*ISSN 2782-2001*
*Системы анализа и обработки данных*
*том 83, № 3, 2021, с. 75–86*

*http://journals.nstu.ru/vestnik*
*Analysis and data processing systems*
*Vol. 83, No. 3, 2021, pp. 75–86*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

INFORMATICS, COMPPUTER ENGINEERING AND CONTROL

УДК 53.088, 511.1

DOI: 10.17212/2782-2001-2021-3-75-86

# Сравнение чисел и анализ переполнения в модулярной арифметике*

**В.И. ГУЖОВ[a], И.О. МАРЧЕНКО[b], Е.Е. ТРУБИЛИНА[c], Д.С. ХАЙДУКОВ[d]**

*630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет*

[a] *av.guzhov@corp.nstu.ru* [b] *bi.o.marchenko@gmail.com* [c] *csilver-kate94@mail.ru* [d] *ddmitriyhaydukov@gmail.com*

Модулярная арифметика работает не с самим числом, а с его остатками от деления на некоторые целые числа. В модульной системе счисления, или системе счисления в остаточных классах, многоразрядное целое число в позиционной системе счисления представляется в виде последовательности нескольких позиционных чисел. Эти числа есть остатки (вычеты) от деления исходного числа на некоторые модули, являющиеся взаимно простыми числами. Преимущество модулярного представления состоит в возможности простого распараллеливания выполнения операций сложения, вычитания и умножения.

При параллельном выполнении арифметических операций применение модульной арифметики позволяет существенно сократить время вычислений. Тем не менее есть ряд недостатков модульного представления чисел, которые ограничивают возможность его использования. К ним относятся медленное преобразование чисел из модульного представления в позиционное, сложность сравнения чисел в модульном представлении, трудность выполнения операции деления, сложность определения наличия переполнения. Использование модульной арифметики оправдано, если существуют быстрые алгоритмы вычисления числа по набору остатков.

В настоящей статье представлен новый алгоритм восстановления чисел из модульного (модулярного) представления на основе разработанного авторами геометрического подхода на примере систем сравнений с двумя модулями. Показано, что в результате увеличения чисел в позиционном исчислении они последовательно меняются по спирали на поверхности двумерного тора. На основе данного подхода был разработан быстрый алгоритм сравнения чисел и алгоритм для определения переполнения при сложении и умножении чисел в модульном представлении.

Рассмотрение для многомерного случая возможно при анализе многомерного тора и исследовании поведения витков на его поверхности.

**Ключевые слова:** модульная арифметика, система сравнений, взаимно простые числа, переполнение, сравнение чисел, модуль, сравнимые по модулю числа, китайская теорема об остатках, переполнение при арифметических операциях

* *Статья получена 20 января 2021 г.*

## ВВЕДЕНИЕ

Суть модулярной (или модульной) арифметики заключается в проведении вычислений не с числом $a$, представленным в позиционной системе, а с остатками от деления числа на различные целые числа $m_i$ [1–5]:

$$b_i = a \bmod m_i \tag{1}$$

Зная набор остатков $(b_1, b_2 \ldots b_n)$, можно в некотором диапазоне однозначно представить и само число $a$.

Главное достоинство модулярного представления состоит в простоте выполнения и возможности простого распараллеливания выполнения операций сложения, вычитания и умножения [6]:

$$\begin{aligned}
&(b_1, b_2 \ldots b_n) + (c_1, c_2 \ldots c_n) = (b_1 + c_1) \bmod m_1, \ldots, (b_n + c_n) \bmod m_n \\
&(b_1, b_2 \ldots b_n) - (c_1, c_2 \ldots c_n) = (b_1 - c_1) \bmod m_1, \ldots, (b_n - c_n) \bmod m_n \\
&(b_1, b_2 \ldots b_n) * (c_1, c_2 \ldots c_n) = (b_1 \cdot c_1) \bmod m_1, \ldots, (b_n \cdot c_n) \bmod m_n
\end{aligned} \tag{2}$$

Использование модульной арифметики обеспечивает значительное ускорение вычислений при параллельном выполнении операций. К уменьшению общего времени выполнения приводит одновременное выполнение операций, которые связаны с разными модулями.

Тем не менее есть недостатки, ограничивающие использование модулярного представления. К ним относятся:

- медленное преобразование чисел из модульного представления в позиционное;
- сложность оценки большего или меньшего числа в модульном представлении;
- трудность выполнения операции деления;
- сложность определения наличия переполнения.

Таким образом, использование модульной арифметики оправдано, если существуют быстрые алгоритмы вычисления числа по набору остатков.

