatrix}\Big\}.$$

Теперь выясним, какой из групп V_4, $\mathbb{Z}_6$, S_3 изоморфна следующая подгруппа. Очевидно, что она не изоморфна V_4, поскольку эти группы содержат разное число элементов. Эта группа не изоморфна S_3, поскольку полученная подгруппа содержит элемент порядка 6 (например, $\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 6 & 7\end{pmatrix}$), а группа S_3 — нет. Таким образом, рассматриваемая подгруппа может быть симметрична $\mathbb{Z}_6$. Для доказательства достаточно построить изоморфизм этих групп. Установлению этого взаимно однозначного соответствия поможет нахождения порядков элементов рассматриваемой подгруппы. Находим:

$$\mathrm{ord}() = 1, \quad \mathrm{ord}\begin{pmatrix}2 & 3\end{pmatrix} = 2, \quad \mathrm{ord}\begin{pmatrix}1 & 6 & 7\end{pmatrix} = 3, \quad \mathrm{ord}\begin{pmatrix}1 & 7 & 6\end{pmatrix} = 3,$$

$$\mathrm{ord}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 7 & 6\end{pmatrix} = 6, \quad \mathrm{ord}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 6 & 7\end{pmatrix} = 6.$$

Будем полагать

$$\begin{array}{rcl} () & \longleftrightarrow & 0, \\ \begin{pmatrix}2 & 3\end{pmatrix} & \longleftrightarrow & 3, \\ \begin{pmatrix}1 & 6 & 7\end{pmatrix} & \longleftrightarrow & 2, \\ \begin{pmatrix}1 & 7 & 6\end{pmatrix} & \longleftrightarrow & 4, \\ \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 7 & 6\end{pmatrix} & \longleftrightarrow & 1, \\ \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 6 & 7\end{pmatrix} & \longleftrightarrow & 5. \end{array}$$

Последние две задачи являются хорошей иллюстрацией *теоремы Кэли*: любая конечная группа изоморфна некоторой подгруппе группы перестановок множества элементов этой группы.

Кольцо целых чисел

Пусть K — множество с операциями $+$ и $\cdot$, удовлетворяющая свойствам:
1) $(K, +)$ — абелева группа,
2) $(a + b) \cdot c = a \cdot c + b \cdot c$ (дистрибутивность),
3) $c \cdot (a + b) = c \cdot a + c \cdot b$. Тогда $(K, +, \cdot)$ называется *кольцом*. Если операция умножения ассоциативна, то кольцо называется *ассоциативным*. Если $(K, \cdot)$ — моноид, то кольцо называется *кольцом с единицей*. Кольцо называется *коммутативным*, если операция умножения коммутативна: $x \cdot y = y \cdot x$. Нейтральный элемент по сложению принято обозначать 0, нейтральный элемент по умножению (для колец с единицей) — 1.

Задача 18. Доказать, что множество целых чисел с операциями сложения и умножения образует коммутативное кольцо с единицей.

Пара важных свойств колец:
1) $a \cdot 0 = 0$, $\forall a \in K$,
2) $0 \neq 1$ (для кольца, в котором больше двух элементов).

Рассмотрим кольцо целых чисел. *Алгоритм Евклида* позволяет находить НОД(a, b) для любых целых чисел a, b. Этот алгоритм заключается в последовательном делении с остатком. Алгоритм останавливается, когда последний остаток равен 0. При этом НОД(a, b) равен последнему ненулевому остатку. Рассмотрим этот алгоритм на примере.

Задача 19. Найти НОД$(111, 90)$ с помощью алгоритма Евклида.
Решение: Число 111 больше 90, поэтому будем делить 111 на 90 с остатком:

$$111 = 1 \cdot 90 + 21.$$

Теперь будем делить 90 на остаток от деления 111 на 90, на 21:

$$90 = 4 \cdot 21 + 6.$$

Далее, делим 21 на остаток от деления 90 на 21:

$$21 = 3 \cdot 6 + 3.$$

Теперь делим 6 на остаток от деления 21 на 6:

$$6 = 2 \cdot 3 + 0.$$

Получили остаток, равный 0. Последний ненулевой остаток равен 3. Поэтому НОД$(111, 90) = 3$. Получили следующий алгоритм:

$$\begin{aligned} 111 &= 1 \cdot \underline{90} + \underline{21}, \\ 90 &= 4 \cdot \underline{21} + \underline{6}, \\ 21 &= 3 \cdot \underline{6} + \underline{3}, \\ 6 &= 2 \cdot \underline{3} + 0. \end{aligned}$$

Задача 20. Найти НОД$(511, 292)$ с помощью алгоритма Евклида.

