ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

Научная статья
УДК 519.6
DOI 10.35266/1999-7604-2023-1-59-72

МЕТОДЫ МАСШТАБИРОВАНИЯ ЧИСЕЛ В МОДУЛЯРНОЙ АРИФМЕТИКЕ: ОБЗОР, РАЗРАБОТКА И ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМОВ

Наталья Сергеевна Золотарева

Сургутский государственный университет, Сургут, Россия
zolotareva_ns@surgu.ru, <https://orcid.org/0000-0001-9751-4232>

Аннотация. Представлено математическое описание двух методов масштабирования чисел в модулярной системе счисления: основанного на интервальной оценке и с использованием итерационного алгоритма масштабирования числа X коэффициентом K , включающего в себя этап расширения системы оснований и непосредственно этап масштабирования. Приведены примеры и представлены результаты работы алгоритмов программ, разработанных на языке Python, моделирующих выполнение алгоритмов на электронно-вычислительной машине. Выполнены оценки сложности алгоритмов для их сравнения и выявления оптимальных.

Ключевые слова: модулярная арифметика, немодульные операции, модульные операции, масштабирование чисел, расширение системы оснований, ранг числа

Для цитирования: Золотарева Н. С. Методы масштабирования чисел в модулярной арифметике: обзор, разработка и оценка сложности алгоритмов // Вестник кибернетики. 2023. Т. 22, № 1. С. 59–72. DOI 10.35266/1999-7604-2023-1-59-72.

Original article

NUMERAL SCALING METHODS IN MODULAR ARITHMETIC: REVIEW, DEVELOPMENT AND ESTIMATION OF THE ALGORITHMS COMPLEXITY

Natalya S. Zolotareva

Surgut State University, Surgut, Russia
zolotareva_ns@surgu.ru, <https://orcid.org/0000-0001-9751-4232>

Abstract. The study describes two methods of numeral scaling in a modular number system: one which is based on the interval estimation and the other one which uses iterative algorithm of scaling number X by the coefficient K and includes both the stage of base system expansion and the scaling stage itself. The authors demonstrate the examples and results of algorithms operation provided by the programs developed via Python that simulate algorithms execution on a computer. Estimates of the algorithms complexity were defined in order to compare them and to detect the most appropriate ones.

Keywords: modular arithmetic, non-modular operations, modular operations, numeral scaling, base system expansion, number rank

For citation: Zolotareva N. S. Numeral Scaling Methods in Modular Arithmetic: Review, Development and Estimation of the Algorithms Complexity. Proceedings in Cybernetics. 2023. Vol. 22, No. 1. P. 59–72. DOI 10.35266/1999-7604-2023-1-59-72.

ВВЕДЕНИЕ

Модулярная арифметика представляет средства для эффективного выполнения модульных операций сложения, вычитания и умножения целых чисел. Действия над числами можно

проводить независимо в параллельных каналах, операции выполняются одновременно, тем самым повышается скорость их выполнения. Однако существуют такие операции, как масштабирование чисел, расширение

системы оснований, вычисление ранга и др., которые препятствуют более широкому внедрению модулярной арифметики. Эта группа операций носит название немодульных операций. Немодульные операции, это операции, в которых необходимо знать информацию обо всем числе, и приходится восстанавливать позиционное представление числа [1–3].

Модулярная система счисления (МСС) характеризуется набором n взаимно простых модулей $\{p_1, p_2, \dots, p_n\}$. В модулярной арифметике любое целое положительное число X представимо как $X = (x_1, x_2, \dots, x_n)$, где x_i – наименьшие неотрицательные остатки от деления числа X на модули p_i , то есть $x_i = |X|_{p_i} = X \pmod{p_i}$, $i = 1, 2, \dots, n$. В рамках модулярной арифметики существует уникальное представление всех целых чисел в диапазоне $0 \leq X < P$, где $P = p_1 \times p_2 \times \dots \times p_n$ – вычислительный диапазон МСС [4].

Если числа X, Y в МСС представимы в виде $X = (x_1, x_2, \dots, x_n), Y = (y_1, y_2, \dots, y_n)$, то выполнение операций сложения, вычитания и умножения реализуется по формуле:

$$\begin{aligned} X * Y &= (x_1, x_2, \dots, x_n) * \\ & * (y_1, y_2, \dots, y_n) = ((x_1 * y_1) \pmod{p_1}, \\ & (x_2 * y_2) \pmod{p_2}, \dots, (x_n * y_n) \pmod{p_n}), \end{aligned} \quad (1)$$

где $*$ обозначает одну из операций: сложение, вычитание или умножение.

МАТЕРИАЛЫ И МЕТОДЫ

На первом этапе осуществлен анализ теоретических и практических разработок отечественных и зарубежных специалистов, связанных с выполнением операции масштабирования в МСС [5–9]. В работе приведено математическое описание и примеры расчета двух методов: метода с использованием интервальных оценок и метода с применением расширения системы оснований. Стоит отметить, что при рассмотрении первого метода дополнительно необходимо рассмотреть процедуру вычисления ранга числа [1, 10], а при рассмотрении второго метода используется операция расширения системы оснований [11, 12].

На втором этапе были разработаны программы на языке Python, моделирующие выполнение алгоритмов на ЭВМ. На третьем этапе произведено сравнение алгоритмов между собой с оценкой их сложности для выявления оптимальных.

Метод с использованием интервальных оценок.

Пусть МСС задана набором положительных попарно взаимно простых чисел $p_1, p_2, \dots, p_n$ числом $X = (x_1, x_2, \dots, x_n)$. Пусть C_X – точное значение отношения $\frac{X}{P}$, где $P = p_1 \times p_2 \times \dots \times p_n$ и представляет собой в общем случае правильную бесконечную дробь.

Определение: под интервальной позиционной характеристикой (ИПХ) модулярного числа X понимается замкнутый вещественный интервал $I_{\frac{X}{P}} = [S_{low}, S_{upp}]$, представленный парой направленно округленных чисел-границ, отвечающих условию $S_{low} \leq C_X \leq S_{upp}$ [1, 13].

Границы, задающие ИПХ, определяются с помощью направленных округлений: нижняя граница округляется до ближайшего машинного числа с недостатком, а верхняя – с избытком:

$$S_{low} = \nabla \sum_{i=1}^n (|x_i \times m_i|_{p_i} \nabla p_i), \quad (2)$$

где S_{low} – интервальная оценка суммы

$$S = \sum_{i=1}^n \frac{|x_i \times m_i|_{p_i}}{p_i} \text{ с округлением «вниз»}.$$

$$S_{upp} = \Delta \sum_{i=1}^n (|x_i \times m_i|_{p_i} \Delta p_i), \quad (3)$$

где S_{upp} – интервальная оценка суммы

$$S = \sum_{i=1}^n \frac{|x_i \times m_i|_{p_i}}{p_i} \text{ с округлением «вверх»}.$$

Символы ∇ и ∇ означают суммирование и деление с плавающей точкой, выполняемые округлением «вниз», аналогично Δ и Δ означают операции с округлением «вверх» [5].

ИПХ $I_{\frac{X}{P}}$ модулярного числа X позволяет единообразным способом учесть погрешность

округлений, неизбежно возникающие при сопоставлении точному значению $C_X = \frac{X}{P}$ представления с ограниченной разрядностью: C_X заключается в гарантированно содержащие это значение границы, направленно округленные до разрядности машинного представления [13].