Если двум целым числам $a$ и $b$ отвечает одинаковый остаток $r$ от деления на некоторое целое число, то эти числа называются сравнимыми по модулю $m$. Для обозначения сравнимости чисел используется специальная операция ($\equiv$):

$$a \equiv b \bmod m. \tag{3}$$

Найдем решение системы:

$$\begin{aligned}
&X \equiv b_1 \ (\bmod m_1) \\
&X \equiv b_2 \ (\bmod m_2) \\
&\ldots \\
&X \equiv b_n \ (\bmod m_n)
\end{aligned} \tag{4}$$

Если числа $(m_1, m_2 \ldots m_n)$ являются ***взаимно простыми числами***, то в некотором диапазоне, определяемом их произведением, существует единственное решение [1, 2]:

$$X \equiv M_1 N_1 b_1 + M_2 N_2 b_2 + \ldots + M_n N_n b_n \bmod (m_1 m_2, \ldots, m_n), \tag{5}$$

где $M_s$ и $N_s$ определены из следующих условий:

$$m_1 m_2 \ldots m_n = M_s m_s \tag{6}$$

$$M_s N_s \equiv 1 (\bmod m_s). \tag{7}$$

Решение является единственным в диапазоне, который определяется произведением модулей $m_1 m_2, \ldots, m_n$.

Нахождение $X$ в формуле (5) требует $n$ умножений и $(n-1)$ операций сложения, вычисления необходимо производить с «длинными» числами (с бóльшим количеством разрядов, чем представление остатков).

В статье предлагается новый алгоритм сравнения модульных чисел и алгоритм определения переполнения при арифметических операциях на основе предложенного авторами геометрического подхода. Рассмотрение выполняется для системы сравнений с двумя модулями.

В качестве эталона в интерференционных измерительных системах используется длина волны лазерного излучения. Следствием этого является периодичность результатов фазовых измерений. Если исключить фазовую неоднозначность, можно увеличить динамический диапазон. В [7–9] приводится способ для восстановления абсолютных значений измеряемой величины интерференционными методами. Этот метод с использованием модульной арифметики получил название G–S-алгоритм [10–13]. Поэтому развитие данных методов играет важную роль не только для компьютерных технологий, но и для ряда инженерных задач.

## 1. БЫСТРЫЙ АЛГОРИТМ ОПРЕДЕЛЕНИЯ ПОЗИЦИОННОГО ЧИСЛА ПО НАБОРУ ОСТАТКОВ

Рассмотрим решение системы сравнений (4) для двух произвольных взаимно простых модулей. Например: $m_1 = 11$, $m_2 = 17$. В данном случае: $M_1 = 17$, $M_2 = 11$, $N_1 = 2$, $N_2 = 14$. Из (5) следует

$$X \equiv 17 \cdot 2\, b_1 + 11 \cdot 14\, b_2 \bmod (11 \cdot 17) = 34\, b_1 + 154\, b_2 \bmod (187). \tag{8}$$

Таблица всех возможных результатов будет иметь вид, показанный на рис. 1. Числа, соответствующие решениям, увеличиваются от $i = 0, m_2 - 1$ последовательно по диагоналям, показанным на рисунке.

| b1 \ b2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 154 | 121 | 88 | 55 | 22 | 176 | 143 | 110 | 77 | 44 | 11 | 165 | 132 | 99 | 66 | 33 |
| 1 | 34 | 1 | 155 | 122 | 89 | 56 | 23 | 177 | 144 | 111 | 78 | 45 | 12 | 166 | 133 | 100 | 67 |
| 2 | 68 | 35 | 2 | 156 | 123 | 90 | 57 | 24 | 178 | 145 | 112 | 79 | 46 | 13 | 167 | 134 | 101 |
| 3 | 102 | 69 | 36 | 3 | 157 | 124 | 91 | 58 | 25 | 179 | 146 | 113 | 80 | 47 | 14 | 168 | 135 |
| 4 | 136 | 103 | 70 | 37 | 4 | 158 | 125 | 92 | 59 | 26 | 180 | 147 | 114 | 81 | 48 | 15 | 169 |
| 5 | 170 | 137 | 104 | 71 | 38 | 5 | 159 | 126 | 93 | 60 | 27 | 181 | 148 | 115 | 82 | 49 | 16 |
| 6 | 17 | 171 | 138 | 105 | 72 | 39 | 6 | 160 | 127 | 94 | 61 | 28 | 182 | 149 | 116 | 83 | 50 |
| 7 | 51 | 18 | 172 | 139 | 106 | 73 | 40 | 7 | 161 | 128 | 95 | 62 | 29 | 183 | 150 | 117 | 84 |
| 8 | 85 | 52 | 19 | 173 | 140 | 107 | 74 | 41 | 8 | 162 | 129 | 96 | 63 | 30 | 184 | 151 | 118 |
| 9 | 119 | 86 | 53 | 20 | 174 | 141 | 108 | 75 | 42 | 9 | 163 | 130 | 97 | 64 | 31 | 185 | 152 |
| 10 | 153 | 120 | 87 | 54 | 21 | 175 | 142 | 109 | 76 | 43 | 10 | 164 | 131 | 98 | 65 | 32 | 186 |

