S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Том 20, № 2, стр. 144–145 (2023) УДК 512.577
https://doi.org/10.33048/semi.2023.20.??? MSC 08A62

ПРЕДСТАВЛЕНИЯ УНАРОВ ВЫЧЕТАМИ ПО МОДУЛЮ ПРОСТОГО ЧИСЛА

Р.Р. АЙДАГУЛОВ, И.Б. КОЖУХОВ, В.А. ЛЕЦКО

Представлено П.П. Петровым

Abstract: We prove that any finite unar can be isomorphically embedded into a unar of the remainders of the division by a prime p with unary operation $f(x) = x^d \mod p$ for suitable prime p and natural number d.

Keywords: representation of unar.

1 Введение

Представления алгебраических систем системами специального вида – распространённая в математике практика. Она позволяет прояснить строение алгебраической системы, установить некоторые её свойства. Ярким примером является представление группы подстановками или матрицами. В работе [1] было доказано существование изоморфного вложения любого конечного унара в унар остатков от деления на n с операцией $f(x) = xa$ и в унар с операцией $f(x) = x^d$, где n и a – подходящие натуральные числа, а операции осуществляются по модулю n (параметр d при этом может быть взят любым натуральным числом, бльшим 1). В настоящей работе мы доказываем, что произвольный конечный унар можно вложить в мультипликативную группу конечного простого поля (порядка p), рассматриваемую как унар с операцией $f(x) = x^d$ при

Ivanov, I.I., Representations of unars by the residues modulo a prime.
Поступила 1 января 2023 г., опубликована 31 декабря 2023 г.

подходящих d и p, причем простое число p можно выбрать бесконечным количеством способов.

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. [2, п. 3.4]) или 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 $x \in S$.

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. И пусть $\mathbb{Z}_n^*$ – множество элементов из $\mathbb{Z}_n$, имеющих обратный элемент по умножению. Очевидно, $(\mathbb{Z}_n^*, ^\wedge d)$ является подунаром унара $(\mathbb{Z}_n, ^\wedge d)$, а $(\mathbb{Z}_n^*, *a)$ – подунаром унара $(\mathbb{Z}_n, *a)$ в случае, когда $a \in \mathbb{Z}_n^*$, т.е. когда a взаимно просто с n.

Хорошо известно, что $\mathbb{Z}_n$ является кольцом относительно операций сложения и умножения по модулю n, а $\mathbb{Z}_n^*$ – группа относительно 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. Если a и n – взаимно простые натуральные числа, то $\mathrm{ord}_n(a)$ обозначает наименьшее натуральное k такое, что $a^k \equiv 1 \mod n$ (т.е. $\mathrm{ord}_n(a)$ – порядок элемента a в группе $\mathbb{Z}_n^*$). Интересное применение имеют унары $\mathbb{Z}_n$ с операцией $f(x) = x^d + 1 \mod n$ в вопросах факторизации чисел (см. [3]).

Основные сведения из теории унаров можно найти в [4], некоторые определения и обозначения мы приведем в следующем разделе.

В работе [1] был приведен краткий обзор результатов по представлениям унаров вычетами.

2 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 рёбрами $(x, f(x))$ для $x \in U$. Унар называется *связным*, если его граф связен. Если унар U является объединением своих попарно не пересекающихсчя подунаров U_i $(i \in I)$, то мы будем говорить, что U является *копроизведением* (в другой терминологии – прямой суммой) унаров U_i, и писать $U = \coprod_{i \in I} U_i$. Ясно, что любой унар являентся копроизведением своих *компонент связности*.

Цикл из k элементов будем обозначать C_k. Элемент x называется циклическим, если $f^k(x) = x$ при некотором $k \geq 1$ (или, что экевивалентно, элемент, лежащий в каком-нибудь цикле). Через $\langle x \rangle$ обозначаем подунар, порождённый 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 назовём минимальным. Минимальных элементов может и не быть.

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

Хорошо известно, что бинарное отношение, заданное по правилу $x \sim y \leftrightarrow \exists s, t \quad f^s(x) = f^t(y)$, является конгруэнцией унара U. Очевидно, классы эквивалентности этой конгруэнции являются компонентами связности унара U. Также ясно, что каждая компонента связности конечного унара содержит ровно один цикл.

