ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 31 № 1 2025

УДК 512.577

ПРЕДСТАВЛЕНИЯ УНАРОВ МНОЖЕСТВОМ ВЫЧЕТОВ[1]

И. Б. Кожухов, В. А. Лецко

В работе найдены точные представления конечного унара (алгебры с одной унарной операцией на конечном носителе) в некоторых стандартных конструкциях. Доказано, что всякий конечный унар может быть точно представлен остатками от деления на n с унарной операцией $f(x) = x \cdot a \mod n$ при подходящих a и n. Кроме того, для каждого натурального $d \geq 2$ существует точное представление любого конечного унара остатками от деления на n с унарной операцией $f(x) = x^d \mod n$ при подходящем n. Далее, для любого $d \geq 3$ всякий конечный унар может быть точно представлен обратимыми остатками от деления на n с операцией $f(x) = x^d \mod n$ при подходящем n (при $d = 2$ данное утверждение неверно).

Ключевые слова: представление унара.

I. B. Kozhukhov, V. A. Letsko. Representation of unars by sets of residues.

We find faithful representations of a finite unar (an algebra with one unary operation on a finite set) in some standard constructions. We prove that every finite unar can be faithfully represented by the residues modulo n with the operation $f(x) = x \cdot a \mod n$ for suitable n and a. Besides, for every integer $d \geq 2$, there exists a faithful representation of every finite unar by residues modulo n with the operation $f(x) = x^d \mod n$ for suitable n. Further, for any $d \geq 3$, every finite unar can be faithfully presented by invertible residues modulo n with the operation $f(x) = x^d \mod n$ for suitable n. (The later assertion is not true for $d = 2$).

Keywords: representations of unar.

MSC: 20M30

DOI: 10.21538/0134-4889-2025-31-1-77-89

Введение

Многие алгебраические системы имеют представления объектами некоторого специального вида, например, группы — подстановками, кольца — матрицами и т. д. Гомоморфизм алгебры в какую-либо алгебру из некоторого класса $\mathcal{K}$ называется *представлением данной алгебры в классе* $\mathcal{K}$, а если этот гомоморфизм инъективный, то он называется *точным представлением*. Широко известны теорема Кэли [1, теорема 13.1.1]: *всякая конечная группа изоморфно вкладывается в группу подстановок* — и ее обобщение [1, утверждение 13.1.3]: *любая группа вкладывается в группу взаимно однозначных преобразований некоторого множества* (*группу обобщенных подстановок*). Известен также полугрупповой вариант теоремы Кэли [2, лемма 1.0]: *всякая полугруппа вкладывается в полугруппу преобразований множества* (*необязательно взаимно однозначных*). Линейные представления групп, полугрупп и ассоциативных алгебр [3; 4], т. е. представления линейными операторами, — это целое направление общей алгебры. Глава 11 монографии [2] целиком посвящена представлениям полугрупп различными преобразованиями множеств. В теории решеток установлено наличие точного представления любой решетки отношениями эквивалентности на множестве, а также подгруппами группы, т. е. любая решетка изоморфно вкладывается в решетку отношений эквивалентности на некотором множестве [5, теорема 1] и в решетку подгрупп некоторой группы [5, теорема 2].

Унар (в другой терминологии — моноунарная алгебра) — это алгебра с одной унарной операцией, т. е. множество U с заданным отображением $f : U \to U$. Унар можно рассматривать как полигон над бесконечной циклической полугруппой $S = \{t, t^2, t^3, \ldots\}$ (см. [6, п. 3.4]) или

[1]Работа выполнена при финансовой поддержке Российского научного фонда (проект № 22-11-00052).

как автомат Мура с однобуквенным входным алфавитом. Интересующие нас конечные унары также рассматривают как динамические системы или функциональные графы.

Для произвольной полугруппы S и элемента $a \in S$ можно рассмотреть унар $(S, *a)$, т. е. S с унарной операцией $f(x) = xa$ для $x \in S$. В работе [7] были получены необходимые и достаточные условия на унар U, чтобы он был изоморфен унару $(S, *a)$ при некоторых S и a.

Для натуральных чисел $n, a, d \geq 2$ пусть $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ — множество остатков от деления целых чисел на n, а $(\mathbb{Z}_n, *a)$ и $(\mathbb{Z}_n, ^\wedge d)$ — унары с операциями $f(x) = xa$ и $f(x) = x^d$ соответственно, где умножение и возведение в степень осуществляются по модулю n.

В ряде работ исследовались количественные характеристики унаров $(\mathbb{Z}_n, ^\wedge d)$. Так, например, в работах [8;9] для этих унаров определялись длины циклов, количества циклов заданной длины и деревья с корнем в вершине, принадлежащей циклу, в статье [10] для них находились асимптотические формулы количества периодических (циклических) вершин и высот деревьев с корнем в цикле. Интерес к унарам $(\mathbb{Z}_n, ^\wedge d)$ во многом обусловлен возможностями применения конструкции возведения в фиксированную степень по модулю натурального числа к генерированию псевдослучайных последовательностей (см., например, [11–13]).

Интересно отметить, что множество $\mathbb{Z}_n$ использовалось для представления полугрупп, а именно в [14] были получены необходимые и достаточные условия вложимости конечной коммутативной полугруппы в полугруппу $(\mathbb{Z}_n, *)$ при подходящем n.

Целью данного исследования является нахождение точных представлений конечных унаров.

Основные результаты работы следующие.

1. Любой конечный унар U изоморфно вкладывается в унар вида $(\mathbb{Z}_n, *a)$ при подходящих n и a.

2. Для любого $d \geq 2$ и любого конечного унара U существует изоморфное вложение U в унар вида $(\mathbb{Z}_n, ^\wedge d)$ при подходящем n.

3. Для любого $d \geq 3$ любой конечный унар U изоморфно вкладывается в унар вида $(\mathbb{Z}_n^*, ^\wedge d)$ при подходящем n.

При этом в утверждениях 1 и 2 число n может быть выбрано сколь угодно большим, в утверждении 3 число n может быть выбрано в виде $n = p_1 p_2 \ldots p_k$, где $p_1, \ldots, p_k$ — различные простые числа, также сколь угодно большие. Утверждение 3 перестает быть верным при $d = 2$.

Набросок доказательства утверждения 1 впервые был опубликован в [15]. Здесь же мы приводим полное его доказательство.

1. Основные определения и обозначения

Пусть (U, f) — унар. Для $x \in U$ полагаем $f^0(x) = x$, $f^1(x) = f(x)$ и $f^{n+1}(x) = f(f^n(x))$ при $n \geq 1$. Унар U можно считать ориентированным графом с вершинами — элементами множества U и ребрами $(x, f(x))$ для $x \in U$. Цикл из k элементов будем обозначать через C_k. Элемент x называется циклическим, если $f^k(x) = x$ при некотором $k \geq 1$ (или, что эквивалентно, это элемент, лежащий в каком-нибудь цикле). Через $\langle x \rangle$ обозначим подунар, порожденный элементом x, т. е. $\langle x \rangle = \{f^n(x) | n \geq 0\}$. Пусть $x \in U$ таков, что $\langle x \rangle$ — конечное множество. Тогда найдутся такие $h \geq 0$ и $t > 0$, что $f^{h+t}(x) = f^h(x)$. Если h и t — наименьшие числа с этим свойством, то они называются соответственно *глубиной* $h(x)$ и *периодом* $p(x)$ элемента x. Ясно, что в конечном унаре каждый элемент имеет глубину и период. *Степень* $\deg x$ элемента x унара — это мощность полного прообраза: $\deg x = |f^{-1}(x)|$. Элемент степени 0 назовем минимальным. Минимальных элементов может и не быть.

Для конечного унара U полагаем $h(U) = \max\{h(x) | x \in U\}$, $d(U) = \max\{\deg x | x \in U\}$.