*Рис. 1*. Порядок последовательного изменения чисел

*Fig. 1.* A sequential change order of numbers

Если продолжить выделенные на рис. 1 диагонали, то можно заметить, что при склейке верхней и нижней строк и левого и правого столбцов образуется тор [15], на поверхности которого решения системы сравнений (8) будут возрастать по спирали (рис. 2) от нуля до $m_1 m_2$.

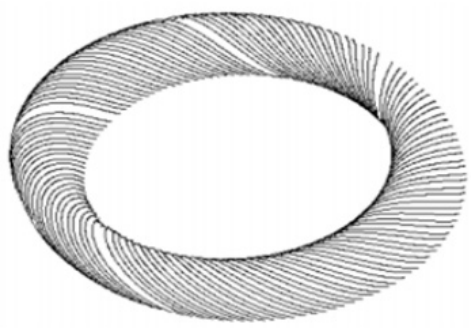

*Рис. 2.* Возрастание чисел при отображении на поверхности двумерного тора

*Fig. 2.* An increase in numbers when displayed on the surface of a two-dimensional torus

Для нахождения решений (8) достаточно определить начальное значения витка на поверхности тора и числа точек на этом витке [16, 17].

Для выбранного примера размер витка $m_1 = 11$. Число $X$ можно найти так:

$$X = n[i] \cdot m_1 + b_1, \tag{9}$$

где $i = 0, m_2 - 1$.

Для того чтобы определить число витков, можно воспользоваться выражением, следуемым из (5):

$$n[i] = M_2 N_2 \; i \bmod (m_1 m_2) = N_2 \; i \bmod (m_2), \tag{10}$$

или для конкретного случая $(m_1 = 11,\ m_2 = 17)$

$$n[i] = 14\, i \bmod (17), \quad i = 0,16. \tag{11}$$

На рис. 3 представлены начальные значения витков $n[i]$, которые определяются выражением (11).

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 11 | 8 | 5 | 2 | 16 | 13 | 10 | 7 | 4 | 1 | 15 | 12 | 9 | 6 | 3 |

*Рис. 3.* Значения витков $n[i]$. Первая строка $i = b_2$. Вторая строка – начальные значения витков

*Fig. 3*. Turn values $n[i]$. The first line is $i = b_2$. The second line is initial values of turns

Для столбцов аналогично:

$$n[i] = 2\, i \bmod (11), \quad i = 0,10. \tag{12}$$

Отложим начальные значения витков (рис. 4).

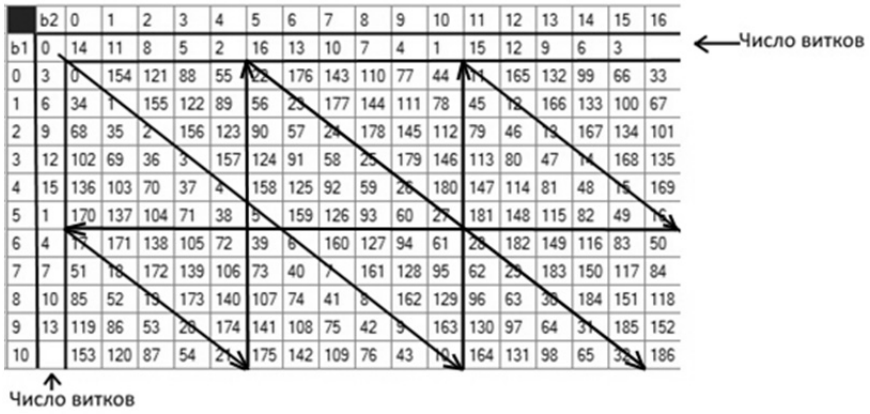


*Рис. 4.* Изменение чисел в таблице решений, начиная с начального значения витка (значения витков – вторая строка и второй столбец в таблице решений)

*Fig. 4.* Changing the numbers in the decision table, starting from the initial value of the iteration (the values of the iterations are the second row and the second column in the decision table)

Числа $X$ на рис. 5 изменяются от нуля до 186 (8). Число витков $n[i]$ изменяется от нуля до 16, т. е. максимальное число витков равно 16.

