Научная статья
УДК 004.312.44 + 519.6
doi: 10.34822/1999-7604-2022-2-85-93

# ПРОГРАММА ПОИСКА МОДУЛЯРНЫХ ОСНОВАНИЙ, ОБЕСПЕЧИВАЮЩИХ НЕОБХОДИМЫЙ ВЫЧИСЛИТЕЛЬНЫЙ ДИАПАЗОН И МИНИМИЗАЦИЮ БИВАЛЕНТНОГО ЭФФЕКТА

***Наталья Сергеевна Золотарева***
*Сургутский государственный университет, Сургут, Россия*
*zolotareva_ns@surgu.ru, http://orcid.org/0000-0001-9751-4232*

***Аннотация.*** В работе анализируется проблема поиска множества пар модулярных оснований, равноотстоящих от среднего основания, которые обеспечивают минимум бивалентного эффекта, а их произведение перекрывает требуемый вычислительный диапазон. Нахождение таких оснований позволяет перераспределением избыточности в регистрах для меньших в паре оснований размещать бинарные комбинации, которые невозможно разместить в регистрах для больших в паре оснований.

***Ключевые слова:*** модулярная арифметика, бивалентный эффект, взаимно простые основания, модулярный процессор

***Для цитирования:*** *Золотарева Н. С. Программа поиска модулярных оснований, обеспечивающих необходимый вычислительный диапазон и минимизацию бивалентного эффекта // Вестник кибернетики. 2022. № 2 (46). С. 85–93. DOI 10.34822/1999-7604-2022-2-85-93.*

Original article

# THE PROGRAM FOR SEARCHING MODULAR BASES PROVIDING A REQUIRED COMPUTATIONAL RANGE AND MINIMIZATION OF BIVALENT EFFECT

***Natalya S. Zolotareva***
*Surgut State University, Surgut, Russia*
*zolotareva_ns@surgu.ru. http://orcid.org/0000-0001-9751-4232*

***Abstract.*** The article analyzes the problem of searching a set of pairs of modular bases equidistant from the mean base. These pairs provide a minimum of the bivalent effect, and their product covers the required computational range. By finding the bases, binary combinations that cannot be placed in registers for larger bases in a pair can be placed in those for smaller bases in a pair by redistribution of redundancy.

***Keywords***: modular arithmetic, bivalent effect, relatively prime bases, modular processor

***For citation:*** *Zolotareva N. S. The Program for Searching Modular Bases Providing a Required Computational Range and Minimization of Bivalent Effect // Proceedings in Cybernetics. 2022. No. 2 (46). P. 85–93. DOI 10.34822/1999-7604-2022-2-85-93.*

## ВВЕДЕНИЕ

Персональные компьютеры, которые человечество использует ежедневно в повседневной жизни, устроены так, что имеют возможность обрабатывать информацию в ограниченном вычислительном диапазоне. Размер обработки данных за один такт, которым процессор обменивается с оперативной памятью, зависит от разрядности процессора. Процессоры могут быть 8, 16, 32 или 64-разрядными. Наиболее распространены 64-разрядные персональные компьютеры. Вычислительный диапазон в этом случае равен $2^{64}$ (около 20 десятичных разрядов). В большинстве случаев такой разрядности вполне достаточно для обычного пользователя. Но что делать, если речь идет о сложных алгоритмах, где нужно решать задачи с числами большой разрядности?

Примером могут служить криптографические алгоритмы. Например, при реализации метода шифрования RSA криптосистеме Рабина требуется обеспечить точность результатов арифметических операций порядка $10^{309}$ [1].

Решением проблемы вычисления с многоразрядными числами было введение в 1950-е годы непозиционной системы счисления, которая носит название «Система остаточных классов», или модулярная арифметика, когда необходимо оперировать не с самим числом $A(0 \le A < P)$, где $P = p_1 \times p_2 \times \ldots \times p_n$ – диапазон представления чисел, а с остатками ($a_1$, $a_2$, …, $a_n$) при делении этого числа $A$ на некоторые натуральные взаимно простые числа ($p_1$, $p_2$, …, $p_n$) – основания модулярной системы, то есть $a_i \equiv A(mod\ p_i)\ 0 \le a_i < p_i$.