Для натурального числа n рассмотрим множество $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ всех остатков от деления на n. Множество $\mathbb{Z}_n$ с операцией умножения по модулю n является конечной коммутативной полугруппой, обозначим её $(\mathbb{Z}_n, *)$. Если зафиксировать какое-либо $a \in \mathbb{Z}_n$, то отображение $\mathbb{Z}_n \to \mathbb{Z}_n$, $x \mapsto x \cdot a$, будет являться унарной операцией. Соответствующий унар обозначим так: $(\mathbb{Z}_n, *a)$. Другой унар возникает на множестве $\mathbb{Z}_n$ относительно операции возведения в степень: $\mathbb{Z}_n \to \mathbb{Z}_n$, $x \mapsto x^d$. Обозначим этот унар следующим образом: $(\mathbb{Z}_n, {}^\wedge d)$.

В настоящей работе через $\mathbb{Z}_n^*$ мы будем обозначать 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. Всюду в работе (a, b) будет обозначать *наибольший общий делитель* чисел a и b, а $[a, b]$ – *наименьшее общее кратное* этих же чисел. Далее, $a \vdots b$ и $c \mid d$ обозначают соответственно "a делится на b" и "c делит d".

3 Утверждение о выборе числа с заданными порядками

В этом разделе мы докажем наличие числа, имеющего заданные порядки по модулям подходящих простых чисел.

Приведём некоторые алгебраические определения, нужные нам для дальнейшего. Многочлен называется *унитарным*, если его старший коэффициент равен 1.Для простого числа p и любого натурального числа a положим

$$\nu_p(a) = \max\{t : p^t \mid a\}.$$

Для натурального числа n *круговой многочлен* $\Phi_n(x)$ определяется следующим образом (см. [5, §13]):

$$\Phi_n(x) = \prod_{(i,n)=1,\, 0\le i<n} (x - \theta^i),$$

где θ – первообразный корень n-й степени из 1. Известно, что $\Phi_n(x)$ – унитарный многочлен с целыми коэффициентами со свободным членом, равным 1 или -1. Имеет место следующее разложение многочлена x^n-1 на неприводимые множители над полем $\mathbb{Q}$:

$$x^n - 1 = \prod_{d\,|\,n} \Phi_d(x).$$

Лемма 1. *Если p – простой делитель числа $a^m - 1$, то $\operatorname{ord}_p(a) \,|\, m$.*

Доказательство. Так как $a^m - 1 \vdots p$, то $a^m = 1$ в группе $\mathbb{Z}_p^*$. Следовательно, $\operatorname{ord}_p(a)|m$. □ □

Лемма 2. *Если $d|m$ и p – простой делитель числа $a^{m/d} - 1$, причём $p \nmid d$, то $\nu_p(a^m - 1) = \nu_p(a^{m/d} - 1)$.*

Доказательство. Пусть $l = \nu_p(a^{m/d} - 1)$. По условию $l \ge 1$. Имеем: $a^{m/d} - 1 = p^l c$, где $p \nmid c$. Далее получаем:

$$a^m - 1 = (1 + p^l c)^d - 1 = dp^l c + \sum_{j=2}^{d} C_d^j p^{lj} c^j.$$

Так как $p \nmid d, c$, то $\nu_p(dp^l c) = l$, в то время как $\nu_p(C_d^j p^{lj} c^j) \ge lj > l$ при $j \ge 2$, поэтому $\nu_p(a^m - 1) = l$. □ □

Следствие 1. *Если простое число $p \,|\, a^{m/d} - 1$ и $p \nmid d$, то $(a^m - 1)/(a^{m/d} - 1) \nvdots p$.*

Лемма 3. *Если p – простое число, $a \ge 2$, $p \,|\, \Phi_n(a)$ и $p \nmid n$, то $\operatorname{ord}_p(a) = n$.*

Доказательство. Предположим, что это не так, т.е. $\operatorname{ord}_p(a) \ne n$. По лемме 1 $\operatorname{ord}_p(a) = n/d$, где $d|n$ и $d > 1$. Так как $p \nmid n$, то $p \nmid d$. По следствию из леммы 2 $(a^n - 1)/(a^{n/d} - 1)$ не делится на p. Имеем:

$$a^n - 1 = \prod_{t|n} \Phi_t(a) = \Phi_n(a) \cdot (a^{n/d} - 1) \cdot \prod_{t|n, t\nmid n/d} \Phi_t(a).$$

Отсюда видно, что $(a^n - 1)/(a^{n/d} - 1) \vdots p$. Мы получили противоречие, а значит, $\operatorname{ord}_p(a) = n$. □ □