Так как таблица прямоугольная, то некоторые витки, значения для которых $b_2 - b_1 < 0$ (например, виток 1), заканчиваются на правом столбце и продолжаются на нулевом столбце, начиная со следующей строки (рис. 4). В таком случае таблицу решений можно представить в виде, в котором значения разорванных витков симметрично отображаются относительно главной диагонали (рис. 5).

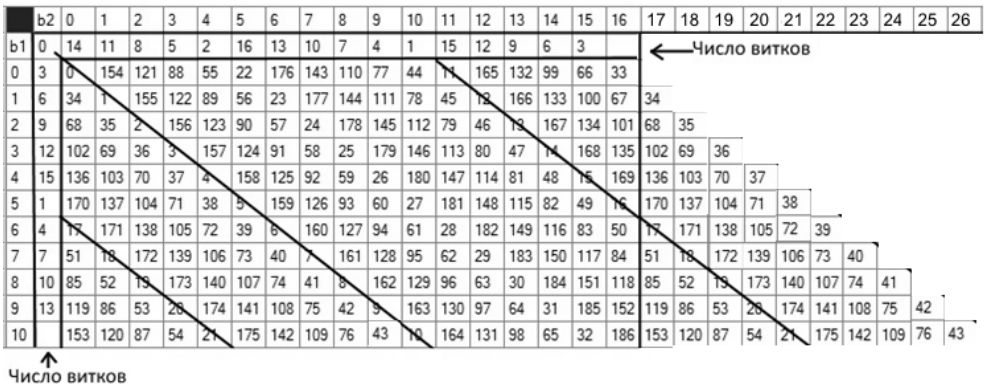


*Рис. 5.* Продолжение таблицы решений (выделены нулевой и первый витки)

*Fig. 5.* Continuation of the decision table (zero and first turns are highlighted)

Число витков можно определить по модульному представлению $(b_1, b_2)$:

$$n[b_1,b_2] = N_2(b_2 - b_1)\bmod(m_2), \quad \text{если} \quad b_2 - b_1 \geq 0; \tag{13}$$

$$n[b_1,b_2] = N_2(b_2 - b_1 + m_2)\bmod(m_2), \quad \text{если} \quad b_2 - b_1 < 0. \tag{14}$$

Например: $m_1 = 11$, $m_2 = 17$, $N_2 = 14$.

$b_2 - b_1 \geq 0$

$X = 27 \;=\; (5,\ 10)$

$$n(b_1,b_2) \;= N_2(b_2 - b_1)\bmod(m_2) = 14\cdot(10-5)\ (mod 17) = \ 2$$

$$X = n[b_1,b_2]\cdot m_1 + b_1 = 2\cdot 11 + 5 = 27$$

$X = 46 \;=\; (2,\ 12)$

$$n(b_1,b_2) \;= N_2(b_2 - b_1)\bmod(m_2) = 14\cdot(12-2)\ (mod 17) = \ 4$$

$$X = n[b_1,b_2]\cdot m_1 + b_1 = 4\cdot 11 + 2 = 46$$

$b_2 - b_1 < 0$

$X = 36 \;=\; (3,\ 2)$

$$n(b_1,b_2) \;= N_2(b_2 - b_1 + m_2)\bmod(m_2) = 14\cdot(2-3+17)\ (mod 17) = \ 3$$

$$X = n[b_1,b_2]\cdot m_1 + b_1 = 3\cdot 11 + 3 = 36$$

$X = 69 \;=\; (3,\ 1)$

$$n(b_1,b_2) \;= N_2(b_2 - b_1 + m_2)\bmod(m_2) = 14\cdot(-2+17)\ (mod 17) = \ 6$$

$$X = n[b_1,b_2]\cdot m_1 + b_1 = 6\cdot 11 + 3 = 69$$

С точки зрения упрощения число витков можно посчитать только один раз и записать в одномерном массиве размером $m_2$ (рис. 6). Индекс в этом массиве будет определяться как $(b_2 - b_1)$ или $(b_2 - b_1 + m_2)$ (13, 14).

На рис. 6 видно, что, зная число витков на торе (рис. 3), можно определить и само число *X*:

$$X = (b_1, b_2) = n(b_1, b_2) \cdot m_1 + b_1, \tag{15}$$

где $n$ является числом витков.

## 2. СРАВНЕНИЕ ЧИСЕЛ В МОДУЛЬНОМ ПРЕДСТАВЛЕНИИ

Для того чтобы сравнить два числа в модулярном представлении вычисляется число витков. Если число витков для одного из чисел больше, чем для другого, то данное число несомненно больше.