Рассмотрим метод масштабирования с использованием интервальных оценок [5]. Данный метод масштабирует число X с коэффициентом K , взаимно простым с P . В результате возвращается частное $Y = \left\lfloor \frac{X}{K} \right\rfloor$, представленное остатками $y_i = |Y|_{p_i}$. В процессе вычислений используются только стандартные операции с плавающей точкой и целочисленные операции по модулям $p_1, p_2, \dots, p_n$ и K . Заранее вычисляются следующие константы: $|P_i^{-1}|_{p_i}$, $|p_i|_K$, $|K^{-1}|_{p_i}$ для $i = 1, 2, \dots, n$, а также $|P|_K$ [5].

Для вычисления k дробные части S_{low} и S_{upp} отбрасываются:

$$k_{low} = [S_{low}], k_{upp} = [S_{upp}]. \quad (4)$$

При этом важны два случая:

1) $k_{low} = k_{upp}$ свидетельствует о том, что S_{low} и S_{upp} вычислены с достаточной точностью. Тогда $k = k_{low} = k_{upp}$.

2) $k_{low} \neq k_{upp}$ свидетельствует о том, что точность вычисления S_{low} и S_{upp} недостаточна для однозначного определения k . В этом случае вычисляется ранг $r(X)$ – характеристика, показывающая сколько раз диапазон системы превышен при переходе от представления X в МСС к его позиционному представлению. Ранг связан с искомым k следующим соотношением:

$$k = r(X) - \sum_{i=1}^n \left\lfloor \frac{x_i \times m_i}{p_i} \right\rfloor. \quad (5)$$

Вычисление ранга числа.

Если в МСС заданы два числа $X = (x_1, x_2, \dots, x_n)$ и $Y = (y_1, y_2, \dots, y_n)$ с соответ-

ствующими рангами r_X и r_Y , то ранг r_{X+Y} суммы двух чисел $X+Y$ определяется по формуле [1]:

$$r_{X+Y} = r_X + r_Y - \sum_{i=1}^n \left\lfloor \frac{x_i + y_i}{p_i} \right\rfloor \times m_i. \quad (6)$$

Определим минимальные числа M_i :

$$\begin{aligned} M_1 &= (1, 1, \dots, 1), \\ M_2 &= (0, p_1, p_1, \dots, p_1), \\ M_3 &= (0, 0, p_1 \times p_2 \pmod{p_3}, \\ & p_1 \times p_2 \pmod{p_4}, \dots, p_1 \times p_2 \pmod{p_n}), \\ M_4 &= (0, 0, 0, p_1 \times p_2 \times p_3 \pmod{p_4}, \\ & p_1 \times p_2 \times p_3 \pmod{p_5}, \dots, \\ & p_1 \times p_2 \times p_3 \pmod{p_n}) \text{ и т. д.} \end{aligned} \quad (7)$$

Далее нужно определить ранги r_1, r_2, r_3, r_4, r_5 минимальных чисел M_1, M_2, M_3, M_4, M_5 по формуле:

$$X = \sum_{i=1}^n x_n \times B_i - r_X \times P. \quad (8)$$

Для этого нужно определить ортогональные базисы по формуле:

$$B_i = \frac{m_i \times P}{p_i} = m_i \times P_i, \quad i = 1, 2, \dots, n, \quad (9)$$

где m_i – целые положительные числа, которые называются весами базиса. Их определяют из сравнений:

$$P_i \times m_i \equiv 1 \pmod{p_i}. \quad (10)$$

$$P_i = \frac{P}{p_i}. \quad (11)$$

Далее к числу X нужно прибавить число M_i столько раз, сколько потребуется для того, чтобы цифра числа X по основанию p_i стала равной нулю. В результате получим число $(0, 0, 0, \dots, 0)$, равное P , ранг которого равен -1 . С другой стороны, расчетный ранг этого числа равен $r_X + \omega_n$, где ω_n – известная нам величина. Откуда вытекает, что:

$$r_x = -\omega_n - 1. \quad (12)$$

$$m_3 = (-1)^n \times F_{n-1} \times 1(\text{mod } p_3), \quad (14)$$

Если k известно, то искомый остаток $|X|_k$ вычисляется по формуле:

$$|X|_k = \left| \left(\sum_{i=1}^n |P_i|_k |x_i \times m_i|_k \right) - |k|P|_k \right|_k. \quad (13)$$

Пример 1. Пусть задана МСС $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$ и число $X = (36, 4, 0, 4, 36)$. Мощность диапазона модулярной системы счисления равна $P = p_1 \times p_2 \times p_3 \times p_4 \times p_5 = 37778931511113441116160$. Необходимо промасштабировать коэффициентом $K = 33053$.

Для заданных модулей и коэффициента масштабирования заранее рассчитываются: $|P|_K = |37778931511113441116160 \times 33053|_K = 13863$.

Применяя формулу (11), вычислим P_i :

$$\begin{aligned} P_1 &= \frac{P}{p_1} = \frac{37778931511113441116160}{32765} = \\ &= 1153027056649273344, \\ P_2 &= \frac{P}{p_2} = \frac{37778931511113441116160}{32767} = \\ &= 1152956679314964480, \\ P_3 &= \frac{P}{p_3} = \frac{37778931511113441116160}{32768} = \\ &= 1152921493869428745, \\ P_4 &= \frac{P}{p_4} = \frac{37778931511113441116160}{32769} = \\ &= 1152886310571376640, \\ P_5 &= \frac{P}{p_5} = \frac{37778931511113441116160}{32771} = \\ &= 1152815950416936960. \end{aligned}$$

Веса базисов вычислим по формуле (10). Для нашего случая:

$$115292149386948745 \times m_3 \equiv 1(\text{mod } 32768).$$

Вычислить m_3 можно, применив метод цепных дробей. Приведем описание:

$$P_3 \times m_3 \equiv 1(\text{mod } p_3),$$

где $F_0 = q_0$, $F_1 = q_0 \times q_1 + 1$, ..., $F_n = q_n \times F_{n-1} + F_{n-2}$,

$$\begin{aligned} \frac{p_3}{P_3} &= \frac{32768}{1152921493869428745} = [q_0, q_1, \\ &q_2, q_3, q_4] = [0, 35184371761152, 3640, 1, 8], \\ &\frac{1}{35184371761152 + \frac{1}{3640 + \frac{1}{1 + \frac{1}{8}}}}. \end{aligned}$$

Поскольку последний элемент q_4 и индекс равен 4, то $n = 4$.

Тогда:

$$\begin{aligned} m_3 &= (-1)^n \times F_{n-1} \times 1(\text{mod } p_1) = (-1)^4 F_{4-1} \times \\ &\times 1(\text{mod } 32768) = 1 \times F_3 \times 1(\text{mod } 32768) = \\ &= 1 \times 3641 \times 1(\text{mod } 32768) = 3641, \\ F_3 &= q_3 \times F_{3-1} + F_{3-2} = q_3 \times F_3 + F_1 = \\ &= q_3(q_2(q_0 \times q_1 + 1) + q_0) + q_0 \times q_1 + 1 = \\ &= 1(35184371761152 + 1) + 0 + 0 \times \\ &\times 35184371761152 + 1 = 3641, \\ 1152921493869428745 \times m_3 &\equiv 3641(\text{mod } 32768), \\ m_3 &= 3641(\text{mod } 32768) = 3641. \end{aligned}$$

