

Цикловая структура степенных отображений в кольце классов вычетов

© 2013 г. В. Е. Тараканов, А. М. Зубков

Введение

В последние десятилетия в связи с применениями датчиков псевдослучайных чисел в криптографии повысился интерес к разработке и исследованию датчиков псевдослучайных чисел, которые, кроме простоты реализации и хороших статистических качеств выходной последовательности, обладают важными для криптографии свойствами, в частности, большим периодом, высокой сложностью восстановления начального значения по отрезку выходной последовательности, невозможностью прогнозирования будущих значений по известным и т. п.

В ряде работ (см., например, [2], [3], [4], [5], [8], [10], [11], [12]) изучаются датчики, основанные на операциях возведения в квадрат или в фиксированную степень по простому или специально подобранному составному модулю.

Так, в [3] изучаются QR-генераторы, т. е. датчики, использующие операцию возведения в квадрат по модулю составного числа $N = pq$, где числа $p \neq q$ — простые и сравнимы с 3 по модулю 4. Пусть $q_N(x)$ обозначает наименьший неотрицательный вычет числа x^2 по модулю N . Последовательность внутренних состояний QR-генератора с модулем N строится по формуле

$$x_{t+1} = \begin{cases} q_N(x_t), & \text{если } q_N(x) < N/2, \\ N - q_N(x) & \text{в противном случае,} \end{cases} \quad (1)$$

и в качестве выходной последовательности рассматривается

$$y_t = q_2(x_t), \quad t = 1, 2, \dots$$

В [2] в качестве обоснования криптографических качеств порождаемой этим генератором последовательности используется сложность задачи извлечения квадратного корня в мультипликативной группе вычетов и задачи факторизации натуральных чисел. В [3] отмечается, что если $N = pq$, где числа $p \neq q$ — простые и сравнимы с 3 по модулю 4, то число квадратичных вычетов равно $\frac{1}{4}(p-1)(q-1)$ и в каждой паре $(x, N-x)$ оба числа не могут быть квадратичными вычетами. Поэтому формула (1) по сути означает, что множество квадратичных вычетов отображается в множество положительных вычетов, меньших $N/2$. Значит, с точностью до этой

замены свойства рекуррентной последовательности (1) совпадают со свойствами последовательности

$$x_{t+1} = x_t^2 \pmod{N}, \quad t = 0, 1, \dots \quad (2)$$

Цикловая структура отображений вида $x \rightarrow x^d \pmod{N}$ для случаев, когда $d \geq 2$ и N — простое число, изучалась в [5], [11], а в [10] рассмотрен случай, когда $N = p^m$ — степень простого числа p . В частности, в [10] показано, что для числа $C_r(d, p^m)$ циклов длины r отображения $x \rightarrow x^d \pmod{p^m}$ справедливы формулы

$$C_r(d, p^m) = \frac{1}{r} \sum_{j: j|r} \mu(j) \text{НОД}(p^m - p^{m-1}, d^{r/j} - 1),$$

$$\sum_{r \geq 1} C_r(d, p^m) = \sum_{j: j|\rho} \frac{\varphi(j)}{\text{ord}_j d},$$

где $\mu(j)$ и $\varphi(j)$ — функции Мебиуса и Эйлера соответственно, $\text{ord}_j d$ при $\text{НОД}(d, j) = 1$ — порядок числа d по модулю j , а число ρ определяется условиями $d = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$ (p_1, \dots, p_s — простые), $p^m - p^{m-1} = p_1^{r_1} \dots p_s^{r_s} \rho$, $\text{НОД}(d, \rho) = 1$. В [4] приведено количественное описание цикловой структуры отображения $x \rightarrow x^d \pmod{N}$ на множестве обратимых элементов кольца \mathbb{Z}_N при любых N и d , использующее, в том числе, мультипликативную структуру числа циклических точек отображения, и для случая, когда N есть произведение двух простых чисел, изучается доля числа циклических точек, лежащих на коротких циклах или на циклах, длины которых не делятся на число, однозначно определяемое по N .

Результатом настоящей работы является конструктивное описание структуры множества циклов отображений $x \rightarrow x^d \pmod{N}$ для произвольных значений d и N . В §§ 1–2 излагается комбинаторно-алгебраический подход к описанию этих цикловых структур. Он позволяет свести задачу к двум следующим: а) описанию цикловых структур степенных отображений на произвольных примарных циклических группах и б) нахождению цикловой структуры отображения на прямом произведении таких групп по известным цикловым структурам отображения на сомножителях. Описание цикловой структуры отображения $f^{(d)} : x \rightarrow x^d$ для примарных циклических групп нечетного порядка содержится в § 3, а для групп четного порядка — в § 4. Наконец, в § 5 с помощью введенной в § 2 операции композиции цикловых структур и результатов, полученных в §§ 3–4, дается описание цикловых структур отображений $f^{(d)}$ на множествах \mathbb{Z}_N^* обратимых элементов кольца \mathbb{Z}_N классов вычетов по модулю N для любых d , $N \geq 2$.

1. Комбинаторно-алгебраический подход к изучению цикловой структуры степенных отображений на кольце \mathbb{Z}_N

Для натурального N обозначим через \mathbb{Z}_N кольцо классов вычетов по модулю N . Элементы \mathbb{Z}_N представляем числами $0, 1, \dots, N-1$. Через \mathbb{Z}_N^* обозначим множество всех чисел из \mathbb{Z}_N , взаимно простых с N .

Для любого натурального $d \geq 2$ равенство $f^{(d)}(x) = x^d \pmod{N}$ определяет отображение $f_N^{(d)} : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$, которому соответствует ориентированный граф G_N^d с множеством вершин $V_N = \{0, 1, \dots, N-1\}$ и множеством ребер $E_N^{(d)} = \{(x, f_N^{(d)}(x)) : x \in \mathbb{Z}_N\}$.

Граф G_N^d разбивается на связные компоненты, каждая из которых состоит из цикла с подходами. Если граф G_N^d состоит из k_1 компонент с циклами длины l_1, \dots, k_r компонент с циклами длины l_r , то будем говорить, что граф G_N^d имеет цикловую структуру

$$\text{Str} \left(f_N^{(d)}, \mathbb{Z}_N \right) = (l_1)^{k_1} \dots (l_r)^{k_r} = \prod_{i=1}^r (l_i)^{k_i}.$$

Аналогичное обозначение будем использовать для цикловой структуры произвольного отображения конечного множества в себя.

1.1. Вспомогательные результаты

Напомним вначале ряд хорошо известных фактов из теории чисел и теории конечных абелевых групп.

Предложение А (китайская теорема об остатках, [6]). Пусть $N = p_1^{v_1} p_2^{v_2} \dots p_m^{v_m}$ — каноническое разложение натурального числа N в произведение степеней простых чисел. Существует взаимно однозначное отображение

$$\mathbb{Z}_N \leftrightarrow \mathbb{Z}_{p_1^{v_1}} \times \mathbb{Z}_{p_2^{v_2}} \times \dots \times \mathbb{Z}_{p_m^{v_m}}, \quad (3)$$

при котором любому элементу $a \in \mathbb{Z}_N$ соответствует вектор (a_1, a_2, \dots, a_m) , $a_i \in \mathbb{Z}_{p_i^{v_i}}$, $i = 1, 2, \dots, m$, где a_1, \dots, a_m — наименьшие неотрицательные вычеты a по модулям $p_1^{v_1}, \dots, p_m^{v_m}$ соответственно, и обратно, каждому такому вектору соответствует элемент $a \in \mathbb{Z}_N$, для которого $a_i \equiv a \pmod{p_i^{v_i}}$, $i = 1, 2, \dots, m$.

Мы фиксируем такое соответствие и, когда это удобно, записываем элемент $a \in \mathbb{Z}_n$ в виде (a_1, a_2, \dots, a_m) . Из соответствия (3) вытекает аналогичная связь между \mathbb{Z}_N^* и $\mathbb{Z}_{p_i^{v_i}}^*$, $i = 1, \dots, m$.

Предложение В. Пусть $N = \prod_{i=1}^m p_i^{v_i}$ — каноническое разложение натурального числа N .

а) Совокупность \mathbb{Z}_N^* всех обратимых элементов кольца \mathbb{Z}_N образует группу по умножению.

б) Имеет место изоморфизм:

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{v_1}}^* \times \mathbb{Z}_{p_2^{v_2}}^* \times \dots \times \mathbb{Z}_{p_m^{v_m}}^* ;$$

если при этом $a = (a_1, \dots, a_m)$, $b = (b_1, \dots, b_m) \in \mathbb{Z}_N^*$, то $ab = (a_1 b_1, \dots, a_m b_m)$.

в) Порядок $|\mathbb{Z}_N^*|$ группы \mathbb{Z}_N^* равен $\varphi(N) = \prod_{i=1}^m (p_i^{v_i} - p_i^{v_i-1})$ (φ — функция Эйлера).

Циклическую группу по умножению с n элементами обозначаем C_n .

Предложение С. Пусть G — конечная абелева группа порядка n и $n = \prod_{i=1}^k u_i^{\alpha_i}$, где u_1, \dots, u_k — попарно различные простые числа, $\alpha_1, \dots, \alpha_k > 0$. Тогда имеет место изоморфизм:

$$G \cong C_{u_1^{\alpha_1}} \times C_{u_2^{\alpha_2}} \times \dots \times C_{u_k^{\alpha_k}}.$$

Следующее предложение описывает подгруппы циклических групп.

Предложение D. Пусть $G = \langle g \rangle = C_n$ – конечная циклическая группа порядка n , порождаемая элементом g .

а) Любая подгруппа $H \subseteq G$ группы G есть циклическая группа и её порядок есть делитель n .

б) Для любого делителя r числа n в G существует единственная подгруппа H порядка r ; она порождается элементом $g^{n/r}$: $H = \langle g^{n/r} \rangle$.

Для отображения ψ конечного множества S в себя назовём подстановочным ядром $\text{Ker}(\psi, S)$ множество всех элементов S , принадлежащих циклам графа отображения ψ . Отображение ψ взаимно однозначно (т. е. является подстановкой) на $\text{Ker}(\psi, S)$ и не взаимно однозначно на любом более широком подмножестве. Укажем некоторые свойства $\text{Ker}(\psi, S)$ в случае, когда ψ – степенное отображение на $S = G$, где G – конечная абелева группа.

Предложение 1. Пусть G – конечная абелева группа и $G(d)$ – совокупность всех её элементов, порядок которых взаимно прост с данным числом $d \geq 2$. Тогда:

а) $G(d)$ – группа;

б) отображение $f : x \rightarrow x^d$ – автоморфизм группы $G(d)$;

в) $\text{Ker}(f, G) = G(d)$.

Аналогичное утверждение для случая, когда $G = \mathbb{Z}_N^*$, содержится в Теореме 1 из [4].

Доказательство. а) Пусть $a_1, a_2 \in G(d)$. Тогда порядок $a_1 a_2$ также взаимно прост с d , так как он является делителем наименьшего общего кратного порядков элементов a_1 и a_2 . Если $a \in G(d)$, то a^{-1} также принадлежит $G(d)$. Таким образом, $G(d)$ – группа.

