$(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ является тождеством в S_k, если для каждого z - порядка k-перестановки выполняется хотя бы одно из следующих правил:

$$z|a \quad \text{и} \quad z|(b-c) \tag{1}$$

$$z|c \quad \text{и} \quad z|(b-a) \tag{2}$$

$$z|b \quad \text{и} \quad z|(a+c) \tag{3}$$

Определение 1. *Циклической перестановкой из k элементов с шагом s будем называть такую циклическую перестановку, в которой элемент с номером i переходит в элемент с номером $i+s \pmod k$.*

Далее будем считать, что элементы перестановки длины k - это числа от 0 до $k-1$.

Лемма 1. *Существуют такие перестановки x и y из S_k, что xy - циклическая перестановка с шагом -1, а yx - циклическая перестановка с шагом 1.*

Доказательство. Рассмотрим перестановку x: $i \to -i \pmod k$ и y: $i \to -i+1 \pmod k$.

$$x = \begin{pmatrix} 0 & 1 & 2 & 3 & ... & k-3 & k-2 & k-1 \\ 0 & k-1 & k-2 & k-3 & ... & 3 & 2 & 1 \end{pmatrix}$$

$$y = \begin{pmatrix} 0 & 1 & 2 & 3 & ... & k-3 & k-2 & k-1 \\ 1 & 0 & k-1 & k-2 & ... & 4 & 3 & 2 \end{pmatrix}$$

Тогда
xy: $i \xrightarrow{y} (-i+1) \xrightarrow{x} (-(-i+1)) == i-1$,
yx: $i \xrightarrow{x} (-i) \xrightarrow{y} (-(-i)+1) == i+1$

$\square$

Лемма 2. *Пусть $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ - тождество в S_k, где k - нечетное. Тогда $a-b+c \equiv 0 \pmod k$.*

Доказательство. Зафиксируем перестановки xy и yx из Леммы 1. Рассмотрим перестановочный автомат, в котором переход по символам осуществляется соответствующими перестановками x и y. Тогда, чтобы $(xy)^a(yx)^b(xy)^c$

$= (yx)^c(xy)^b(yx)^a$ было тождеством для такого автомата, требуется, чтобы автомат закончил читать обе части равенства в одном состоянии, то есть

$$(-a) + b + (-c) \equiv c + (-b) + a \pmod k \tag{4}$$

что эквивалентно

$$2(a - b + c) \equiv 0 \pmod k \tag{5}$$

Из того, что k нечетно, следует

$$(a - b + c) \equiv 0 \pmod k$$

. □

Лемма 3. *Пусть $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ - тождество в S_k, где k - четное. Тогда $a - b + c \equiv 0 \pmod{\frac{k}{2}}$.*

Доказательство. Рассмотрим перестановочный автомат, как в доказательстве Леммы 2. Аналогично, получим

$$2(a - b + c) \equiv 0 \pmod k \tag{6}$$

Из того, что k четно, следует

$$(a - b + c) \equiv 0 \pmod{\frac{k}{2}}$$

. □

Следствие 1. *Пусть $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ - тождество в S_k. Тогда $a - b + c \equiv 0 \pmod{\frac{\operatorname{lcm}(k)}{2}}$.*

Доказательство. Из Леммы 2 $a - b + c \equiv 0$ по модулю наименьшего общего кратного всех нечетных чисел, меньших k. По Лемме 3 $a-b+c \equiv 0$ по модулю предмаксимальной степени числа 2, не превосходящей k. Отсюда следует, что $a - b + c \equiv 0 \pmod{\frac{\operatorname{lcm}(k)}{2}}$. □

Теорема 1. *Пусть $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ - тождество в S_k и $a + b + c \leq \frac{\operatorname{lcm}(k)}{2}$. Тогда $b = a + c$.*

Доказательство. Сразу заметим, что ни одно из чисел a, b, c не равно 0, так как в противном случае мы будем рассматривать тождество другого типа.

Из Следствия 1 вытекает, что

$$b - a - c = \frac{\mathrm{lcm}(k)}{2} m,$$

где $m \in \mathbb{Z}$. Откуда

$$b = a + c + \frac{\mathrm{lcm}(k)}{2} m > 0.$$

Получим цепочку неравенств

$$0 < a + c + \frac{\mathrm{lcm}(k)}{2} m < \frac{\mathrm{lcm}(k)}{2} + \frac{\mathrm{lcm}(k)}{2} m = \frac{\mathrm{lcm}(k)}{2}(m+1),$$

то есть $m > -1$.

С другой стороны, подставим b в $a + b + c$, получим

$$2(a+c) + \frac{\mathrm{lcm}(k)}{2} m \leq \frac{\mathrm{lcm}(k)}{2}$$

или

$$2(a+c) \leq \frac{\mathrm{lcm}(k)}{2}(1-m)$$

Поскольку сумма a и c должна быть положительным числом, требуется

$$\frac{\mathrm{lcm}(k)}{2}(1-m) > 0,$$

то есть $m < 1$.