Лемма 4. *Если $(n, k) = 1$, то $\Phi_k(x) \,|\, \Phi_k(x^n)$.*

Доказательство. Пусть θ – первообразный корень k-й степени из 1. Тогда $\Phi_k(x) = \prod_{(i,k)=1}(x - \theta^i)$. Так как $\Phi_k(x)$ не имеет кратных корней, то достаточно доказать, что все корни многочлена $\Phi_k(x)$ являются корнями многочлена $\Phi_k(x^n)$. Возьмём произвольный корень многочлена $\Phi_k(x)$. Он имеет вид θ^i, где $(i,k) = 1$. Так как $(n,k) = 1$, то $\theta^{ni} = \theta^j$ при некотором j таком, что $(j,k) = 1$ и $0 \le j < k$. Следовательно, θ^i – корень многочлена $\Phi_k(x^n)$. □ □

Следствие 2. *Для любого целого числа a при $(n,k) = 1$ имеет место соотношение $\Phi_k(a) \mid \Phi_k(a^n)$.*

Доказательство. Действительно, так как $\Phi_k(x)$ и $\Phi_k(x^n)$ – унитарные многочлены и $\Phi_k(x) \mid \Phi_k(x^n)$, то $\Phi_k(x^n) = \Phi_k(x) \cdot f(x)$, где $f(x)$ – многочлен с целыми коэффициентами. Поэтому $\Phi_k(a^n) \vdots \Phi_k(a)$. □ □

Лемма 5. *Числа a и $\Phi_n(a)$ взаимно просты.*

Доказательство. Многочлен $\Phi_n(x)$ является многочленом с целыми коэффициентами со старшим коэффициентом 1 и со свободным членом ± 1, поэтому $\Phi_n(a) = a^m + \alpha_1 a^{m-1} + \ldots + \alpha_{m-1} a \pm 1$, где $\alpha_1, \ldots, \alpha_{m-1}$ – целые числа. Следовательно, $(\Phi_n(a), a) = 1$. □ □

Обозначим через $\mathrm{rad}(a)$ произведение всех простых делителей числа a.

Лемма 6. *Если $n, a \ge 2$ – натуральные числа, то $\Phi_n(a) \ge 2$.*

Доказательство. Имеем: $\Phi_n(a) = \prod_{(i,n)=1}(a - \theta^i)$. Так как $|a - \theta^i| > 1$ при $(i,n) = 1$, то $|\Phi_n(a)| > 1$. Но $\Phi_n(a)$ – натуральное число. Следовательно, $\Phi_n(a) \ge 2$. □ □

Предложение 1. *Пусть $k_1, \ldots, k_s \ge 2$ – натуральные числа, необязательно различные. Тогда существуют различные простые числа $p_1, \ldots, p_s$ и число b такие, что $\mathrm{ord}_{p_i} b = k_i$ при $i = 1, \ldots, s$.*

Доказательство. Перенумеруем числа $k_1, \ldots, k_s$ так, чтобы первые несколько чисел $k_1, \ldots, k_t$ были различны, а каждое из остальных совпадало с одним из $k_1, \ldots, k_t$. Пусть k_i $(1 \le i \le t)$ входит в набор $k_1, \ldots, k_s$ ровно l_i раз. Положим $l = \max(l_1, \ldots, l_t)$. Возьмём число u такое, что $2^u > l$. Далее, возьмём какие-либо различные простые числа $q_1, \ldots, q_u \not\mid \mathrm{rad}(k_1 \ldots k_t)$. Положим $m = q_1 \ldots q_u$, $a = m \cdot \mathrm{rad}(k_1 \ldots k_t)$ и $b = a^m$.

Пусть D – множество всех делителей d числа m таких, что $d > 1$. Очевидно, $|D| = 2^u - 1$, и по ранее обусловленному $2^u \ge l$. Для $i \le t$ и $d \in D$ рассмотрим $\Phi_{k_i d}(a)$. По лемме 6 $\Phi_{k_i d}(a) \ge 2$. Пусть $p_{i,d}$ – какой-либо простой делитель числа $\Phi_{k_i d}(a)$:

$$p_{i,d} \mid \Phi_{k_i d}(a) \ (i = 1, \ldots, t, \ d \in D).$$

Так как $|D| \ge l_i$ при всех $i \in \{1, \ldots, t\}$, то нам достаточно будет доказать, что числа $p_{i,d}$ различны и $\mathrm{ord}_{p_{i,d}} b = k_i$ при всех i, d.