Например:

$b_2 - b_1 \geq 0$

$X = 27 \;=\; (5,\ 10) \rightarrow n(b_1, b_2) \;=\; 2$

$X = 46 \;=\; (2,\ 12) \rightarrow n(b_1, b_2) \;=\; 4$

$(2,\ 12) > (5,\ 10)$

$b_2 - b_1 < 0$

$X = 36 \;=\; (3,\ 2) \rightarrow n(b_1, b_2) \;=\; 3$

$X = 69 \;=\; (3,\ 1) \rightarrow n(b_1, b_2) \;=\; 6$

$(3,\ 1) > (3,\ 2)$

Если число витков одинаково, определяется положение числа на расширенной диагонали (по величине $b_1$).

Например:

$X = 13 \;=\; (2,\ 13) \rightarrow n(b_1, b_2) = 1 \quad b_1 = 2$

$X = 19 \;=\; (8,\ 2) \rightarrow n(b_1, b_2) = 1 \quad b_1 = 8$

$(8,\ 2) > (2,\ 13)$

Так, сравнение чисел в модулярном представлении выполняется достаточно просто.

При сложении или умножении может наступить **переполнение**. Переполнение возникает, если в результате выполнения арифметического действия число превышает максимальное.

## 3. ОПРЕДЕЛЕНИЕ ПЕРЕПОЛНЕНИЯ ПРИ СЛОЖЕНИИ ЧИСЕЛ В МОДУЛЬНОМ ПРЕДСТАВЛЕНИИ

Рассмотрим операцию сложения (2).

При сложении двух чисел в модульном представлении (15) с использованием подсчета числа витков

$$n(b_1,b_2)\cdot m_1 + b_1 + n(c_1,c_2)\cdot m_1 + c_1 = \left[n(b_1,b_2) + n(b_1,b_2)\right] + b_1 + c_1. \quad (16)$$

Если учитывать, что $b_1 + c_1$ максимально изменяются от нуля до $(2m_1 - 1)$, то сложение этих чисел может привести к увеличению числа витков на 1.

Так, при сложении двух чисел в модульном представлении переполнение наступит в следующих случаях:

1) если сумма числа витков больше максимального числа витков;

2) если $b_1 + c_1 \geq m_1$, то к сумме числа витков добавляется 1, а эта сумма превышает максимальное число витков.

Рассмотрим примеры, представленные в таблице. Максимальное число витков не может превышать 16.

**Сложение чисел в модульном представлении**

**Addition of numbers in modular representation**

| | | |
|---|---|---|
| Число витков | 11+16 = 27 | (0,11) + (5,16) = (5, 27) = (5, 10)<br>1 1 2 |
| | 21+21 = 42 | (10,4) + (10,4) = (20, 8) = (9, 8)<br>1 1 3 |
| | 143 +43 = 186 | (0,7) + (10,9) = (10, 16)<br>13 3 16 |
| | **144 +43 = 187** | **(1,8) + (10,9) = (11, 17) = (0, 0)**<br>**13 3 0** |

В таблице представлены значения чисел в модульной форме и значения витков. Полужирным шрифтом выделены примеры сложения чисел, когда наступает переполнение.

Рассмотрим, как определить переполнение при умножении.

## 4. ОПРЕДЕЛЕНИЕ ПЕРЕПОЛНЕНИЯ ПРИ УМНОЖЕНИИ ЧИСЕЛ В МОДУЛЬНОМ ПРЕДСТАВЛЕНИИ

Рассмотрим операцию умножения (2). При умножении в модульном представлении имеем

$$\left[n(b_1,b_2)\cdot m_1 + b_1\right]\cdot\left[n(c_1,c_2)\cdot m_1 + c_1\right] =$$

$$= \left[n(b_1,b_2)\cdot n(c_1,c_2)\cdot m_1\cdot m_1 + n(c_1,c_2)\cdot b_1\cdot m_1 + n(b_1,b_2)\cdot c_1\cdot m_1 + b_1c_1\right] \bmod m_1 =$$

$$= n(b_1,b_2)\cdot n(c_1,c_2)\cdot m_1 + n(c_1,c_2)\cdot b_1 n(b_1,b_2)\cdot c_1 + b_1c_1 = n_p m_1 + b_1c_1, \quad (17)$$

где число витков будет

$$n_p = n(b_1,b_2)\cdot n(c_1,c_2)\cdot m_1 + n(c_1,c_2)\cdot b_1 + n(b_1,b_2)\cdot c_1. \quad (18)$$

Так, при умножении двух чисел в модульном представлении переполнение наступит в следующих случаях:

1) если результирующее число витков больше максимального числа витков;

2) если $b_1c_1 \geq m_1$, то к сумме числа витков добавляется целая часть $\mathrm{int}\left[b_1c_1 / m_1\right]$, и эта сумма превышает максимальное число витков.

