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

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

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

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

$\mathrm{lcm}(k)$ - наименьшее общее кратное всех чисел, меньших либо равных k.

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

Доказательство. Пусть L_1, L_2, L_3 - наименьшие общие кратные порядков, для которых выполняются правила (1), (2) и (3) из наблюдения соответственно. Тогда, в соответствии с правилами из наблюдения

$$a = x_1L_1$$
$$c = x_2L_2$$
$$b = x_3L_3$$

а также

$$x_3L_3 - x_2L_2 = y_1L_1 \tag{4}$$

$$x_3L_3 - x_1L_1 = y_2L_2 \tag{5}$$

$$x_1L_1 + x_2L_2 = y_3L_3 \tag{6}$$

где $\quad x_1,\, x_2,\, x_3,\, y_2 \in \mathbb{N}, \quad y_1,\, y_3 \in \mathbb{Z}.$

Выразим x_3L_3 из (4) и (5):

$$x_2L_2 + y_1L_1 = x_1L_1 + y_2L_2$$

скомпонуем

$$(y_1 - x_1)L_1 = (y_2 - x_2)L_2 \tag{7}$$

и рассмотрим решения получившегося уравнения (7).

1. $y_1 = x_1$. Тогда
$$(y_1 - x_1)L_1 = (y_2 - x_2)L_2 = 0$$
откуда $y_2 = x_2$. Подставив получившееся в равенства (4) - (6) получим $y_3 = x_3$, откуда следует, что $b = a + c$.

2. $y_1 > x_1$. Тогда из (7) $y_2 > x_2$.
$$x_3L_3 = x_2L_2 + y_1L_1 > x_2L_2 + x_1L_1 = y_3L_3$$

т.е. $x_3 > y_3$. Пусть

$$\begin{aligned} y_1 &= x_1 + t_1 \\ y_2 &= x_2 + t_2 \\ x_3 &= y_3 + t_3 \end{aligned}$$

где $t_1, t_2, t_3 \in \mathbb{N}$. Подставим в (4) - (6):

$$\begin{aligned} (y_3 + t_3)L_3 - x_2L_2 &= (x_1 + t_1)L_1 \\ (y_3 + t_3)L_3 - x_1L_1 &= (x_2 + t_2)L_2 \\ x_1L_1 + x_2L_2 &= y_3L_3 \end{aligned}$$

Сложив первое и третье равенства, получим

$$t_3L_3 = t_1L_1$$

Сложив второе и третье равенства, получим

$$t_3L_3 = t_2L_2$$

Т.е. каждое из чисел t_1L_1, t_2L_2, t_3L_3 должно делиться на L_1, L_2, L_3. Значит

$$t_1L_1 = t_2L_2 = t_3L_3 \geq \mathrm{lcm}(L_1, L_2, L_3) = \mathrm{lcm}(k)$$

Получается

$$b = x_3L_3 = (y_3 + t_3)L_3 = y_3L_3 + t_3L_3 \geq y_3L_3 + \mathrm{lcm}(k) > \mathrm{lcm}(k)$$

Но $a + b + c \leq \mathrm{lcm}(k)$ по условию. Противоречие.

3. $y_1 < x_1$ (все аналогично 2 пункту). Тогда из (7) $y_2 < x_2$

$$x_3L_3 = x_2L_2 + y_1L_1 < x_2L_2 + x_1L_1 = y_3L_3$$

т.е. $x_3 < y_3$. Пусть

$$\begin{aligned} x_1 &= y_1 + t_1 \\ x_2 &= y_2 + t_2 \\ y_3 &= x_3 + t_3 \end{aligned}$$

где $t_1, t_2, t_3 \in \mathbb{N}$. Подставим в (4) - (6):

$$\begin{aligned} x_3L_3 - (y_2 + t_2)L_2 &= y_1L_1 \\ x_3L_3 - (y_1 + t_1)L_1 &= y_2L_2 \\ (y_1 + t_1)L_1 + (y_2 + t_2)L_2 &= (x_3 + t_3)L_3 \end{aligned}$$

Сложив первое и третье равенства, получим

$$t_1L_1 = t_3L_3$$

Сложив второе и третье равенства, получим

$$t_2L_2 = t_3L_3$$

Т.е. каждое из чисел t_1L_1, t_2L_2, t_3L_3 должно делиться на L_1, L_2, L_3. Значит

$$t_1L_1 = t_2L_2 = t_3L_3 \geq \mathrm{lcm}(L_1, L_2, L_3) = \mathrm{lcm}(k)$$

Получается

$$a = x_1L_1 = (y_1 + t_1)L_1 = y_1L_1 + t_1L_1 \geq y_1L_1 + \mathrm{lcm}(k) > \mathrm{lcm}(k)$$

Но $a + b + c \leq \mathrm{lcm}(k)$ по условию. Противоречие.

□

Следствие 1. *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 $a+b+c \leq \mathrm{lcm}(k)$ (тогда кратчайшее тождество также удовлетворяет этому условию, а по теореме для всех тождеств с таким свойством выполняется $b = a + c$).

Пусть $b := \frac{\mathrm{lcm}(k)}{2}$. Тогда из всех возможных порядков b не делится на порядки, кратные $x = 2^m$, где $m = \max\{i \in \mathbb{N} \mid 2^i \leq k\}$ и только на них.

Если $x = k$, то $a = k \leq \frac{\mathrm{lcm}(k)}{2}$.

Пусть $x < k$ и $a := \mathrm{lcm}(x, \mathrm{lcm}(k - x))$.

$x > \frac{k}{2}$ (т.к. максимальная степень двойки, не превосходящая k), значит $k - x < \frac{k}{2}$. По теореме Чебышёва (постулат Бертрана) между $\frac{k}{2}$ и k всегда найдется простое число. Обозначим его за p. Тогда p не делит $a = \mathrm{lcm}(x, \mathrm{lcm}(k - x))$, но делит $\mathrm{lcm}(k)$. Значит $a \leq \frac{\mathrm{lcm}(k)}{p} \leq \frac{\mathrm{lcm}(k)}{2}$.

$c := b - a$. Искомое тождество построено. □