Аналогично вычислим m_1 , m_2 , m_4 , m_5 , получим:

$$m_1 = 9784, m_2 = 30719, m_4 = 2048, m_5 = 19344.$$

Определим ортогональные базисы по формуле (9):

$$\begin{aligned} B_1 &= m_1 \times P_1 = 9784 \times 1153027056649273344 = \\ &= 11281216722256490397696, \\ B_2 &= m_2 \times P_2 = 30719 \times 1152956679314964480 = \\ &= 3541767631876393861120, \\ B_3 &= m_3 \times P_3 = 3641 \times 1152921493869428745 = \\ &= 4197787159178590060545, \\ B_4 &= m_4 \times P_4 = 2048 \times 1152886310571376640 = \\ &= 2361111164050179358720, \\ B_5 &= m_5 \times P_5 = 19344 \times 1152815950416936960 = \\ &= 22300071744865228554240. \end{aligned}$$

Вычислим $|P_i|_K$:

$$\begin{aligned} |P_1|_K &= |1153027056649273344|_{33053} = 5380, \\ |P_2|_K &= |1152956679314964480|_{33053} = 9347, \\ |P_3|_K &= |1152921493869428745|_{33053} = 3697, \\ |P_4|_K &= |1152886310571376640|_{33053} = 28267, \\ |P_5|_K &= |1152815950416936960|_{33053} = 9714. \end{aligned}$$

Вычислим $|K^{-1}|_{p_i}$:

$$\begin{aligned} |K^{-1}|_{p_1} &= |33053^{-1}|_{32765} = 4892, \\ |K^{-1}|_{p_2} &= |33053^{-1}|_{32767} = 22112, \\ |K^{-1}|_{p_3} &= |33053^{-1}|_{32768} = 18741, \\ |K^{-1}|_{p_4} &= |33053^{-1}|_{32769} = 11423, \\ |K^{-1}|_{p_5} &= |33053^{-1}|_{32771} = 4997. \end{aligned}$$

Вычислим $c_i = |x_i \times m_i|_{p_i}$:

$$\begin{aligned} X &= (x_1, x_2, x_3, x_4) = (36, 4, 0, 4, 36), \\ c_1 &= |x_1 \times m_1|_{p_1} = |36 \times 9784|_{32765} = 24574, \\ c_2 &= |x_2 \times m_2|_{p_2} = |4 \times 30719|_{32767} = 24575, \\ c_3 &= |x_3 \times m_3|_{p_3} = |0 \times 3641|_{32768} = 0, \\ c_4 &= |x_4 \times m_4|_{p_4} = |4 \times 2048|_{32769} = 8192, \\ c_5 &= |x_5 \times m_5|_{p_5} = |36 \times 19344|_{32771} = 8193. \end{aligned}$$

Тогда, применяя формулу (4):

$$\begin{aligned} k_{low} &= [\nabla(24574 \nabla 32765 + 24575 \nabla 32767 + \\ &+ 0 \nabla 32768 + 8192 \nabla 32769 + 8193 \nabla 32771)] = \\ &= [\nabla(0, 75 + 0, 74 + 0 + 0, 24 + 0, 25)] = [\nabla 1, 98] = 1, \\ k_{upp} &= [\Delta(24574 \Delta 32765 + 24575 \Delta 32767 + \\ &+ 0 \Delta 32768 + 8192 \Delta 32769 + 8193 \Delta 32771)] = \\ &= [\Delta(0, 75 + 0, 75 + 0 + 0, 25 + 0, 25)] = [\Delta 2] = 2. \end{aligned}$$

Поскольку $k_{low} \neq k_{upp}$, это свидетельствует о том, что точность вычисления S_{low} и S_{upp} недостаточна для однозначного определения k . В этом случае вычисляется ранг $r(X)$ [5].

Вычислим минимальные числа M_i по формуле (7):

$$\begin{aligned} M_1 &= (1, 1, 1, 1, 1), \\ M_2 &= (0, 32765, 32765, 32765, 32765), \\ M_3 &= (0, 0, 32765 \times 32767 \pmod{32768}, \\ &32765 \times 32767 \pmod{32769}, \\ &32765 \times 32767 \pmod{32771}) = (0, 0, 3, 8, 24), \\ M_4 &= (0, 0, 0, 32765 \times 32767 \times 32768 \pmod{32769}, \\ &32765 \times 32767 \times 32768 \pmod{32771}) = \\ &= (0, 0, 0, 32761, 32699), \\ M_5 &= (0, 0, 0, 0, 32765 \times 32767 \times 32768 \times \\ &\times 32769 \pmod{32771}) = (0, 0, 0, 0, 144). \end{aligned}$$

Определим ранги r_1, r_2, r_3, r_4, r_5 минимальных чисел M_1, M_2, M_3, M_4, M_5 по формуле (8):

$$\begin{aligned} M_1 &= (1, 1, 1, 1, 1) = 1 \times B_1 + 1 \times B_2 + 1 \times B_3 + 1 \times B_4 + \\ &+ 1 \times B_5 = 1 \times 11281216722256490397696 + \\ &+ 1 \times 35417676231876393861120 + \\ &+ 1 \times 4197797159178590060545 + \\ &+ 1 \times 2361111164050179358720 + \\ &+ 1 \times 22300071744865228554240 = \\ &= 75557863022226882232321 \\ &\pmod{37778931511113441116160} = 1, \end{aligned}$$

тогда $1 = 75557863022226882232321 - r_1 \times 37778931511113441116160$, выражаем r_1 :

$$\begin{aligned} r_1 \times 37778931511113441116160 &= \\ &= 75557863022226882232320, \\ r_1 &= 2. \end{aligned}$$

$$\begin{aligned} M_2 &= (0, 32765, 32765, 32765, 32765) = 0 \times B_1 + \\ &+ 32765 \times B_2 + 32765 \times B_3 + 32765 \times B_4 + \\ &+ 32765 \times B_5 = 0 \times 11281216722256490397696 + \\ &+ 32765 \times 35417676231876393861120 + \\ &+ 32765 \times 4197787159178590060545 + \\ &+ 32765 \times 2361111164050179358720 + \\ &+ 32765 \times 22300071744865228554240 = \\ &= (0 + 1160460161737430044859596800 + \\ &+ 7306618507205509213579673600) \pmod{P} = \\ &= 2106024316018529888461488125 \\ &\pmod{37778931511113441116160} = 32765, \end{aligned}$$

тогда $32765 = 2106024316018529888461488125 - r_2 \times 37778931511113441116160$, выражаем r_2 :

$$\begin{aligned} r_2 \times 37778931511113441116160 &= \\ &= 2106024316018529888461455360, \\ r_2 &= 55746. \end{aligned}$$

$$\begin{aligned} M_3 &= (0, 0, 3, 8, 24) = 0 \times B_1 + 0 \times B_2 + \\ &+ 3 \times B_3 + 8 \times B_4 + 24 \times B_5 = \\ &= 0 \times 11281216722256490397696 + \\ &+ 0 \times 35417676231876393861120 + \\ &+ 24 \times 22300071744865228554240 = \\ &= (0 + 0 + 12593361477535770181635 + \\ &+ 18888889312401434869760 + \\ &+ 535201721876765485301760) \bmod P = \\ &= 566683972666702690353155 \\ &(\bmod 37778931511113441116160) = \\ &= 1073610755, \end{aligned}$$

тогда $1073610755 = 566683972666702690353155 - r_3 \times 37778931511113441116160$, выражаем r_3 :

$$\begin{aligned} r_3 \times 37778931511113441116160 &= \\ &= 566683972666701616742400, \\ r_3 &= 15. \end{aligned}$$

$$\begin{aligned} M_4 &= (0, 0, 0, 32761, 32699) = 0 \times B_1 + 0 \times B_2 + \\ &+ 0 \times B_3 + 32761 \times B_4 + 32699 \times B_5 = \\ &= (0 \times 11281216722256490397696 + \\ &+ 0 \times 35417676231876393861120 + \\ &+ 0 \times 4197787159178590060545 + \\ &+ 32761 \times 2361111164050179358720 + \\ &+ 32699 \times 22300071744865228554240) \bmod P = \\ &= (0 + 0 + 0 + 77352362845447925971025920 + \\ &+ 729190045985348108495093760) \bmod P = \\ &= 806542408830796034466119680 \\ &(\bmod 37778931511113441116160) = \\ &= 35180077219840, \end{aligned}$$