С 60-х годов прошлого века начались работы по созданию цифровых вычислительных машин на основе модулярной арифметики. Однако, несмотря на наличие преимуществ модулярной арифметики (выполнение арифметических операций сложения, вычитания и умножения не требует переноса в следующий разряд, малая разрядность остатков, действия над числами можно проводить независимо в параллельных каналах), есть и недостатки: отсутствие простого алгоритма деления и сравнения чисел, сложность выполнения операций, которые требуют округления результата, затруднение перевода из позиционной системы счисления в модулярную и др. В таком случае необходимо знать информацию обо всем числе и приходится восстанавливать его позиционное представление. В связи с этим построение универсальных вычислительных машин с использованием модулярной арифметики можно считать неэффективным. Но построение цифровых вычислительных машин, специализированных под конкретные задачи, на основе модулярной арифметики оказалось весьма успешным, так как модулярная арифметика применяется в вычислительных системах достаточно широко уже несколько десятилетий [2–6].

## МАТЕРИАЛЫ И МЕТОДЫ

**Анализ и проектирование модулярной арифметики модулярного процессора.** Введем следующие определения:

**Определение.** Модулярный процессор – это специализированное техническое устройство, работающее на основе модулярной арифметики.

**Определение.** Числовым диапазоном будем называть числовую величину, которая не превышает максимума типового диапазона. В нашем случае типовым диапазоном считается 16-разрядный. Для беззнакового двоичного 16-разрядного кода числовым диапазоном представляемых значений будет от 0 до $2^n - 1 = 65535$.

**Определение.** Вычислительный диапазон – входной переменный параметр программного комплекса генерации оснований модулярной арифметики для решения нужной проблемы.

Проанализируем и спроектируем модулярную арифметику модулярного процессора для воспроизведения на $n$-разрядном серийном позиционном процессоре. В нем реализована беззнаковая целочисленная арифметика, то есть числа меняются от 0 до $2^n - 1$ включительно. Условная середина $2^{n-1}$, где $n = 16$ (рис. 1).

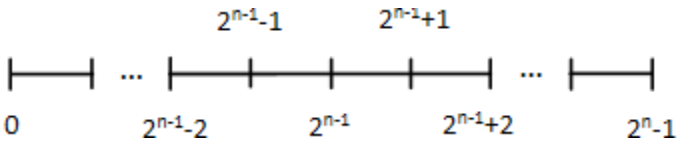


**Рис. 1. Беззнаковое представление целых чисел**
*Примечание:* составлено автором на основании данных, полученных в исследовании.

**Определение.** Числа $p_1$, $p_2$, …, $p_n$ называются взаимно простыми, если ($p_1$, $p_2$, …, $p_n$) = 1, то есть наибольший общий делитель этих чисел равен 1.

**Определение.** Числа $p_1$, $p_2$, …, $p_n$ называются попарно взаимно простыми, если наибольший общий делитель чисел ($p_i$, $p_j$) = 1, где $i \ne j$, $i, j = 1, 2, \ldots, n$.

**Определение.** Основаниями $p_1$, $p_2$, …, $p_n$ модулярной арифметики, или по-другому модулями, будем называть простые (взаимно простые) числа, если для любых двух индексов $i \neq j$, $i, j = 1, 2, \ldots, n$ выполняется $(p_i, p_j) = 1$.

**Определение.** Обрабатываемые числовые данные ($a_1$, $a_2$, … $a_n$) в модулярных форматах данных будем называть вычетами (остатками) по модулю, где $a_i \in Z$, $0 \leq a_i < p_i$.

Вычеты по модулю размещаются в цифровых регистрах, которые в совокупности составляют операционную разрядную сетку модулярного процессора.

При проектировании технических устройств, работающих на основе модулярной арифметики, возникает избыточность двоичного регистрового представления, которая называется бивалентным эффектом. Она возникает из-за несоизмеримости оснований модулярной арифметики со степенью двойки.

**Определение.** Бивалентным эффектом [7–8] отдельного модулярного основания называется величина

$$\delta_i(p_i) = [\log_2 p_i] - \log_2 p_i = n_i - \log_2 p_i \geq 0,$$

где $[\log_2 p_i]$ – целая не меньшая часть числа, которая представляет собой регистровую битность отдельного модулярного основания.

**Определение.** Величину $\Delta_n$, равную сумме бивалентных эффектов каждого отдельного модулярного основания, будем называть суммарным бивалентным эффектом для $n$-регистровой бинарной разрядной сетки модулярного процессора:

$$\Delta_n = \sum_{i=1}^{n} \delta_i(p_i).$$

Основания модулярной арифметики не являются степенями двух. Степенью двойки выберем среднее основание.