Тривиально проверяется, что бинарное отношение, заданное по правилу

$$x \sim y \leftrightarrow \exists s, t \quad f^s(x) = f^t(y),$$

является отношением эквивалентности на множестве U. Также ясно, что классы эквивалентности данного отношения являются *компонентами связности* графа, соответствующего унару U. Очевидно, каждая компонента связности конечного унара содержит ровно один цикл. Унар называется *связным*, если его граф связен.

Очевидно, всякий конечный связный унар имеет единственный цикл. Если C_k — цикл в конечном связном унаре U, то полагаем $c(U) = k$.

Если унар U является объединением своих попарно непересекающихся подунаров U_i ($i \in I$), то будем говорить, что U есть *копроизведение* (в другой терминологии — прямая сумма) унаров U_i, и писать $U = \coprod_{i\in I} U_i$. Ясно, что любой унар — это копроизведение своих компонент связности.

Безусловно, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ является кольцом относительно операций сложения и умножения по модулю n. Однако на элементы множества $\mathbb{Z}_n$ можно смотреть как на обычные целые числа, что мы и будем делать в вопросах, связанных с делимостью, разложением на множители и т. д. В настоящей работе через $\mathbb{Z}_n^*$ обозначим мультипликативную группу кольца вычетов $\mathbb{Z}_n$. Она состоит в точности из элементов кольца $\mathbb{Z}_n$, имеющих обратный элемент по умножению или, что эквивалентно, взаимно простых с n.

Порядок элемента a в группе G мы будем обозначать через $o(a)$. Если a и n — натуральные числа такие, что $(n, a) = 1$, то $\mathrm{ord}_n(a)$ обозначает наименьшее натуральное k, при котором $a^k \equiv 1 \mod n$ (т. е. $\mathrm{ord}_n(a) = o(a)$ в группе $\mathbb{Z}_n^*$).

Всюду в работе (a, b) — *наибольший общий делитель* чисел a и b. Далее $a \vdots b$ и $c \mid d$ обозначают соответственно "a делится на b" и "c делит d". Буква φ обозначает всюду *функцию Эйлера*.

2. Универсальный унар

Конечный связный унар X назовем *универсальным* и обозначим его как $U(k, m, r)$, если выполнены следующие условия:

1) $c(X) = k$;

2) $h(X) = r$;

3) $\deg x = m$ для любого элемента x такого, что $h(x) < r$.

Ясно, что $m = 1$ равносильно $r = 0$, а унар $U(k, 1, 0)$ будет в этом случае циклом длины k. Поэтому мы сосредоточим внимание на случае $k \geq 1$, $m \geq 2$, $r \geq 1$. Очевидно, что для такого набора параметров существует единственный с точностью до изоморфизма универсальный унар $U(k, m, r)$.

Приведем простую числовую реализацию универсального унара. А именно, унар $U(k, m, r)$ может быть рассмотрен как множество строк

$$X = \{(i_0, i_1, \ldots, i_t) | i_0 \in \mathbb{Z}_k;\ t \leq r;\ i_1, \ldots, i_t \in \{0, 1, \ldots, m-1\};\ i_1 \neq 0\}$$

с операцией

$$f((i_0, i_1, \ldots, i_t)) = \begin{cases} (i_0, i_1, \ldots, i_{t-1}), & \text{если } t \geq 1, \\ (i_0 + 1 \pmod k), & \text{если } t = 0. \end{cases}$$

На рис. 1 изображен граф, являющийся одной из компонент связности унара $(\mathbb{Z}_{40}, *2)$. Он является универсальным унаром $U(4, 2, 3)$. Если вершины цикла 8, 16, 32, 24 обозначить соответственно как 0, 1, 2, 3, то согласно нумерации элементов универсального унара будем иметь, например, такие равенства: $24 = (3)$, $12 = (3, 1)$, $6 = (3, 1, 0)$, $26 = (3, 1, 1)$, $13 = (3, 1, 1, 0)$.

Следующее утверждение очевидно, поэтому его доказательство мы не приводим.

Теорема 1. *Конечный связный унар X, у которого $c(X) = k$, $d(X) = m$, $h(X) = r$, изоморфно вкладывается в универсальный унар $U(k, m, r)$.*

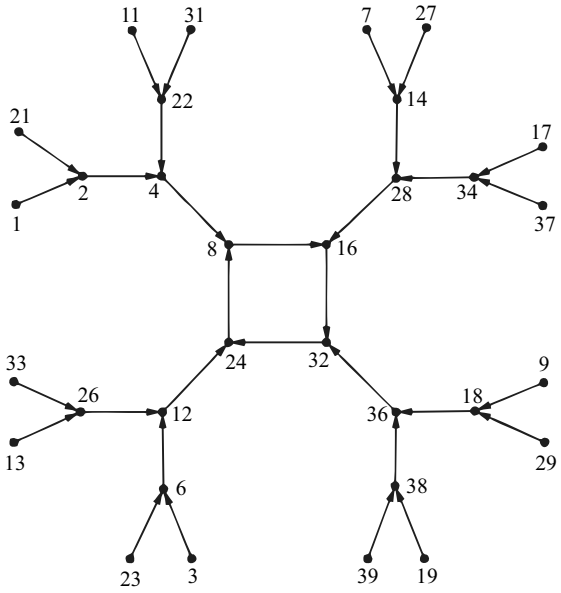

Рис. 1. Универсальный унар

3. Вложение конечного унара в унар $(\mathbb{Z}_n, *a)$

Для описания характеристик унара $(\mathbb{Z}_n, *a)$ введем некоторые обозначения. Пусть $d = (n, a)$ и $b \in \mathbb{Z}_n \setminus \{0\}$. Разложим d на простые множители:

$$d = \prod_{i=1}^{s} p_i^{\delta_i} \tag{1}$$

(здесь p_i — различные простые числа и все $\delta_i > 0$). Тогда будем иметь

$$a = a_0 \prod_{i=1}^{s} p_i^{\alpha_i}, \quad n = n_0 \prod_{i=1}^{s} p_i^{\nu_i}, \quad b = b_0 \prod_{i=1}^{s} p_i^{\beta_i}, \tag{2}$$

где

$$(n_0, d) = (a_0, d) = (b_0, d) = 1. \tag{3}$$

Положим далее

$$b_1 = \frac{b_0}{(n_0, b_0)}, \quad n_1 = \frac{n_0}{(n_0, b_0)}.$$

Приведем ряд лемм, проясняющих строение унара $(\mathbb{Z}_n, *a)$.

Лемма 1. *Каждый ненулевой элемент унара $\mathbb{Z}_n$ либо минимален, либо имеет степень $d = (n, a)$. То есть если $b \in \mathbb{Z}_n \setminus \{0\}$, то*

$$\deg b = \begin{cases} d & \text{при } d \,|\, b, \\ 0 & \text{в противном случае.} \end{cases}$$

Доказательство. Степень вершины b равна количеству решений в $\mathbb{Z}_n$ сравнения $ax \equiv b \pmod n$, а это сравнение не имеет решений при $d \not| b$ и имеет ровно d решений при $d \,|\, b$. □

Лемма 2. $(\mathbb{Z}_n, *a)$ *является объединением циклов тогда и только тогда, когда* $(n, a) = 1$.

Доказательство. Из предыдущей леммы следует, что при $d = 1$ у каждого элемента ровно один прообраз. В случае конечного унара это условие равносильно тому, что он является объединением циклов. □

Лемма 3. *Глубина элемента $b \in \mathbb{Z}_n \setminus \{0\}$ равна наименьшему целому неотрицательному h такому, что $\beta_i + h\alpha_i \geq \nu_i$ при всех $i = 1, 2, \ldots, s$. В частности, элемент b является циклическим тогда и только тогда, когда $\beta_i \geq \nu_i$ при всех $i = 1, 2, \ldots, s$.*

Доказательство. Пусть для некоторого i имеет место неравенство $\beta_i + h\alpha_i < \nu_i$. Тогда сравнение $ba^{h+t} \equiv ba^h \pmod{n}$ не может выполняться ни при каком $t \geq 1$, поскольку после деления обеих частей и модуля на $p_i^{\beta_i + h\alpha_i}$ левая часть и модуль будут делиться на p_i, а правая — нет.