тогда $35180077219840 = 806542408830796034466119680 - r_4 \times 37778931511113441116160$, выражаем r_4 :

$$\begin{aligned} r_4 \times 37778931511113441116160 &= \\ &= 806542408830760854388899840, \\ r_4 &= 21349. \end{aligned}$$

$$\begin{aligned} M_5 &= (0, 0, 0, 0, 144) = 0 \times B_1 + 0 \times B_2 + \\ &+ 0 \times B_3 + 0 \times B_4 + 144 \times B_5 = \\ &= (0 \times 11281216722256490397696 + \\ &+ 0 \times 35417676231876393861120 + \\ &+ 0 \times 4197787159178590060545 + \\ &+ 0 \times 2361111164050179358720 + \\ &+ 144 \times 22300071744865228554240) \bmod P = \\ &= (0 + 0 + 0 + 0 + 3211210331260592911810560) \\ &\bmod P = 3211210331260592911810560 \\ &(\bmod 37778931511113441116160) = \\ &= 1152815950416936960, \end{aligned}$$

тогда $1152815950416936960 = 3211210331260592911810560 - r_5 \times 37778931511113441116160$, выражаем r_5 :

$$\begin{aligned} r_5 \times 37778931511113441116160 &= \\ &= 3211209178444642494873600, \\ r_5 &= 85. \end{aligned}$$

Далее найдем ранг числа $X = (36, 4, 0, 4, 36)$. Проведем обнуление остатка $x_1 = 3$ по первому модулю $p_1 = 32765$.

Сложим число X с M_1 :

$$\begin{aligned} X + M_1 &= (36, 4, 0, 4, 36) + (1, 1, 1, 1, 1) = \\ &= (37, 5, 1, 5, 37). \end{aligned}$$

Ранг суммы определяется по формуле (6):

$$\begin{aligned} r &= (r_A + 2) - \left\{ \left[\frac{36+1}{32765} \right] \times 9784 + \right. \\ &+ \left[\frac{4+1}{32767} \right] \times 30719 + \left[\frac{0+1}{32768} \right] \times 3641 + \\ &+ \left. \left[\frac{4+1}{32769} \right] \times 2048 + \left[\frac{36+1}{32771} \right] \times 19344 \right\} = \\ &= (r_A + 2) - (37 \times 9784 + 5 \times 30719 + 1 \times 3641 + \\ &+ 5 \times 2048 + 19344 \times 37) = r_A + 2 - 1245212 = \\ &= r_A - 1245210. \end{aligned}$$

Так как остаток $x_1 = 3$ числа $(36, 4, 0, 4, 36)$ не обнулился, сложим два числа:

$$\begin{aligned} (37, 5, 1, 5, 37) + (1, 1, 1, 1, 1) &= \\ &= (38, 6, 2, 6, 38). \end{aligned}$$

Ранг суммы двух чисел определим следующим образом:

$$\begin{aligned} r &= (r_A + 2) + r_1 - \left\{ \left[\frac{37+1}{32765} \right] \times 9784 + \right. \\ &+ \left[\frac{5+1}{32767} \right] \times 30719 + \left[\frac{1+1}{32768} \right] \times 3641 + \\ &+ \left. \left[\frac{5+1}{32769} \right] \times 2048 + \left[\frac{37+1}{32771} \right] \times 19344 \right\} = \\ &= r_A + 2 - 1245210 - (38 \times 9784 + 6 \times 30719 + \\ &+ 2 \times 3641 + 6 \times 2048 + 19344 \times 38) = \\ &= r_A + 2 - 1245210 - 1310748 = r_A - 2555956. \end{aligned}$$

Аналогично, продолжая обнуление остатка $x_1 = 3$, в конечном итоге получим число $(0, 32733, 32729, 32733, 32765)$, $r = r_A + 55674$.

Обнуление остатка $x_2 = 4$ по второму модулю $p_2 = 32767$ числа $(0, 32733, 32729, 32733, 32765)$.

Сложим два числа:

$$\begin{aligned} &(0, 32733, 32729, 32733, 32765) + M_2 = \\ &= (0, 32733, 32729, 32733, 32765) + \\ &+ (0, 32765, 32765, 32765, 32765) = \\ &= (0, 32731, 32726, 32739, 32759). \end{aligned}$$

Ранг суммы двух чисел определим следующим образом:

$$\begin{aligned} r &= (r_A + 55674) + 55746 - \left\{ \left[\frac{0+0}{32765} \right] \times 9784 + \right. \\ &+ \left[\frac{32733+32765}{32767} \right] \times 30719 + \\ &+ \left[\frac{32729+32765}{32768} \right] \times 3641 + \\ &+ \left[\frac{32733+32765}{32769} \right] \times 2048 + \\ &+ \left. \left[\frac{32765+32765}{32771} \right] \times 19344 \right\} = (r_A + 55674) + \\ &+ 55746 - (0 \times 9784 + 32731 \times 30719 + \\ &+ 32726 \times 3641 + 32729 \times 2048 + 32759 \times 19344) = \\ &= (r_A + 55674) + 55746 - 1825338043 = \\ &= r_A - 1825226623. \end{aligned}$$

Аналогично, продолжая обнуление остатка $x_2 = 4$, в конечном итоге получим число $(0, 0, 15, 40, 120)$, $r = r_A + 39$.

В конечном итоге необходимо провести обнуление всех остатков числа X .

Для остатка $x_3 = 0$ получим число $(0, 0, 0, 32761, 32699)$, $r = r_A + 21313$.

Для остатка $x_4 = 4$ получим число $(0, 0, 0, 0, 144)$, $r = r_A + 49$.

Для остатка $x_5 = 36$ получим число $(0, 0, 0, 0, 0)$, $r = r_A - 37$.

Применяя формулу (12), получим:

$$\begin{aligned} r_A - 37 &= -1, \\ r_A &= 36. \end{aligned}$$

Ранг связан с искомым k следующим соотношением (5):

$$\begin{aligned} k &= 36 - \left(\left[\frac{36 \times 9784}{32765} \right] + \left[\frac{4 \times 30719}{32767} \right] + \right. \\ &+ \left. \left[\frac{0 \times 3641}{32768} \right] + \left[\frac{4 \times 2048}{32769} \right] + \left[\frac{36 \times 19344}{32771} \right] \right) = \\ &= 36 - ([10, 75 + 3, 74 + 0 + 0, 24 + 21, 25]) = \\ &= 36 - 34 = 2. \end{aligned}$$

Следовательно, $k = 2$. Найдем $|X|_K$ по формуле (13):

$$\begin{aligned} |X|_K &= \left\| 5380 \times 24574 \right\|_{33053} + \\ &+ \left\| 9347 \times 24575 \right\|_{33053} + \left\| 3697 \times 0 \right\|_{33053} + \\ &+ \left\| 28267 \times 8192 \right\|_{33053} + \left\| 9714 \times 8193 \right\|_{33053} - \\ &- \left\| 2 \left\| 37778931511113441116160 \right\|_{33053} \right\|_{33053} \Big|_{33053} = \\ &= \left\| 29173 + 17228 + 0 + 26999 + 28231 - 8102 \right\|_{33053} = \\ &= \left\| 93529 \right\|_{33053} = 27423. \end{aligned}$$

Вычислим масштабированные остатки y_i в соответствии с формулой (15):

$$y_i = \left\| x_i - |X|_K \Big|_{p_i} \times |K^{-1}| \Big|_{p_i} \right\|_{p_i}. \quad (15)$$

$$y_1 = \left\| 36 - 27423 \right\|_{32765} \times \left\| 4892 \right\|_{32765} = 31646,$$

$$y_2 = \left\| 4 - 27423 \right\|_{32767} \times \left\| 22112 \right\|_{32767} = 31640,$$

$$y_3 = \left\| 0 - 27423 \right\|_{32768} \times 18741 \Big|_{32768} = 31637,$$

$$y_4 = \left\| 4 - 27423 \right\|_{32769} \times 11423 \Big|_{32769} = 31634,$$

$$y_5 = \left\| 36 - 27423 \right\|_{32771} \times 4997 \Big|_{32771} = 31628,$$

Таким образом, $Y = (31646, 31640, 31637, 31634, 31628) = 129941 = \left[\frac{4294967296}{33053} \right]$.