б) Пусть e – единица группы G . Тогда $f(e) = e$, и если $a \in G(d)$, то из $f(a) = a^d = e$ следует, что $a = e$. Покажем, далее, что если $a \in G(d)$, $a \neq e$, имеет порядок $m > 1$, $(m, d) = 1$, то существует единственный элемент $b \in G(d)$, для которого $f(b) = a$, и он имеет вид $b = a^x$, $0 < x < m$.

Действительно, мы можем определить x из сравнения $xd \equiv 1 \pmod{m}$, которое, ввиду условия $(m, d) = 1$, имеет единственное решение $x \in \{1, 2, \dots, m-1\}$.

Предположим теперь, что $f(c) = a$ для некоторого $c \in G(d)$. Тогда $c^d(a^{-x})^d = e$, т. е. $(ca^{-x})^d = e$. Но в п. а) мы показали, что $G(d)$ – группа, следовательно, ca^{-x} имеет порядок, взаимно простой с d . Поэтому должно быть $ca^{-x} = e$ и $c = a^x = b$. Таким образом, отображение f взаимно однозначно на группе $G(d)$. Кроме того, $f(a_1 a_2) = f(a_1) f(a_2)$ для $a_1, a_2 \in G(d)$, и мы получаем, что f – автоморфизм группы $G(d)$.

в) В п. б) мы фактически показали, что $G(d) \subseteq \text{Ker}(f, G)$. Докажем теперь, что $G(d) = \text{Ker}(f, G)$.

Допустим противное: $x \in \text{Ker}(f, G)$, но $x \notin G(d)$. Тогда порядок x делится на некоторый отличный от 1 делитель d' числа d . Следовательно, порождаемая x циклическая группа $\langle x \rangle$ содержит, согласно Предложению D, циклическую подгруппу $\langle b \rangle$, $b \neq e$, порядка d' , т. е. $b^{d'} = e$ и, следовательно, $f(b) = b^d = e$. Так как b есть степень x , то b принадлежит некоторому циклу, т. е. $b \in \text{Ker}(f, G)$. Как мы заметили выше, также $e \in \text{Ker}(f, G)$. Таким образом $f(b) = f(e) = e$ для двух различных элементов $b, e \in \text{Ker}(f, G)$. Но, по определению, f должно быть взаимно

однозначным на $\text{Ker}(f, G)$. Это противоречие показывает, что $\text{Ker}(f, G) = G(d)$. Предложение доказано.

Следствие 1. Пусть G — прямое произведение примарных циклических групп:

$$G = \prod_{p \in P} C_{p^{v_p}}, \quad v_p > 0,$$

где P — конечный набор простых чисел. Если на G действует степенное отображение $f^{(d)}$, $d \geq 2$, то

$$\text{Ker}(f^{(d)}, G) = \prod_{p \in P: p \nmid d} C_{p^{v_p}};$$

если при этом P не содержит простых чисел, не делящих d , то $\text{Ker}(f^{(d)}, G) = C_1$ состоит из единственного элемента e (единицы группы G).

Замечание 1. Если N — составное число и $N = p_1^{v_1} p_2^{v_2} \dots p_m^{v_m}$ — его разложение на простые множители, то граф G_N^d отображения $f^{(d)}(x) = x^d \pmod{N}$ распадается на 2^m изолированных подграфов $G_N^d(\varepsilon_1, \dots, \varepsilon_m)$, $\varepsilon_1, \dots, \varepsilon_m \in \{0, 1\}$, где множество $V_N(\varepsilon_1, \dots, \varepsilon_m)$ вершин подграфа $G_N^d(\varepsilon_1, \dots, \varepsilon_m)$ состоит из всех таких $x \in \mathbb{Z}_N$, что x делится на p_j тогда и только тогда, когда $\varepsilon_j = 1$, $j \in \{1, \dots, m\}$. Цикловая структура ограничения $f_N^{(d)}$ на $V_N(\varepsilon_1, \dots, \varepsilon_m)$ совпадает с цикловой структурой отображения $f_{N(\varepsilon_1, \dots, \varepsilon_m)}^{(d)}$, где $N(\varepsilon_1, \dots, \varepsilon_m) = \prod_{j=1}^m p_j^{\varepsilon_j v_j}$. Поэтому в дальнейшем основное внимание будет уделяться цикловой структуре отображения $f_N^{(d)}$ на мультипликативной абелевой группе \mathbb{Z}_N^* , состоящей из множества $V_N(0, \dots, 0)$ всех вычетов, взаимно простых с N , т. е. обратимых элементов кольца \mathbb{Z}_N .

1.2. Автоморфизмы примарных циклических групп и степенные отображения

Как мы установим далее, цикловая структура степенного отображения $f^{(d)}$ на \mathbb{Z}_N^* полностью определяется цикловыми структурами вида $\text{Str}(f^{(d)}, C_{p^\alpha})$, где C_{p^α} — произвольная примарная циклическая группа (p — простое, α — целое число). Обозначим через $\text{pm}(C_n)$ совокупность всех отображений $f^{(d)}$, где $d < n$ и взаимно просто с n .

В этом разделе мы остановимся на связи степенных отображений с автоморфизмами этих групп. Группу всех автоморфизмов группы G обозначаем $\text{Aut } G$. Структура группы $\text{Aut } G$ для примарной циклической группы G определяется следующим образом (см. [9]).

Предложение Е. Пусть p — простое число, $\alpha \geq 1$ — целое.

- Если p нечетно, то $\text{Aut } C_{p^\alpha}$ — циклическая группа порядка $p^\alpha - p^{\alpha-1}$.
- Если $p = 2$, $\alpha \geq 2$, то $\text{Aut } C_{2^\alpha}$ изоморфна прямому произведению:

$$\text{Aut } C_{2^\alpha} \cong C_2 \times C_{2^{\alpha-2}};$$

если $\alpha = 1$, то $\text{Aut } C_2 = \{\varepsilon\}$ (ε — тождественное отображение).

Рассматриваем действие $f^{(d)}$ на группы C_n . Ясно, что оно зависит только от наименьшего неотрицательного вычета числа d по модулю n . Поэтому можно считать, что $d < n$. На $\text{pm}(C_n)$ определим операцию \circ как последовательное выполнение отображений $f^{(d_1)}$ и $f^{(d_2)}$ из $\text{pm}(C_n)$: $f^{(d_1)} \circ f^{(d_2)} = f^{(d_3)}$, где $d_3 \equiv d_1 d_2 \pmod{n}$, $d_3 < n$. Для $f^{(d)} \in \text{pm}(C_n)$ определяется обратное отображение: $(f^{(d)})^{-1} = f^{(d^{-1})}$, где $d^{-1} < n$ — решение сравнения $xd \equiv 1 \pmod{n}$.

Ясно, что относительно операции \circ совокупность $\text{pm}(C_n)$ — группа с единицей $f^{(1)} = \varepsilon$; назовем её *группой степенных отображений*.

Предложение 2. *Группа степенных отображений $\text{pm}(C_n)$ изоморфна группе \mathbb{Z}_n^* .*

Утверждение очевидно.

Рассмотрим теперь группы степенных отображений для примарных циклических групп C_{p^α} . Порождающий элемент группы C_{p^α} обозначаем через g , единицу — через e .

Предложение 3. *Для всякого простого p и целого $\alpha \geq 1$ группа $\text{pm}(C_{p^\alpha})$ изоморфна группе $\text{Aut } C_{p^\alpha}$.*

Доказательство. Всякое отображение $f^{(d)} \in \text{pm}(C_{p^\alpha})$ взаимно однозначно и удовлетворяет соотношениям

$$f^{(d)}(x_1 x_2) = f^{(d)}(x_1) f^{(d)}(x_2), \quad x_1, x_2 \in C_{p^\alpha}, \quad f^{(d)}(e) = e,$$

т. е. оно порождает автоморфизм группы C_{p^α} . Обозначим его ψ_d . Ясно также, что произведению $f^{(d_1)} \circ f^{(d_2)}$ отвечает автоморфизм $\psi_{d_1} \psi_{d_2} = \psi_{d_3}$, где $d_3 \equiv d_1 d_2 \pmod{p^\alpha}$, $d_3 < p^\alpha$. Автоморфизм ψ_d при $d \neq 1$ не может быть тождественным: из $\psi_d = \varepsilon$ следовало бы $\psi_d(g) = g^d = g$ и $g^{d-1} = e$, что невозможно, так как $0 < d-1 < p^\alpha$, а $g^k \neq e$, если $0 < k < p^\alpha$. Таким образом, мы получаем изоморфное вложение: $\text{pm}(C_{p^\alpha}) \subseteq \text{Aut } C_{p^\alpha}$.

С другой стороны, если ψ — любой автоморфизм группы $C_{p^\alpha} = \langle g \rangle$, то $\psi(g) = g^d$, и g^d должен также быть порождающим элементом. Поэтому d не делится на p . Далее, для любого $h = g^a \in C_{p^\alpha}$ имеем $\psi(h) = \psi(g^a) = (\psi(g))^a = (g^d)^a = h^d$. Следовательно, $\psi = \psi_d$, $p \nmid d$; при этом $\psi = \varepsilon$ равносильно $d = 1$. Тем самым получаем противоположное изоморфное вложение: $\text{Aut } C_{p^\alpha} \subseteq \text{pm}(C_{p^\alpha})$. В итоге приходим к изоморфизму: $\text{pm}(C_{p^\alpha}) \cong \text{Aut } C_{p^\alpha}$. Предложение доказано.

Следствие 2. *Всякое степенное отображение $f^{(d)}$ на группе C_{p^α} , где p — нечётное простое, $\alpha \geq 1$, $p \nmid d$, есть степень некоторого отображения $f^{(d_1)}$, где d_1 — элемент порядка $p^\alpha - p^{\alpha-1}$ в группе $\mathbb{Z}_{p^\alpha}^*$.*

Следствие 3. *Всякое степенное отображение $f^{(d)}$ на группе C_{2^α} , где $\alpha \geq 3$ и d нечётно, представляется в виде произведения $(f^{(d_1)})^w \circ (f^{(d_2)})^s$, $0 \leq w < 2^{\alpha-2}$, $s = 0$ или 1 , и $d_1, d_2 \in \mathbb{Z}_{2^\alpha}^*$ — элементы порядков $2^{\alpha-2}$ и 2 соответственно.*

Нетрудно заметить, что при $\alpha \geq 3$ в группе $\mathbb{Z}_{2^\alpha}^* \cong \langle d_1 \rangle \times \langle d_2 \rangle$, где d_1, d_2 — элементы порядков, соответственно, $2^{\alpha-2}$ и 2 , в качестве d_2 всегда можно взять $2^\alpha - 1$, т. е. каждый элемент $\mathbb{Z}_{2^\alpha}^*$ записывать в виде $\pm d_1^w$, $0 \leq w < 2^{\alpha-2}$.

Мы можем теперь при любых d и N описать алгебраическое строение подстановочного ядра $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$ отображения $f^{(d)}$, т. е. максимального подмножества в \mathbb{Z}_N^* , на котором $f^{(d)}$ действует как подстановка. Пусть

$$N = 2^{\alpha_0} p_1^{\alpha_1} \dots p_m^{\alpha_m}, \text{ где } \alpha_0 = 0, \text{ если } N \text{ нечётно,} \quad (4)$$

— каноническое разложение для N , пусть $L_i = (p_i - 1)p_i^{\alpha_i - 1}$ и

$$L_i = \prod_{j=1}^{r_i} u_{ij}^{\alpha_{ij}}, \quad u_{ij} \text{ — простые числа, } \alpha_{ij} > 0, \quad (5)$$

— каноническое разложение для $L_i > 1$, а

$$U_i(d) = \{u_{i1}, u_{i2}, \dots, u_{ir_i}\}, \quad i = 1, \dots, m, \quad (6)$$

— множество всех простых и не делящих d делителей L_i , а $U_0(d) = \{2\}$ только при $\alpha_0 \geq 2$ и нечётном d , в остальных случаях $U_0(d) = \emptyset$.

