$(xy)^a(yx)^b(xy)^c = (yx)^c(xy)^b(yx)^a$ 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. *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 такие, что xy - циклическая перестановка с шагом -1, а yx - циклическая перестановка с шагом 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 2. *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 1. Аналогично, получим

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

Из того, что k четно, следует

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

. $\square$

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 1 $a-b+c \equiv 0$ по модулю наименьшего общего кратного всех нечетных чисел, меньших k. По Лемме 2 $a-b+c \equiv 0$ по модулю предмаксимальной степени числа 2, не превосходящей k. Отсюда следует, что $a-b+c \equiv 0 \pmod{\frac{\operatorname{lcm}(k)}{2}}$. $\square$

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

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

где $m \in \mathbb{Z}$. Откуда

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

Получим цепочку неравенств

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

то есть $m > -1$.

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

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

или

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

Поскольку сумма a и c должна быть положительным числом, требуется

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

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 $a+b+c \le \frac{\operatorname{lcm}(k)}{4}$ (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 $\frac{\operatorname{lcm}(k)}{4}$ (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 3. *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 $b \ne a + c$, поскольку их четность не совпадает. Противоречие. $\square$

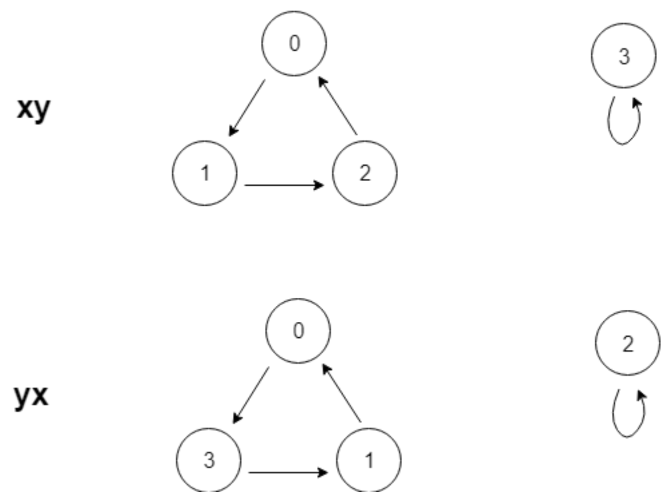

Рис. 1:

Лемма 4. *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 $(xy)^b$).

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

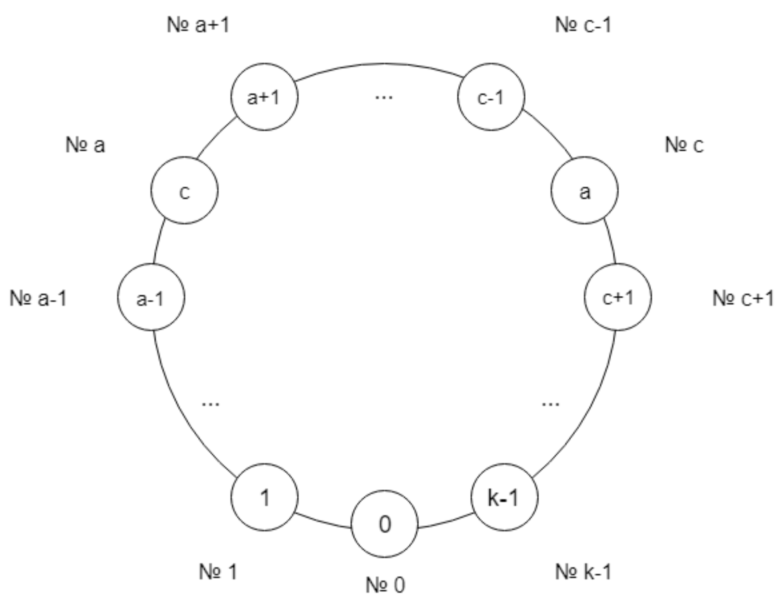

Рис. 2: Цикл xy автомата $\mathscr{A}$

прочтения $(yx)^c$ окажется в состоянии 1 и перейдет в состояние 2 после $(xy)^b$).