Применяя несколько раз теорему 13.5 из [5], получим, что $\Phi_{k_i d}(x) \mid \Phi_{k_i}(x^d)$, а так как m/d и k_i взаимно просты, то по лемме 4 $\Phi_{k_i}(x^d) \mid \Phi_{k_i}(x^m)$. Таким образом, $\Phi_{k_i d}(x) \mid \Phi_{k_i}(x^m)$. Так как все эти многочлены унитарные, то

$$p_{i,d} \mid \Phi_{k_i d}(a) \mid \Phi_{k_i}(a^d) \mid \Phi_{k_i}(a^m) = \Phi_{k_i}(b).$$

Докажем, что $p_{i,d} \nmid k_i d$. Предположим, что $p_{i,d} \mid k_i d$. Так как $p_{i,d}$ – простое, то либо $p_{i,d} \mid k_i$, либо $p_{i,d} \mid d$. Разберём эти случаи в отдельности.

1-й случай: $p_{i,d} \mid k_i$. Тогда $p_{i,d} \mid a$. Но соотношения $p_{i,d} \mid a$ и $p_{i,d} \mid \Phi_{k_i d}(a)$ противоречат друг другу, так как по лемме 5 числа a и $\Phi_n(a)$ взаимно просты.

2-й случай: $p_{i,d} \mid d$. Так как d – произведение каких-либо из чисел $q_1, \ldots, q_u$, то $p_{i,d} = q_j$ при некотором j. Следовательно, $p_{i,d} \mid a$. Мы снова получаем, что $p_{i,d} \mid a$ и $p_{i,d} \mid \Phi_{k_i d}(a)$, т.е. противоречие с леммой 5.

Таким образом, $p_{i,d} \nmid k_i d$. Так как $p_{i,d} \mid \Phi_{k_i d}(a)$ и $p_{i,d} \nmid k_i d$, то по лемме 3 $\mathrm{ord}_{p_{i,d}} a = k_i d$. Отсюда ясно, что все $p_{i,d}$ различны.

Осталось доказать, что $\mathrm{ord}_{p_{i,d}} b = k_i$. Действительно, мы ранее доказали, что $p_{i,d} \mid \Phi_{k_i}(b)$. Так как $p_{i,d}$ – простые и $p_{i,d} \nmid k_i$, то по лемме 3 $\mathrm{ord}_{p_{i,d}} b = k_i$. □ □

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

Теперь мы готовы доказать основной результат.

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

Доказательство. Пусть конечный унар U характеризуется следующими параметрами:

$r(U) = r$ – максимум степеней элементов;

$h(U) = h$ – максимальная глубина элементов;

l – количество петель;

$c_1, \ldots, c_t$ – длины циклов компонент связности, не содержащих петель.

Пусть натуральные числа $d, n_1, \ldots, n_t$ таковы, что $d \geq r$, $d - 1 \geq l$ и для всех $i \in \{1, \ldots, t\}$ $\mathrm{ord}_{n_i} d = c_i$. Существование такоих чисел гарантируется предложением 1. Рассмотрим арифметическую пргрессию $1 + i \cdot d^h[d-1, n_1, \ldots n_t]$ $(i = 1, 2, \ldots)$. По теореме Дирихле о простых числах в арифметической прогрессии (см., например, [6, глава V, §3, теорема 3]) в этой прогрессии бесконечно много простых чисел. Возьмём любое из них и обозначим его чероез p.

Докажем, что U изоморфно вкладывается в унар $(\mathbb{Z}_p^*, {}^\wedge d)$. В самом деле, $(\mathbb{Z}_p^*, \cdot) \cong (\mathbb{Z}_{p-1}, +)$. Поэтому достаточно обосновать наличие требуемых характеристик у унара $(\mathbb{Z}_{p-1}, *d)$.

Согласно лемме 1 из работы [1] все элементы $(\mathbb{Z}_{p-1}, *d)$, не являющиеся минимальными, имеют степень d, которая по построению не меньше r. По лемме 3 из той же работы [1] минимальные элементы унара $(\mathbb{Z}_{p-1}, *d)$ имеют глубину, не меньшую h.