Метод с применением расширения системы оснований.

Для того, чтобы воспользоваться вторым методом, необходимо рассмотреть немодульную операцию расширения системы оснований [11, 12].

Задачу расширения системы оснований можно сформулировать следующим образом: найти остаточное представление числа по новому основанию (новым основаниям), если известно представление числа по другим основаниям, то есть найти остаток от деления на число, если известны остатки от деления на другие числа [14, 15].

Одним из путей решения поставленной задачи является перевод числа из МСС в обобщенную позиционную систему счисления (ОПСС) с дополнительным финальным шагом.

Расширение системы оснований с помощью характеристик ОПСС.

Пусть МСС состоит из оснований $p_1, p_2, \dots, p_n$. Объем диапазона этой системы будет равен $P = p_1 \times p_2 \times \dots \times p_n$. Добавим к числу оснований МСС новое основание $p_{(n+1)}$. Объем диапазона этой системы равен $\rho = p_1 \times p_2 \times \dots \times p_{(n+1)}$. Тогда любое число X из диапазона $[0; \rho)$ в ОПСС представимо в виде [15]:

$$X = a_{n+1} \times p_1 \times p_2 \times \dots \times p_n + a_n \times p_1 \times p_2 \times \dots \times p_{n-1} + \dots + a_3 \times p_1 \times p_2 + a_2 \times p_1 + a_1.$$

Если число X будет лежать в первоначальном диапазоне $[0; P)$, то в ОПСС цифра $a_{(n+1)} = 0$. Этот факт и используется для получения остатка от деления числа X на новое основание МСС $p_{(n+1)}$.

Пусть число X имело представление $(\alpha_1, \alpha_2, \dots, \alpha_n)$ по основаниям $p_1, p_2, \dots, p_n$. Добавим новое основание $p_{(n+1)}$, тогда число $x = (\alpha_1, \alpha_2, \dots, \alpha_n, |x|_{p_{n+1}})$ в системе осно-

ваний $p_1, p_2, \dots, p_n, p_{(n+1)}$, где $|x|_{p_{n+1}}$ – остаток от деления числа x на p_{n+1} , то есть искомая цифра по новому основанию.

Для определения этой цифры рассматриваем алгоритм перевода числа из МСС в ОПСС, включая проводимые операции неизвестную цифру $|x|_{p_{n+1}}$. При этом последовательно будем получать цифры ОПСС $a_1, a_2, \dots, a_n$ и выражения для цифры $a_{(n+1)}$. Но так как по предположению число $X \in [0; P)$, то цифра $a_{(n+1)} = 0$. Из полученного соотношения и определяем искомую цифру $|x|_{p_{n+1}}$ [16].

Вернемся к операции масштабирования чисел с применением расширения системы оснований. Масштабирование модулярных чисел выполняется на основании общего алгоритма масштабирования: пусть K – коэффициент масштабирования; Y – результат масштабирования числа X коэффициентом K ; тогда результат масштабирования вычисляется по формуле:

$$Y = \frac{X - |X|_K}{K}, \tag{16}$$

где $|X|_K$ – остаток от деления числа X по модулю K [15].

Для случая масштабирования модулярных чисел коэффициентом, взаимно простым с основаниями МСС, используется итерационный алгоритм на основе алгоритма, предложенного сингапурскими и австралийскими учеными [7–9].

1. Определение $|X|_K$, или так называемый этап расширения системы оснований, – получение остатка $|x|_{p_{n+1}}$ от деления числа, представленного в МСС остатками $x_1, x_2, \dots, x_n$ по модулям $p_1, p_2, \dots, p_n$, на число $p_{(n+1)} = K$.

2. Непосредственно масштабирование по каждому модулю выполняется по формуле (15):

$$y_i = \left\| x_i - |X|_{K|_{p_i}} \times |K^{-1}|_{p_i} \right\|_{p_i},$$

где $|K^{-1}|_{p_i}$ – мультипликативная инверсия по модулю p_i коэффициента K [9].

Пример 2. Пусть задана МСС $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$ и число $X = (36, 4, 0, 4, 36)$. Мощность диапазона модулярной системы счисления равна $P = p_1 \times p_2 \times p_3 \times p_4 \times p_5 = 37778931511113441116160$. Необходимо промасштабировать коэффициентом $K = 33053$.

На первом этапе расширим систему оснований $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$ числом $p_{(n+1)} = K = 33053$. Тогда число X в расширенной системе оснований будет иметь вид $X = (36, 4, 0, 4, 36, |x|_{33053})$.

Предварительно необходимо вычислить константы t_{kj} , используя формулу:

$$t_{kj} = \left| \frac{1}{pk} \right|_{p_j}, \quad (17)$$

$$t_{12} = \left| \frac{1}{p_1} \right|_{p_2} = \left| \frac{1}{32765} \right|_{32767} = 16383.$$

Опишем как вычислить $\left| \frac{1}{32765} \right|_{32767}$. Эта запись равносильна $\frac{1}{32765} \pmod{32767}$. Введем следующее обозначение:

$$\frac{1}{p_1} = x, \\ p_1 \times x \equiv 1 \pmod{p_2}.$$

То есть $p_1 \times x - 1 : m$.

Тогда:

$$\frac{1}{32765} = x.$$

Вычислим сравнение:

$$32765 \times x \equiv 1 \pmod{32767}.$$

Здесь можно воспользоваться алгоритмом цепных дробей.

$$1 + \frac{1}{16382 + \frac{1}{2}},$$

$$\frac{32767}{32765} = [q_0, q_1, q_2] = [1, 16382, 2],$$

$n = 2$, так как q_2 последний элемент,

$$x = (-1)^n \times F_{n-1} \times 1 \pmod{p_2} = \\ = (-1)^2 \times F_{2-1} \times 1 \pmod{32767} = \\ = 1 \times F_1 \times 1 \pmod{32767} = 16383 \pmod{32767} = \\ = 16383,$$

$$F_1 = q_0 \times q_1 + 1 = 1 \times 16382 + 1 = 16383.$$

Вернемся к нашему сравнению:

$$32765 \times x \equiv 1 \pmod{32767}.$$

Подставим $x = 16383$:

$$32765 \times 16383 \equiv 1 \pmod{32767}, \\ 536788995 \equiv 1 \pmod{32767}.$$

Действительно, $536788995 - 1 : 32767$.