Пусть теперь $\beta_i + h\alpha_i \geq \nu_i$ при всех i. Так как $(n_0, a) = 1$ и $n_1 \mid n_0$, то также $(n_1, a) = 1$. По теореме Эйлера мы получаем, что $a^t \equiv 1 \pmod{n_1}$ при некотором $t > 0$. Умножив на $b_1 \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i}$, получим

$$a^t b_1 \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i} \equiv b_1 \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i} \pmod{n_1}.$$

Теперь умножим обе части сравнения и модуль на (n_0, b_0):

$$a^t b_0 \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i} \equiv b_0 \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i} \pmod{n_0}.$$

Затем умножим обе части сравнения и модуль на $\prod_{i=1}^{s} p_i^{\nu_i}$, имеем

$$a^t b \prod_{i=1}^{s} p_i^{h\alpha_i} \equiv b \prod_{i=1}^{s} p_i^{h\alpha_i} \pmod{n}.$$

Наконец, умножив на a_0^h, приходим к $a^t ba^h \equiv ba^h \pmod{n}$. То есть $ba^{h+t} \equiv ba^h \pmod{n}$. Это означает, что элемент ba^h принадлежит циклу. □

Лемма 4. *Период элемента $b \in \mathbb{Z}_n \setminus \{0\}$ равен $\operatorname{ord}_{n_1} a$.*

Доказательство. Период элемента b равен наименьшему положительному t такому, что $ba^{h+t} \equiv ba^h \pmod{n}$ при некотором h, для которого элемент ba^h является циклическим. Воспользовавшись соотношениями (1) и (2) и разделив обе части сравнения и модуль на n/n_0, получим

$$b_0 a_0^h a^t \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i} \equiv b_0 a_0^h \prod_{i=1}^{s} p_i^{\beta_i + h\alpha_i - \nu_i} \pmod{n_0}.$$

Так как $(a_0, n_0) = (n_0, p_i) = 1$ для всех i, то сравнения по модулю n_0 можно сокращать на a_0 и p_i. Поэтому мы получим $b_0 a^t \equiv b_0 \pmod{p}$. Разделив обе части сравнения и модуль на (b_0, n_0), имеем $a^t \equiv b_1 \pmod{n_1}$, где $b_1 = b_0/(b_0, n_0)$. Наконец, разделив обе части сравнения на b_1 (это можно сделать, так как n_1 и b_1 взаимно просты), получим $a^t \equiv 1 \pmod{n_1}$. Наименьшее натуральное t, удовлетворяющее этому сравнению, по определению равно порядку числа a по модулю n_1. □

Лемма 5. *При $n = a^h n_0$ каждая компонента связности унара $(\mathbb{Z}_n, *a)$ изоморфна унару $U(t, a, h)$, где $t = \operatorname{ord}_c a$ для некоторого $c \mid n_0$.*

Доказательство. То, что степень каждого элемента, не являющегося минимальным, равна a, следует из леммы 1. Далее, из лемм 3 и 1 вытекает, что минимальные элементы каждой компоненты имеют глубину h. Наконец, из леммы 4 определяем, что возможные длины циклов каждой из компонент связности, не содержащей 0, являются порядками числа a по модулям делителей числа n_0. □

Теорема 2. *Любой конечный унар изоморфно вкладывается в унар* $(\mathbb{Z}_n, *a)$ *при подходящих* n, a.

Доказательство. Положим $H = h(U)$ и $D = d(U)$, и пусть $U = K_1 \cup \ldots \cup K_m$ — разложение унара U на компоненты связности. Так как унар U конечный, то каждая компонента K_i содержит единственный цикл; обозначим его через C_i. Пусть $|C_i| = t_i$ для $i = 1, \ldots, m$.

Возьмем $i = 1$ и рассмотрим арифметическую прогрессию $S_1 = \{1 + t_1, 1 + 2t_1, 1 + 3t_1, \ldots\}$. По теореме Дирихле о простых числах в арифметической прогрессии [16, гл. V, § 3, теорема 3] в последовательности S_1 бесконечно много простых чисел. Выберем какое-либо простое число $q_1 \in S_1$. Предположим, что простые числа $q_1 < \ldots < q_{j-1}$ уже выбраны и $j \leq m$. Применяя упоминавшуюся теорему Дирихле к арифметической прогрессии $S_j = \{1+t_j, 1+2t_j, 1+3t_j, \ldots\}$, найдем простое число $q_j \in S_j$ такое, что $q_j > q_{j-1}$. Соответственно, будут взяты простые числа $q_1 < \ldots < q_m$ такие, что $q_i = 1 + w_i t_i$ при некоторых $w_i \in \mathbb{Z}$ $(i = 1, \ldots, m)$.

Для каждого $i \leq m$ выберем числа a_i и g_i следующим образом. Так как число q_i простое, то группа $\mathbb{Z}_{q_i}^*$ циклическая. Пусть g_i — какой-либо образующий элемент этой группы (мы рассматриваем его просто как целое число). Очевидно, $o(g_i) = q_i - 1$. Положим $a_i = g_i^{w_i}$. Так как $w_i \,|\, q_i - 1$, то $o(a_i) = o(g_i)/w_i = (q_i - 1)/w_i = t_i$.

Положим $n_0 = q_1 \ldots q_m$. Согласно Китайской теореме об остатках существует натуральное число a такое, что $a \equiv a_i \pmod{q_i}$ при $i = 1, \ldots, m$. Поскольку решений у этой системы сравнений бесконечно много, то выберем решение a так, чтобы было выполнено неравенство $a \geq D$. Положим $n = a^H n_0$. Таким образом, нами выбраны параметры n и a.

Для $i = 1, 2, \ldots, m$ положим $b_i = n_0/q_i = q_1 \ldots q_{i-1} q_{i+1} \ldots q_m$ и $x_i = a^H b_i$. Докажем, что множество $A_i = \{x_i, x_i a, \ldots, x_i a^{t_i - 1}\}$ — цикл длины t_i в унаре $(\mathbb{Z}_n, *a)$. Так как $o(a_i) = t_i$ и $a \equiv a_i \pmod{q_i}$, то $a^{t_i} \equiv a_i^{t_i} \equiv 1 \pmod{q_i}$. Следовательно, $a^{t_i} - 1 \vdots q_i$. Поэтому $x_i(a^{t_i} - 1) = a^H b_i (a^{t_i} - 1) \vdots a^H (n_0/q_i)\, q_i$, т. е. $x_i(a^{t_i} - 1) = 0$ в $\mathbb{Z}_n$. Значит, x_i — циклический элемент унара $(\mathbb{Z}_n, *a)$. Убедимся, что элементы $x_i, x_i a, \ldots, x_i a^{t_i - 1}$ различны. Поскольку $x_i a^{t_i} = x$, нам достаточно доказать, что $x_i a^k \neq x$ при $1 \leq k < t_i$. Пусть $x_i a^k = x_i$ в $\mathbb{Z}_n$. Тогда $x_i(a^k - 1) \vdots n$. Следовательно, $a^H q_1 \ldots q_{i-1} q_{i+1} \ldots q_m (a^k - 1) \vdots n$. Это означает, что $a^k - 1 \vdots q_i$. Но $\operatorname{ord}_{q_i} a = t_i$, отсюда $k \geq t_i$. Итак, A_i — цикл длины t_i для $i = 1, \ldots, m$. Докажем, что $A_i \cap A_j = \varnothing$ при $i \neq j$. Действительно, если $A_i \cap A_j \neq \varnothing$, то $A_i = A_j$, а значит, $x_i - x_j a^k \vdots n$. Но это невозможно, так как $x_j a^k$ делится на q_i, а x_i взаимно просто с q_i.