Для каждого n_i $(1 \le i \le t)$ в группе $(\mathbb{Z}_{p-1}, *)$ существует подгруппа, в которой мультипликативный порядок элемента d равен c_i. Поэтому по лемме 4 из работы [1] соответствующая компонента унара $(\mathbb{Z}_{p-1}, *a)$ имеет, по крайней мере, один цикл длины c_i. Требуемое число петель обеспечено тем, что $d-1 \,|\, p-1$, откуда следует, что в $\mathbb{Z}_p^*$ имеется $d-1$ элементов x, для которых $x^d = x$. □ □

Замечание 1. *Значительный произвол в выборе простых чисел в доказательстве предложения 1, а также бесконечность множества простых чисел в арифметической прогрессии с взаимно простыми первым членом и разностью показывают, что существует бесконечно много пар чисел d и p, для которых данный конечный унар изоморфно вкладывается в $(\mathbb{Z}_p^*, {}^\wedge d)$.*

Замечание 2. *Отметим, что числа n_i не обязаны быть ни простыми (как в предложении 1), ни даже взаимно простыми. На практике это позволяет существенно уменьшить подходящие d и p. Насколько радидакально это уменьшение, показывает приведенный ниже пример.*

Пример 1. *Пусть требуется вложить в $(\mathbb{Z}_p^*, {}^\wedge d)$ унар, характеризующийся следующими параметрами (в обозначениях теоремы 1): $r = 4$, $h = 2$, $l = 3$, $c_1 = 5$, $c_2 = 6$, $c_3 = 8$, $c_4 = 10$. Непосредственная проверка показывает, что в качестве d можно взять число 5. Поскольку $\mathrm{ord}_{11}(5) = 5$, $\mathrm{ord}_9(5) = 6$, $\mathrm{ord}_{32}(5) = 8$, $\mathrm{ord}_{33}(5) = 10$, можно положить $n_1 = 11$, $n_2 = 9$, $n_3 = 32$, $n_4 = 33$. Уже при $i = 1$ число $1 + i \cdot 5^2[5-1, 11, 9, 32, 33] = 79201$ является простым, и его можно взять в качестве p. Разумеется, в получаемом унаре возникают и "лишние" компоненты. В данном случае к 7 требуемым компонентам добавятся еще 119. Точнее, в соответствующем унаре глубина минимальных элементов равна 2, степени остальных элементов равны 5, а компоненты связности характеризуются списком $\langle 1, 4\rangle$, $\langle 2, 10\rangle$, $\langle 4, 6\rangle$, $\langle 5, 8\rangle$, $\langle 6, 8\rangle$, $\langle 8, 6\rangle$, $\langle 10, 20\rangle$, $\langle 12, 4\rangle$, $\langle 20, 12\rangle$, $\langle 24, 4\rangle$, $\langle 30, 16\rangle$, $\langle 40, 12\rangle$, $\langle 60, 8\rangle$, $\langle 120, 8\rangle$. Здесь первые числа в каждой паре означают длину цикла, а вторые – количество компонент, имеющих цикл этой длины.*

Таким образом, нам удалось обойтись числами $d = 5$ и $p = 79201$, в то время как минимальное d, определяемое предложением 1, равно 2042040^{17017} (в десятичной записи этого числа более 100 000 знаков), и простое число p также запредельно большое.

References

[1] I.B.Kozhukhov, V.A.Letsko, , *Representatioms of unars by a set of residues*, Trudy Inst. Mat. Mekh. UrO RAN, **31**:1 (2025), 77–89.

[2] I.B.Kozhukhov, A.V.Mikhalev, *Acts over semigroups*, J. Math. Sci. (New York), **269**:3 (2023), 362—401.

[3] R. Crandall, C. Pomerance, , *Prime numbers. A computational perspective*, 2nd Ed., Springer (2006), 597 pp.

[4] D. Jakubíková-Studenovská, J. Pócs J. *Monounary algebras*, UPJS, Košice (2009), 302 pp.
[5] V.V. Prasolov, , *Polynomials*, Springer (2004), XIII + 301 pp.
[6] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Pres, New York and London (1966), x+435 pp., ISBN-13 978-0121178512.

Rustem Rimovich Aidagulov
Lomonosov Moscow State Univ.,
Leninskiye Gory, 1,
119991, Moscow, Russia
Email address: a_rust@bk.ru

Igor Borisovich Kozhukhov
National Research Univ. MIET,
Shokin square, 1,
124498, Moscow, Russia
Lomonosov Moscow State Univ.,
Leninskiye Gory, 1,
119991, Moscow, Russia
Email address: kozhuhov_i_b@mail.ru

Vladimir Alexandrovich Letsko
Volgograd State Soc.-Ped. Univ.,
prosp. V.I. Lenina, 27,
400005, Volgograd, Russia
Email address: val-etc@yandex.ru