Предложение 4. Пусть $d \geq 2$, $f^{(d)} : x \rightarrow x^d$ — отображение, определенное на \mathbb{Z}_N^* , N — число из (4). Тогда $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$ представляется в виде прямого произведения примарных циклических групп:

$$\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) \cong \begin{cases} C(d, \alpha_0) \prod_{i=1}^m \left(\prod_{u_{ij} \in U_i(d)} C_{u_{ij}^{\alpha_{ij}}} \right), & \text{если } U(d) \neq \emptyset, \\ C_1, & \text{если } U(d) = \emptyset, \end{cases} \quad (7)$$

где u_{ij}, α_{ij} — числа из формулы (5), $C(d, n) = C_2 \times C_{2^{n-2}}$ при $n \geq 2$ и нечётном d , в остальных случаях $C(d, n) = C_1$, $U(d) \stackrel{\text{def}}{=} \bigcup_{i=0}^m U_i(d)$, а $U_i(d)$ — множества из (6).

Доказательство. Из Предложения В следует, что $\mathbb{Z}_N^* \cong \prod_{i=0}^m \mathbb{Z}_{p_i^{\alpha_i}}^*$ (здесь $p_0 = 2$). Из Предложений Е, 2 и 3 вытекает, что группа $\mathbb{Z}_{p_i^{\alpha_i}}^*$ при нечётном p_i изоморфна C_{L_i} для L_i из (5). Применяя затем Предложение С, мы получаем, что C_{L_i} — прямое произведение примарных циклических групп:

$$\mathbb{Z}_{p_i^{\alpha_i}}^* \cong C_{L_i} \cong \prod_{j=1}^{r_i} C_{u_{ij}^{\alpha_{ij}}}, \quad i = 1, 2, \dots, m, \quad (8)$$

где u_{ij}, α_{ij}, r_i определены в (5).

Аналогично,

$$\mathbb{Z}_{2^n}^* \cong \begin{cases} C_2 \times C_{2^{n-2}}, & n \geq 2, \\ C_1, & n = 1. \end{cases} \quad (9)$$

Следовательно, при любых $d, N \geq 2$ группа $\mathbb{Z}_{p_i^{\alpha_i}}^*$ изоморфна прямому произведению циклических групп вида (8) или (9). Далее, используя Предложение 1, нетрудно заметить, что

$$\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) = \mathbb{Z}_N^*(d) \cong \prod_{i=0}^m \mathbb{Z}_{p_i^{\alpha_i}}^*(d) = \prod_{i=0}^m \text{Ker}(f^{(d)}, \mathbb{Z}_{p_i^{\alpha_i}}^*).$$

Если $U_0(d) \neq \emptyset$, то $\text{Ker}(f^{(d)}, \mathbb{Z}_{2^{\alpha_0}}^*) = C(d, \alpha_0)$ в силу (9). Наконец, по Следствию 1, $\text{Ker}(f^{(d)}, \mathbb{Z}_{p_i^{\alpha_i}}^*) \cong \prod_{u_{ij} \in U_i(d)} C_{u_{ij}^{\alpha_{ij}}}$, $i = 1, \dots, m$. Итак,

$$\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) \cong C(d, \alpha_0) \prod_{i=1}^m \left(\prod_{u_{ij} \in U_i(d)} C_{u_{ij}^{\alpha_{ij}}} \right),$$

если хотя бы одно из множеств $U_i(d)$, $i = 0, 1, \dots, m$, не пусто, и $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) = C_1$, если $U(d) = \bigcup_{i=0}^m U_i(d) = \emptyset$.

Предложение доказано.

Таким образом, мы сможем найти цикловую структуру отображения $f^{(d)}$ на \mathbb{Z}_N^* , если:

а) найдем формулу для $\text{Str}(f^{(d)}, C_{u^\alpha})$, где u — простое число, не делящее d , $\alpha \geq 1$, и

б) укажем правило нахождения $\text{Str}(f^{(d)}, C_{u_1^{\alpha_1}} \times \dots \times C_{u_r^{\alpha_r}})$ по $\text{Str}(f^{(d)}, C_{u_i^{\alpha_i}})$, $i = 1, \dots, r$.

Рассмотрим сперва задачу б).

2. Композиция цикловых структур

Пусть S — конечное множество, ψ — подстановка на S , имеющая k_1 циклов длины l_1 , k_2 циклов длины l_2, \dots, k_r циклов длины r , $k_1 l_1 + k_2 l_2 + \dots + k_r l_r = |S|$. Цикловую структуру ψ обозначаем, как и раньше, через

$$\text{Str}(\psi, S) = (l_1)^{k_1} (l_2)^{k_2} \dots (l_r)^{k_r} = \prod_{i=1}^r (l_i)^{k_i};$$

при этом $(l)^k$ называем *фрагментом* $\text{Str}(\psi, S)$, если он совпадает с одним из $(l_i)^{k_i}$, $i = 1, 2, \dots, r$.

Пусть $\mathbb{H} = (H_1, \dots, H_M; \pi_1, \dots, \pi_M)$ — система из M конечных множеств и действующих на них подстановок π_r , $r = 1, \dots, M$. Мы будем рассматривать системы, удовлетворяющие условию

$$\pi_r(x) = \pi_s(x) \quad \text{для всех } x \in H_r \cap H_s \text{ и } 1 \leq r < s \leq M. \quad (10)$$

Если множества H_r в системе \mathbb{H} попарно не пересекаются, то такая система удовлетворяет условию (10). Другим интересным для нас примером систем со свойством (10) является система $\mathbb{H} = (H_1, \dots, H_M; \pi_1, \dots, \pi_M)$ таких подгрупп H_1, \dots, H_M конечной группы G и подстановок π_1, \dots, π_M , что $H_r \cap H_s = \{e\}$, $1 \leq r < s \leq M$, где e — единичный элемент группы G , и $\pi_r(e) = e$, $r = 1, \dots, M$.

Для системы \mathbb{H} удовлетворяющей условию (10), определим действующую на прямом произведении $H = H_1 \times \dots \times H_M$ подстановку $\pi = \pi_1 \times \dots \times \pi_M$:

$$\pi(a_1, a_2, \dots, a_M) = (\pi_1(a_1), \pi_2(a_2), \dots, \pi_M(a_M)). \quad (11)$$

Цикловую структуру $\text{Str}(\pi_1 \times \dots \times \pi_M, H_1 \times \dots \times H_M)$ подстановки (11) для системы множеств $H = (H_1, \dots, H_M; \pi_1, \dots, \pi_M)$, удовлетворяющей условию (10), назовём *композицией* структур $\text{Str}(\pi_r, H_r)$, $r = 1, \dots, M$. Операцию композиции обозначим символом \star :

$$\star_{i=1}^M \text{Str}(\pi_i, H_i) = \text{Str}(\pi_1 \times \pi_2 \times \dots \times \pi_M, H_1 \times H_2 \times \dots \times H_m). \quad (12)$$

Операция \star в (12) обладает, очевидно, свойствами коммутативности и ассоциативности.

Предложение 5. Пусть система множеств и подстановок $H = (H_1, \dots, H_M; \pi_1, \dots, \pi_M)$ удовлетворяет условию (10) и при этом каждая подстановка π_i на H_i состоит из одного фрагмента: $\pi_i = (l_i)^{k_i}$, $i = 1, \dots, M$. Тогда

$$\text{Str}(\pi_1 \times \dots \times \pi_M, H_1 \times \dots \times H_m) = (\text{НОК}(l_1, \dots, l_M))_{\frac{k_1 \dots k_M l_1 \dots l_M}{\text{НОК}(l_1, \dots, l_M)}}.$$

Действительно, каждый элемент $(a_1, \dots, a_M) \in H_1 \times \dots \times H_M$ принадлежит, очевидно, циклу длины $\text{НОК}(l_1, \dots, l_M)$. Число элементов в $H_1 \times \dots \times H_M$ равно $k_1 l_1 k_2 l_2 \dots k_M l_M$. Следовательно, рассматриваемая подстановка имеет в точности $\frac{k_1 \dots k_M l_1 \dots l_M}{\text{НОК}(l_1, \dots, l_M)}$ циклов длины $\text{НОК}(l_1, \dots, l_M)$.

Следствие 4. Пусть $H = (H_1, \dots, H_M; \pi_1, \dots, \pi_M)$ — система из множеств и подстановок, удовлетворяющая условию (10). Пусть, далее, $\text{Str}(\pi_r, H_r) = \prod_{j_r=1}^{t_r} (l_{rj_r})^{k_{rj_r}}$ и $H_{rj_r} \subseteq H_r$ — подмножество, на котором действует фрагмент $\pi_{rj_r} = (l_{rj_r})^{k_{rj_r}}$, $j_r = 1, \dots, t_r$, $r = 1, \dots, M$. Тогда:

а) для любого набора $\vec{j} = (j_1, \dots, j_M)$, $1 \leq j_r \leq t_r$, $r = 1, \dots, M$, система $H(\vec{j}) = (H_{1j_1}, \dots, H_{Mj_M}; \pi_{1j_1}, \dots, \pi_{Mj_M})$ удовлетворяет условию (10) и

$$\begin{aligned} \text{Str}(\pi, H(\vec{j})) &= \star_{r=1}^M \text{Str}(\pi_{rj_r}, H_{rj_r}) = \\ &= (\text{НОК}(l_{1j_1}, \dots, l_{Mj_M}))_{\frac{k_{1j_1} l_{1j_1} \dots k_{Mj_M} l_{Mj_M}}{\text{НОК}(l_{1j_1}, \dots, l_{Mj_M})}}, \end{aligned} \quad (13)$$

б) для $H = H_1 \times \dots \times H_M$ и $\pi = \pi_1 \times \dots \times \pi_M$ справедливо равенство

$$\text{Str}(\pi, H) = \prod_{\vec{j}} (\star_{r=1}^M \text{Str}(\pi_{rj_r}, H_{rj_r})), \quad (14)$$

где произведение берется по всем $T = t_1 t_2 \dots t_M$ наборам \vec{j} .

Доказательство. а) Всякая система $H(\vec{j})$ удовлетворяет условию (10), так как этому условию удовлетворяет система H . Поэтому для любого \vec{j} из Предложения 5 следует, что $\star_{j=1}^M \text{Str}(\pi_{rj_r}, H_{rj_r})$ состоит из одного фрагмента, цикловая структура которого выражается формулой (13).