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

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* 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:

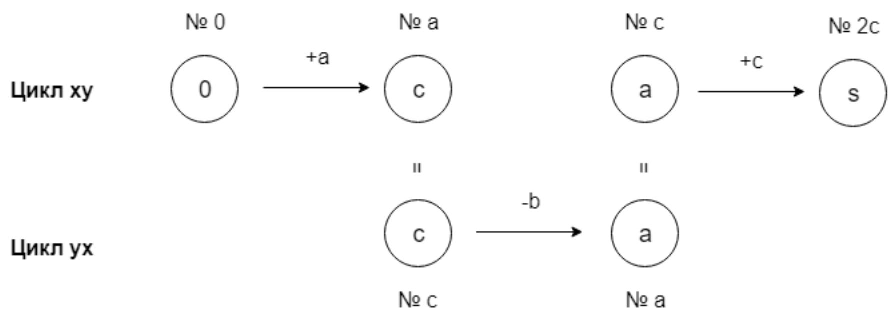

Рис. 3: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{A}$

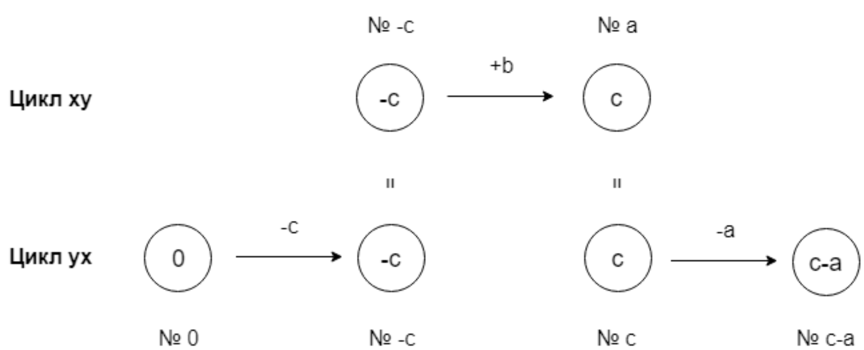

Рис. 4: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{A}$

- $-c \not\equiv_k a$ 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:

   - $2a - b = a - c$ 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.