Например:

$$12 \cdot 13 = 156 \quad (1,12) \cdot (2,13) = (2,3)$$

$$b_1c_1 < m_1 \quad 2 < 11$$

$$n(1,12) = 1 \quad n(2,13) = 1 \quad n(2,3) = 14 \rightarrow n_p = 11 + 1 + 2 = 14.$$

В подобном случае переполнения не возникает.

$$51 \cdot 14 = 204 \quad (7,0) \cdot (4,4) = (6,0)$$

$$b_1c_1 > m_1 \quad 28 > 11 \quad \mathrm{int}\left[28 / 11\right] = 2$$

$$n(7,0) = 1 \quad n(4,4) = 0 \quad n(6,0) = 1 \rightarrow n_p = 16 + 2 > 16.$$

Возникает переполнение.

## ЗАКЛЮЧЕНИЕ

Использование модульной арифметики позволяет легко распараллелить выполнение операций, что приводит к резкому сокращению общего времени вычислений. Кроме того, использование модульных операций позволяет сократить размер разрядов чисел, что приводит к упрощению вычислительных устройств.

Основными недостатками модульного представления числа являются: медленное преобразование чисел из модульного представления в позиционное, сложность определения большего или меньшего числа в модулярном представлении, сложность проверки возникновения переполнения в результате математических операций.

В статье рассмотрен быстрый алгоритм восстановления чисел из модульного представления на основе представления решений системы сравнений в виде тора. Это позволяет упростить восстановление чисел с помощью нахождения числа витков и определения положения числа на этом витке.

На основе этого подхода разработаны быстрые алгоритмы сравнения чисел и алгоритмы определения переполнения при сложении и умножении чисел в модульном представлении.

Переход к многомерному случаю возможен при рассмотрении поведения витков на поверхности многомерного тора.

## СПИСОК ЛИТЕРАТУРЫ

1. *Бухштаб А.А.* Теория чисел. – М.: Просвещение, 1966. – 384 с.

2. *Виноградов И.М.* Основы теории чисел. – 8-е изд., испр. – М.: Наука, 1972. – 168 с.

3. *Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б.* Введение в теорию чисел. – 2-е изд. – М.: Изд-во МГУ, 1995. – 159 с.

4. *Сизый С.В.* Лекции по теории чисел. – М.: Физматлит, 2007. – 190 с.

5. *Осипов Н.Н.* Теория чисел. – Красноярск: ИКИТ СФУ, 2008. – 117 с.

6. *Кнут Д.Э.* Искусство программирования. Т. 2. Получисленные алгоритмы. – 3-е изд. – М.: Вильямс, 2007. – 832 с.

7. *Gushov V.I., Solodkin Yu.N.* Automatic processing of fringe patterns in integer interferometers // Optics and Lasers in Engineering. – 1991. – Vol. 14, iss. 4–5. – P. 311–324.

8. Solution of the problem of phase ambiguity by integer interferometry / V.I. Guzhov, S.P. Il'inykh, R.A. Kuznetsov, A.R. Vagizov // Optoelectronics, Instrumentation and Data Processing. – 2013. – Vol. 49, iss. 2. – P. 178–183.

9. *Гужов В.И., Солодкин Ю.Н.* Использование свойств целых чисел для расшифровки интерферограмм // Оптика и спектроскопия. – 1988. – Т. 65, № 6. – С. 1123–1128.

10. Measurement system based on multi wavelength interferometry for long gauge block calibration / M. Wengierow, L. Salbut, Z. Ramotowski, R. Szumski, K. Szykiedans // Metrology and Measurement Systems. – 2013. – Vol. 20, iss. 3. – P. 479–490.

11. *Zhong J., Zhang Y.* Absolute phase-measurement technique based on number theory in multifrequency grating projection profilometry // Applied Optics. – 2001. – Vol. 40, N 4. – P. 492–500.

12. *Kujawińska M., Osten W.* Fringe pattern analysis methods: up-to-date review // Proceedings SPIE. – 1998. – Vol. 3407. – P. 56–66.

13. Frequency-multiplex Fourier-transform profilometry: a single-shot three-dimensional shape measurement of objects with large height discontinuities and/or surface isolations / M. Takeda, Q. Gu, M. Kinoshita, H. Takai, Y. Takahashi // Applied Optics. – 1997. – Vol. 36, N 22. – P. 5347–5354.