Пусть K_i — компонента связности унара $(\mathbb{Z}_n, *a)$, содержащая цикл A_i. Поскольку циклы A_i попарно не пересекаются, то также $K_i \cap K_j = \varnothing$ при $i \neq j$. По лемме 5 $K_i \equiv U(t_i, a, H)$. Ввиду того что $a \geq D$, требуемое вложение унара U в унар $(\mathbb{Z}_n, *a)$ теперь следует из теоремы 1. □

Наше доказательство позволяет конструктивно находить нужные a, n для любого наперед заданного конечного унара. Более того, из доказательства следует, что для любого конечного унара существует бесконечно много представлений классами вычетов по модулю. Поиск минимального n для точного представления данного конечного унара в общем случае является достаточно сложной задачей. На конкретных примерах этот вопрос рассматривался в [17, гл. 3.5]. В компьютерных экспериментах по поиску минимального n принимала участие Ю. В. Ишанкулова, бывшая в то время ученицей средней школы.

Естественно возникает вопрос: существует ли одно число a такое, что любой конечный унар вкладывается в унар $(\mathbb{Z}_n, *a)$ при подходящем n? Ответ на этот вопрос отрицательный, как покажут следующие ниже примеры. Они основаны на элементарных фактах: 1) однородное уравнение $kx = 0$ имеет ровно (n, k) решений в группе $(\mathbb{Z}_n, +)$; 2) неоднородное уравнение $kx = b$ либо не имеет решений, либо также имеет ровно (n, k) решений.

Пример 1. Возьмем унар U, состоящий из a нулей (неподвижных элементов), т. е. $U = \{x_1, x_2, \ldots, x_a\}$, где $f(x_i) = x_i$ при $i = 1, 2, \ldots, a$. Если бы он вкладывался в унар $(\mathbb{Z}_n, *a)$,

то тогда было бы $f(x) = ax$, и уравнение $(a-1)x = 0$ имело бы не менее a различных решений, что невозможно.

Приведем теперь пример, показывающий, что не существует такого a, что всякий связный унар вкладывается в унар $(\mathbb{Z}_n, *a)$ при подходящем n.

П р и м е р 2. Пусть $U = \{x_1, x_2, \ldots, x_a, y\}$, где $f(x_i) = f(y) = y$ при $i = 1, 2, \ldots, a$. Если бы он вкладывался в унар $(\mathbb{Z}_n, *a)$, то уравнение $ax = y$ имело бы не менее $a + 1$ различных решений, что невозможно.

4. Вложение конечного унара в унар $(\mathbb{Z}_n, {}^\wedge d)$

Доказательству второго основного результата работы предпошлем серию лемм. Первая лемма этой серии является хорошо известным утверждением для аддитивных групп и колец и легко проверяется для полугрупп, поэтому доказательство его мы не приводим.

Лемма 6. *Пусть $n_1, \ldots n_s$ — натуральные числа такие, что $(n_i, n_j) = 1$ при $i \neq j$. Тогда отображение $\theta : \mathbb{Z}_{n_1 \ldots n_s} \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$, где $\theta(x) = (x \mod n_1, \ldots, x \mod n_s)$ является изоморфизмом колец,* (аддитивных) абелевых групп, а также мультипликативных полугрупп. Кроме того, изоморфизм θ индуцирует изоморфизм групп

$$\mathbb{Z}^*_{n_1 \ldots n_s} \cong \mathbb{Z}^*_{n_1} \times \ldots \times \mathbb{Z}^*_{n_s}.$$

Лемма 7. *Пусть $d, k_1, \ldots, k_t$ — натуральные числа и $d \geq 2$. Тогда для любого натурального l существуют различные простые числа $p_1, \ldots, p_t \geq l$ и элементы $x_1 \in \mathbb{Z}^*_{p_1}$, ... , $x_t \in \mathbb{Z}^*_{p_t}$ такие, что $o(x_i) = d^{k_i} - 1$ при $i = 1, \ldots, t$.*

Д о к а з а т е л ь с т в о. По теореме Дирихле о простых числах в арифметических прогрессиях множество $A = \{1 + (d^{k_1} - 1)t | t \in \mathbb{N}\}$ содержит бесконечно много простых чисел. Выберем простое число $p_1 \in A$ такое, что $p_1 \geq l$. Имеем $p_1 = 1 + (d^{k_1} - 1)t$ при некотором $t \in \mathbb{N}$. Пусть θ — образующий элемент группы $\mathbb{Z}^*_{p_1}$. Тогда $o(\theta) = p_1 - 1$, а поскольку $p_1 - 1 = (d^{k_1} - 1)t$, то $o(\theta^t) = d^{k_1} - 1$, поэтому можно положить $x_1 = \theta^t$. Пусть уже выбраны простые числа $p_1, \ldots, p_j$ и элементы $x_1 \in \mathbb{Z}^*_{p_1}, \ldots, x_j \in \mathbb{Z}^*_{p_j}$ такие, что $l \leq p_1 < p_2 < \ldots < p_j$ и $o(x_i) = d^{k_i} - 1$ при $i = 1, \ldots, t$. Если $j < t$, то выберем p_{j+1} и x_{j+1} следующим образом. Используя вышеупомянутую теорему Дирихле, найдем простое число $p_{j+1} > p_j$ такое, что $(p_{j+1} - 1) \vdots (d^{k_{j+1}} - 1)$. В этом случае $p_{j+1} - 1 = (d^{k_{j+1}} - 1)s$ при некотором $s \in \mathbb{N}$. Осталось взять $x_{j+1} = \omega^s$, где ω — образующий элемент группы $\mathbb{Z}^*_{p_{j+1}}$. □

Лемма 8. *Для любых натуральных чисел l, r и d, где $d \geq 2$, существует простое число p такое, что $p \geq l$ и в группе $\mathbb{Z}^*_p$ найдутся элементы $a_1, a_2, \ldots, a_{\varphi(d^r)}$ такие, что подунар унара $(\mathbb{Z}^*_p, {}^\wedge d)$, порожденный этими элементами, изоморфен унару $U(1, d, r)$.*

Д о к а з а т е л ь с т в о. Выберем простое число p так, чтобы $p \geq l$ и $p - 1 \vdots d^r$ (это можно сделать ввиду теоремы Дирихле об арифметических прогрессиях). Имеем $p = 1 + d^r s$, где $s \in \mathbb{N}$. Подгруппа $\{x^s | x \in \mathbb{Z}^*_p\}$ группы $\mathbb{Z}^*_p$ — циклическая группа порядка d^r. В ней ровно $\varphi(d^r)$ элементов порядка d^r. Обозначим эти элементы как $a_1, a_2, \ldots, a_{\varphi(d^r)}$. Очевидно, унар, состоящий из элементов $(a_i)^{d^j}$, с операцией возведения в степень d изоморфен унару $U(1, d, r)$. □

На рис. 2 изображен унар, построенный в лемме 8, где взято $d = 2$.

Пусть U — унар и $x, y \in U$. Элемент x будем называть *предшественником* элемента y, если $f(x) = y$.

Унар $\underbrace{U \times \ldots \times U}_{n}$ будем обозначать как U^n.