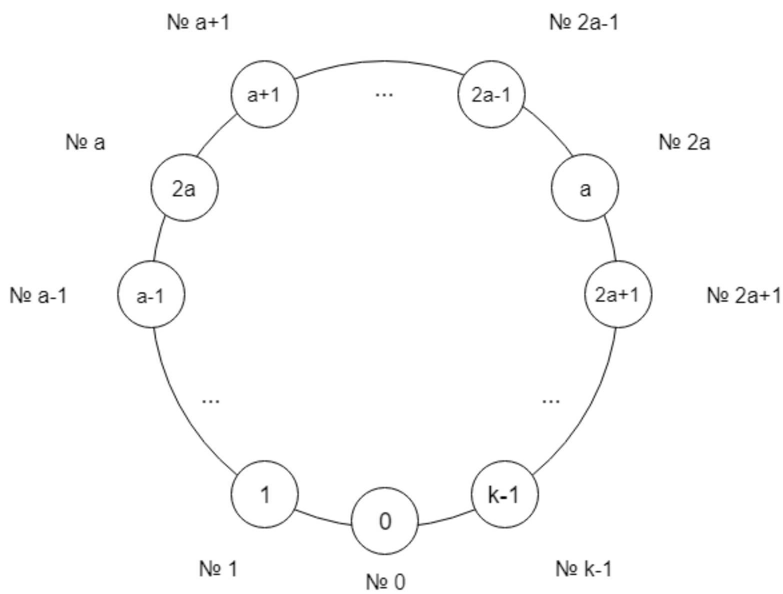

Рис. 5: Цикл yx автомата $\mathscr{B}$

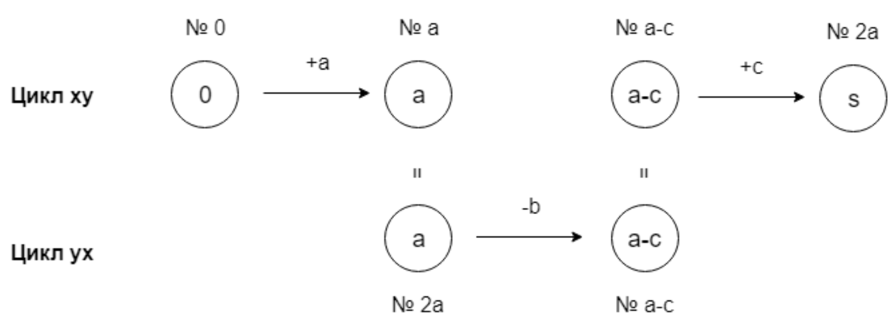

Рис. 6: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{B}$

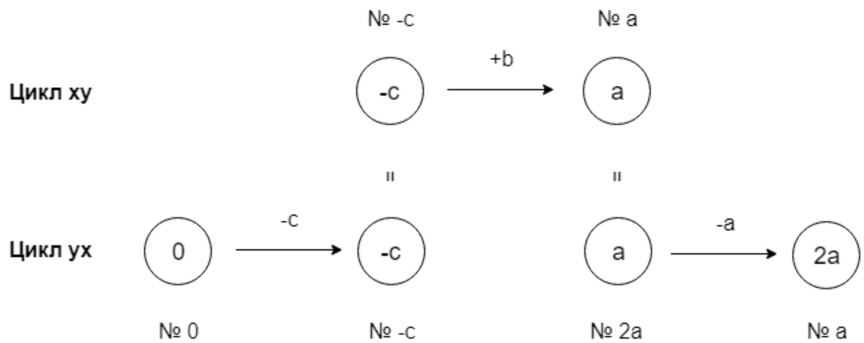

Рис. 7: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{B}$

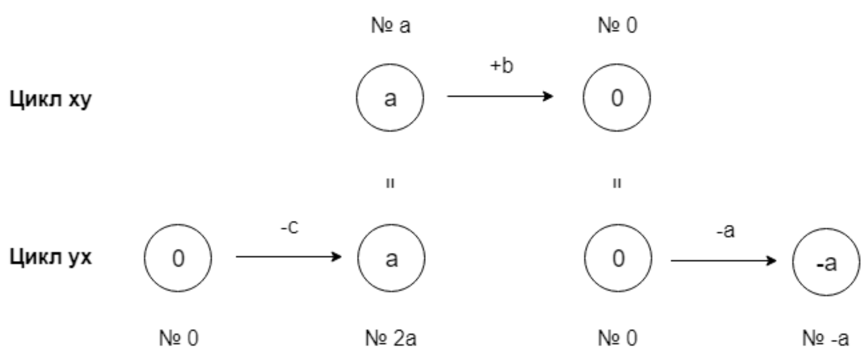

Рис. 8: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{B}$ в случае, когда $2a \equiv_k -c$

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 $a \equiv_k \frac{2k}{3}$, а из того, что $2a + c \equiv_k 0$ следует, что $a \equiv_k c$.

   Пусть $k = 3m$, $m \in \mathbb{N}$. Рассмотрим перестановочный автомат $\mathscr{C}$ такой, что xy - циклическая перестановка из k элементов с шагом 1, а yx - циклическая перестановка из k элементов с шагом 1, в которой поменяли местами состояния $2m$ и z, где $z \not\equiv 0(\mod k)$, $z \not\equiv m(\mod k)$ и $z \not\equiv 2m(\mod k)$ (см. Рис. 9). Такое z существует, если $k > 3$.

   Покажем, что автомат $\mathscr{C}$ закончит читать слова $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$ в разных состояниях.

