

---

**ПРЕДСТАВЛЕНИЯ УНАРОВ ВЫЧЕТАМИ ПО  
МОДУЛЮ ПРОСТОГО ЧИСЛА****Р.Р. Айдагулов, И.Б. Кожухов, В.А. Лецко***Представлено С.В. Судоплатовым*

**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  $f(x) = x^d \pmod p$  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, большим 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

---

AIDAGULOV, R.R., KOZHUKHOV, I.B., LETSKO, V.A., REPRESENTATIONS OF UNARS  
BY THE RESIDUES MODULO A PRIME.

© 2025 AIDAGULOV R.R., KOZHUKHOV I.B., LETSKO V.A..

Поступила 10 октября 2025 г., опубликована 9 декабря 2025 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  $f : U \rightarrow U$ . Унар можно рассматривать как полигон над бесконечной циклической полугруппой  $S = \{t, t^2, t^3, \dots\}$  (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  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  – 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  $\text{ord}_n(a)$  обозначает наименьшее натуральное  $k$  такое, что  $a^k \equiv 1 \pmod n$  (т.е.  $\text{ord}_n(a)$  – порядок элемента  $a$  в группе  $\mathbb{Z}_n^*$ ). Интересное применение имеют унары  $\mathbb{Z}_n$  с операцией  $f(x) = x^d + 1 \pmod n$  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 связан. Если унар  $U$  является объединением своих попарно не пересекающихся 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 является 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 эквивалентно, 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  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  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  $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ ,  $x \mapsto x \cdot a$ , 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:  $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ ,  $x \mapsto x^d$ . 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,  $a : b$  и  $c | d$  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

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

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

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

где  $\theta$  – 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  $\text{ord}_p(a) | m$ .

*Доказательство.* Так как  $a^m - 1 \not\equiv 0 \pmod{p}$ , то  $a^m = 1$  в группе  $\mathbb{Z}_p^*$ . Следовательно,  $\text{ord}_p(a) | m$ .  $\square$

**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  $l \geq 1$ . 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  $\nu_p(C_d^j p^{lj} c^j) \geq lj > l$  при  $j \geq 2$ , поэтому  $\nu_p(a^m - 1) = l$ .  $\square$

**Следствие 1.** Если простое число  $p | a^{m/d} - 1$  и  $p \nmid d$ , то  $(a^m - 1)/(a^{m/d} - 1) \not\equiv 0 \pmod{p}$ .

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

*Доказательство.* Предположим, что это не так, т.е.  $\text{ord}_p(a) \neq n$ . По лемме 1  $\text{ord}_p(a) = n/d$ , 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  $(a^n - 1)/(a^{n/d} - 1) \not\equiv 0 \pmod{p}$ . Мы получили противоречие, а значит,  $\text{ord}_p(a) = n$ .  $\square$

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

*Доказательство.* Пусть  $\theta$  – 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  $\theta^i$ , где  $(i, k) = 1$ . Так как  $(n, k) = 1$ , то  $\theta^{ni} = \theta^j$  при некотором  $j$  таком, что  $(j, k) = 1$  и  $0 \leq j < k$ . Следовательно,  $\theta^i$  – корень многочлена  $\Phi_k(x^n)$ .  $\square$

**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  $\Phi_k(a^n) : \Phi_k(a)$ .  $\square$

**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  $\pm 1$ , поэтому  $\Phi_n(a) = a^m + \alpha_1 a^{m-1} + \dots + \alpha_{m-1} a \pm 1$ , где  $\alpha_1, \dots, \alpha_{m-1}$  – целые числа. Следовательно,  $(\Phi_n(a), a) = 1$ .  $\square$

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

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

*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,  $\Phi_n(a) \geq 2$ .  $\square$