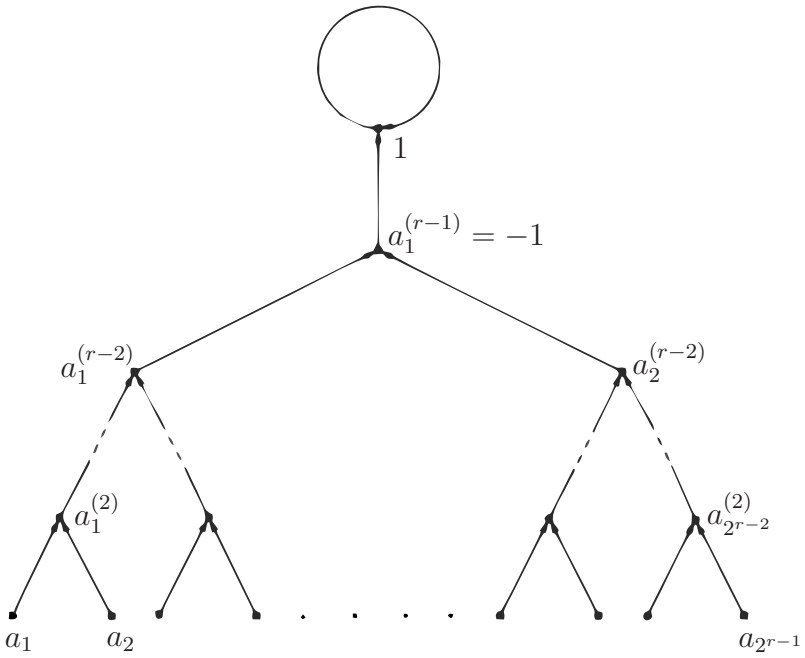

Рис. 2

Лемма 9. *Если $m \le n^t - 1$, то унар $U(1,m,r)$ изоморфно вкладывается в унар $U(1,n,r)^t$.*

Доказательство. Пусть z — нуль (неподвижный элемент) унара $U(1,n,r)$. Тогда $z' = \underbrace{(z,z,\ldots,z)}_{t}$ — нуль унара $U(1,n,r)^t$. Поскольку $\deg z = n$ и $f(z) = z$, то $f^{-1}(z) = \{z, u_1, \ldots, u_{n-1}\}$. Элемент z' имеет ровно n^t предшественников — это элементы $(x_1,\ldots,x_t)$ такие, что $x_i \in \{z,u_1,\ldots,u_{n-1}\}$ и не все x_i равны z. Используя условие $m \le n^t - 1$, выберем m различных элементов из $f^{-1}(z') \setminus \{z'\}$. У каждого из этих элементов имеется ровно n^t предшественников. Выберем m различных из них. Далее выбираем m их предшественников и т. д. После r шагов данного процесса окажется, что все эти элементы вместе с элементом z' образуют подунар, изоморфный унару $U(1,m,r)$. □

Лемма 10. *Имеет место изоморфизм $C_k \times U(1,m,r) \cong U(k,m,r)$.*

Доказательство. Элемент из $C_k \times U(1,m,r)$ можно записать в виде $(\nu,(1,i_1,\ldots,i_t))$. Определим отображение $\phi : C_k \times U(1,m,r) \to U(k,m,r)$ следующим образом: $\phi((\nu,(1,i_1,\ldots,i_t))) = (\nu+t,i_1,\ldots,i_t)$. Очевидно, ϕ взаимно однозначно. Проверим сохранение операции. Имеем $f(\phi((\nu,(1,i_1,\ldots,i_t)))) = f((\nu+t,i_1,\ldots,i_t))$. Если $t>0$, то

$$f((\nu+t,i_1,\ldots,i_t)) = (\nu+t,i_1,\ldots,i_{t-1},\phi(f(\nu,(1,i_1,\ldots,i_t))))$$

$$= \phi((\nu+1,(1,i_1,\ldots,i_{t-1}))) = (\nu+1+t-1,i_1,\ldots,i_{t-1}) = (\nu+t,i_1,\ldots,i_{t-1}).$$

Если $t=0$, то $\phi(f((\nu,(1)))) = \phi((\nu+1,(1))) = (\nu+1,(1)) = f((\nu,(1))) = f(\phi((\nu,(1))))$. Во всех случаях $\phi(f(x)) = f(\phi(x))$, поэтому ϕ — изоморфизм. □

Лемма 11. *Если унары $U_1,\ldots,U_t$ изоморфно вкладываются в унары $(\mathbb{Z}_{n_1}^*,{}^\wedge d)$, ... ,$(\mathbb{Z}_{n_t}^*,{}^\wedge d)$ соответственно, причем числа $n_1,\ldots,n_t$ попарно взаимно просты, то унар $U_1 \times \ldots \times U_t$ изоморфно вкладывается в унар $(\mathbb{Z}_{n_1\ldots n_t}^*,{}^\wedge d)$.*

Доказательство. Действительно, хорошо известно, что в случае, когда $n_1,\ldots,n_t$ попарно взаимно просты, отображение

$$\mathbb{Z}_{n_1\ldots n_t} \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_t}, \quad x \mapsto (x \bmod n_1, \ldots, x \bmod n_t)$$

является изоморфизмом колец, аддитивных групп, мультипликативных полугрупп, а значит, унаров с операцией $x \mapsto x^d$. При этом ограничение этого отображения на $\mathbb{Z}^*_{n_1 \dots n_t}$ будет осуществлять изоморфизм унаров $(\mathbb{Z}^*_{n_1 \dots n_t}, {}^\wedge d)$ и $\prod_{i=1}^t (\mathbb{Z}^*_{n_i}, {}^\wedge d)$. □

Предложение 1. *Для любого натурального числа $d \geq 2$ любой конечный связный унар изоморфно вкладывается в унар вида $(\mathbb{Z}^*_n, {}^\wedge d)$ при некотором $n \in \mathbb{N}$. (При этом n можно считать равным произведению различных простых чисел, которые, в свою очередь, можно считать сколь угодно большими).*

Доказательство. Пусть l — произвольное натуральное число. Ввиду теоремы 1 нам достаточно доказать, что унар $U((k, m, r)$ вкладывается в унар указанного вида, т. е. в унар $\mathbb{Z}^*_n, {}^\wedge d)$, где $n = p_1 \dots p_t$ — произведение различных простых чисел, причем $p_1, \dots, p_t \geq l$.

По лемме 7 (если взять $t = 1$) существуют простое число $p \geq l$ и элемент $x \in \mathbb{Z}^*_p$ такие, что $o(x) = d^k - 1$. Тогда $\{x, x^d, \dots, x^{d^{k-1}}\}$ — цикл длины k унара $\mathbb{Z}^*_p, {}^\wedge d)$. Значит, цикл C_k вкладывается в $(\mathbb{Z}^*_p, {}^\wedge d)$.

Возьмем натуральное число t такое, что $d^t \geq m + 1$. Согласно лемме 9 унар $U(1, m, r)$ вкладывается в $U(1, d, r)^t$. Используя несколько раз лемму 8, построим t вложений унара $U(1, d, r)$ в унары $(\mathbb{Z}^*_{p_i}, {}^\wedge d)$ $(i = 1, \dots, t)$, причем простые числа p_i можно выбрать так, чтобы были выполнены неравенства $p < p_1 < \dots < p_t$. Далее, применив лемму 11, мы получим вложение унара $U(1, d, r)^t$ в унар $(\mathbb{Z}^*_{p_1 \dots p_t}, {}^\wedge d)$.

С учетом леммы 10 $C_k \times U(1, m, r) \cong U(k, m, r)$, а так как C_k вкладывается в $(\mathbb{Z}^*_p, {}^\wedge d)$, а $U(1, m, r)$ — в $(\mathbb{Z}^*_{p_1 \dots p_t}, {}^\wedge d)$, то по лемме 11 унар $U(k, m, r)$ изоморфно вкладывается в унар $(\mathbb{Z}^*_{pp_1 \dots p_t}, {}^\wedge d)$. □

Теперь мы готовы доказать еще один из основных результатов работы.

Теорема 3. *Для любого натурального числа $d \geq 2$ и любого конечного унара U существует натуральное число n такое, что U изоморфно вкладывается в унар $(\mathbb{Z}_n, {}^\wedge d)$. При этом n может быть выбрано в виде $n = p_1 p_2 \dots p_t$, где $p_1, \dots, p_t$ — различные простые числа, которые, в свою очередь, могут быть выбраны сколь угодно большими.*

Доказательство. Пусть $U_1, \dots, U_s$ — компоненты связности унара U. Тогда $U = U_1 \sqcup \dots \sqcup U_s$. Он является копроизведением своих компонент связности.