   (a) $a \equiv_k c \equiv_k m$, $b \equiv_k 2m$

   Начальным состоянием в автомате $\mathscr{C}$ назначим состояние m.

   $\mathscr{C}$ закончит читать $(xy)^a(yx)^b(xy)^c$ в состоянии z (см. Рисунок 10), а слово $(yx)^c(xy)^b(yx)^a$ - в состоянии $2m$ (см. Рисунок 11). Корректность переходов:

   - $z + 2m \not\equiv_k z$, так как $2m =\equiv_k 2a \not\equiv_k 0$ по заданному ограничению;

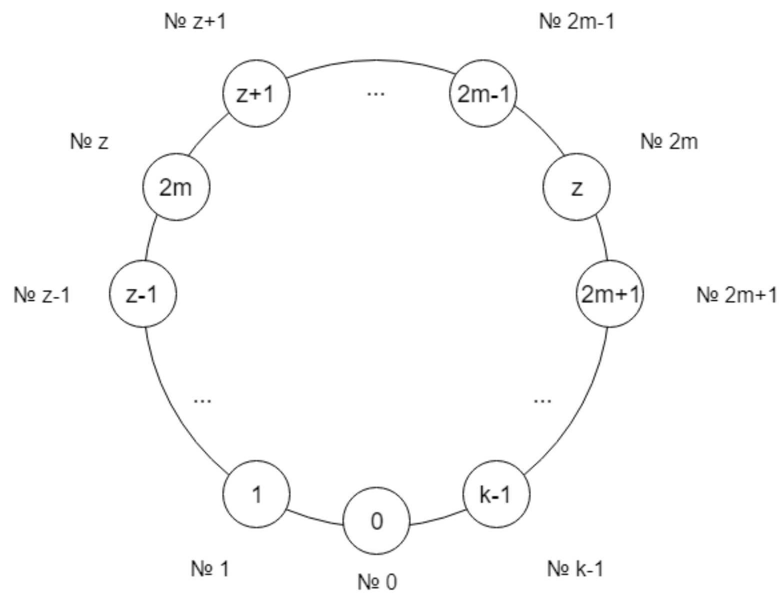

Рис. 9: Цикл yx автомата $\mathscr{C}$

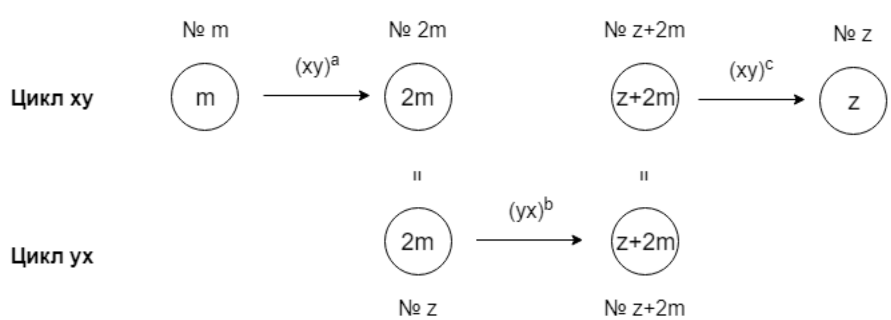

Рис. 10: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{C}$ при $a \equiv_k \frac{k}{3}$

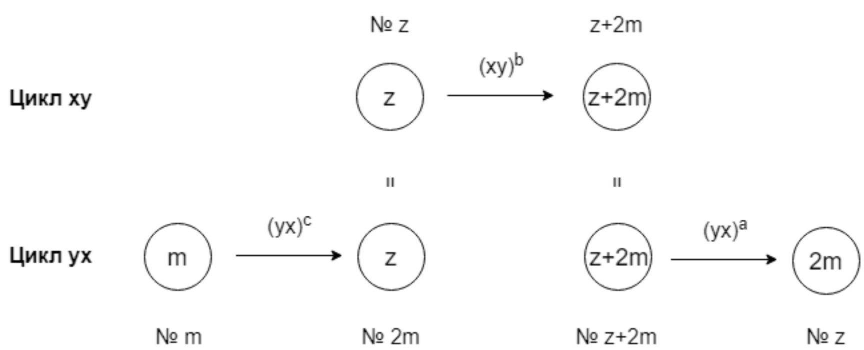

Рис. 11: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{C}$ при $a \equiv_k \frac{k}{3}$

