$(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ 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 $i+s$ (mod 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: $i \to -i($ mod $k)$ и y: $i \to -i+1($ mod $k)$.

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

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

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

□

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

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

что эквивалентно

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

Из того, что k нечетно, следует

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

. □

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

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

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

Из того, что k четно, следует

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

. □

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

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 $a - b + c \equiv 0 \ (\mod \frac{\mathrm{lcm}(k)}{2})$. □

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

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. □

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 $(xy)^b$).

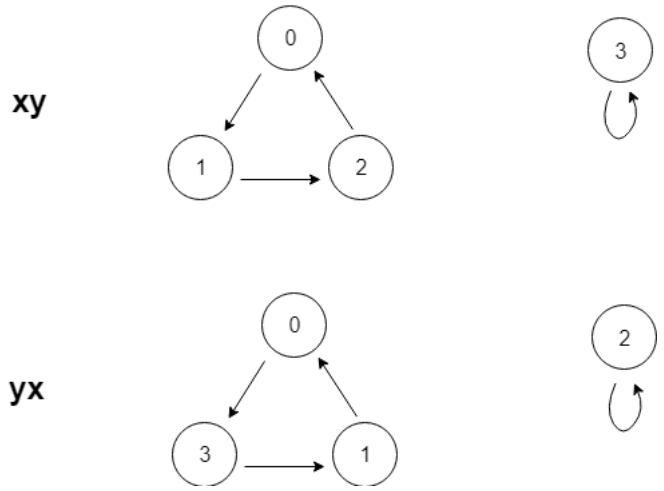

Рис. 1:

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. □

Лемма 6. *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* k.

Доказательство. От противного. Пусть ни одно из чисел a, b, c не делится на k. Разберем несколько случаев.

1. $2a \equiv_k 0$.

   Поскольку мы предположили, что $a \not\equiv_k 0$, значит $a \equiv_k \frac{k}{2}$. Так как $a + c = b$, $b \not\equiv_k 0$ по предположению, то $c \not\equiv_k a$.

   Рассмотрим автомат $\mathscr{A}$, в котором xy - перестановка с шагом 1, в которой поменяли местами a и c, а yx - перестановка с шагом -1 (см. Рисунок 2). Данный автомат различит слова $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$.

   $\mathscr{A}$ закончит читать второе слово в состоянии $c - a$ (см. Рисунок 4). Корректность переходов:

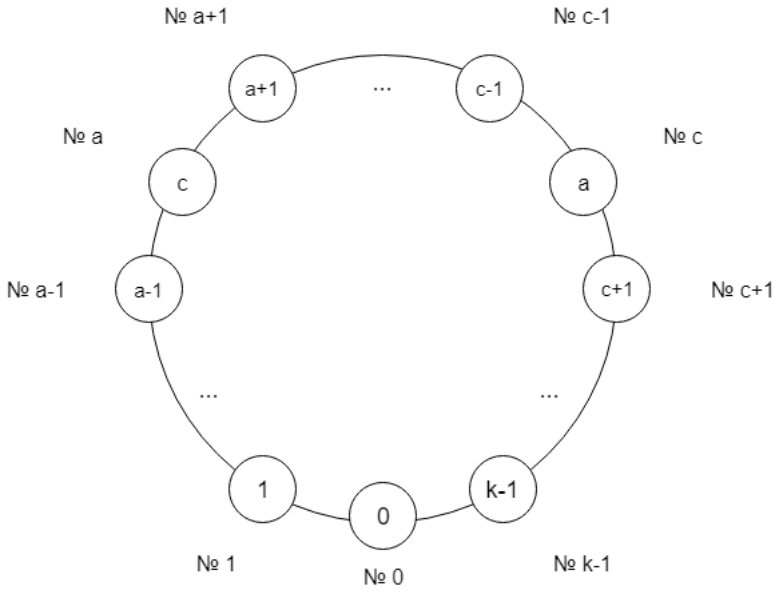

Рис. 2: Цикл xy автомата $\mathscr{A}$

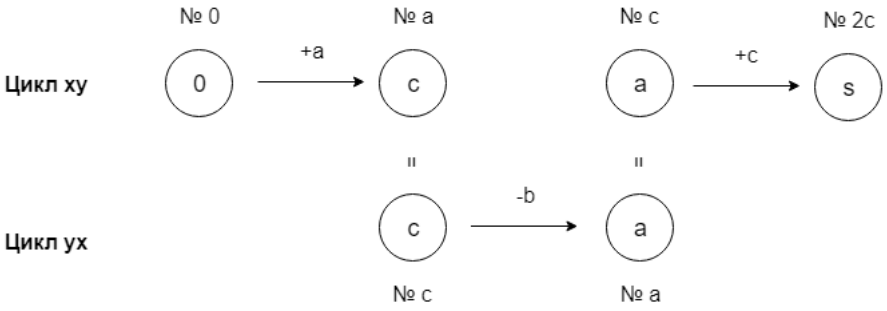

Рис. 3: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{A}$

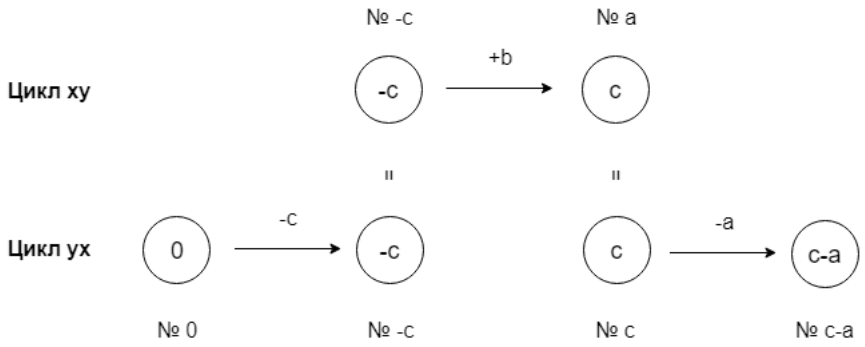

Рис. 4: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{A}$

- $-c \not\equiv_k a$ и $-c \not\equiv_k c$ поскольку иначе в обоих случаях он был бы равен $\frac{k}{2}$ и совпадал бы с a;
- $b - c = a$ из Теоремы 1.

$\mathscr{A}$ закончит читать второе слово в состоянии с номером $2c$ (см. Рисунок 4). Корректность переходов:

- $c - b \equiv_k -a$ из Теоремы 1, а $a \equiv_k -a$ поскольку $a \equiv_k \frac{k}{2}$;
- $2c \not\equiv_k c$ поскольку по предположению $c \not\equiv_k 0$.

Конечное состояние при чтении $(yx)^c(xy)^b(yx)^a$ зависит от того, совпадает ли $2c$ с a по модулю k:

- $2c \equiv_k a$, тогда состоянием с номером $2c$ будет состояние c, которое не совпадает с $c-a$, поскольку $-a$ не сравнимо с нулем по модулю k;
- $2c \not\equiv_k a$, тогда конечным состоянием будет $2c$, которое не совпадает с $c - a$, поскольку $a + c \not\equiv_k 0$.

2. $2a \not\equiv_k 0$ и $2a \not\equiv_k -c$

   Рассмотрим автомат $\mathscr{B}$, в котором xy - перестановка с шагом 1, а yx - перестановка с шагом -1, в которой поменяли местами a и $2a$ (см. Рисунок 5). Данный автомат различит слова $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$.

   $\mathscr{B}$ закончит читать $(xy)^a(yx)^b(xy)^c$ в состоянии a (см. Рисунок 6). Корректность переходов:

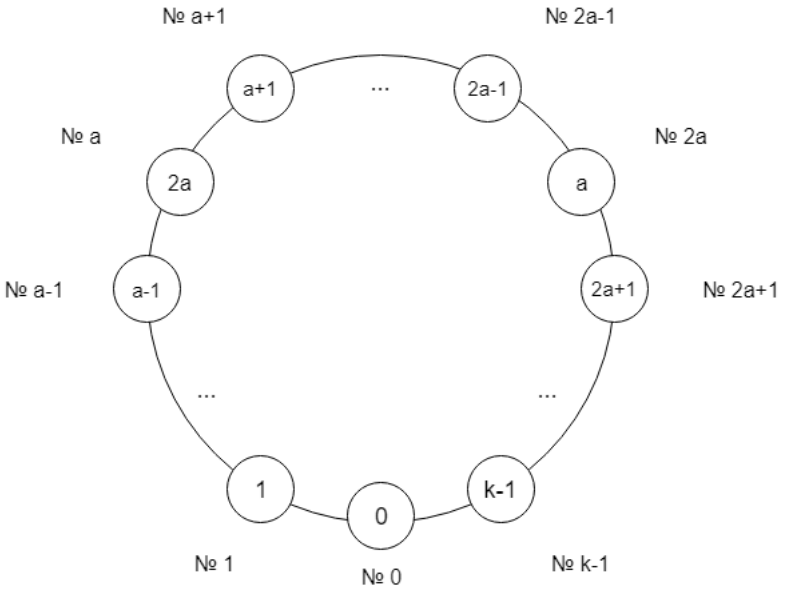

Рис. 5: Цикл yx автомата $\mathscr{B}$

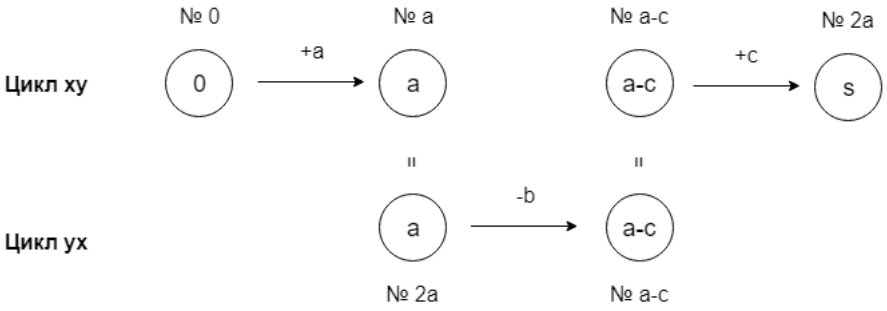

Рис. 6: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{B}$

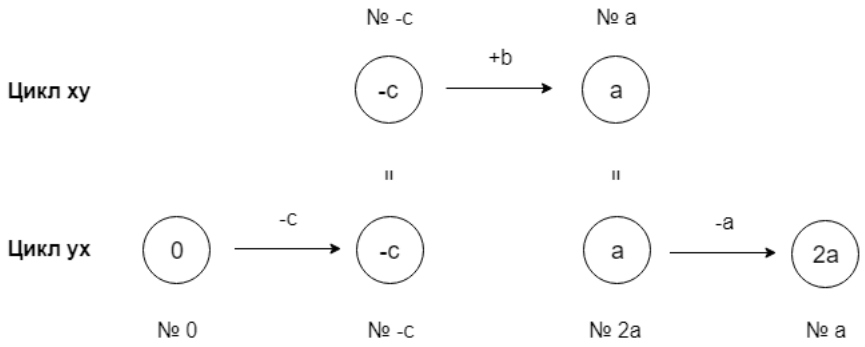

Рис. 7: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{B}$

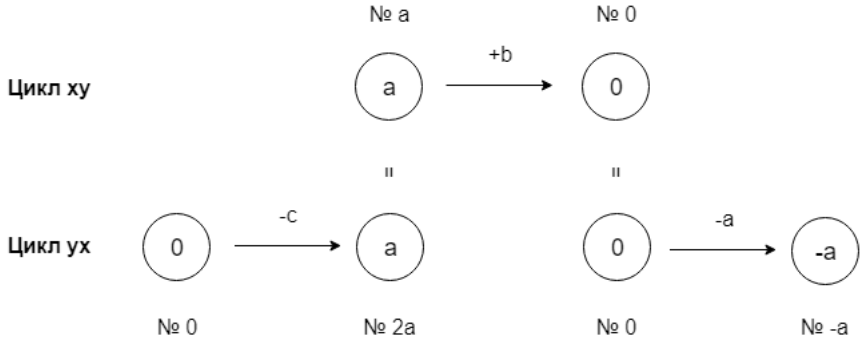

Рис. 8: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{B}$ в случае, когда $2a \equiv_k -c$

- $2a - b = a - c$ по Теореме 1, $a - c \not\equiv_k a$, так как $-c \not\equiv_k 0$ по предположению, и $a - c \not\equiv_k 2a$, так как $a + c \not\equiv_k 0$ также по предположению.

$\mathscr{B}$ закончит читать $(yx)^c(xy)^b(yx)^a$ в состоянии $2a$ (см. Рисунок 7). Корректность переходов:

- $-c \not\equiv_k a$, поскольку $a + c \not\equiv_k 0$ по предположению, и $-c \not\equiv_k 2a$ по заданному ограничению;
- $b - a = c$ по Теореме 1.

Состояния a и $2a$ не совпадают, так как $a \not\equiv_k 0$ по предположению.

3. $2a \not\equiv_k 0$ и $2a \equiv_k -c$ и $3a \not\equiv_k 0$

Рассмотрим автомат $\mathscr{B}$ из предыдущего случая (см. Рисунок 5). В этом случае этот автомат также разделит рассматриваемую пару слов.

Чтение слова $(xy)^a(yx)^b(xy)^c$ будет абсолютно таким же, как и в предыдущем случае. Чтение слова $(yx)^c(xy)^b(yx)^a$ закончится в состоянии $-a$ (см. Рисунок 8). Корректность переходов:

- $2a \equiv_k -c$ по заданному ограничению;
- $a + b \equiv_k 0$ поскольку $a + b = 2a + c \equiv_k 2a - 2a = 0$ по Теореме 1 и заданному ограничению;
- $-a \not equiv_k a$, так как $2a \not\equiv_k 0$, и $-a \not equiv_k a$, поскольку $3a \not\equiv_k 0$ по заданному ограничению.

Состояния a и $-a$ также не совпадают.

4. $2a \not\equiv_k 0$ и $2a \equiv_k -c$ и $3a \equiv_k 0$

   Поскольку $3a \equiv_k 0$, то $a \equiv_k \frac{k}{3}$ или $a \equiv_k \frac{2k}{3}$

□