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

*Доказательство.* Перенумеруем числа  $k_1, \dots, k_s$  так, чтобы первые несколько чисел  $k_1, \dots, k_t$  были различны, а каждое из остальных совпадало с одним из  $k_1, \dots, k_t$ . Пусть  $k_i$  ( $1 \leq i \leq t$ ) входит в набор  $k_1, \dots, k_s$  ровно  $l_i$  раз. Положим  $l = \max(l_1, \dots, l_t)$ . Возьмём число  $u$  такое, что  $2^u > l$ . Далее, возьмём какие-либо различные простые числа  $q_1, \dots, q_u \nmid \text{rad}(k_1 \dots k_t)$ . Положим  $m = q_1 \dots q_u$ ,  $a = m \cdot \text{rad}(k_1 \dots k_t)$  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  $2^u \geq l$ . Для  $i \leq t$  и  $d \in D$  рассмотрим  $\Phi_{k_i d}(a)$ . По лемме 6  $\Phi_{k_i d}(a) \geq 2$ . Пусть  $p_{i,d}$  – какой-либо простой делитель числа  $\Phi_{k_i d}(a)$ :

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

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

Применяя несколько раз теорему 13.5 из [5], получим, что  $\Phi_{k_id}(x) \mid \Phi_{k_i}(x^d)$ , 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,  $\Phi_{k_id}(x) \mid \Phi_{k_i}(x^m)$ . Так как все эти многочлены унитарные, то

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

Докажем, что  $p_{i,d} \nmid k_id$ . Предположим, что  $p_{i,d} \mid k_id$ . 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  $p_{i,d} \mid \Phi_{k_id}(a)$  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  $q_1, \dots, q_u$ , 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  $p_{i,d} \mid \Phi_{k_id}(a)$ , т.е. противоречие с леммой 5.

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

Осталось доказать, что  $\text{ord}_{p_{i,d}} b = k_i$ . 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  $\text{ord}_{p_{i,d}} b = k_i$ .  $\square$

#### 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;

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

Пусть натуральные числа  $d, n_1, \dots, n_t$  таковы, что  $d \geq r$ ,  $d - 1 \geq l$  и для всех  $i \in \{1, \dots, t\}$   $\text{ord}_{n_i} d = c_i$ . Существование таких чисел гарантируется предложением 1. Рассмотрим арифметическую прогрессию  $1 + i \cdot d^h [d - 1, n_1, \dots, n_t]$  ( $i = 1, 2, \dots$ ). 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 через  $p$ .

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  $n_i$  ( $1 \leq i \leq t$ ) 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  $d-1 \mid p-1$ , откуда следует, что в  $\mathbb{Z}_p^*$  имеется  $d-1$  элементов  $x$ , для которых  $x^d = x$ .  $\square$

**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 радикально 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  $\text{ord}_{11}(5) = 5$ ,  $\text{ord}_9(5) = 6$ ,  $\text{ord}_{32}(5) = 8$ ,  $\text{ord}_{33}(5) = 10$ , 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, *Representations 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. Zbl 1517.20092
- [3] R. Crandall, C. Pomerance, *Prime numbers. A computational perspective*, 2nd Ed., Springer, 2005. Zbl 1088.11001
- [4] D. Jakubíková-Studenovská, J. Pócs, *Monounary algebras*, UPJS, Košice, 2009. Zbl 1181.08001
- [5] V.V. Prasolov, *Polynomials*, Springer, 2004. Zbl 1063.12001
- [6] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966. Zbl 0145.04902

RUSTEM RIMOVICH AIDAGULOV  
LOMONOSOV MOSCOW STATE UNIV.,  
LENINSKIYE GORY, 1,  
119991, MOSCOW, RUSSIA  
Email address: [a\\_rust@bk.ru](mailto: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: [kozuhov\\_i\\_b@mail.ru](mailto:kozuhov_i_b@mail.ru)

VLADIMIR ALEXANDROVICH LETSKO  
VOLGOGRAД STATE SOC.-PED. UNIV.,  
PROSP. V.I. LENINA, 27,  
400005, VOLGOGRAД, RUSSIA  
Email address: [val-etc@yandex.ru](mailto:val-etc@yandex.ru)