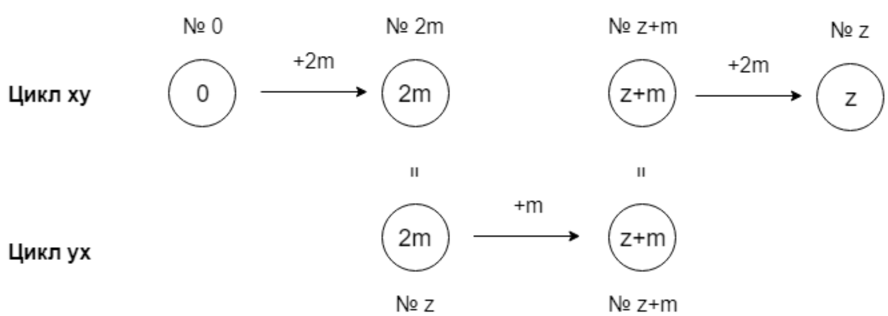

Рис. 12: Чтение слова $(xy)^a(yx)^b(xy)^c$ автоматом $\mathscr{C}$ при $a \equiv_k \frac{2k}{3}$

- $z + 2m \not\equiv_k 2m$, так как $z \not\equiv_k 0$ по выбору z.

Состояние z не совпадает с $2m$ по выбору z.

(b) $a \equiv_k c \equiv_k 2m$, $b \equiv_k m$

Начальным состоянием в автомате $\mathscr{C}$ назначим состояние 0. $\mathscr{C}$ закончит читать $(xy)^a(yx)^b(xy)^c$ в состоянии z (см. Рисунок 12), а слово $(yx)^c(xy)^b(yx)^a$ - в состоянии $2m$ (см. Рисунок 13). Корректность переходов:

- $z + m \not\equiv_k z$, так как $m =\equiv_k 2a \not\equiv_k 0$ по заданному ограничению;
- $z + m \not\equiv_k m$, так как $z \not\equiv_k 0$ по выбору z.

Состояние z не совпадает с $2m$ по выбору z.

Рассмотрены все возможные случаи, и для каждого из них приведен автомат, разделяющий пару слов, которая по условию была тождеством.

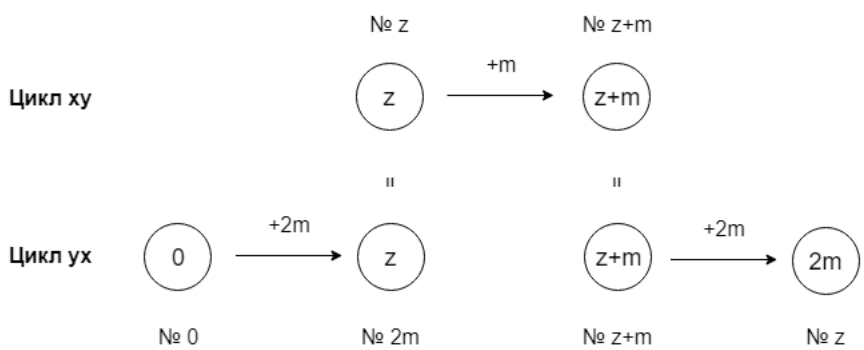

Рис. 13: Чтение слова $(yx)^c(xy)^b(yx)^a$ автоматом $\mathscr{C}$ при $a \equiv_k \frac{2k}{3}$

Значит, наше предположение о том, что ни одно из чисел a, b, c не делится на k, было ложным. □

Теорема 2. *Если $(xy)^a(yx)^b(xy)^c \equiv_k (yx)^c(xy)^b(yx)^a$ и $k \geq 4$, то для любого порядка ord перестановки из k элементов хотя бы одно из чисел a, b, c делится на ord.*

Доказательство. Если перестановка представима в виде одного цикла (здесь опускаются тривиальные циклы из одного состояния), значит порядок перестановки ord меньше либо равен k, и утверждение доказано Леммами 3 - 5.