То есть:

$$t_{12} = \left| \frac{1}{p_1} \right|_{p_2} = \left| \frac{1}{32765} \right|_{32767} = 16383.$$

Далее аналогично находим остальные константы t_{kj} .

$$t_{12} = \left| \frac{1}{32765} \right|_{32767} = 16383; t_{13} = \left| \frac{1}{32765} \right|_{32768} = 21845;$$

$$t_{14} = \left| \frac{1}{32765} \right|_{32769} = 8192; t_{15} = \left| \frac{1}{32765} \right|_{32771} = 27309;$$

$$t_{16} = \left| \frac{1}{32765} \right|_{33053} = 28118; t_{23} = \left| \frac{1}{32767} \right|_{32768} = 32767;$$

$$t_{24} = \left| \frac{1}{32767} \right|_{32769} = 16384; t_{25} = \left| \frac{1}{32767} \right|_{32771} = 24578;$$

$$t_{26} = \left| \frac{1}{32767} \right|_{33053} = 10748; t_{34} = \left| \frac{1}{32768} \right|_{32769} = 16384;$$

$$t_{35} = \left| \frac{1}{32768} \right|_{32771} = 21847; t_{36} = \left| \frac{1}{32768} \right|_{33053} = 14149;$$

$$t_{45} = \left| \frac{1}{32769} \right|_{32771} = 16385; t_{46} = \left| \frac{1}{32769} \right|_{33053} = 21531;$$

$$t_{56} = \left| \frac{1}{32771} \right|_{33053} = 28013.$$

Константы t_{kj} запишем в виде матрицы $k \times j$:

$$\begin{pmatrix} 0 & 16383 & 21845 & 8192 & 27309 & 28118 \\ 0 & 0 & 32767 & 16384 & 24578 & 10748 \\ 0 & 0 & 0 & 16384 & 21847 & 14149 \\ 0 & 0 & 0 & 0 & 16385 & 21531 \\ 0 & 0 & 0 & 0 & 0 & 28013 \end{pmatrix}.$$

Далее найдем $a_1, a_2, a_3, a_4, a_5, a_6$ по формулам (18):

$$\begin{aligned} a_1 &\equiv \alpha_1 \pmod{p_1}, \\ a_2 &\equiv (\alpha_2 - a_1) \times t_{12} \pmod{p_2}, \\ a_3 &\equiv ((\alpha_3 - a_1) \times t_{13} - a_2) \times t_{23} \pmod{p_3}, \\ &\vdots \\ a_n &\equiv (((\dots(\alpha_n - a_1) \times t_{1n} - a_2) - \dots - a_{n-1}) \times \\ &\quad \times t_{n-1n} \pmod{p_n}). \end{aligned} \quad (18)$$

$$\begin{aligned} X &= (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, |x|_{p_{n+1}}) = \\ &= (36, 4, 0, 4, 36, |x|_{33053}), \end{aligned}$$

$$p_1 = 32765, p_2 = 32767, p_3 = 32768, p_4 = 32769, \\ p_5 = 32771, p_6 = 33053.$$

$$\begin{aligned} a_1 &\equiv \alpha_1 \pmod{p_1} = 36 \pmod{32765} = 36, \\ a_2 &\equiv (\alpha_2 - a_1) \times t_{12} \pmod{p_2} = (4 - 36) \times \\ &\quad \times 16383 \pmod{32767} = -524256 \pmod{32767} = 16, \\ a_3 &\equiv ((\alpha_3 - a_1) \times t_{13} - a_2) \times t_{23} \pmod{p_3} = \\ &= ((0 - 36) \times 21845 - 16) \times 32767 \pmod{32768} = \\ &= -25769148412 \pmod{32768} = 4, \\ a_4 &\equiv (((\alpha_4 - a_1) \times t_{14} - a_2) \times t_{24} - a_3) \times t_{34} \pmod{p_4} = \\ &= (((4 - 36) \times 8192 - 16) \times 16384 - 4) \times \\ &\quad \times 16384 \pmod{32769} = -70373039210496 \\ &\quad \pmod{32769} = 0, \\ a_5 &\equiv (((((\alpha_5 - a_1) \times t_{15} - a_2) \times t_{25} - a_3) \times t_{35} - a_4) \times \\ &\quad \times t_{45}) \pmod{p_5} = (((36 - 36) \times 27309 - 16) \times \\ &\quad \times 24578 - 4) \times 21847 - 0) \times 16385 \pmod{32771} = \\ &= -140769703034940 \pmod{32771} = 0. \end{aligned}$$

Запишем результат в виде табл. 1.

Таблица 1

Промежуточные вычисления расширения системы оснований

Действия	Модули						Цифры ОПСС
	$p_1 = 32765$	$p_2 = 32767$	$p_3 = 32768$	$p_4 = 32769$	$p_5 = 32771$	$p_6 = 33053$	
$x - a_1$	36 36	4 36	0 36	4 36	36 36	$ x _{33053}$ 36	$a_1 = 36$
$x - a_1 \times t_{1j}$	0	32735 16383	32732 21845	32737 8192	0 27309	$ x _{33053} - 36$ 28118	
$x_1 - a_2$		16 16	12 16	8 16	0 16	$28118 x _{33053} +$ $+ 12395$ 16	$a_2 = 16$
$x_1 - a_2 \times t_{2j}$		0	32764 32767	32761 16384	32755 24578	$28118 x _{33053} +$ $+ 12379$ 10748	
$x_2 - a_3$			4 4	4 4	4 4	$8685 x _{33053} +$ $+ 11167$ 4	$a_3 = 4$
$x_2 - a_3 \times t_{3j}$			0	0 16384	0 21847	$8685 x _{33053} +$ $+ 11163$ 14149	
$x_3 - a_4$				0 0	0 0	$26064 x _{33053} +$ $+ 18053$ 0	$a_4 = 0$
$x_3 - a_4 \times t_{4j}$				0	0 16385	$26064 x _{33053} +$ $+ 18053$ 21531	
$x_4 - a_5$					0	$10150 x _{33053} +$ $+ 28916$ 0	$a_5 = 0$

Действия	Модули						Цифры ОПСС
	$p_1 = 32765$	$p_2 = 32767$	$p_3 = 32768$	$p_4 = 32769$	$p_5 = 32771$	$p_6 = 33053$	
$x_4 - a_5 \times t_{5j}$						$10150 x _{33053} + 28916$ 28013	
x_5						$10044 x _{33053} + 27090$	$a_6 = 10044 x _{33053} + 27090$

Примечание: составлено автором на основании данных, полученных в исследовании.

Поскольку $a_6 = 0$, то $10044|x|_{33053} + 27090 = 0$, $1044|x|_{33053} = -27090$, $|x|_{33053} = 27423$.

Расширенное представление числа $X = 4294967296 = (36, 4, 0, 4, 36, |x|_{33053}) = (36, 4, 0, 4, 36, 27423)$ по основаниям $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$, $p_6 = 33053$.

Таким образом, $|X|_K = 27423$.

На втором этапе вычислим масштабированные остатки y_i в соответствии с формулой (15).