**Определение.** Под неоднородностью блоков цифрового модульного регистра понимается их различная длина, выраженная в элементарных (двоичных) ячейках для размещения разрядов числового значения остатка в бинарном коде.

Поскольку остатки – это целые числа, лежащие в пределах от нуля до значения модуля, уменьшенного на единицу, то в двоичных неоднородных блоках цифрового модульного регистра невозможно безызбыточное размещение вычетов в блоках цифрового регистра. Так как для представления остатков используются не все возможные двоичные комбинации, появляется информационная избыточность [9–14].

Метод сведения к нулю бивалентного эффекта работает для пар модулярных оснований, находящихся на одинаковом расстоянии от некоторого среднего основания.

Среднее основание по технологическим причинам удобно выбирать $2^n$ для двоичной элементной базы, что позволяет уменьшить бивалентный эффект. При этом, чем больше показатель степени, тем больше таких оснований и проще процесс поиска и моделирования.

Общая задача состоит в получении проектировщиком спецкомпьютера множества модулярных оснований, произведение которых перекрывает требуемый вычислительный диапазон. Полученные основания позволяют экономить бинарную разрядность процессора.

**Разработка алгоритма.** На первом этапе был разработан алгоритм поиска модулярных оснований. Перечислим этапы разработки алгоритма:

1. Нахождение простых чисел в диапазоне от 0 до $2^n$.
2. Нахождение пар простых чисел, равноотстоящих от середины – это $2^{n-1}$.
3. Нахождение пар простых (взаимно простых) чисел, равноотстоящих от середины.
4. Вычисление бивалентного эффекта найденных пар чисел.
5. Для составных чисел в парах указываются канонические разложения.
6. Для каждой пары чисел указывается разность с серединным числом.

Приведем фрагмент примера работы программы при $n = 8$ (рис. 2).

```
All primes:
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 10
9 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229
233 239 241 251
Prime pairs:
[107, 149] [89, 167] [83, 173] [59, 197] [29, 227] [23, 233] [17, 239] [5, 251]

Mutually prime pairs:
[127, 129] [125, 131] [123, 133] [121, 135] [119, 137] [117, 139] [115, 141] [113, 14
3] [111, 145] [109, 147] [107, 149] [105, 151] [103, 153] [101, 155] [99, 157] [97, 1
59] [95, 161] [93, 163] [91, 165] [89, 167] [87, 169] [85, 171] [83, 173] [81, 175] [
79, 177] [77, 179] [75, 181] [73, 183] [71, 185] [69, 187] [67, 189] [65, 191] [63, 1
93] [61, 195] [59, 197] [57, 199] [55, 201] [53, 203] [51, 205] [49, 207] [47, 209] [
45, 211] [43, 213] [41, 215] [39, 217] [37, 219] [35, 221] [33, 223] [31, 225] [29, 2
27] [27, 229] [25, 231] [23, 233] [21, 235] [19, 237] [17, 239] [15, 241] [13, 243] [
11, 245] [9, 247] [7, 249] [5, 251] [3, 253] [1, 255]

Lets take 2 first pairs from prime pairs
[89, 107, 149, 167]
bivalent defect =  0.17992676969624277
pair [89,167]:
distance to middle:  39
89  :  [89]
167  :  [167]

pair [107,149]:
distance to middle:  21
107  :  [107]
149  :  [149]


Lets take 2 first pairs from mutually prime pairs
[125, 127, 129, 131]
bivalent defect =  0.0008807716050434067
pair [125,131]:
distance to middle:  3
125  :  [5, 5, 5]
131  :  [131]

pair [127,129]:
distance to middle:  1
127  :  [127]
129  :  [3, 43]
```

**Рис. 2. Пример работы программы поиска модулярных оснований**
*Примечание:* составлено автором на основании данных, полученных в исследовании.

## РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

В табл. 1–2 приведены результаты работы программы вычисления бивалентного эффекта в зависимости от выбранных модулей.

Сравнивая табл. 1 и 2, можно сделать вывод, что, чем дальше мы отклоняемся от серединного основания, тем больше становится бивалентный эффект, а добавляя к простым числам взаимно простые числа, мы расширяем множество модулярных оснований.