Возьмем любое натуральное число l. Согласно предложению 1 найдутся различные простые числа

$$p_{11}, \dots, p_{1k_1}, p_{21}, \dots, p_{2k_2}, \dots, p_{s1}, \dots, p_{sk_s}$$

такие, что $p_{ij} \geq l$ при всех i, j и унар U_i изоморфно вкладывается в унар $(\mathbb{Z}_{n_i} *, {}^\wedge d)$, где $n_i = p_{i1} p_{i2} \dots p_{[t_i}$ $(i = 1, 2, \dots, s)$. Поскольку p_{ij} различны, то $\mathbb{Z}_n \cong \prod_{i=1}^s \mathbb{Z}_{n_i}$ как унары с операцией $x \mapsto x^d$. Пусть $\theta_i : U_i \to (\mathbb{Z}^*_{n_i}, {}^\wedge d)$ — вышеупомянутые вложения. Тогда отображение $\theta : U \to (\mathbb{Z}_n, {}^\wedge d)$,

$$x \mapsto (\underbrace{0, \dots, 0}_{i-1}, \theta_i(x), \underbrace{0, \dots, 0}_{s-i})$$

$(x \in U_i)$ является вложением унаров. □

Замечание 1. Было бы неправильным утверждать, что всякий конечный унар вкладывается в унар вида $(\mathbb{Z}^*_n, {}^\wedge 2)$. Действительно, унар, содержащий два различных нуля, не может быть вложен в $(\mathbb{Z}^*_n, {}^\wedge 2)$, так как в противном случае в группе $\mathbb{Z}^*_n$ было бы два различных идемпотента.

Интересен вопрос о том, существует ли такое $d \geq 3$, что любой конечный унар вкладывается в унар вида $(\mathbb{Z}^*_n, {}^\wedge d)$ при подходящем n. Оказывается, все $d \geq 3$ обладают этим свойством. К доказательству данного утверждения мы сейчас приступим, предварительно доказав ряд лемм.

Лемма 12. *Для любых $m_1, m_2 \geq 2$ и $r \geq 1$ имеет место изоморфизм унаров*

$$U(1, m_1 m_2, r) \cong U(1, m_1, r) \times U(1, m_2, r).$$

Доказательство. Будем обозначать через $M(U)$ множество всех минимальных элементов унара U. Нетрудно доказать, что у конечного связного унара U, не являющегося циклом, $M(U)$ — единственная неприводимая система образующих. Положим $U_1 = U(1, m_1, r)$, $U_2 = U(1, m_2, r)$, $M_1 = M(U_1)$, $M_2 = M(U_2)$. Соотношение $U_1 \times U_2 \cong U(1, m_1 m_2, r)$ будет доказано, если мы убедимся, что унар $U_1 \times U_2$ удовлетворяет условиям 1)–3) в определении унара $U(1, m, r)$ при $m = m_1 m_2$ (см. разд. 2).

Условие 1) выполнено, так как циклом унара $U_1 \times U_2$ является одноэлементное множество $\{((0), (0))\}$. Очевидно, $h((u_1, u_2)) = \max(h(u_1), h(u_2))$, отсюда $h(U_1 \times U_2) = r$. Следовательно, выполнено условие 2). Наконец, пусть $(u_1, u_2) \in (U_1 \times U_2) \setminus M(U_1 \times U_2)$. Тогда $u_1 \in U_1 \setminus M(U_1)$ и $u_2 \in U_2 \setminus M(U_2)$. Очевидно, $f^{-1}((u_1, u_2)) = f^{-1}(u_1) \times f^{-1}(u_2)$, поэтому $|f^{-1}((u_1, u_2))| = |f^{-1}(u_1)| \cdot |f^{-1}(u_2)| = m_1 m_2$; соответственно, выполнено условие 3). □

Лемма 13. *Пусть $d \geq 3$, а t и l — произвольные натуральные числа. Тогда существует простое число $p \geq l$ такое, что унар $(\mathbb{Z}_{p-1}, *d)$ имеет подунар, являющийся циклом длины t и не содержащий элемента 0.*

Доказательство. По теореме Дирихле о простых числах в арифметических прогрессиях в прогрессии $\{1 + s(d^t - 1) | s \in \mathbb{N}\}$ содержится бесконечно много простых чисел. Возьмем простое число $p \geq l$ такое, что $p = 1 + s(d^t - 1)$ при некотором $s \in \mathbb{N}$. Очевидно, элементы $s, ds, d^2 s, \ldots, d^{t-1} s$ различны и $d \cdot d^{t-1} s = s$, поэтому $\{s, ds, d^2 s, \ldots, d^{t-1} s\}$ — цикл длины t. Обозначим через $o(s)$ порядок элемента s в группе $(\mathbb{Z}_{p-1}, +)$. Так как $p - 1 = s(d^t - 1)$, то $o(s) = d^t - 1$. По условию $d \geq 3$, соответственно, $d^t - d^{t-1} = d^{t-1}(d-1) \geq 2$. Отсюда следует, что $d^t - 1 > d^{t-1}$, а значит, $d^{t-1} s \neq 0$. □

Лемма 14. *Пусть $d \geq 3$, а l и r — произвольные натуральные числа. Тогда существуют простое число $p \geq l$ и изоморфное вложение унаров $\alpha : U(1, d, r) \to (\mathbb{Z}_{p-1}, *d)$ такие, что $0 \notin \mathrm{im}\alpha$.*

Доказательство. По теореме Дирихле в прогрессии $\{sd^r(d-1) + 1 | s \geq 1\}$ содержится бесконечно много простых чисел. Поэтому существует простое $p \geq l$ такое, что $p = 1 + sd^r(d-1)$ при некотором $s \geq 1$. В группе $(\mathbb{Z}_{p-1}, +)$ элемент s имеет порядок $o(s) = d^r(d-1)$. Следовательно, элементы $s, ds, d^2 s, \ldots, d^r s$ различны и $d^r s = d^{r+1} s$. Так как $d \geq 3$, то $o(s) = d^r(d-1) > d^r$, отсюда $d^r s \neq 0$. Имеется d^r элементов вида $s + i(p-1)/d^r$ $(i = 0, 1, \ldots, d^r - 1)$, при умножении на d получаем d^{r-1} элементов вида $ds + i(p-1)/d^{r-1}$ $(i = 0, 1, \ldots, d^{r-1} - 1)$, умножение на d^j $(j < r)$ дает d^{r-j} элементов вида $d^j s + i(p-1)/d^{r-j}$ и т. д. Наконец, при $j = r$ мы получаем ровно один элемент $d^r s$. Дальнейшее умножение на d оставляет этот элемент неизменным: $d \cdot d^r s = d^r s$. Ясно, что элементы $s + i(p-1)/d^r$ $(i = 0, 1, \ldots, d^r - 1)$ порождают унар, изоморфный унару $U(1, d, r)$. □

Лемма 15. *Пусть $d \geq 3$, а l, m, r — произвольные натуральные числа. Тогда существуют натуральное число k, различные простые числа $p_1, \ldots, p_k \geq l$ и изоморфное вложение унаров*

$$\beta : U(1, m, r) \to (\mathbb{Z}_{p_1 - 1}, *d) \times \ldots \times (\mathbb{Z}_{p_k - 1}, *d)$$

такие, что $\mathrm{im}\beta \subseteq (\mathbb{Z}_{p_1 - 1} \setminus \{0\}) \times \ldots \times (\mathbb{Z}_{p_k - 1} \setminus \{0\})$.

Доказательство. Найдем k, при котором $d^k \geq m$. Применяя k раз лемму 14, найдем простые числа $p_1, \ldots, p_k$ такие, что $l \leq p_1 < p_2 < \ldots < p_k$, и изоморфные вложения $\alpha_i : U(1, d, r) \to (\mathbb{Z}_{p_i - 1}, *d)$ $(i = 1, 2, \ldots, k)$ такие, что $0 \notin \mathrm{im}\alpha_i$ при $i = 1, 2, \ldots, k$. Отсюда получаем вложение $\alpha : \underbrace{U(1, d, r) \times \ldots \times U(1, d, r)}_{k} \to (\mathbb{Z}_{p_1 - 1}, *d) \times \ldots \times (\mathbb{Z}_{p_k - 1}, *d)$.