Для этого вычислим $|K^{-1}|_{p_i}$:

$$|K^{-1}|_{p_1} = |33053^{-1}|_{32765} = 4892,$$

$$|K^{-1}|_{p_2} = |33053^{-1}|_{32767} = 22112,$$

$$|K^{-1}|_{p_3} = |33053^{-1}|_{32768} = 18741,$$

$$|K^{-1}|_{p_4} = |33053^{-1}|_{32769} = 11423,$$

$$|K^{-1}|_{p_5} = |33053^{-1}|_{32771} = 4997.$$

Тогда:

$$y_1 = \left\| 36 - 27423 \right\|_{32765} \times 4892 \Big|_{32765} = 31646,$$

$$y_2 = \left\| 4 - 27423 \right\|_{32767} \times 22112 \Big|_{32767} = 31640,$$

$$y_3 = \left\| 0 - 27423 \right\|_{32768} \times 18741 \Big|_{32768} = 31637,$$

$$y_4 = \left\| 4 - 27423 \right\|_{32769} \times 11423 \Big|_{32769} = 31634,$$

$$y_5 = \left\| 36 - 27423 \right\|_{32771} \times 4997 \Big|_{32771} = 31628,$$

Таким образом, $Y = (31646, 31640, 31637, 31634, 31628) = 129941 = \left[\frac{4294967296}{33053} \right]$.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

На высокоуровневом языке программирования Python разработаны алгоритмы выполнения рассмотренных выше немодульных операций. Ниже приведены фрагменты алгоритмов и результаты их работы (рис. 1–3).

```
##### Масштабирование чисел в МСС #####
##### Метод с использованием интервальных оценок #####
Base = [32765, 32767, 32768, 32769, 32771] M = 37778931511113441116160
X = (36, 4, 0, 4, 36)
scale_factor = 33053
4294967296
----- масштабирование с использованием интервальных оценок -----
pk = 4051
basis = [1153027056649273344, 1152956679314964480, 1152921493869428745, 1152886310571376640, 1152815950416936960]
weights = [9784, 30719, 3641, 2048, 19344]
pik = [5380, 9347, 3697, 28267, 9714]
k_inv = [4892, 22112, 18741, 11423, 4997]
c = [24574, 24575, 0, 8192, 8193]
s_low = 1.98 k_low = 1
s_upp = 2.02 k_upp = 2
k = 2
x_k = 27423
(31646, 31640, 31637, 31634, 31628)

##### Метод, с применением расширения системы оснований #####
Base = [32765, 32767, 32768, 32769, 32771] M = 37778931511113441116160
X = (36, 4, 0, 4, 36)
scale_factor = 33053
4294967296
new_res = (36, 4, 0, 4, 36, 27423)
k_inv = [4892, 22112, 18741, 11423, 4997]
(31646, 31640, 31637, 31634, 31628)
129941
```

Рис. 1. Результаты работы алгоритма «Масштабирование чисел в МСС»

Примечание: составлено автором на основании данных, полученных в исследовании.

```
----- Определение ранга по алгоритму -----
M = [[1, 1, 1, 1, 1], [0, 32765, 32765, 32765, 32765], [0, 0, 3, 8, 24], [0, 0,
0, 32761, 32699], [0, 0, 0, 0, 144]]
M_rank = [2, 55746, 15, 21349, 85]
[0, 32733, 32729, 32733, 32765] 55674
[0, 0, 15, 40, 120] 39
[0, 0, 0, 32761, 32699] 21313
[0, 0, 0, 0, 144] 49
[0, 0, 0, 0, 0] -37
rank (по алгоритму) = 36
```

Рис. 2. Результаты работы алгоритма «Вычисление ранга числа»

Примечание: составлено автором на основании данных, полученных в исследовании.

```
##### Расширение системы оснований с помощью характеристик ОПС #####
Base = [32765, 32767, 32768, 32769, 32771] M = 3777893151113441116160
(36, 4, 0, 4, 36)
----- расширение системы оснований -----
t_matrix = [[0, 16383, 21845, 8192, 27309, 28118], [0, 0, 32767, 16384, 24578,
10748], [0, 0, 0, 32768, 21847, 14149], [0, 0, 0, 0, 16385, 21531], [0, 0, 0, 0,
0, 28013]]
A_matrix = [36, 16, 4, 0, 0, 27090]
28118 x + 12395
8685 x + 11167
26064 x + 18053
10150 x + 28916
10044 x + 27090
(36, 4, 0, 4, 36, 27423)
4294967296
```

Рис. 3. Результаты работы алгоритма «Расширение системы оснований с помощью характеристик ОПС»

Примечание: составлено автором на основании данных, полученных в исследовании.

Сравнение математического описания и результатов разработанных алгоритмов показывают их совпадение, что подтверждает верность проведенных вычислений.

На третьем этапе была проведена оценка сложности разработанных алгоритмов.

Основным критерием эффективности методов выполнения немодульных операций в МСС является оценка асимптотической сложности – оценка сложности алгоритма с использованием предельного перехода при стремлении к бесконечности размерности входных данных.

В данной работе для обозначения оценки сложности алгоритмов используется O -нотация.

O -нотация определяет функцию, которая показывает, как будет изменяться вычислительная сложность алгоритма с изменением количества входных данных в худшем случае. Вычислительная сложность показывает, как изменится время исполнения и объем занятой памяти в зависимости от размера входных данных.

Введем обозначения: $O(n)$ – оценка количества операций, где n – количество модулярных оснований на входе алгоритма (m – максимальное основание МСС). В работе количество модулярных оснований равно 5, то есть $n = 5$, максимальное основание МСС $m = 32771$. Отразим это в табл. 2.

Таблица 2

Оценка сложности методов выполнения немодульных операций в МСС

Операции	Оценка количества	Общая сложность метода
Масштабирование чисел в МСС с использованием интервальных оценок		
Вычисление мультипликативной инверсии	$O(n)$ сложностью $O(\log^2(m))$	$O(n \times \log^2(m))$
Деление по модулю	$O(n)$	
Умножение	$O(n)$	
Сложение	$O(n)$	
Масштабирование чисел в МСС с применением расширения системы оснований		
Вычисление мультипликативной инверсии	$O(n^2)$ сложностью $O(\log^2(m))$	$O(n^2 \times \log^2(m))$
Деление по модулю	$O(n^2)$	
Умножение	$O(n^2)$	

Сложение	$O(n^2)$	
<i>Окончание табл. 2</i>		
Операции	Оценка количества	Общая сложность метода
Расширение системы оснований с помощью характеристик ОПСС		
Деление по модулю	$O(n^2)$	$O(n^2 \times \log^2(m))$
Умножение	$O(n^2)$	
Сложение	$O(n^2)$	
Вычисление мультипликативной инверсии	$O(n^2)$ сложностью $O(\log^2(m))$	
Вычисление ранга числа		
Умножение	$O(n)$	$O(n^2)$
Деление по модулю	$O(n^2)$	
Умножение	$O(n^2)$	
Сложение	$O(n^2)$	

Примечание: составлено автором на основании данных, полученных в исследовании.

ЗАКЛЮЧЕНИЕ

Рассмотрены алгоритмы масштабирования чисел в модулярной системе счисления. Алгоритмы используют произвольные наборы модулей, обеспечивающих вычисления в большом динамическом диапазоне. В качестве примера набора оснований МСС выбраны числа $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$ с мощностью диапазона $P = 37778931511113441116160$. Вычислительный диапазон близок к значению $2^{75} = 37778931862957161709568$. Для интерпретации результатов исследования на практике взяты числа $A = 2^{32} = 4294967296 = (36, 4, 0, 4, 36)$, $B = 2^{30} = 1073741824 = (9, 1, 0, 1, 9)$.

Первый алгоритм масштабирования чисел в МСС применяется для коэффициентов масштабирования произвольного вида, взаимно простых с основаниями МСС. Отличие его от известных алгоритмов состоит в использовании новой процедуры определения остатка от деления масштабируемого числа на коэффициент масштабирования, основанной на принципах интервальной арифметики [5]. Второй метод с расширением системы модулярных оснований более традиционный. Сравнивая оценки сложности методов, делаем вывод, что метод с использованием интервальных оценок является более эффективным.