Пусть k-перестановка представима в виде произведения двух циклов с длинами c_1 c_2. Тогда порядок перестановки равен $lcm(c_1, c_2)$. От противного, предположим, что ни одно из чисел a, b, c не делится на $lcm(c_1, c_2)$. Рассмотрим несколько вариантов.

1. $c_1|a$ и $c_2|b$.

   Тогда $c_1 \not| c$ и $c_2 \not| c$, поскольку иначе разность $b - c$ делилась бы на c_1 или c_2 соответственно, а это повлекло бы за собой или $c_2|a$, или $c_1|b$. Также, исходя из Теоремы 1, $c_1|(b-c)$, откуда $b \equiv_{c_1} c$.

   Рассмотрим автомат $\mathscr{A}$ с переходами по xy и yx, изображенный на рисунке 14. Начальное состояние автомата - 0; циклы, длинами c_1 и c_2, у разных перестановок отличаются только одним состоянием (состояние s у перестановки xy располагается в цикле c_2, а у перестановки yx - в цикле c_1; аналогичная ситуация с состоянием t), остальные вершины у циклов с одинаковыми длинами совпадают.

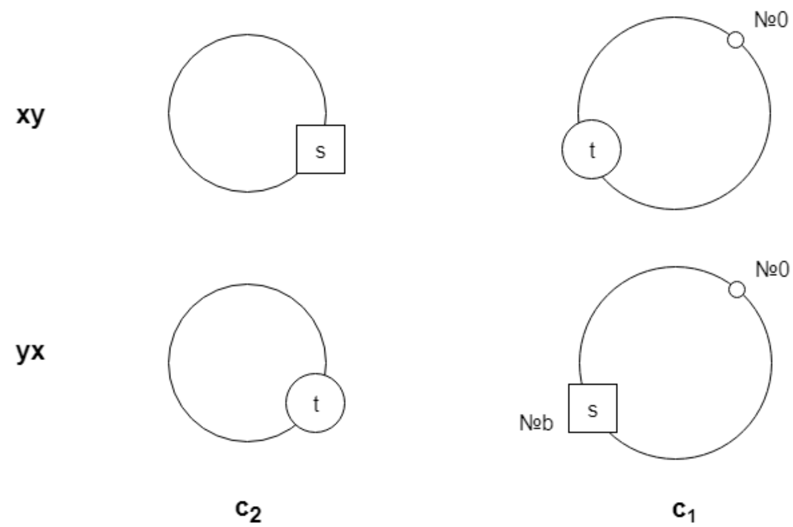

Рис. 14: Автомат $\mathscr{A}$

Покажем, что данный автомат различит строки $(xy)^a(yx)^b(xy)^c$ и $(yx)^c(xy)^b(yx)^a$.

- Читаем $(xy)^a(yx)^b(xy)^c$

  $0.(xy)^a = 0$, так как $c_1|a$. $0.(yx)^b = s$ по выбору вершины s, и автомат переходит к циклу c_2. $s.(xy)^c = w$, где w - вершина цикла длины c_1 перестановки xy, не совпадающая с s, поскольку $c_1 \nmid c$.
- Читаем $(yx)^c(xy)^b(yx)^a$

  $0.(yx)^c = s$, так как $b \equiv_{c_1} c$; автомат переходит к циклу c_2. $s.(xy)^b = s$ поскольку $c_2|b$; автомат переходит к циклу c_1. $s.(yx)^a = s$, поскольку $c_1|a$.