б) Для любого $h \in \prod_{r=1}^M H_r$ найдется такой вектор $\vec{j} = (j_1, \dots, j_M)$, что $h \in H(\vec{j})$. Ясно также, что если $\vec{j} \neq \vec{j}'$, то $H(\vec{j}) \cap H(\vec{j}') = \emptyset$. Поэтому H разбивается на T попарно не пересекающихся множеств $H(\vec{j})$. Пусть $(n)^K$ — произвольно взятый фрагмент в $\text{Str}(\pi, H)$ и $H(n)$ — множество всех элементов H , принадлежащих циклам

длины n ; имеем $|H(n)| = Kn$. Мы видели в п. а), что $\text{Str}(\pi, H(\bar{j}))$ для любого \bar{j} состоит из одного фрагмента (см. (13)). Если $h \in H(n)$, то h входит в одно из множеств $H(\bar{j}_1), \dots, H(\bar{j}_x)$, где $H(\bar{j}_i)$ при $i = 1, \dots, x$ — все множества $H(\bar{j})$ с цикловой структурой вида $(n)^k$, т. е. $\text{Str}(\pi, H(\bar{j}_i)) = (n)^{k^{(i)}}$, $i = 1, \dots, x$. Сравнивая число элементов в $H(n)$ и во всех этих $H(\bar{j}_i)$, $i = 1, \dots, x$, получаем: $Kn = k^{(1)}n + \dots + k^{(x)}n$, или $K = k^{(1)} + \dots + k^{(x)}$. Таким образом, $(n)^K = \prod_{i=1}^x (n)^{k^{(i)}}$. Это доказывает справедливость утверждения б).

Мы будем далее применять Предложение 5 и Следствие 4 к случаю, когда $H = H_1 \times \dots \times H_M$, где H_r ($r = 1, \dots, M$) — примарные циклические группы, а π_r — степенное отображение $f^{(d)}$, действующее на H_r как подстановка.

3. Цикловая структура степенных отображений на примарной циклической группе нечётного порядка

Пусть сначала $u \geq 2$ — простое число, $\alpha \geq 1$ — целое, $C_{u^\alpha} = \langle g \rangle$ — примарная циклическая группа с единицей e , порождаемая элементом g . Для целых чисел $d \geq 2$, не делящихся на u , рассматриваем отображения $f^{(d)}$ на группе C_{u^α} : $f^{(d)}(x) = x^d$. Поскольку $g^{u^\alpha} = e$, результат действия $f^{(d)}$ зависит фактически только от наименьшего неотрицательного вычета \bar{d} числа d по модулю u^α . Поэтому далее мы часто вместо $f^{(d)}$ рассматриваем отображение $f^{(\bar{d})}$, ограничивая тем самым область значений d отрезком $[1, u^\alpha - 1]$. Отметим сразу частный случай, когда цикловая структура отображения определяется тривиально.

Предложение 6. Пусть $u \geq 2$ — простое число, $\alpha \geq 1$ — целое. Тогда

$$\text{Str}(f^{(d)}, C_{u^\alpha}) = (1)^{u^\alpha}$$

для любого $d \equiv 1 \pmod{u^\alpha}$.

Ввиду Предложения 6 исключаем случай $d \equiv 1 \pmod{u^\alpha}$ из дальнейшего рассмотрения — в этом параграфе и в § 4.

Каждое целое число из $[1, u^\alpha - 1]$ можно записать как значение в точке u многочлена степени не выше $\alpha - 1$ с коэффициентами из $\{0, 1, \dots, u - 1\}$:

$$d = t_0 + t_1 u + \dots + t_{\alpha-1} u^{\alpha-1}, \quad t_i \in \{0, 1, \dots, u - 1\}, \quad 0 \leq i < \alpha. \quad (15)$$

Таким образом, всякое d можно представить элементом (15) кольца \mathbb{Z}_{u^α} . Ясно, что в (15) $d \in \mathbb{Z}_{u^\alpha}^*$ тогда и только тогда, когда $t_0 \neq 0$.

Далее в этом параграфе мы рассматриваем только нечётные простые u . Цикловая структура степенных отображений на примарной группе C_{2^α} будет описана в § 4.

Мы видели в § 1 (Предложения 2 и 3, Следствие 2), что при нечётном u группа $\text{pr}(C_{u^\alpha})$ и изоморфная ей группа $\mathbb{Z}_{u^\alpha}^*$ — циклические группы порядка $u^\alpha - u^{\alpha-1}$ и потому каждый элемент $d \in \mathbb{Z}_{u^\alpha}^*$ имеет порядок, являющийся делителем $(u - 1)u^{\alpha-1}$.

Укажем некоторые нужные нам свойства элементов кольца \mathbb{Z}_{u^α} .

Лемма 1. Пусть u — нечётное простое, $\alpha \geq 1$ — целое число, $d \geq 2$ — целое число, $u \nmid d$, $d \not\equiv 1 \pmod{u^\alpha}$, представленное в виде (12) :

$$d = \sum_{i=0}^{\alpha-1} t_i u^i, \quad 0 \leq t_i \leq u-1, \quad i = 0, 1, \dots, \alpha-1.$$

Порядок d в группе $\mathbb{Z}_{u^\alpha}^*$ есть степень u в том и только в том случае, когда $t_0 = 1$. Если $t_0 = 1$, то порядок d равен $u^{\alpha-\beta}$, где $\beta = \min_{1 \leq k \leq \alpha-1} \{k : t_k \neq 0\}$.

Действительно, при $t_0 \neq 1$ элемент d из (15) не может иметь порядок, равный степени u , по малой теореме Ферма. Если же $d = 1 + \sum_{i=\beta}^{\alpha-1} t_i u^i$, $t_\beta \neq 0$, то порядок d в $\mathbb{Z}_{u^\alpha}^*$, очевидно, равен $u^{\alpha-\beta}$.

Для произвольного целого $d \geq 2$, не делящегося на нечётное простое u , вводим два параметра, которые, как будет показано в Предложении 7, полностью определяют цикловую структуру степенного отображения $f^{(d)}$ на циклической группе C_{u^α} , $\alpha \geq 1$.

1) Обозначим через $\text{ord}(d)$ порядок числа d по модулю u :

$$\text{ord}(d) = \text{ord}(d, u) = \min \{k : d^k \equiv 1 \pmod{u}\} \quad (16)$$

($\text{ord}(d)|(u-1)$ по малой теореме Ферма). Ясно, что $d^{\text{ord}(d)} - 1$ делится на некоторую степень u^r числа u , $r \geq 1$.

2) Обозначим через ρ наибольшую не превышающую α степень u , на которую делится $d^{\text{ord}(d)} - 1$:

$$\rho = \rho(d, u) = \max_{1 \leq \beta \leq \alpha} \left\{ \beta : u^\beta \mid \left(d^{\text{ord}(d)} - 1 \right) \right\}. \quad (17)$$

Отметим, что для нахождения параметров $\text{ord}(d)$ и ρ не нужно находить представление d в виде (15). Предложение 7 мы формулируем в предположении $2 \leq d \leq u^\alpha - 1$ лишь для удобства изложения.

Предложение 7. Пусть u — нечётное простое число, $\alpha \geq 1$ — целое число и для целого числа d , где $2 \leq d \leq u^\alpha - 1$, $u \nmid d$, рассматриваем степенное отображение $f^{(d)} : x \rightarrow x^d$ на группе C_{u^α} . Тогда

$$\text{Str} \left(f^{(d)}, C_{u^\alpha} \right) = (1) (\text{ord}(d))^{\frac{u^\rho - 1}{\text{ord}(d)}} \prod_{i=1}^{\alpha-\rho} (\text{ord}(d) u^i)^{\frac{u-1}{\text{ord}(d)} u^\rho - 1}, \quad (18)$$

где $\text{ord}(d)$, ρ — величины из (16) и (17) соответственно.

Доказательство. Найдем порядок d в группе $\mathbb{Z}_{u^\alpha}^*$. Порядок этой группы равен $(u-1)u^{\alpha-1}$. Поэтому порядок элемента d есть число вида $vu^{\alpha-\beta}$, где $v|(u-1)$, $1 \leq \beta \leq \alpha$. Так как $(u, v) = 1$, то порядок элемента d^v есть либо 1 (при $\beta = \alpha$), либо положительная степень u . В первом случае $d^v \equiv 1 \pmod{u^\alpha}$, и потому $v = \text{ord}(d)$. Во втором, по лемме 1, $d^v \equiv 1 + \sum_{i=1}^{\alpha-1} t_i u^i$, и вновь $v = \text{ord}(d)$. Тогда, по определению ρ , $d^v = d^{\text{ord}(d)} \equiv 1 + \sum_{i=\rho}^{\alpha-1} t_i u^i \pmod{u^\alpha}$, $t_\rho \neq 0$. По лемме 1 порядок элемента в правой части сравнения есть $u^{\alpha-\rho}$, и мы получаем, что порядок d в $\mathbb{Z}_{u^\alpha}^*$ есть $\text{ord}(d)u^{\alpha-\rho}$.

Введём теперь некоторую классификацию элементов группы C_{u^α} , не равных e . Всякий элемент представим в виде

$$h = g^{s(u)u^\beta}, \quad (19)$$

где $s(u) = s_\beta + s_{\beta+1}u + \dots + s_{\alpha-1}u^{\alpha-\beta-1}$, $s_\beta, s_{\beta+1}, \dots, s_{\alpha-1} \in \mathbb{Z}_u$, $s_\beta \neq 0$, при некотором β , $0 \leq \beta \leq \alpha - 1$. Для $\beta = 0, 1, \dots, \alpha - 1$ обозначим через S_β совокупность всех элементов, представимых в виде (19) при данном β . Определим, далее, разбиение $C_{u^\alpha} \setminus \{e\}$ на непересекающиеся множества:

$$\text{при } \alpha - \rho > 0: \quad C_{u^\alpha} \setminus \{e\} = S_0 \cup S_1 \cup \dots \cup S_{\alpha-\rho-1} \cup \tilde{S}_{\alpha-\rho}, \quad (20)$$

где $\tilde{S}_{\alpha-\rho} = S_{\alpha-\rho} \cup S_{\alpha-\rho+1} \cup \dots \cup S_{\alpha-1}$;

$$\text{при } \alpha - \rho = 0: \quad C_{u^\alpha} \setminus \{e\} = \tilde{S}_0.$$

Число элементов в S_β равно $|S_\beta| = u^{\alpha-\beta} - u^{\alpha-\beta-1}$; число элементов в $\tilde{S}_{\alpha-\rho}$, как нетрудно заметить, равно $|\tilde{S}_{\alpha-\rho}| = u^\rho - 1$. Будем рассматривать действие $f^{(d)}$ на компонентах разбиения (20).

Найдем длины циклов, которым принадлежат элементы этих подмножеств. Ясно, что эти длины — делители $\text{ord}(d)u^{\alpha-\rho}$, порядка элемента d в группе $\mathbb{Z}_{u^\alpha}^*$. По определению ρ

$$d^{\text{ord}(d)} \equiv 1 + t_\rho u^\rho + \sum_{i=\rho+1}^{\alpha-1} t_i u^i \pmod{u^\alpha}, \quad t_i \in \mathbb{Z}_u, \quad t_\rho \neq 0. \quad (21)$$

Рассмотрим два случая.