Решение: Число 511 больше 292, поэтому будем делить 511 на 292 с остатком. Получим следующий алгоритм:

$$\begin{aligned} 511 &= 1 \cdot \underline{292} + \underline{219}, \\ 292 &= 1 \cdot \underline{219} + \underline{73}, \\ 219 &= 3 \cdot \underline{73} + 0. \end{aligned}$$

Таким образом, НОД$(511, 292) = 73$.

Задача 21. Найти НОД$(1313, 13953)$ с помощью алгоритма Евклида.

Решение: Число 13953 больше 1313, поэтому будем делить 13953 на 1313 с остатком. Получим следующий алгоритм:

$$\begin{aligned} 13953 &= 10 \cdot \underline{1313} + \underline{823}, \\ 1313 &= 1 \cdot \underline{823} + \underline{490}, \\ 823 &= 1 \cdot \underline{490} + \underline{333}, \\ 490 &= 1 \cdot \underline{333} + \underline{157}, \\ 333 &= 2 \cdot \underline{157} + \underline{19}, \\ 157 &= 8 \cdot \underline{19} + \underline{5}, \\ 19 &= 3 \cdot \underline{5} + \underline{4}, \\ 5 &= 1 \cdot \underline{4} + \underline{1}, \\ 4 &= 4 \cdot \underline{1} + 0. \end{aligned}$$

Таким образом, НОД$(1313, 13953) = 1$, то есть числа 13953 и 1313 являются взаимно простыми.

Если НОД$(a, b) = d$, то существуют такие целые числа u, v, что имеет место равенство

$$d = u \cdot a + v \cdot b,$$

то есть d линейно выражается через числа a, b. Такое представление иногда называют *отношением Безу.*

Задача 22. Найти линейное представление НОД$(111, 90)$ через числа 111 и 90 с помощью алгоритма Евклида.

Решение: Сначала выразим остатки от деления, получаемые по алгоритму Евклида. Алгоритм Евклида для этих чисел был применен в задаче 18. Имеем:

$$\begin{aligned} 111 = 1\cdot 90 + 21 &\;\to\; 21 = 111 - 1\cdot 90,\\ 90 = 4\cdot 21 + 6 &\;\to\; 6 = 90 - 4\cdot 21,\\ 21 = 3\cdot 6 + 3 &\;\to\; 3 = 21 - 3\cdot 6. \end{aligned}$$

Теперь выражаем последний ненулевой остаток, полученный в третьей строке алгоритма Евклида, через остальные остатки:

$$3 = 21 - 3\cdot 6.$$

Вместо 6 подставляем выражение, полученное во второй строке алгоритма Евклида:

$$3 = 21 - 3\cdot \underline{6} = 21 - 3\cdot(90 - 4\cdot 21) = 21 - 3\cdot 90 + 12\cdot 21 = 13\cdot 21 - 3\cdot 90.$$

Обратите внимание, что не нужно выполнять умножение при таком раскрытии скобок. Далее, подставляем вместо 21 выражение, полученное в первой строке алгоритма Евклида:

$$3 = 13\cdot \underline{21} - 3\cdot 90 = 13\cdot(111 - 90) - 3\cdot 90 = 13\cdot 111 - 16\cdot 90.$$

Итак, имеем

$$3 = \text{НОД}(111, 90) = 13\cdot 111 - 16\cdot 90.$$

Задача 23. Найти линейное представление НОД(1232, 1672) через числа 1232 и 1672 с помощью алгоритма Евклида.

Решение: Реализуем алгоритм Евклида для этих чисел:

$$\begin{aligned} 1672 &= 1\cdot \underline{1232} + \underline{440},\\ 1232 &= 2\cdot \underline{440} + \underline{352},\\ 440 &= 1\cdot \underline{352} + \underline{88},\\ 352 &= 4\cdot \underline{88} + 0. \end{aligned}$$

Итак, НОД(1232, 1672) = 88. Выразим 88 через 1232 и 1672. Сначала выражаем остатки от деления:

$$\begin{aligned} 1672 = 1\cdot 1232 + 440 &\;\to\; 440 = 1672 - 1\cdot 1232,\\ 1232 = 2\cdot 440 + 352 &\;\to\; 352 = 1232 - 2\cdot 440,\\ 440 = 1\cdot 352 + 88 &\;\to\; 88 = 440 - 1\cdot 352. \end{aligned}$$