14. *Арнольд И.В.* Теоретическая арифметика. – М.: Учпедгиз, 1938. – 480 с.

15. *Гильберт Д., Кон-Фоссен С.* Наглядная геометрия. – М.: Наука, 1981. – 344 с.

16. *Гужов В.И., Кабак Е.С., Орлов И.С.* Использование модулярной арифметики при фазовых измерениях // Автоматика и программная инженерия. – 2015. – № 1 (1). – С. 97–107.

17. *Гужов В.И.* Методы измерения 3D профиля объектов. Фазовые методы: учебное пособие. – Новосибирск: Изд-во НГТУ, 2016. – 83 с.

*Гужов Владимир Иванович*, доктор технических наук, профессор кафедры систем сбора и обработки данных (ССОД) Новосибирского государственного технического уиверситета. Направление научных исследований – высокоточные оптические измерительные системы. Автор более 268 публикаций. E-mail: v.guzhov@corp.nstu.ru

*Марченко Илья Олегович*, кандидат технических наук, доцент кафедры ССОД. Направление исследований – бесконтактное измерение методами структурированного освещения. Автор 40 публикаций. E-mail: i.o.marchenko@gmail.com

*Трубилина Екатерина Евгеньевна*, аспирант, ассистент кафедры ССОД. Направление исследований – структурированное освещение. Имеет 16 публикаций. E-mail: silverkate94@mail.ru

*Хайдуков Дмитрий Сергеевич*, кандидат технических наук, ассистент кафедры ССОД. Автор более 30 работ. Область научных интересов: голография, бесконтактное измерение деформаций. E-mail: dmitriyhaydukov@gmail.com

*Guzhov Vladimir I.*, D.Sc. (Eng.), professor at the department of data collection and data processing systems, NSTU. The main field of his scientific research is high-precision measuring systems. He is the author of more than 268 publications. Email: v.guzhov@corp.nstu.ru

*Marchenko Ilya O.*, Ph.D, associate professor at the department of data collection and data processing systems. The main field of research is a non-contact measurement by the methods of struc-tured lighting. He is the author of 40 publications. E-mail: i.o.marchenko@gmail.com

*Trubilina Ekaterina E.*, postgraduate student, assistant of the data collection and data processing systems department. The main field of research is structured lighting. She has 16 publications. Email: sil-ver-kate94@mail.ru

*Khaidukov Dmitry*, Ph.D, assistant, Department SSOD. He is the author of more than 30 works. Re-search interests: holography, contactless measurement of deformations. E-mail: dmitriyhaydu-kov@gmail.com

DOI: 10.17212/2782-2001-2021-3-75-86

## *Comparison of numbers and analysis of overflow in modular arithmetic*[*]

*V.I. GUZHOV[a], I.O. MARCHENKO[b], E.E. TRUBILINA[c], D.S. KHAIDUKOV[d]*

*Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation*

[a] *av.guzhov@corp.nstu.ru* [b] *bi.o.marchenko@gmail.com* [c] *csilver-kate94@mail.ru*
[d] *ddmitriyhaydukov@gmail.com*

**Abstract**

The method of modular arithmetic consists in operating not with a number, but with its remainders after division by some integers. In the modular number system or the number system in the residual classes, a multi-bit integer in the positional number system is represented as a sequence of several positional numbers. These numbers are the remainders (residues) of dividing the original number into some modules that are mutually prime integers. The advantage of the modular representation is that it is very simple to perform addition, subtraction and multiplication operations.

In parallel execution of operations, the use of modular arithmetic can significantly reduce the computation time. However, there are drawbacks to modular representation that limit its use. These include a slow conversion of numbers from modular to positional representation; the complexity of comparing numbers in modular representation; the difficulty in performing the division operation; and the difficulty of determining the presence of an overflow. The use of modular arithmetic is justified if there are fast algorithms for calculating a number from a set of remainders.

This article describes a fast algorithm for converting numbers from modular representation to positional representation based on a geometric approach. The review is carried out for the case of a comparison system with two modules. It is also shown that as a result of increasing numbers in positional calculus, they successively change in a spiral on the surface of a two-dimensional torus.

Based on this approach, a fast algorithm for comparing numbers and an algorithm for detecting an overflow during addition and multiplication of numbers in modular representation were developed.

Consideration for the multidimensional case is possible when analyzing a multidimensional torus and studying the behavior of the turns on its surface.

**Keywords:** modular arithmetic, comparison system, coprime integers, overflow, comparison of numbers, module, numbers comparable in absolute value, Chinese Remainder Theorem, overflow during arithmetic operations

[*] *Received 20 January 2021.*

## REFERENCES

1. Bukhshtab A.A. *Teoriya chisel* [The theory of numbers]. Moscow, Prosveshchenie Publ., 1966. 384 p.

2. Vinogradov I.M. *Osnovy teorii chisel* [Fundamentals of the theory of numbers]. 8th ed. Moscow, Nauka Publ., 1972. 168 p.