1) Пусть β — одно из чисел $0, 1, \dots, \alpha - \rho - 1$. Ввиду (21)

$$u^\beta d^{\text{ord}(d)u^\gamma} \equiv u^\beta + t_\rho u^{\beta+\rho+\gamma} \begin{cases} \equiv u^\beta \pmod{u^\alpha}, & \gamma = \alpha - \rho - \beta, \\ \not\equiv u^\beta \pmod{u^\alpha}, & \gamma < \alpha - \rho - \beta. \end{cases} \quad (22)$$

Из (22) следует, что g^{u^β} принадлежит циклу длины $\text{ord}(d)u^{\alpha-\rho-\beta}$. Так как $(a, u) = 1$, то любой элемент $h = g^{au^\beta} \in S_\beta$, тоже принадлежит некоторому циклу той же длины, и мы получаем, что при любом $\beta = 0, 1, \dots, \alpha - \rho - 1$ все элементы S_β принадлежат циклам длины $\text{ord}(d)u^{\alpha-\rho-\beta}$.

2) Пусть $h \in \tilde{S}_{\alpha-\rho}$, т. е. $h = g^{au^{\alpha-\rho+k}}$, где $(a, u) = 1$, $k \geq 0$. Тогда ввиду (21)

$$au^{\alpha-\rho+k} d^{\text{ord}(d)} \equiv au^{\alpha-\rho+k} + at_\rho u^{\rho+\alpha-\rho+k} \equiv au^{\alpha-\rho+k} \pmod{u^\alpha},$$

и поэтому каждый элемент $\tilde{S}_{\alpha-\rho}$ принадлежит циклу длины $\text{ord}(d)$. Таким образом, для $\beta = 0, 1, \dots, \alpha - \rho - 1$ все элементы S_β распределяются по

$$\frac{|S_\beta|}{\text{ord}(d)u^{\alpha-\rho-\beta}} = \frac{u^{\alpha-\beta} - u^{\alpha-\beta-1}}{\text{ord}(d)u^{\alpha-\rho-\beta}} = \frac{u-1}{\text{ord}(d)} u^{\rho-1}$$

циклам длины $\text{ord}(d)u^{\alpha-\rho-\beta}$:

$$\text{Str}\left(f^{(d)}, S_\beta\right) = (\text{ord}(d)u^{\alpha-\rho-\beta})^{\frac{u-1}{\text{ord}(d)}u^{\rho-1}}, \quad \beta = 0, 1, \dots, \alpha - \rho - 1. \quad (23)$$

Все элементы $\tilde{S}_{\alpha-\rho}$ входят в

$$\frac{|\tilde{S}_{\alpha-\rho}|}{\text{ord}(d)} = \frac{u^\rho - 1}{\text{ord}(d)}$$

циклов длины $\text{ord}(d)$, и

$$\text{Str}\left(f^{(d)}, \tilde{S}_{\alpha-\rho}\right) = \text{ord}(d)^{\frac{u^\rho-1}{\text{ord}(d)}}. \quad (24)$$

В последовательности цикловых структур

$$\text{Str}\left(f^{(d)}, \tilde{S}_{\alpha-\rho}\right), \text{Str}\left(f^{(d)}, \tilde{S}_{\alpha-\rho-1}\right), \dots, \text{Str}\left(f^{(d)}, \tilde{S}_1\right), \text{Str}\left(f^{(d)}, \tilde{S}_0\right)$$

длины циклов в каждой из структур делятся на длины циклов во всех предшествующих. Поэтому $\text{Str}\left(f^{(d)}, C_{u^\alpha}\right)$ получается объединением всех фрагментов в (23), (24) и фрагмента (1) (соответствующего единице e):

$$\text{Str}\left(f^{(d)}, C_{u^\alpha}\right) = (1) \left(\text{ord}(d)^{\frac{u^\rho-1}{\text{ord}(d)}} \prod_{i=1}^{\alpha-\rho} (\text{ord}(d) u^i) \right)^{\frac{u-1}{\text{ord}(d)} u^{\rho-1}},$$

т. е. справедлива формула (18).

Предложение доказано.

Если мы произвольно берём натуральное число d , то, при любом нечётном простом u с вероятностью $1 - \frac{1}{u}$ это будет число с $\rho(d, u) = 1$. В этом случае формула (18) упрощается.

Следствие 5. Пусть u — нечётное простое, $\alpha \geq 1$ — целое число. Если $d \geq 2$, $u \nmid d$, $\rho(d, u) = 1$, то

$$\text{Str}\left(f^{(d)}, C_{u^\alpha}\right) = (1) \prod_{i=0}^{\alpha-1} (\text{ord}(d) u^i)^{\frac{u-1}{\text{ord}(d)}};$$

в частности,

$$\text{Str}\left(f^{(d)}, C_u\right) = (1) (\text{ord}(d))^{\frac{u-1}{\text{ord}(d)}}.$$

4. Цикловая структура степенного отображения на примарной циклической 2-группе

В этом параграфе мы найдём формулы для цикловой структуры степенного отображения $f^{(d)}$ (где d — произвольное целое нечётное число) на группе C_{2^α} , $\alpha \geq 1$ — любое целое число. Вначале отметим несколько частных случаев.

Предложение 8. а) Для любого нечётного d

$$\text{Str}\left(f^{(d)}, C_2\right) = (1)^2;$$

б) для любого нечётного $d \geq 3$

$$\text{Str}\left(f^{(d)}, C_4\right) = \begin{cases} (1)^4, & d \equiv 1 \pmod{4}, \\ (1)^2(2), & d \equiv -1 \pmod{4}. \end{cases}$$

Утверждения очевидны.

Предложение 9. Пусть $C_{2^\alpha} = \langle g \rangle$, e – единица группы C_{2^α} . Тогда

$$\text{Str} \left(f^{(2^\alpha-1)}, C_{2^\alpha} \right) = (1)^2 (2)^{2^{\alpha-1}-1}.$$

Действительно, для любого целого a и $d = 2^\alpha - 1$ справедливо равенство $g^{ad} = g^{-a}$, и поэтому имеется 2 цикла длины 1: (e) , $(g^{2^{\alpha-1}})$ и $2^{\alpha-1} - 1$ циклов длины 2: (g^k, g^{-k}) , $k = 1, 2, \dots, 2^{\alpha-1} - 1$.

Учитывая Предложения 8, 9 и Предложение 6 в § 3, мы далее здесь всегда предполагаем, что $\alpha \geq 3$ и $3 \leq d < 2^\alpha - 2$. Найдём, прежде всего, порядок d в группе $\mathbb{Z}_{2^\alpha}^*$. Следствие 3 в § 2 показывает, что он есть степень 2 и не превосходит $2^{\alpha-2}$. Укажем конкретный способ его нахождения. Для нечётного d и целого числа $\alpha \geq 3$ при $3 \leq d < 2^\alpha$ определяем целочисленный параметр v :

$$\begin{aligned} v &= v(d, \alpha) = \\ &= \max \left\{ k \in \{2, \dots, \alpha - 1\} : \begin{cases} 2^k | (d - 1), & d \equiv 1 \pmod{4}, \\ 2^k | (d + 1), & d \equiv -1 \pmod{4} \end{cases} \right\}. \end{aligned} \quad (25)$$

Лемма 2. Пусть $\alpha \geq 3$ – целое число, d – нечётное целое из множества $\{3, \dots, 2^\alpha - 3\}$. Тогда порядок d в группе $\mathbb{Z}_{2^\alpha}^*$ равен $2^{\alpha-v}$, где v – число из (25).

Доказательство. Пусть $d \equiv 1 \pmod{4}$. Тогда $d - 1$ делится на 2^v и $d = 1 + 2^v n$, где n – нечётное число. Таким образом,

$$d \equiv 1 + 2^v n \pmod{2^{v+1}}.$$

Отсюда получаем:

$$d^{2^k} \equiv 1 + 2^{v+k} n \pmod{2^{v+k+1}}, \quad n \text{ нечётно}, \quad k = 1, 2, \dots, \quad (26)$$

и $d^{2^{\alpha-v}} \equiv 1 \pmod{2^\alpha}$ при $k = \alpha - v$; очевидно, что $d^{2^k} \not\equiv 1 \pmod{2^\alpha}$, если $k < \alpha - v$.

Пусть теперь $d \equiv -1 \pmod{4}$. Имеем тогда

$$d \equiv -1 + 2^v n \pmod{2^{v+1}}, \quad n \text{ нечётно}. \quad (27)$$

Из (27) получается:

$$d^{2^k} \equiv 1 - 2^{v+k} n \pmod{2^{v+k+1}}, \quad n \text{ нечётно}, \quad k = 1, 2, \dots \quad (28)$$

Отсюда снова следует, что порядок d есть $2^{\alpha-v}$. Лемма доказана.

Отметим некоторые сравнения, следующие из (26) и, соответственно, (27), (28).

Если $\alpha \geq 3$, $d \in \{3, \dots, 2^\alpha - 3\}$ и $d \equiv 1 \pmod{4}$, то

$$2^\beta d^{2^{\alpha-v-\gamma}} \equiv 2^\beta + 2^{\alpha-\gamma+\beta} \pmod{2^{\alpha-\gamma+\beta+1}}, \quad (29)$$

для целых $\beta, \gamma, \beta \geq 0, 0 \leq \gamma \leq \alpha - v - 1$.

Если $\alpha \geq 3$, $d \in \{3, \dots, 2^\alpha - 3\}$, $d \equiv -1 \pmod{4}$, то

$$2^\beta d \equiv -2^\beta + 2^{v+\beta} \pmod{2^{v+\beta+1}} \quad (30)$$

и

$$2^\beta d^{2^{\alpha-v-\gamma}} \equiv 2^\beta - 2^{\alpha-\gamma+\beta} \pmod{2^{\alpha-\gamma+\beta+1}}, \quad (31)$$

для целых $\beta, \gamma \geq 0$, $0 \leq \gamma \leq \alpha - v - 1$.

Введём, аналогично §3, классификацию элементов C_{2^α} . Пусть для $\beta = 0, 1, \dots, \alpha - 1$

$$S_\beta = \left\{ g^{a2^\beta}, a \text{ нечётно} \right\}, \quad (32)$$

а также

$$\tilde{S}_{\alpha-\beta} = S_{\alpha-\beta} \cup S_{\alpha-\beta+1} \cup \dots \cup S_{\alpha-1}, \quad \beta = 1, \dots, \alpha - 1. \quad (33)$$

Ясно, что $S_\beta \cap S_{\beta'} = \emptyset$, если $\beta' \neq \beta$. Нетрудно также показать, что

$$|S_\beta| = 2^{\alpha-\beta-1}, \quad \beta = 0, 1, \dots, \alpha - 1, \quad (34)$$

и

$$\left| \tilde{S}_{\alpha-\beta} \right| = 2^\beta - 1. \quad (35)$$

Предложение 10. Пусть $\alpha \geq 3$ — целое, d — нечётное целое число из множества $\{3, \dots, 2^\alpha - 3\}$. Тогда

$$\text{Str} \left(f^{(d)}, C_{2^\alpha} \right) = \begin{cases} (1)^{2^v} \prod_{i=v}^{\alpha-1} (2^{\alpha-i})^{2^{v-1}}, & d \equiv 1 \pmod{4}, \\ (1)^2 (2)^{2^v-1} \prod_{i=v}^{\alpha-2} (2^{\alpha-i})^{2^{v-1}}, & d \equiv -1 \pmod{4}, \end{cases}$$

где v — число из (25).