Выражаем остатки, последовательно поднимаясь от третьей строки алгоритма Евклида к первой:

$$88 = 440 - 1\cdot\underline{352} = 440 - (1232 - 2\cdot 440) = 3\cdot\underline{440} - 1232 = 3\cdot(1672 - 1\cdot 1232) - 1232 = 3\cdot 1672 - 4\cdot 1232.$$

Итак, имеем

$$88 = \text{НОД}(1232, 1672) = 3\cdot 1672 - 4\cdot 1232.$$

Уравнение в целых числах

$$ax + by = d$$

имеет решение относительно x, y, если d делится на НОД(a, b). Для нахождения частного решения такого уравнения нужно найти линейное представление НОД(a, b) через числа a и b, после чего полученное соотношение умножить на результат деления d на НОД(a, b). Такие уравнения называют *линейными диофантовыми уравнениями*. Для нахождения общего решения уравнения нужно добавить линейно результат решения однородного уравнения

$$ax + by = 0,$$

выраженное в целых числах.

Задача 24. Решить уравнение в целых числах

$$34x + 77y = 1.$$

Решение: Это уравнение имеет решения, если НОД$(34, 77) = 1$. Достаточно очевидно, что это так, но мы все равно найдем НОД$(34, 77)$ с помощью алгоритма Евклида:

$$\begin{aligned}
77 &= 2 \cdot \underline{34} + \underline{9}, \\
34 &= 3 \cdot \underline{9} + \underline{7}, \\
9 &= 1 \cdot \underline{7} + \underline{2}, \\
7 &= 3 \cdot \underline{2} + \underline{1}, \\
2 &= 2 \cdot 1 + 0.
\end{aligned}$$

Итак, НОД$(34, 77) = 1$. Теперь найдем линейное представление НОД$(34, 77)$ через 34 и 77. Имеем:

$$\begin{aligned}
77 = 2 \cdot 34 + 9 \quad &\to \quad 9 = 77 - 2 \cdot 34, \\
34 = 3 \cdot 9 + 7 \quad &\to \quad 7 = 34 - 3 \cdot 9, \\
9 = 1 \cdot 7 + 2 \quad &\to \quad 2 = 9 - 1 \cdot 7, \\
7 = 3 \cdot 2 + 1 \quad &\to \quad 1 = 7 - 3 \cdot 2.
\end{aligned}$$

Выражаем остатки, поднимаясь от четвертой строки алгоритма Евклида к первой:

$$1 = 7 - 3 \cdot \underline{2} = 7 - 3 \cdot (9 - 1 \cdot 7) = -3 \cdot 9 + 4 \cdot \underline{7} = -3 \cdot 9 + 4 \cdot (34 - 3 \cdot 9) = -15 \cdot \underline{9} + 4 \cdot 34 =$$

$$= -15 \cdot (77 - 2 \cdot 34) + 4 \cdot 34 = 34 \cdot 34 - 15 \cdot 77.$$

Таким образом, частное решение уравнения равно

$$\tilde{x} = 34, \quad \tilde{y} = -15.$$

Решим однородное уравнение

$$34x + 77y = 0.$$

Здесь для нахождения x, y достаточно взять

$$x_0 = 77t, \quad y_0 = -34t.$$

Таким образом, общее решение уравнения будет равно

$$x = x_0 + \tilde{x} = 34 + 77t, \quad y = y_0 + \tilde{y} = -15 - 34t,$$

где t — произвольное целое число.

Задача 25. Решить уравнение в целых числах

$$15x - 37y = 1.$$

Решение: Реализуем алгоритм Евклида для нахождения НОД$(15, 37)$:

$$\begin{array}{rcl} 37 & = & 2 \cdot \underline{15} + \underline{7}, \\ 15 & = & 2 \cdot \underline{7} + \underline{1}, \\ 7 & = & 7 \cdot \underline{1} + 0. \end{array}$$

Выражаем остатки:

$$\begin{array}{rcl} 37 = 2 \cdot 15 + 7 & \to & 7 = 37 - 2 \cdot 15, \\ 15 = 2 \cdot 7 + 1 & \to & 1 = 15 - 2 \cdot 7. \end{array}$$

Имеем:

$$1 = 15 - 2 \cdot \underline{7} = 15 - 2 \cdot (37 - 2 \cdot 15) = 5 \cdot 15 - 2 \cdot 37.$$