*Таблица 1*

**Модулярные основания пар простых чисел и их бивалентный эффект**

| **Пары простых чисел, равноотстоящих от $2^{15}$** | **Диапазон представления чисел – $P = p_1 \times p_2 \times \ldots \times p_n$** | **Бивалентный эффект** |
|---|---|---|
| [32603,32933]<br>[32693,32843] | 37 777 776 061 352 155 578 | $4{,}413821855742128 \times 10^{-5}$ |
| [32579,32957]<br>[32603,32933]<br>[32693,32843] | 40 562 228 714 841 111 876 699 216 379 904 | $9{,}213426904253197 \times 10^{-5}$ |
| [32537,32999]<br>[32579,32957]<br>[32603,32933]<br>[32693,32843] | $4{,}355119700469221870010422714824 4 \times 10^{40}$ | 0,00016383266182273815 |

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

*Таблица 2*

**Модулярные основания пар простых, взаимно простых пар чисел и их бивалентный эффект**

| **Пары простых и взаимно простых чисел, равноотстоящих от $2^{15}$** | **Диапазон представления чисел – $P = p_1 \times p_2 \times \ldots \times p_n$** | **Бивалентный эффект** |
|---|---|---|
| [32765,32771]<br>[32767,32769] | 37 778 931 511 113 441 116 160 | $1{,}3436142864975409 \times 10^{-8}$ |
| [32763,32773]<br>[32765,32771]<br>[32767,32769] | 40 564 817 885 040 734 757 146 206 371 840 | $4{,}702650358012761 \times 10^{-8}$ |
| [32761,32775]<br>[32763,32773]<br>[32765,32771]<br>[32767,32769] | $4{,}355613955843538448544236156421 6 \times 10^{40}$ | $1{,}1286361356610541 \times 10^{-7}$ |

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

Покажем на примере вычисление бивалентного эффекта для оснований $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$:

$$\delta_1(32765) = [\log_2 32765] - \log_2 32765 = $$
$$= 15 - 14{,}999868 = 0{,}000132,$$
$$\delta_2(32767) = [\log_2 32767] - \log_2 32767 = $$
$$= 15 - 14{,}999956 = 0{,}000044,$$
$$\delta_3(32768) = [\log_2 32768] - \log_2 32768 = $$
$$= 15 - 15 = 0,$$
$$\delta_4(32769) = [\log_2 32769] - \log_2 32769 = $$
$$= 15 - 15{,}000044 = 0{,}000044,$$
$$\delta_5(32771) = [\log_2 32771] - \log_2 32771 = $$
$$= 15 - 15{,}000132 = 0{,}000132,$$
$$\Delta_5 = \sum_{i=1}^{5} \delta_1(32765) + \delta_2(32767) + \delta_3(32768) +$$
$$+\delta_4(32769) + \delta_5(32771) = 0{,}000132 +$$
$$+ 0{,}000044 + 0 - 0{,}000044 - 0{,}000132 = 0.$$

Модулярная арифметика с множеством оснований $\{p_1, p_2, p_3, p_4, p_5\} = \{32765, 32767, 32768, 32769, 32771\}$ имеет суммарный бивалентный эффект, равный нулю.

Выполним сравнение арифметических операций в модулярной системе счисления с различными основаниями. В первом случае основания подобраны таким образом, что бивалентный эффект стремится к нулю, а именно равен 0,00000001343614286497540 9, во втором случае бивалентный эффект равен 0,04183008662934107.

1. Выполним арифметические операции сложения, умножения и вычитания чисел $A$ и $B$ в модулярной системе счисления с основаниями $p_1 = 32765$, $p_2 = 32767$, $p_3 = 32768$, $p_4 = 32769$, $p_5 = 32771$.

Диапазон системы определится как $P = p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6 =$ $= 37778931511113441116160$. $P \approx 2^{75} =$ $= 37778931862957161709568$.

Сложим число $A = 2^{32} = 4294967296$ с числом $B = 2^{30} = 1073741824$.

По выбранным основаниям числа $A$ и $B$ в системе остаточных классов будут представлены как

$$A = 2^{32} = (36, 4, 0, 4, 6),$$
$$B = 2^{30} = (9, 1, 0, 1, 9).$$

Операции сложения и умножения в модулярной арифметике реализуются по правилам: если числа $A$ и $B$ представлены остатками $\alpha_i$ и $\beta_i$ по основаниям $p_i$

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$
$$B = (\beta_1, \beta_2, \ldots, \beta_n),$$

тогда результаты операций сложения и умножения $A + B$ и $A \times B$ представлены остатками $\gamma_i$ и $\delta_i$ по тем же основаниям $p_i$:

$$A + B = (\gamma_1, \gamma_2, \ldots, \gamma_n),$$
$$A \times B = (\delta_1, \delta_2, \ldots, \delta_n),$$