Доказательство. Рассмотрим разбиение:

$$C_{2^\alpha \setminus \{e\}} = S_0 \cup S_1 \cup \dots \cup S_{\alpha-v-1} \cup \tilde{S}_{\alpha-v}, \quad (36)$$

где S_β ($\beta = 0, 1, \dots, \alpha - v - 1$), $\tilde{S}_{\alpha-v}$ — множества, соответственно, из (32) и (33). Найдём сначала $\text{Str} \left(f^{(d)}, S_\beta \right)$, $\beta = 0, 1, \dots, \alpha - v - 1$. Для этого заметим, что длина цикла, которому принадлежит каждый из элементов $h = g^{2^\beta a} \in S_\beta$ (a нечётно), равна $2^{\alpha-v-\beta}$.

Действительно, $2^\beta d^{\alpha-v-\gamma} \equiv 2^\beta \pm 2^{\alpha-\gamma+\beta} \pmod{2^{\alpha-\gamma+\beta+1}}$ согласно (29) и (31), и потому $a2^\beta d^{\alpha-v-\gamma} \equiv a2^\beta \pmod{2^\alpha}$ тогда и только тогда, когда $\gamma \leq \beta$. Следовательно, длина цикла, которому принадлежит всякий элемент $h \in S_\beta$, на самом деле равна $2^{\alpha-v-\beta}$. Так как $|S_\beta| = 2^{\alpha-\beta-1}$ по (34), то число таких циклов равно $\frac{2^{\alpha-\beta-1}}{2^{\alpha-v-\beta}} = 2^{v-1}$

и

$$\text{Str} \left(f^{(d)}, S_\beta \right) = (2^{\alpha-v-\beta})^{2^{v-1}}, \quad \beta = 0, 1, \dots, \alpha - v - 1. \quad (37)$$

Рассмотрим далее действие $f^{(d)}$ на $\tilde{S}_{\alpha-v}$. Если $d \equiv 1 \pmod{4}$, то непосредственно проверяется, что $h^d \equiv h \pmod{2^\alpha}$ для любого $h \in \tilde{S}_{\alpha-v}$. Так как $|\tilde{S}_{\alpha-v}| = 2^v - 1$ (см. (35)), то

$$\text{Str} \left(f^{(d)}, \tilde{S}_{\alpha-v} \right) = (1)^{2^v-1}, \text{ если } d \equiv 1 \pmod{4}. \quad (38)$$

Пусть теперь $d \equiv -1 \pmod{4}$. Сравнение (30) показывает, что $2^\beta d \equiv -2^\beta \pmod{2^\alpha}$ для всех $\beta \geq \alpha - v$, и потому $h^d = h^{-1}$, если $h \in \tilde{S}_{\alpha-v}$. Таким образом (учитывая, что $|\tilde{S}_{\alpha-v}| = 2^v - 1$), мы получаем, что при действии $f^{(d)}$, $d \equiv -1 \pmod{4}$, на $\tilde{S}_{\alpha-v}$ имеется один цикл $(g^{2^{\alpha-1}})$ длины 1 и $\frac{1}{2}(2^v - 2) = 2^{v-1} - 1$ циклов (g^{ad}, g^{-a}) , $a = 1, 2, \dots, 2^{v-1} - 1$, длины 2, т.е.

$$\text{Str}\left(f^{(d)}, \tilde{S}_{\alpha-v}\right) = (1)(2)^{2^{v-1}-1}, \text{ если } d \equiv -1 \pmod{4}. \quad (39)$$

Из (37) и (39) следует, что при $d \equiv -1 \pmod{4}$ циклы длины 2 возникают в результате действия $f^{(d)}$ на два подмножества в разбиении (36): на $S_{\alpha-v-1}$ и на $\tilde{S}_{\alpha-v}$. Поэтому общее число циклов длины 2 при $d \equiv -1 \pmod{4}$ есть $2^{v-1} + 2^{v-1} - 1 = 2^v - 1$.

Заметим теперь, что в последовательности цикловых структур

$$\text{Str}\left(f^{(d)}, \tilde{S}_{\alpha-v}\right), \text{Str}\left(f^{(d)}, S_{\alpha-v-1}\right), \dots, \text{Str}\left(f^{(d)}, S_1\right), \text{Str}\left(f^{(d)}, S_0\right)$$

длины циклов в каждой из структур делятся на длины циклов всех предшествующих. Поэтому из (36)–(38) и, соответственно, (36), (37) и (39) следует, что

$$\text{Str}\left(f^{(d)}, C_{2^\alpha}\right) = (1)^{2^v} \prod_{i=v}^{\alpha-1} (2^{\alpha-i})^{2^{v-1}}, \text{ если } d \equiv 1 \pmod{4},$$

и

$$\text{Str}\left(f^{(d)}, C_{2^\alpha}\right) = (1)^2 (2)^{2^{v-1}} \prod_{i=v}^{\alpha-2} (2^{\alpha-i})^{2^{v-1}}, \text{ если } d \equiv -1 \pmod{4},$$

где v — число из (25) ($2 \leq v \leq \alpha - 1$).

Предложение доказано.

5. Цикловая структура степенного отображения $f^{(d)}$ на \mathbb{Z}_N^* при произвольных d и N

Мы можем теперь найти цикловую структуру отображения $f^{(d)}$ на множестве \mathbb{Z}_N^* обратимых элементов кольца \mathbb{Z}_N для произвольных d и N . Как мы видели в § 1, она может быть определена как цикловая структура подстановки, индуцируемой $f^{(d)}$ на максимальном подмножестве $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) \subseteq \mathbb{Z}_N^*$, для которого данное отображение является взаимно однозначным. В Предложении 4 было описано алгебраическое строение $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$. Пусть

$$N = 2^{\nu_0} \prod_{i=1}^m p_i^{\nu_i} \quad (40)$$

— каноническое разложение N ($\nu_0 = 0$, если N нечётно), пусть $L_i = p_i^{\nu_i} - p_i^{\nu_i-1}$ и при $L_i > 1$

$$L_i = \prod_{u|L_i} u^{\alpha(u,i)}, \quad i = 0, 1, \dots, m, \quad (41)$$

— каноническое разложение числа L_i . В каждом таком разложении u пробегает все различные простые делители L_i , а $\alpha(u, i)$ — максимальный показатель степени u , на которую делится L_i ; числа $u^{\alpha(u, i)}$ называем *примарными компонентами* в разложениях (41). Напомним (см. Предложение В), что

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{2^{\nu_0}}^* \times \prod_{i=1}^m \mathbb{Z}_{p_i^{\nu_i}}^*.$$

Кроме того (см. п. 1.2),

$$\begin{aligned} \mathbb{Z}_{2^{\nu_0}}^* &\cong C_2 \times C_{2^{\nu_0-2}} \quad \text{при } \nu_0 \geq 2, \quad \mathbb{Z}_2^* \cong C_1, \\ \mathbb{Z}_{p_i^{\nu_i}}^* &\cong C_{L_i} \cong \prod_{u|L_i} C_{u^{\alpha(u, i)}}. \end{aligned}$$

При $i = 1, \dots, m$ обозначим через $U_i = U_i(d) = (u_{i1}, u_{i2}, \dots, u_{is_i})$ множество всех различных простых делителей L_i , взаимно простых с d , а через $\tilde{U}_i = \tilde{U}_i(d) = (u_{i1}^{\alpha_{i1}}, u_{i2}^{\alpha_{i2}}, \dots, u_{is_i}^{\alpha_{is_i}})$ — множество соответствующих примарных компонент в (41) (если $s_i = 0$, то $U_i = \tilde{U}_i = \emptyset$). Пусть также при нечетном d

$$U_0 = \begin{cases} (u_{01}, u_{02}), & \text{где } u_{01} = u_{02} = 2, \text{ если } \nu_0 \geq 2, \\ (u_{01}), & \text{где } u_{01} = 2, \text{ если } \nu_0 = 1, \end{cases}$$

и

$$\tilde{U}_0 = \begin{cases} (u_{01}^{\alpha_{01}}, u_{02}^{\alpha_{02}}), & \text{где } \alpha_{01} = 1, \alpha_{02} = \nu_0 - 2, \text{ если } \nu_0 \geq 2, \\ (u_{01}^{\alpha_{01}}), & \text{где } \alpha_{01} = 1, \text{ если } \nu_0 = 1, \end{cases}$$

а при четном d положим $U_0 = \tilde{U}_0 = \emptyset$. Заменяем двойные индексы в наборах $U = (U_0, U_1, \dots, U_m)$, $\tilde{U} = (\tilde{U}_0, \tilde{U}_1, \dots, \tilde{U}_m)$ номера от 1 до M :

$$U = (u_1, u_2, \dots, u_M), \quad \tilde{U} = (u_1^{\alpha_1}, u_2^{\alpha_2}, \dots, u_M^{\alpha_M}). \quad (42)$$

В этих обозначениях формулу (7) в Предложении 4 из § 1 можно записать в виде

$$\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) \cong \prod_{r=1}^M C_{u_r^{\alpha_r}}; \quad (43)$$

здесь $M = \begin{cases} s_1 + \dots + s_m & \text{при } \nu_0 = 0, \\ 1 + s_1 + \dots + s_m & \text{при } \nu_0 = 1, \text{ Далее, будем иметь в виду представление} \\ 2 + s_1 + \dots + s_m & \text{при } \nu_0 \geq 2. \end{cases}$

$\text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$ в виде (43).

Введем обозначения $H = \text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$, $H_r = C_{u_r^{\alpha_r}}$. Изоморфизм в формуле (43) означает соответствующее китайской теореме об остатках взаимно однозначное соответствие

$$z \Leftrightarrow (h_1, h_2, \dots, h_M),$$

где $z \in \text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$, а h_r (при каждом $r = 1, \dots, M$) — элемент кольца \mathbb{Z}_N , принадлежащий циклической подгруппе $C_{u_r^{\alpha_r}}$ группы \mathbb{Z}_N^* ; при этом $u_r^{\alpha_r}$ — примарная компонента разложения (41) для некоторого числа L_i , $i \in \{0, 1, \dots, m\}$. Ясно, что

$1 \Leftrightarrow (1, 1, \dots, 1)$. Так как $C_{u_r^{\alpha_r}} \cap C_{u_s^{\alpha_s}} = \{1\}$ при $1 \leq r < s \leq M$ и $1^d = 1$, то система $H_\pi = (C_{u_1^{\alpha_1}}, C_{u_2^{\alpha_2}}, \dots, C_{u_M^{\alpha_M}}; \pi_1, \dots, \pi_M)$, где подстановки π_r соответствуют отображениям $h \rightarrow h^d$, $h \in H_r$ ($r = 1, \dots, M$), удовлетворяет условиям (10) из § 2. Соответствующая подстановка $\pi = \pi_1 \times \dots \times \pi_M$ — это отображение $f^{(d)} : z \rightarrow z^d$ для любого $z \in \text{Ker}(f^{(d)}, \mathbb{Z}_N^*) = \mathbb{Z}_N^*(d)$. Поэтому можно использовать результаты § 2 для нахождения $\text{Str}(f^{(d)}, \mathbb{Z}_N^*) = \text{Str}(\pi, H) = \text{Str}(f^{(d)}, H_1 \times \dots \times H_M)$ по цикловым структурам $\text{Str}(f^{(d)}, C_{u_r^{\alpha_r}})$, $r = 1, \dots, M$, описанным в §§ 3–4. Если u_r нечетно, то согласно Предложению 7

$$\text{Str}(\pi_r, H_r) = \begin{cases} (1)(a_r)^{(u_r^{\alpha_r}-1)/a_r} \prod_{j=1}^{\alpha_r-\rho_r} (a_r u_r^j)^{(u_r-1)u_r^{\rho_r-1}/a_r}, & d \not\equiv 1 \pmod{u_r^{\alpha_r}}, \\ (1)u_r^{\alpha_r}, & d \equiv 1 \pmod{u_r^{\alpha_r}}, \end{cases} \quad (44)$$

где $a_r = \text{ord}(d, u_r)$, $\rho_r = \rho(d, u_r)$ — число из (17); если $\alpha_r = 1$ и, следовательно, $\rho_r = 1$, то все фрагменты в (44), кроме первых двух, отсутствуют.