Таким образом, частное решение данного уравнения равно

$$\tilde{x} = 5, \quad \tilde{y} = 2.$$

Обратите внимание, что в качестве $\tilde{y}$ берем 2, поскольку знак минус уже учтен в записи уравнения. Решение однородного уравнения равно

$$x_0 = 37t, \quad y_0 = 15t.$$

Обратите внимание, что и здесь y_0 положителен, поскольку знак минус учтен в записи уравнения. Таким образом, общее решение данного уравнения равно

$$x = x_0 + \tilde{x} = 5 + 37t, \quad y = y_0 + \tilde{y} = 2 + 15t,$$

где t — произвольное целое число. Например, пары чисел $(5, 2)$ (при $t = 0$), $(42, 17)$ (при $t = 1$), $(-32, -13)$ (при $t = -1$) являются частными решениями уравнения.

Задачи для самостоятельного решения

Задача 1. Для перестановок, заданных в S_7 в табличном виде

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 6 & 5 & 7 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 2 & 7 & 3 & 4 & 5 \end{pmatrix}$$

найти перестановки $\alpha \circ \beta$ и $\beta \circ \alpha$, α^{-1}, β^{-1}, $\alpha^2 = \alpha \circ \alpha$, $\beta \circ \alpha^{-1}$, $\beta^{-1} \circ \alpha$, $\alpha^2 \circ \beta^{-1}$.

Задача 2. Записать перестановку, заданную в табличном виде в S_{10}

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 4 & 2 & 5 & 8 & 10 & 9 & 6 & 7 \end{pmatrix},$$

в виде произведения независимых циклов.

Задача 3. Вычислить произведение перестановок, заданных в S_7 в виде произведения независимых циклов:

$$\alpha = \begin{pmatrix}1 & 3 & 4 & 7\end{pmatrix}\begin{pmatrix}2 & 5 & 6\end{pmatrix}, \quad \beta = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4 & 5 & 7\end{pmatrix}.$$

Задача 4. Решить уравнение в группе перестановок S_7:

$$\begin{pmatrix}1 & 4 & 2 & 5\end{pmatrix}\begin{pmatrix}3 & 5 & 7\end{pmatrix} X \begin{pmatrix}2 & 4 & 6 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 7 & 5\end{pmatrix} = \begin{pmatrix}1 & 5 & 6 & 2\end{pmatrix}\begin{pmatrix}2 & 3 & 6 & 4 & 5\end{pmatrix}\begin{pmatrix}1 & 3 & 7 & 4\end{pmatrix}.$$

Задача 5. Решить уравнение в группе перестановок S_8:

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

Проверить результат, подставив вместо X полученный результат и выполнив умножение.

Задача 6. Определить четность и порядок перестановки

$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 7 & 10 & 3 & 2 & 1 & 8 & 6 & 9 & 5 & 4\end{pmatrix}.$$

Задача 7. Вычислить

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 10 & 1 & 8 & 2 & 5 & 3 & 9 & 7 & 6 & 4\end{pmatrix}^{2507}.$$

Для полученной перестановки определить ее порядок и четность.

Задача 8. Вычислить

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 4 & 2 & 1 & 5 & 8 & 3 & 6 & 7\end{pmatrix}^{576} \circ \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 4 & 6 & 1 & 3 & 8 & 2 & 5 & 7\end{pmatrix}^{199}$$

Для полученной перестановки определить ее порядок и четность.

Задача 9. В группе перестановок S_5 найти подгруппу, порожденную транспозициями $\sigma = \begin{pmatrix}1 & 3\end{pmatrix}$ и $\tau = \begin{pmatrix}2 & 4\end{pmatrix}$. Какой из следующих групп изоморфна эта группа: $\mathbb{Z}_4$, $\mathbb{Z}_5$, V_4(четверная группа Клейна)?

Задача 10. В группе перестановок S_9 найти подгруппу, порожденную транспозицией $\sigma = \begin{pmatrix}2 & 8\end{pmatrix}$ и циклом $\tau = \begin{pmatrix}1 & 7 & 9\end{pmatrix}$. Какой из следующих групп изоморфна эта группа: V_4, $\mathbb{Z}_6$, S_3?

Задача 11. Найти НОД$(48, 195)$ с помощью алгоритма Евклида. Найти линейное представление НОД$(48, 195)$ через числа 48 и 195.

Задача 12. Решить уравнение в целых числах

$$17x + 93y = 1.$$

Задача 13. Решить уравнение в целых числах

$$13x - 17y = 1.$$

Привести три различных частных решения уравнения.