Поскольку $w \neq s$, автомат различит слова, что противоречит тождественности пары.

2. $c_1|a$ и $c_2|$.

   Рассуждая аналогично предыдущему случаю, получим, что $b \equiv_{c_1} c$, $c_1 \nmid b$, $c_2 \nmid b$.

   Рассмотрим автомат $\mathscr{A}$ из предыдущего случая, и покажем, что он и здесь различит рассматриваемую пару слов.

- Читаем $(xy)^a(yx)^b(xy)^c$
  $0.(xy)^a = 0$, так как $c_1|a$. $0.(yx)^b = s$ по выбору вершины s; автомат переходит к циклу c_2. $s.(xy)^c = s$, поскольку $c_2|c$.
- Читаем $(yx)^c(xy)^b(yx)^a$
  $0.(yx)^c = s$, так как $b \equiv_{c_1} c$; автомат переходит к циклу c_2. $s.(xy)^b = v$, где v - вершина цикла длины c_2 перестановки xy, не совпадающая с s, поскольку $c_2 \not| b$. $v.(yx)^a = v$, поскольку $c_1|a$.

Так как v и s не совпадают, также приходим к противоречию.

3. Случай $c_1|c$ и $c_2|b$ симметричен первому, поэтому можно построить аналогичный автомат. Остальные случаи аналогичны рассмотренным с точностью до смены длин циклов местами.

Получается, что для любой перестановки, представляемой в виде объединения двух циклов, хотя бы одно из чисел a, b, c делится на наименьшее общее кратное их длин (то есть, делится на обе длины одновременно).

Предположим теперь, что k-перестановка представима в виде объединения трех циклов с длинами c_1, c_2, c_3. Для каждой пары циклов, как мы уже доказали, наименьшее общее кратное их длин делит хотя бы одно из чисел a, b, c. Всего таких пар в этом случае три. В зависимости их распределениям по числам a, b, c, можно также рассмотреть несколько случаев.

1. Все три НОК-а делят один показатель. Тогда этот показатель делится и на $\mathrm{lcm}(c_1, c_2, c_3)$;

2. Два из трех НОК-ов делят один показатель. Без ограничения общности, $\mathrm{lcm}(c_1, c_2)|a$ и $\mathrm{lcm}(c_1, c_3)|a$. Тогда очевидно $\mathrm{lcm}(c_1, c_2, c_3)|a$;

3. На каждый из показателей приходится по одной паре. Без ограничения общности, $\mathrm{lcm}(c_1, c_2)|a$ и $\mathrm{lcm}(c_1, c_3)|b$, $\mathrm{lcm}(c_2, c_3)|c$. Поскольку, $c_1|a$ и $c_1|b$, $c_1|(b-a)$, а по Теореме 1 $b - a = c$, значит и $c_1|c$. Получается, что c делится на все три длины циклов, а значит делится на их НОК.

Значит, для порядков, соответствующие которым перестановки разбиваются на три цикла, теорема тоже доказана.

Теперь описанные ранее случаи представим как базу индукции по наименьшему числу "циклов"n, на которые можно разбить порядок (то есть соответствующую ему перестановку). Предположим, что для всех $n < m$ теорема доказана. Докажем для $n = m$. Пусть некоторый порядок есть $\mathrm{lcm}(c_1, c_2, ..., c_n)$. По предположению индукции НОК любых $n-1$-их длин циклов делит хотя бы одно из чисел a, b, c. Поскольку таких $n-1$-наборов больше чем 3, хотя бы на одно из этих чисел придется хотя бы 2 набора. Без ограничения общности пусть $\mathrm{lcm}(c_1, c_2, ..., c_{n-1})|a$ и $\mathrm{lcm}(c_2, c_3, ..., c_n)|a$. Но тогда a делится на $\mathrm{lcm}(c_1, c_2, ..., c_n)$. Теорема доказана. $\square$