3. Galochkin A.I., Nesterenko Yu.V., Shidlovskii A.B. *Vvedenie v teoriyu chisel* [Introduction to the theory of numbers]. Moscow, MSU Publ., 1995. 159 p.

4. Sizyi S.V. *Lektsii po teorii chisel* [Lectures on the theory of numbers]. Moscow, Fizmatlit Publ., 2007. 190 p.

5. Osipov N.N. Teoriya chisel [The theory of numbers]. Krasnoyarsk, SibFU Institute of space and information technologies Publ., 2008. 117 p.

6. Knuth D. *Iskusstvo programmirovaniya*. T. 2. *Poluchislennye algoritmy* [The art of computer programming. Vol. 2. Seminumerical algorithms]. 3rd ed. Moscow, Vil'yams Publ., 2007. 832 p. (In Russian).

7. Gushov V.I., Solodkin Yu.N. Automatic processing of fringe patterns in integer interferometers. *Optics and Lasers in Engineering*, 1991, vol. 14, iss. 4–5, pp. 311–324.

8. Guzhov V.I., Il'inykh S.P., Kuznetsov R.A., Vagizov A.R. Solution of the problem of phase ambiguity by integer interferometry. *Optoelectronics, Instrumentation and Data Processing*, 2013, vol. 49, iss. 2, pp. 178–183.

9. Guzhov V.I., Solodkin Yu.N. Ispol'zovanie svoistv tselykh chisel dlya rasshifrovki interferogramm [Using the properties of integer numbers to decrypt interferograms]. *Optika i spektroskopiya = Optics and Spectroscopy*, 1988, vol. 65, no. 6, pp. 1123–1128. (In Russian).

10. Wengierow M., Salbut L., Ramotowski Z., Szumski R., Szykiedans K. Measurement system based on multi wavelength interferometry for long gauge block calibration. *Metrology and Measurement Systems*, 2013, vol. 20, iss. 3, pp. 479–490.

11. Zhong J., Zhang Y. Absolute phase-measurement technique based on number theory in multifrequency grating projection profilometry. *Applied Optics*, 2001, vol. 40, no. 4, pp. 492–500.

12. Kujawińska M., Osten W. Fringe pattern analysis methods: up-to-date review. *Proceedings SPIE.*, 1998, vol. 3407, pp. 56–66.

13. Takeda M., Gu Q., Kinoshita M., Takai H.,Takahashi Y. Frequency-multiplex Fourier-transform profilometry: a single-shot three-dimensional shape measurement of objects with large height discontinuities and/or surface isolations. *Applied Optics*, 1997, vol. 36, no. 22, pp. 5347–5354.

14. Arnol'd I.V. *Teoreticheskaya arifmetika* [Theoretical Arithmetic]. Moscow, Uchpedgiz Publ., 1938. 480 p.

15. Hilbert D., Cohn-Vossen S. *Naglyadnaya geometriya* [Visual geometry]. Moscow, Nauka Publ., 1981. 344 p.

16. Guzhov V.I., Kabak E.S., Orlov I.S. Ispol'zovanie modulyarnoi arifmetiki pri fazovykh izmereniyakh [Use of modular arithmetic with phase measurements]. *Avtomatika i programmnaya inzheneriya = Automatics and Software Enginery*, 2015, no. 1 (1), pp. 97–107.

17. Guzhov V.I. *Metody izmereniya 3D profilya ob"ektov. Fazovye metody* [Methods for measuring 3D profile objects. Phase methods]. Novosibirsk, NSTU Publ., 2016. 83 p.

Для цитирования:

Сравнение чисел и анализ переполнения в модулярной арифметике / В.И. Гужов, И.О. Марченко, Е.Е. Трубилина, Д.С. Хайдуков // Системы анализа и обработки данных. – 2021. – № 3 (83). – С. 75–86. – DOI: 10.17212/2782-2001-2021-3-75-86.

For citation:

Guzhov V.I., Marchenko I.O., Trubilina E.E., Khaidukov D.S. Sravnenie chisel i analiz perepolneniya v modulyarnoi arifmetike [Comparison of numbers and analysis of overflow in modular arithmetic]. *Sistemy analiza i obrabotki dannykh = Analysis and Data Processing Systems*, 2021, no. 3 (83), pp. 75–86. DOI: 10.17212/2782-2001-2021-3-75-86.