Список источников

1. Исупов К. С. Методика выполнения базовых немодульных операций в модулярной арифметике с применением интервальных позиционных характеристик // Известия высших учебных заведений. Поволжский регион. Технические науки. 2013. № 3. С. 26–39.
2. Лавриненко А. Н., Червяков Н. И. Исследование немодульных операций в системе остаточных классов // Научные ведомости БелГУ. Серия: История. Политология. Экономика. Информатика. 2012. № 1, Вып. 21/1. С. 110–121.
3. Червяков Н. И., Авербух В. М., Бабенко М. Г. и др. Приближенный метод выполнения немодульных операций в системе остаточных классов // Фундаментальные исследования. 2012. № 6–1. С. 189–193.
4. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. М.: Советское радио, 1968. 439 с.
5. Исупов К. С., Князьков В. С., Куваев А. С. Эффективное масштабирование в системе остаточных классов с использованием интервальных оценок // Вычислительные технологии. 2018. Т. 23, № 3. С. 39–57.

References

1. Isupov K. S. Methods of Basic Non-Modular Operations in Modular Arithmetic Using Interval Positional Characteristics. University Proceedings. Volga Region. Technical Sciences. 2013. No. 3. P. 26–39. (In Russian).
2. Lavrienko A. N., Chervyakov N. I. Nomodal Operations Research in System of Residual Classes. Nauchnye vedomosti BelGU. Seriya: Istoriia. Politologiya. Ekonomika. Informatika. 2012. No. 1, Is. 21/1. P. 110–121. (In Russian).
3. Chervyakov N. I., Averbukh V. M., Babenko M. G. et al. Approximate Method of Implementation Non-Modular Operations in the Residue Number System. Fundamental Research. 2012. No. 6–1. P. 189–193. (In Russian).
4. Akushsky I. Ya., Yuditsky D. I. Mashinnaiia arifmetika v ostatochnykh klassakh. Moscow: Sovetskoe radio, 1968. 439 p. (In Russian).
5. Isupov K. S., Knyazkov V. S., Kuvaev A. S. Efficient Scaling in RNS Using Interval Estimations. Computational Technologies. 2018. Vol. 23, No. 3. P. 39–57. (In Russian).
6. Chervyakov N. I., Lavrienko I. N., Lavrienko S. V. et al. Metody i algoritmy okrugleniia, masshtabirovaniia i

6. Червяков Н. И., Лавриненко И. Н., Лавриненко С. В. и др. Методы и алгоритмы округления, масштабирования и деления чисел в модулярной арифметике // 50 лет модулярной арифметике : Юбилейн. (V) междунар. науч.-техн. конф., Зеленоград, 23–25 ноября 2005 г. Зеленоград : Ангстрем, 2006. С. 291–310.
7. Chang C. H., Low J. Y. S. Simple, Fast, and Exact RNS Scaler for The Three-Moduli Set ($2n - 1$, $2n$, $2n + 1$). IEEE Transactions on Circuits and Systems I: Regular Papers. 2011. Vol. 58, No. 11. P. 2686–2697.
8. Kong Y., Phillips B. Fast Scaling in the Residue Number System. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2009. Vol. 17, No. 3. P. 443–447.
9. Коржавина А. С., Князьков В. С. Метод умножения с масштабированием результата для высокоточных модулярно-позиционных интервально-логарифмических вычислений // Инженерные технологии и системы. 2019. Т. 29, № 2. С. 187–204.
10. Исупов К. С., Завиялов А. А. Об эффективности нового алгоритма вычисления ранга в системе остаточных классов // Advanced Science. 2017. № 4. С. 21.
11. Гапочкин А. В., Барбарян В. Г., Калмыков М. И. и др. Применение операции расширения системы оснований модулярного кода для обнаружения и коррекции ошибки // Успехи современного естествознания. 2014. № 11–2. С. 56–58.
12. Коржавина А. С., Князьков В. С. Методы расширения базиса в системе остаточных классов: обзор и анализ вычислительной сложности // Современные наукоемкие технологии. 2017. № 12. С. 37–42.
13. Исупов К. С. Метод выполнения немодульных операций в системе остаточных классов на основе интервальных позиционных характеристик // Фундаментальные исследования. 2013. № 4–3. С. 566–570.
14. Червяков Н. И. Методы масштабирования модулярных чисел, используемые при цифровой обработке сигналов // Инфокоммуникационные технологии. 2006. Т. 4, № 3. С. 15–24.
15. Червяков Н. И., Ляхов П. А., Копыткова Л. Б. и др. Обработка информации в системе остаточных классов (СОК). Ставрополь : Северо-Кавказ. федер. ун-т, 2016. 225 с.
16. Червяков Н. И. Нейронная сеть для расширения кортежа числовой системы вычетов : патент № 2256226 С2 Рос. Федерация, МПК G06N 3/04. № 2003124041/09 ; заявл. 30.07.2003 ; опубл. 10.07.2005 ; заявитель Ставропол. гос. ун-т. deleniia chisel v moduliarnoi arifmetike. 50 let moduliarnoi arifmetike : Proceedings of the Anniversary (V) International Scientific and Engineering Conference, Zelenograd, November 23–25, 2005. Zelenograd : Angstrom, 2006. P. 291–310. (In Russian).
7. Chang C. H., Low J. Y. S. Simple, Fast, and Exact RNS Scaler for The Three-Moduli Set ($2n - 1$, $2n$, $2n + 1$). IEEE Transactions on Circuits and Systems I: Regular Papers. 2011. Vol. 58, No. 11. P. 2686–2697.
8. Kong Y., Phillips B. Fast Scaling in the Residue Number System. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2009. Vol. 17, No. 3. P. 443–447.
9. Korzhavina A. S., Knyazkov V. S. The Multiplication Method with Scaling the Result for High-Precision Residue Positional Interval Logarithmic Computations. Engineering Technologies and Systems. 2019. Vol. 29, No. 2. P. 187–204. (In Russian).
10. Isupov K. S., Zaviyalov A. A. Ob effektivnosti novogo algoritma vychisleniia ranga v sisteme ostatochnykh klassov. Advanced Science. 2017. No. 4. P. 21. (In Russian).
11. Gapochkin A. V., Barbaryan V. G., Kalmykov M. I. et al. Application Operations Expansion System Bases Modular Code for Detection and Correction Errors. Advances in Current Natural Sciences. 2014. No. 11–2. P. 56–58. (In Russian).
12. Korzhavina A. S., Knyazkov V. S. Base Extension in Residue Number Systems: A Review and Cost Analysis. Modern High Technologies. 2017. No. 12. P. 37–42. (In Russian).
13. Isupov K. S. Method for Implementation Non-Modular Operations in RNS Based on Interval Positional Characteristic. Fundamental Research. 2013. No. 4–3. P. 566–570. (In Russian).
14. Chervyakov N. I. Methods of Scaling Modular of the Numbers, Used at Digital Processing Signals. Infokommunikatsionnye tekhnologii. 2006. Vol. 4, No. 3. P. 15–24. (In Russian).
15. Chervyakov N. I., Lyakhov P. A., Kopytkova L. B. et al. Obrabotka informatsii v sisteme ostatochnykh klassov (SOK). Stavropol : North-Caucasus Federal University, 2016. 225 p. (In Russian).
16. Chervyakov N. I. Neuron Network for Broadening Tuple of Numeric Subtractions System : Patent No. 2256226 C2 Russian Federation, IPS G06N 3/04. No. 2003124041/09 ; Claim of July 30, 2003 ; Published on July 10, 2005 ; Proprietor Stavropol State University. (In Russian).

Информация об авторе

Н. С. Золотарева – аспирант.

Information about the author

N. S. Zolotareva – Postgraduate.