Ввиду леммы 12 унар $U(1,d^k,r)$ изоморфен унару $(U(1,d,r))^k$. Так как $m \le d^k$, то $U(1,m,r)$ можно считать подунаром унара $U(1,d^k,r)$. Следовательно, существует вложение $\beta : U(1,m,r) \to \prod_{i=1}^{k}(\mathbb{Z}_{p_i-1},{*}d)$. Включение $\mathrm{im}\beta \subseteq \prod_{i=1}^{k}(\mathbb{Z}_{p_i-1}\setminus\{0\})$ очевидно. □

Лемма 16. *Пусть $d \ge 3$, а k,l,m,r — произвольные натуральные числа. Тогда существуют различные простые числа $p_1,p_2 \ge l$ и изоморфное вложение унаров*

$$\gamma : U(k,m,r) \to (\mathbb{Z}_{p_1-1},{*}d) \times (\mathbb{Z}_{p_2-1},{*}d),$$

причем если $\gamma(u) = (x,y)$, то $x,y \ne 0$.

Доказательство. Согласно лемме 13 существуют простое число $p_1 \ge l$ и изоморфное вложение $\alpha : C_k \to (\mathbb{Z}_{p_1-1},{*}d)$ такие, что $0 \notin \alpha(C_k)$. По лемме 14 найдутся простое число $p_2 > p_1$ и изоморфное вложение $\beta : U(1,m,r) \to (\mathbb{Z}_{p_2-1},{*}d)$ такие, что $0 \notin \mathrm{im}\beta$. В соответствии с леммой 10 $U(k,m,r) \cong C_k \times U(1,m,r)$, следовательно, отображение $\gamma = \alpha \times \beta$ будет обладать требуемыми свойствами. □

Теперь мы готовы доказать еще один из основных результатов работы.

Теорема 4. *Пусть $d \ge 3$ — натуральное число. Тогда для любого конечного унара U существуют натуральное число n и инъективный гомоморфизм унаров $\xi : U \to (\mathbb{Z}_n^*,{\wedge}\,d)$. При этом число n может быть выбрано в виде произведения различных простых чисел: $n = p_1p_2\ldots p_t$, а сами простые числа p_i могут быть выбраны сколь угодно большими.*

Доказательство. Зададимся произвольным натуральным числом l. Разложим унар U на компоненты связности: $U = U_1 \sqcup \ldots \sqcup U_s$. Вложим U_i в универсальные унары $U(k_i,m_i,r_i)$ для $i = 1,2,\ldots,s$ — пусть $\alpha_i : U_i \to U(k_i,m_i,r_i)$ $(i = 1,2,\ldots,s)$ суть соответствующие вложения унаров. Далее будем вкладывать унары $U(k_i,m_i,r_i)$ в унары вычетов. По лемме 16 можно найти простые числа p_1, p_2 такие, что $l \le p_1 < p_2$, и изоморфное вложение унаров $\beta_1 : U(k_1,m_1,r_1) \to (\mathbb{Z}_{p_1-1},{*}d) \times (\mathbb{Z}_{p_2-1},{*}d)$, причем $\mathrm{im}\,\beta_1 \subseteq (\mathbb{Z}_{p_1-1}\setminus\{0\}) \times (\mathbb{Z}_{p_2-1}\setminus\{0\})$. Для любого простого числа p кольцо $\mathbb{Z}_p$ является полем, а так как мультипликативная группа конечного поля циклическая, то имеет место изоморфизм групп $(\mathbb{Z}_p^*,\cdot) \cong (\mathbb{Z}_{p-1},+)$. Следовательно, учитывая лемму 6, получаем, что существует вложение унаров $\gamma_1 : U(k_1,m_1,r_1) \to (\mathbb{Z}_{p_1}^*,{\wedge}\,d) \times (\mathbb{Z}_{p_2}^*,{\wedge}\,d)$, причем $\mathrm{im}\,\gamma_1 \subseteq (\mathbb{Z}_{p_1}^*\setminus\{1\}) \times (\mathbb{Z}_{p_2}^*\setminus\{1\})$. Затем найдем простые числа p_3,p_4 такие, что $p_2 < p_3 < p_4$, и вложение $\gamma_2 : U(k_2,m_2,r_2) \to (\mathbb{Z}_{p_3}^*,{\wedge}\,d) \times (\mathbb{Z}_{p_4}^*,{\wedge}\,d)$ такое, что $\mathrm{im}\,\gamma_2 \subseteq (\mathbb{Z}_{p_3}^*\setminus\{1\}) \times (\mathbb{Z}_{p_4}^*\setminus\{1\})$. И так далее. В конце процесса найдем простые числа p_{2s-1}, p_{2s} такие, что $p_{2s-2} < p_{2s-1} < p_{2s}$, и вложение унаров $\gamma_s : U(k_s,m_s,r_s) \to (\mathbb{Z}_{p_{2s-1}}^*,{\wedge}\,d) \times (\mathbb{Z}_{p_{2s}}^*,{\wedge}\,d)$ такое, что $\mathrm{im}\,\gamma_s \subseteq (\mathbb{Z}_{p_{2s-1}}^*\setminus\{1\}) \times (\mathbb{Z}_{p_{2s}}^*\setminus\{1\})$.

Положим $n_i = p_{2i-1}p_{2i}$. Каждое γ_i определяет вложение унаров $\delta_i : U(k_i,m_i,r_i) \to (\mathbb{Z}_{n_i}^*,{\wedge}\,d)$ такое, что $\mathrm{im}\,\delta_i \not\ni 1$ $(i = 1,2,\ldots,s)$. Произвольный элемент $x \in \prod_{i=1}^{s}\mathbb{Z}_{n_i}^*$ будем обозначать в виде строки $(x_1,\ldots,x_s)$, где $x_i \in \mathbb{Z}_{n_i}^*$ при $i = 1,2,\ldots,s$. Теперь построим отображение унаров $\delta : \coprod_{i=1}^{s}U(k_i,m_i,r_i) \to \prod_{j=1}^{s}(\mathbb{Z}_{n_j}^*,{\wedge}\,d)$, полагая

$$(\delta(u))_j = \begin{cases} \delta_i(u), & \text{если } j = i, \\ 1, & \text{если } j \ne i. \end{cases}$$

Нетрудно проверить, что δ — изоморфное вложение унаров. Поскольку U вкладывается в $\coprod_{i=1}^{s}U(k_i,m_i,r_i)$, то унар U изоморфно вкладывается в унар $(\mathbb{Z}_{p_1p_2\ldots p_{2s}}^*,{\wedge}\,d)$. □

Замечание 2. Заметим, что при $d = 2$ утверждение теоремы неверно. Более того, не всякий конечный унар вкладывается в унар вида $(\mathbb{Z}_n^*,{\wedge}\,2)$ — см. замечание 1.

По-видимому, если показатель d в $(\mathbb{Z}_n^*,{\wedge}d)$ не фиксировать заранее, а подбирать для каждого конкретного унара, то всегда можно обойтись простым n. Данное предположение сформулируем в виде гипотезы.

Предположение 1. *Для каждого конечного унара существует точное его представление в $(\mathbb{Z}_p^*,{\wedge}d)$ при подходящих натуральном d и простом p.*

Авторы выражают благодарность рецензенту за ряд ценных замечаний.