Для упрощения формул будем обозначать величину $v(\bar{d}, \alpha_r)$ из (25) через v_r (\bar{d} — наименьший неотрицательный вычет d по модулю 2^{α_r}). Если $u_r = 2$, то при $\alpha_r \geq 3$ согласно Предложениям 9 и 10

$$\text{Str}(\pi_r, H_r) = \begin{cases} (1)^{2^{v_r}} (2)^{2^{v_r-1}} \prod_{j=v_r}^{\alpha_r-2} (2^{\alpha_r-j})^{2^{v_r-1}}, & d \equiv 1 \pmod{4}, \\ (1)^{2^{v_r}} (2)^{2^{v_r-1}} \prod_{j=v_r}^{\alpha_r-2} (2^{\alpha_r-j})^{2^{v_r-1}}, & d \not\equiv 1 \pmod{2^{\alpha_r}}, \\ (1)^{2^{\alpha_r}}, & d \equiv -1 \pmod{4}, \\ (1)^{2^{\alpha_r}}, & d \equiv 1 \pmod{2^{\alpha_r}}, \end{cases} \quad (45)$$

а при $\alpha_r = 1$ или 2, согласно Предложению 8, соответственно,

$$\text{Str}(\pi_r, H_r) = (1)^2 \text{ и } \text{Str}(\pi_r, H_r) = \begin{cases} (1)^4, & d \equiv 1 \pmod{4}, \\ (1)^2 (2), & d \equiv -1 \pmod{4}; \end{cases} \quad (46)$$

если же $v_r > \alpha_r - 2$, т. е. $v_r = \alpha_r - 1$, то все фрагменты в (45), помимо первых двух, отсутствуют.

Далее, каждое из множеств H_r , $r = 1, \dots, M$, разбивается на непересекающиеся подмножества H_{rj_r} так, что на H_{rj_r} подстановка π_r действует как какой-либо один фрагмент из структур в (44), (45) или (46). А именно, при $d \not\equiv 1 \pmod{u_r^{\alpha_r}}$:

$$\text{Str}(\pi_r, H_{rj_r}) = \begin{cases} (a_r u_r^{j_r})^{\frac{1}{a_r}(u_r-1)u_r^{\rho_r-1}}, & u_r \text{ нечётно}, 1 \leq j_r \leq \alpha_r - \rho_r, \\ (2^{j_r})^{2^{v_r-1}}, & u_r = 2, \alpha_r \geq 3, 2 \leq j_r \leq \alpha_r - v_r; \end{cases} \quad (47)$$

$$\begin{aligned} \text{Str}(\pi_r, H_{r,0}) &= (a_r)^{\frac{1}{a_r}(u_r^{\rho_r}-1)}, & u_r \text{ нечётно}, \\ \text{Str}(\pi_r, H_{r,1}) &= \begin{cases} (2)^{2^{v_r-1}}, & u_r = 2, \alpha_r \geq 3, d \equiv 1 \pmod{4}, \\ (2)^{2^{v_r-1}}, & u_r = 2, \alpha_r \geq 3, \\ (2), & u_r = 2, \alpha_r = 2, d \equiv -1 \pmod{4}; \end{cases} \end{aligned} \quad (48)$$

$$\text{Str}(\pi_r, H_{r,-1}) = \begin{cases} (1), & u_r \text{ нечётно}, \\ (1)^{2^{v_r}}, & u_r = 2, \alpha_r \geq 2, d \equiv 1 \pmod{4}, \\ (1)^2, & u_r = 2, \alpha_r \geq 2, d \equiv -1 \pmod{4}. \end{cases} \quad (49)$$

Кроме того, пусть $H_{r,-1} = C_{u_r^{\alpha_r}}$, если $d \equiv 1 \pmod{u_r^{d_r}}$.

Предложение 11. Пусть $d \geq 2$, $N \geq 2$ – любое натуральное число, представленное в виде (40), $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) \cong \prod_{r=1}^M C_{u_r^{\alpha_r}}$ – представление (43) для набора $U(d, N)$ простых чисел в (42). Пусть, далее, $a_r = \text{ord}(d, u_r)$, $\rho_r = \rho(d, u_r)$ – число в (17) и $v_r = v(\bar{d}, \alpha_r)$ – число в (25), где \bar{d} – наименьший неотрицательный вычет d по модулю 2^{α_r} .

а) Число n является длиной цикла в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$ тогда и только тогда, когда

$$n = \text{НОК}(l_1, l_2, \dots, l_M), \quad (50)$$

где $l_r \in \{1, a_r, a_r u_r, \dots, a_r u_r^{\alpha_r - \rho_r}\}$ при нечётном u_r , а если $u_r = 2$, то

$$l_r \in \begin{cases} \{1, 2, \dots, 2^{\alpha_r - v_r}\}, & \text{если } \alpha_r \geq 3, \\ \{1, 2\}, & \text{если } \alpha_r = 2, d \equiv -1 \pmod{4}, \end{cases}$$

и $l_r = 1$, если $u_2 = 2$ и при этом либо $\alpha_r = 2$, $d \equiv 1 \pmod{4}$, либо $\alpha_1 = \dots = \alpha_M = 1$.

б) Пусть n – число из (50). Тогда общее число циклов длины n в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$ равно

$$\frac{1}{n} \sum \prod_{r=1}^M b_r, \quad (51)$$

где $b_r = u_r^{\alpha_r}$ при $d \equiv 1 \pmod{u_r^{\alpha_r}}$, а если $d \not\equiv 1 \pmod{u_r^{\alpha_r}}$, то:

1) при нечётном u_r ,

$$b_r = \begin{cases} 1, & \text{если } l_r = 1, \\ u_r^{\rho_r} - 1, & \text{если } l_r = a_r, \\ (u_r - 1)u_r^{j_r + \rho_r - 1}, & \text{если } l_r = a_r u_r^{j_r}, 1 \leq j_r \leq \alpha_r - \rho_r; \end{cases}$$

2) при $u_r = 2$ и $d \equiv 1 \pmod{4}$

$$b_r = \begin{cases} 2^{v_r}, & \text{если } l_r = 1, \\ 2^{j_r + v_r - 1}, & \text{если } l_r = 2^{j_r}, 1 \leq j_r \leq \alpha_r - v_r; \end{cases}$$

3) при $u_r = 2$ и $d \equiv -1 \pmod{4}$

$$b_r = \begin{cases} 2, & \text{если } l_r = 1 \text{ или } l_r = 2, \alpha_r = 2, \\ 2(2^{v_r} - 1), & \text{если } l_r = 2, \alpha_r \geq 3, \\ 2^{j_r + v_r - 1}, & \text{если } l_r = 2^{j_r}, \alpha_r > 3, 2 \leq j_r \leq \alpha_r - v_r; \end{cases}$$

суммирование в (51) производится по всем возможным представлениям n в виде (50).

Доказательство. а) Исходя из набора $U(d, N)$ в (42), состоящего из простых чисел, не делящих d , и представления $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*) = H$ в виде прямого произведения (43), рассмотрим действие отображения $f^{(d)}$ на введённых выше множествах H_1, \dots, H_M , каждое из которых соответствует числу $u_r \in U(d, N)$. Положим при нечётном u_r

$$I_r = \begin{cases} \{-1\}, & \text{если } d \equiv 1 \pmod{u_r^{\alpha_r}}, \\ \{-1, 0, 1, \dots, \alpha_r - \rho_r\}, & \text{если } d \not\equiv 1 \pmod{u_r^{\alpha_r}}, u_r \text{ нечетно,} \end{cases}$$

а при $u_r = 2$

$$I_r^{(0)} = \begin{cases} \{-1\}, & \text{если } d \equiv 1 \pmod{u_r^{\alpha_r}}, \\ \{-1, 1, 2, \dots, \alpha_r - v_r\}, & \text{если } d \not\equiv 1 \pmod{u_r^{\alpha_r}}, u_r = 2, \alpha_r \geq 3, \\ \{-1, 1\}, & \text{если } d \not\equiv 1 \pmod{u_r^{\alpha_r}}, d \equiv -1 \pmod{4}, u_r = \alpha_r = 2. \end{cases}$$

Возьмём произвольно последовательность j_1, j_2, \dots, j_M , где $j_r \in I_r$, если u_r нечётно, и $j_r \in I_r^{(0)}$ при $u_r = 2$. Ей соответствует прямое произведение

$$H_{1j_1} \times H_{2j_2} \times \dots \times H_{Mj_M} \quad (52)$$

подмножеств множеств H_r , $r = 1, \dots, M$; как отмечено выше, на $H_1 \times \dots \times H_M$ и, следовательно, на (52), определена подстановка $\pi = \pi_1 \times \dots \times \pi_M$, где π_r — подстановка на H_r , индуцируемая отображением $f^{(d)}$. Цикловая структура для каждого H_{rj_r} в (52) состоит из одного фрагмента, поэтому, согласно Следствию 4, $\text{Str}(\pi, H_{1j_1} \times \dots \times H_{Mj_M})$ также состоит из одного фрагмента, и длина цикла в ней есть

$$n = \text{НОК}(l_1, l_2, \dots, l_M), \text{ где } l_r = \begin{cases} 1, & j_r = -1, \\ a_r u_r^{j_r}, & j_r \in I_r \setminus \{-1\}, u_r \text{ нечетное,} \\ 2^{j_r}, & j_r \in I_r \setminus \{-1\}, u_r = 2. \end{cases} \quad (53)$$

Отсюда следует, что l_r может принимать всего t_r различных значений, где при $d \not\equiv 1 \pmod{u_r^{\alpha_r}}$

$$t_r = \begin{cases} \alpha_r - \rho_r + 2, & \text{если } u_r \text{ нечетно,} \\ \alpha_r - v_r + 1, & \text{если } u_r = 2, \alpha_2 \geq 3, \\ 2, & \text{если } u_r = 2, \alpha_r = 2, d \equiv -1 \pmod{4}, \end{cases}$$

и $t_r = 1$ при $d \equiv 1 \pmod{u_r^{\alpha_r}}$.

Применяем теперь Следствие 4 к системе $H = (H_1, \dots, H_M; f^{(d)}, \dots, f^{(d)})$ и получаем, что множество всех длин циклов в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*) = \text{Str}(\pi, H)$ — это совокупность всех различных чисел вида (50), где каждое l_r пробегает все t_r значений, указанных в (53).