Значит, при заданных ограничениях $m = 0$, что влечет $b = a + c$. $\square$

Следствие 2. *Для кратчайшего тождества вида* $(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ *выполняется* $b = a + c$.

Доказательство. Достаточно показать, что существуют тождества, для которых $a+b+c \leq \frac{\mathrm{lcm}(k)}{4}$ (тогда кратчайшее тождество также удовлетворяет этому условию, а по теореме для всех тождеств с таким свойством выполняется $b = a + c$).

Пусть $m = 2k/3$, $a := lcm(m)$, $c := lcm(k - m) \cdot P(m)$, $b := a + c$, где $P(m)$ - произведение всех простых и степеней простых чисел из множества $\{m+1, ..., k\}$. a и c взяты из доказательства длины тождества из двух блоков. Оттуда же понятно, что любой порядок перестановки делит или a, или c, а, благодаря выбору b, делит и соответствующую разность. Длина такого тождества, конечно, в два раза больше длины тождества из двух блоков ($e^{\frac{2}{3}k+O(\frac{k}{\log k})}$), однако все равно асимптотически меньше, чем $\frac{\mathrm{lcm}(k)}{4}$ (который равен $e^{k+O(\frac{k}{\log k})}$). $\square$

Теперь, вооружившись утверждением о связи показателей степеней рассматриваемого тождества, можно доказать обратное утверждение, т.е. если $(xy)^a(yx)^b(xy)^c \equiv_k (yx)^c(xy)^b(yx)^a$, то выполняется хотя бы одно из условий 1 - 3. Для этого нам понадобится доказать еще несколько лемм. Однако заметим сразу, что равенство $b = a + c$ делает истинной вторые части утверждений 1 - 3, если первые истинны.

Лемма 4. *Если* $(xy)^a(yx)^b(xy)^c \equiv_k (yx)^c(xy)^b(yx)^a$, *тогда хотя бы одно из чисел a, b, c делится на 2.*

Доказательство. От противного. Пусть a, b, c нечетны. Тогда $b \neq a + c$, поскольку их четность не совпадает. Противоречие. $\square$

Лемма 5. *Если* $(xy)^a(yx)^b(xy)^c \equiv_k (yx)^c(xy)^b(yx)^a$ *и* $k \geq 4$, *тогда хотя бы одно из чисел a, b, c делится на 3.*

Доказательство. От противного. Пусть ни одно из чисел a, b, c не делится на 3. Тогда возможны лишь два варианта:

1. $a \equiv_3 c \equiv_3 1$ и $b \equiv_3 2$
2. $a \equiv_3 c \equiv_3 2$ и $b \equiv_3 1$

(В остальных случаях хотя бы одно из чисел оказывается кратным трем)

Рассмотрим автомат относительно символов xy, yx на рисунке 1. Такой автомат можно получить, взяв за перестановку по x $(0)(1,2,3)$, по y - $(1)(3,2,0)$. Начальное состояние 0.

В первом случае автомат закончит читать левую часть тождества в состоянии 3 (после прочтения $(xy)^a$ окажется в состоянии 1, затем, прочитав $(yx)^b$ придет в состояние 3 в цикле), а правую - в состоянии 1 (после прочтения $(yx)^c$ окажется в состоянии 3 и в нем останется после $(xy)^b$).

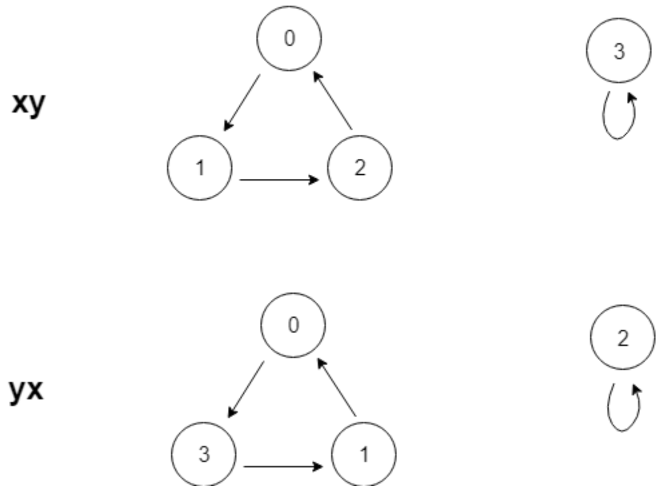

Рис. 1:

Во втором случае автомат закончит читать левую часть тождества в состоянии 1 (после прочтения $(xy)^a$ окажется в состоянии 2, затем, прочитав $(yx)^b$ останется в состоянии 2), а правую - в состоянии 2 (после прочтения $(yx)^c$ окажется в состоянии 1 и перейдет в состояние 2 после $(xy)^b$).

Получили противоречие с тем, что данная пара - тождество. $\square$