СПИСОК ЛИТЕРАТУРЫ

1. **Каргаполов М.И., Мерзляков Ю.И.** Основы теории групп. Москва: Наука, 1977. 240 с.
2. **Клиффорд А., Престон Г.** Алгебраическая теория полугрупп: в 2 т. Москва: Мир, 1972. Т. 1, 286 р.; Т. 2, 423 с.
3. **Кэртис Ч., Райнер И.** Теория представлений конечных групп и ассоциативных алгебр. Москва: Наука, 1969. 668 с.
4. **Steinberg B.** Representation theory of finite monoids. Cham: Springer, 2016. 317 p. https://doi.org/10.1007/978-3-319-43932-7
5. **Whitman P.M.** Lattices, equivalence relations, and subgroups // Bull. Amer. Math. Soc. 1946. Vol. 52, no. 6. P. 507–522.
6. **Кожухов И.Б., Михалёв А.В.** Полигоны над полугруппами // Фундам. и прикл. математика. 2020. Т. 23, no. 3. С. 141–199.
7. **Zelinka B.** Graphs of semigroups. // Časopis pro pěstování matematiky. 1981. Vol. 106, no. 4. P. 407–408. https://doi.org/10.21136/CPM.1981.108493
8. **Lucheta C., Miller E., Reiter C.** Digraphs from powers modulo p // Fibonacci Q. 1996. Vol. 34, no. 3. P. 226–239. https://doi.org/10385/f4752j454
9. **Wilson B.** Power digraphs modulo p // Fibonacci Q. 1998. Vol. 36, no. 3. P. 229–239.
10. **Min Sha**. On the cycle structure of repeated expontiation modulo a prime power // Fibonacci Q. 2011. Vol. 49, no. 4. P. 340–347. https://doi.org/10.1080/00150517.2011.12428034
11. **Somer L., Křižek M.** The structure of digraphs associated with the congruence $x^k \equiv y \pmod{n}$) // Czechoslovak Math. J. 2011. Vol. 61, no. 2. P. 337–358. https://doi.org/10.1007/s10587-011-0079-x
12. **Martin G., Pomerance C.B.** The iterated Carmichael λ-function and the number of cycles of the power generator // Acta Arithmetica. 2005. Vol. 118, no. 4. P. 305–335. https://doi.org/10.4064/aa118-4-1
13. **Kurlberg P., Pomerance C.B.** On the periods of the linear congruential and power generators // Acta Arithmetica. 2005. Vol. 119, no. 2. P. 149–169. https://doi.org/10.4064/aa119-2-2
14. **Parker E.T.** On multiplicative semigroups of residue classes // Proc. Amer. Math. Soc. 1954. Vol. 5, no. 4. P. 612–616.
15. **Слободской Г., Лецко В.А.** О представлении конечных унаров в $\mathbb{Z}_n$ // Вестник СНО: сб. ст. / Волгоград. гос. педагог. ун-т. Сер. “Математика и техника”. № 7. Волгоград: Изд-во “Перемена 1995. С. 3–6.
16. **Боревич З.И., Шафаревич И.Р.** Теория чисел. Москва : Наука (Физматлит), 1985. 504 с.
17. **Лецко В.А.** От задачи к исследованию. СПб.: СМИО Пресс, 2021. 336 с.

Поступила 25.09.2024
После доработки 11.02.2025
Принята к публикации 17.02.2025

Кожухов Игорь Борисович
д-р физ.-мат. наук, профессор
Нац. исслед. университет МИЭТ;
механико-математический факультет МГУ;
Гос. академия нар. хоз-ва и гос. службы
г. Москва
e-mail: kozhuhov_i_b@mail.ru
Лецко Владимир Александрович
канд. пед. наук, доцент
Волгоградский гос. соц.-педагог. университет
г. Волгоград
e-mail: val-etc@yandex.ru

REFERENCES

1. Kargapolov M.I., Merzljakov J.I. *Fundamentals of the theory of groups*. Ser. Graduate texts in mathematics. New York, Springer, 1979, 221 p., ISBN-10: 1461299667 . Original Russian text published in Kargapolov M.I., Merzljakov J.I. *Osnovy teorii grupp*, Moscow, Nauka Publ., 1977, 240 p.

2. Clifford A.H., Preston G.B. *The algebraic theory of semigroups*. Math. Surv., no. 7, Providence, Rhode Island, Amer. Math. Soc., vol. I, 1961, 244 p. ISBN: 9780821802717; vol. II, 1967, 352 p., ISBN: 9780821802724. Translated to Russian under the title *Algebraicheskaya teoriya polugrupp*, Moscow, Mir Publ., 1972, vol. 1, 286 p.; vol. 2, 423 p.
3. Curtis C.W., Reiner I. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publ. Ser., vol. 356, Amer. Math. Soc., 1966, 689 p. ISBN: 0821869450. Translated to Russian under the title *Teoriya predstavleniy konechnykh grupp i assotsiativnykh algebr*, Moscow, Nauka Publ., 1969, 668 p.
4. Steinberg B. *Representation theory of finite monoids*. Cham, Springer, 2016, 317 p. https://doi.org/10.1007/978-3-319-43932-7
5. Whitman P.M. Lattices, equivalence relations, and subgroups. *Bull. Amer. Math. Soc.*, 1946, vol. 52, no. 6, pp. 507–522.
6. Kozhukhov I.B., Mikhalev A.V. Acts over semigroups. *J. Math. Sci.*, 2023, vol. 269, no. 3, pp. 362–401. https://doi.org/10.1007/s10958-023-06287-3
7. Zelinka B. Graphs of semigroups. *Časopis pro pěstování mat.*, 1981, vol. 106, no. 4, pp. 407–408. https://doi.org/10.21136/CPM.1981.108493
8. Lucheta C., Miller E., Reiter C. Digraphs from powers modulo p. *Fibonacci Q.*, 1996, vol. 34, no. 3, pp. 226–239. https://doi.org/10385/f4752j454
9. Wilson B. Power digraphs modulo n. *Fibonacci Q.*, 1998, vol. 36, no. 3, pp. 229–239.
10. Min Sha. On the cycle structure of repeated expontiation modulo a prime power. *Fibonacci Q.*, 2011, vol. 49, no. 4, pp. 340–347. https://doi.org/10.1080/00150517.2011.12428034
11. Somer L., Křižek M. The structure of digraphs associated with the congruence $x^k \equiv y \pmod{n}$. *Czech. Math. J.*, 2011, vol. 61, no. 2, pp. 337–358. https://doi.org/10.1007/s10587-011-0079-x
12. Martin G., Pomerance C.B. The iterated Carmichael λ-function and the number of cycles of the power generator. *Acta Arithmetica*, 2005, vol. 118, no. 4, pp. 305–335. https://doi.org/10.4064/aa118-4-1
13. Kurlberg P., Pomerance C.B. On the periods of the linear congruential and power generators. *Acta Arithmetica*, 2005, vol. 119, no. 2, pp. 149–169. https://doi.org/10.4064/aa119-2-2
14. Parker E.T. On multiplicative semigroups of residue classes. *Proc. Amer. Math. Soc.*, 1954, vol. 5, no. 4, pp. 612–616.
15. Slobodskoy G., Letsko V.A. On the representation of finite unars in $\mathbb{Z}_n$. In: *Vestnik SNO: sbornik statei* / Volgograd. gos. pedagog. un-t. Ser, "Matematika i Tekhnika". No 7. Volgograd: Izd-vo "Peremena", 1995. P. 3–6 (in Russian).
16. Borevich Z.I., Shafarevich I.R. *Number theory*. Orlando, Florida, Academic Press Inc., 1986, 435 p. ISBN-13: 978-0121178512. Original Russian text was published in Borevich Z.I., Shafarevich I.R. *Teoriya chisel*, Moscow, Nauka Publ., 1985, 504 p.
17. Letsko V.A. *Ot zadachi k issledovaniyu* [From problem to research], St. Petersburg, SMIO Press, 2021, 336 p. ISBN: 978-5-7704-0368-8.

Received September 25, 2024
Revised February 11, 2025
Accepted February 17, 2025

Funding Agency: This work was supported by the Russian Science Foundation (project no. 22-11-00052).

Igor Borisovich Kozhukhov, Dr. Phys.-Math. Sci., Prof., Nat. Res. Univ. MIET; Fac. of Mech. and Math. of Moscow State Univ.; Russian Presidental Academy of Nat. Econom. and Public Admin., Moscow, Russia, e-mail: kozhuhov_i_b@mail.ru.

Vladimir Alexandrovich Letsko, Cand. Sci. (Pedagog.), Volgograd State Socio-Pedagogical University Volgograd, Russia, e-mail: val-etc@yandex.ru.

Cite this article as: I. B. Kozhukhov, V. A. Letsko. Representation of unars by sets of residues. *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, 2025, vol. 31, no. 1, pp. 77–89.