б) Пусть n — длина цикла в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$. Как показано в п. а), это означает, что существует вектор $\vec{j} = (j_1, \dots, j_M)$, где $j_r \in I_r$ или $I_r^{(0)}$, для которого справедливо (53):

$$n = \text{НОК}(l_1, \dots, l_M),$$

и $(l_r)^{k_r}$, $r = 1, \dots, M$, — фрагмент цикловой структуры $\text{Str}(\pi_r, H_r)$. Следовательно, согласно Следствию 4,

$$\star_{r=1}^M (l_r)^{k_r} = (n)^K,$$

где

$$K = K(\bar{j}) = \frac{k_1 \dots k_M l_1 \dots l_M}{\text{НОК}(l_1, \dots, l_M)} = \frac{k_1 l_1 \dots k_M l_M}{n}. \quad (54)$$

Найдём выражение для числителя этой дроби.

Предположим сначала, что $d \not\equiv 1 \pmod{u_r^{\alpha_r}}$. Тогда, если u_r нечётно, то $k_r l_r = 1$ при $l_r = 1$, а при $l_r \neq 1$

$$k_r l_r = \begin{cases} a_r u_r^{j_r} \cdot \frac{(u_r - 1) u_r^{\rho_r - 1}}{a_r} = (u_r - 1) u_r^{j_r + \rho_r - 1}, & \text{когда } 1 \leq j_r \leq \alpha_r - \rho_r, \\ a_r \cdot \frac{u_r^{\rho_r} - 1}{a_r} = u_r^{\rho_r} - 1, & \text{когда } j_r = 0. \end{cases}$$

Мы видим, что $k_r l_r = b_r$. Легко проверяется справедливость этого равенства также во всех случаях, когда $u_r = 2$, и при $d \equiv 1 \pmod{u_r^{\alpha_r}}$. Итак, $\prod_{r=1}^M k_r l_r = \prod_{r=1}^M b_r$ и, ввиду (54),

$$K = K(\bar{j}) = \frac{1}{n} \prod_{r=1}^M b_r. \quad (55)$$

Пусть $\bar{j}^{(1)}, \dots, \bar{j}^{(t)}$ — те и только те M -мерные векторы, которые приводят к представлению n в виде (53). Как мы уже убедились, каждое такое представление даёт K_i циклов длины n , где K_i — число в (55) — при значениях b_r , вычисляемых по координатам данного вектора $\bar{j}^{(i)}$, $i = 1, \dots, t$. Поэтому общее число циклов длины n равно

$$\sum_{i=1}^t K_i = \frac{1}{n} \sum_{i=1}^t \prod_{r=1}^M b_r,$$

где суммирование производится по всем возможным представлениям n в виде (53).

Предложение доказано.

Полученные результаты дают конкретный способ нахождения $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$ при любых d и N .

- 1) Для N в форме (40) находим набор простых чисел $U(d, N)$ из (42) и представление (43) для $\text{Ker}(f^{(d)}, \mathbb{Z}_N^*)$ в виде прямого произведения примарных циклических групп.
- 2) Для каждого $u_r \in U(d, N)$ находим числа $a_r = \text{ord}(d, u_r)$ и $\rho(d, u_r)$ из (17), если u_r нечётно, и $v_r(\bar{d}, \alpha_r)$ из (25) при $u_r = 2$, и получаем структуру $\text{Str}(f^{(d)}, C_{u_r^{\alpha_r}})$, используя формулу (18) или Предложения 8–10.
- 3) Берём по порядку все M -выборки фрагментов из $\text{Str}(f^{(d)}, C_{u_r^{\alpha_r}})$, $r = 1, \dots, M$, по одному из каждой структуры, и находим по формуле (50) для всех циклов в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$ их длины, а по формуле (55) — общее число циклов каждой длины n .

Отметим некоторые следствия полученных результатов. Укажем формулу для максимальной длины цикла степенного отображения.

Следствие 6. Пусть $d \geq 2$, $N \geq 2$ — произвольное натуральное число в форме (40), $U(d, N)$ — набор в (42), для которого построено прямое произведение (43), $U'(d, N)$ — набор из M' чисел, $0 \leq M' \leq M$, получающийся из $U(d, N)$ удалением всех u_r , для которых $d \equiv 1 \pmod{u_r^{\alpha_r}}$. Тогда, если $M' \neq 0$, то максимальная длина цикла в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$ есть

$$n_{\max} = \text{НОК}(\Lambda_1, \Lambda_2, \dots, \Lambda_{M'}), \quad (56)$$

где, для $u_r \in U'(d, N)$,

$$\Lambda_r = \begin{cases} a_r u_r^{\alpha_r - \rho_r}, & \text{если } u_r \text{ нечётно,} \\ 2^{\alpha_r - v_r}, & \text{если } u_r = 2, \alpha_r \geq 3, \\ 2, & \text{если } u_r = 2, \alpha_r = 2, d \equiv -1 \pmod{4}, \end{cases} \quad (57)$$

и $a_r = \text{ord}(d, u_r)$, $v_r = v(\bar{d}, \alpha_r)$ — число из (25), $\rho_r = \rho(d, u_r)$ — число из (17). Если $M' = 0$, то $n_{\max} = 1$.

Справедливость утверждения следует из Предложения 11, а также того факта (см. Предложения 7 и 10), что длина максимального цикла в $\text{Str}(f^{(d)}, C_{u_r^{\alpha_r}})$ делится на длины всех остальных циклов.

Приведем формулы для цикловых структур в нескольких частных случаях, представляющих интерес для приложений.

Следствие 7. Пусть d чётно, $N = p_1 \dots p_m$ — произведение t различных простых чисел, $U(d, N)$ — набор (42) из M простых чисел, по которому строится разложение (43). Предположим также, что

$$d \not\equiv 1 \pmod{u_r^{\alpha_r}} \quad \text{для любого } u_r \in U(d, N). \quad (58)$$

В этих условиях:

а) число n является длиной цикла в $\text{Str}(f^{(d)}, \mathbb{Z}_N^*)$ тогда и только тогда, когда

$$n = \text{НОК} \left(\left(a_1 u_1^{j_1} \right)^{\delta_1}, \left(a_2 u_2^{j_2} \right)^{\delta_2}, \dots, \left(a_M u_M^{j_M} \right)^{\delta_M} \right), \quad (59)$$

где $a_r = \text{ord}(d, u_r)$, $r = 1, \dots, M$, для некоторых M -мерных векторов $\bar{\delta} = (\delta_1, \dots, \delta_M) \in \{0, 1\}$ и $\bar{j} = (j_1, \dots, j_M)$, где $0 \leq j_r \leq \alpha_r - \rho_r$;

б) общее число циклов длины n равно

$$\frac{1}{n} \sum \prod_{r=1}^M b_r, \quad b_r = \begin{cases} 1, & \text{если } \delta_r = 0, \\ u_r^{\rho_r} - 1, & \text{если } j_r = 0, \delta_r = 1, \\ (u_r - 1) u_r^{j_r + \rho_r - 1}, & \text{если } j_r > 0, \delta_r = 1, \end{cases} \quad (60)$$

суммирование производится по всем возможным представлениям n в виде (59).

Действительно, ввиду чётности d , все числа u_r в (42) нечётные. Поэтому, согласно Предложению 7 (формула (18)), числа l_r в (50) принимают значения 1 или a_r , если $j_r = 0$, и значения $a_r u_r^{j_r}$, если $j_r > 0$; соответствующие фрагменты в $\text{Str}(\pi_r, H_r)$, $H_r = C_{u_r^{\alpha_r}}$ принимают значения (1), $(a_r)^{(u_r^{\rho_r} - 1)/a_r}$ или $(a_r u_r^{j_r})^{(u_r - 1)u_r^{\rho_r - 1}/a_r}$.

Ясно тогда, что равенство (50) равносильно (59), если $\delta_r = 0$ при тех и только тех r , при которых $l_r = 1$. Далее, ввиду условия (58) и чётности d , число b_r может принимать только значения 1, $u_r^{\rho_r} - 1$ или $(u_r - 1)u_r^{j_r + \rho_r - 1}$, $j_r = 1, \dots, \alpha_r - \rho_r$. Следовательно, справедливо также утверждение об общем числе циклов длины n .

Дважды простым называется такое простое число p , что $q = \frac{1}{2}(p - 1)$ — также простое.

Следствие 8. Пусть выполнены условия Следствия 7, все числа p_1, \dots, p_m — дважды простые и $U(d, N) = (q_1, q_2, \dots, q_M)$, где $q_r = \frac{1}{2}(p_r - 1)$, $q_r \nmid d$, $r = 1, \dots, M$. Тогда цикловая структура $\text{Str}(d, \mathbb{Z}_N^*)$ описывается следующим образом.

а) Число n является длиной цикла в том и только том случае, когда

$$n = \text{НОК}\left(a_1^{\delta_1}, a_2^{\delta_2}, \dots, a_M^{\delta_M}\right), \quad (61)$$

где $a_r = \text{ord}(d, q_r)$ для $q_r \in U(d, N)$, $\bar{\delta} = (\delta_1, \dots, \delta_M) \in \{0, 1\}^M$.

б) Если n можно представить в виде (61) в точности при t различных векторах $\bar{\delta}^{(1)}, \dots, \bar{\delta}^{(t)}$, а $R_1^{(i)}$ — совокупность всех тех $r \in \{1, \dots, M\}$, для которых $\delta_r^{(i)} = 1$ в $\bar{\delta}^{(i)} = (\delta_1^{(i)}, \dots, \delta_M^{(i)})$. Тогда общее число циклов длины n равно

$$\frac{1}{n} \sum_{i=1}^t \prod_{r \in R_1^{(i)}} (q_r - 1).$$

в) Максимальная длина цикла равна $n_{\max} = \text{НОК}(a_1, a_2, \dots, a_M)$.

Справедливость утверждения устанавливаем, учитывая соотношения (56)–(60).

Список литературы

1. Борович З. И., Шафаревич И. Р., *Теория чисел*. Наука, Москва, 1964.
2. Brands S., Gill R., Cryptography, statistics and pseudorandomness. I. *Probab. Math. Statist.* (1995) **15**, 101–114.
3. Brands S., Gill R., Cryptography, statistics and pseudorandomness. II. *Probab. Math. Statist.* (1996) **16**, №1, 1–17.
4. Brennan J. J., Geist B., Analysis of iterated modular exponentiation: the orbits of $x^a \pmod N$. *Des., Codes and Cryptography* (1998) **13**, 229–245.
5. Chou W.-S., Shparlinski I. E., On the cycle structure of repeated exponentiation modulo a prime. *J. Number Theory* (2004) **107**, 345–356.
6. Виноградов И. М., *Основы теории чисел*. Наука, Москва, 1981.
7. Ленг С., *Алгебра*. Мир, Москва, 1968.

8. El-Mahassni E. D., On the distribution of the power generator over a residue ring for parts of the period. *Rev. Mat. Comput.* (2008) **21**, 319–325.
9. Холл М., *Теория групп*. ИЛ, Москва, 1962.
10. Sha Min, On the cycle structure of repeated exponentiation modulo a prime power. *arXiv:1101.3482v1[math.NT]* 8 Jan 2011.
11. Vasiga T., Shallit J., On the iteration of certain quadratic maps over $\text{GF}(p)$. *Discrete Math.* (2004) **277**, 219–240.
12. Wilson B., Power digraphs modulo n . *Fibonacci Quart.* (1998) **36**, 229–239.

Статья поступила 01.08.2012.