где выполняются соотношения:

$$\gamma_i = \alpha_i + \beta_i (\mathrm{mod}\ p_i),$$
$$\delta_i = \alpha_i \times \beta_i (\mathrm{mod}\ p_i),$$

Результатом являются числа:

$$\gamma_i = \alpha_i + \beta_i - \left[\frac{\alpha_i + \beta_i}{p_i}\right] p_i,$$

$$\delta_i = \alpha_i \times \beta_i - \left[\frac{\alpha_i \times \beta_i}{p_i}\right] p_i.$$

Применяя правила к нашему примеру, получим:

$$A + B = (36 + 9 - \left[\frac{36+9}{32765}\right] \times 32765,$$
$$4 + 1 - \left[\frac{4+1}{32767}\right] \times 32767,$$
$$0 + 0 - [0 + 0] \times 32768,$$
$$4 + 1 - \left[\frac{4+1}{32769}\right] \times 32769,$$
$$36 + 9 - \left[\frac{36+9}{32771}\right] \times 32771) =$$
$$= (45, 5, 0, 5, 45).$$

$$A - B = (36 - 9 - \left[\frac{36-9}{32765}\right] \times 32765,$$
$$4 - 1 - \left[\frac{4-1}{32767}\right] \times 32767,$$
$$0 - 0 - [0 - 0] \times 32768,$$
$$4 - 1 - \left[\frac{4-1}{32769}\right] \times 32769,$$
$$36 - 9 - \left[\frac{36-9}{32771}\right] \times 32771) =$$
$$= (27, 3, 0, 3, 27).$$

$$A \times B = (36 \times 9 - \left[\frac{36 \times 9}{32765}\right] \times 32765,$$
$$4 \times 1 - \left[\frac{4 \times 1}{32767}\right] \times 32767,$$
$$0 \times 0 - [0 \times 0] \times 32768,$$
$$4 \times 1 - \left[\frac{4 \times 1}{32769}\right] \times 32769,$$
$$36 \times 9 - \left[\frac{36 \times 9}{32771}\right] \times 32771) =$$
$$= (324, 4, 0, 4, 324).$$

2. Выполним арифметические операции сложения, вычитания и умножения чисел $A$ и $B$ в модулярной системе счисления с основаниями $p_1 = 11749$, $p_2 = 19071$, $p_3 = 32768$, $p_4 = 46465$, $p_5 = 53787$.

Диапазон системы определится как $P = p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6 =$ $= 183496408472352831897 60$. $P \approx 2^{74} =$ $= 188894659314785808547 84$.

По выбранным основаниям числа $A$ и $B$ в модулярной системе счисления будут представлены следующим образом:

$$A = 2^{32} = (2856, 6457, 0, 21486, 21559),$$
$$B = 2^{30} = (714, 6382, 0, 28604, 45730).$$

Выполняя аналогичные вычисления, согласно правилам выполнения арифметических операций получим:

$$A + B = (3570, 12839, 0, 3625, 13502),$$
$$A - B = (2142, 75, 0, 39347, 29616),$$
$$A \times B = (6607, 15214, 0, 39454, 31147).$$

Сравнивая результаты, можно сделать следующие выводы:

1. В первом случае мы получили малоразрядные остатки, с которыми работать проще.

2. В первом случае мы получили остатки, симметричные относительно нуля, чего нельзя сказать о втором случае.

3. При выполнении арифметических операций над числами в модулярной арифметике достаточно оперировать с остатками этих чисел.

На втором этапе разработан алгоритм поиска модулярных оснований, обеспечивающий минимизацию бивалентного эффекта, а их произведение близко к вычислительному диапазону. Количество оснований переменное, необходимое для перекрытия диапазона в проблемной задаче. Вычислительный диапазон является входным переменным параметром программного комплекса генерации оснований модулярной арифметики для решения нужной проблемы. На рис. 3 показана работа программы для вычислительного диапазона равного $2^{75}$.

```
Pairs set closest to middle
[32765, 32767, 32768, 32769, 32771]
covering interval =  37778931511113441116160  < 2^ 75
bivalent defect =  1.3436142864975409e-08

pair [32765,32771]:
distance to middle:  3
32765  :  [5, 6553]
32771  :  [32771]

pair [32767,32769]:
distance to middle:  1
32767  :  [7, 31, 151]
32769  :  [3, 3, 11, 331]

--------------------------------
Best pairs set from 1000 random pairs set
[12597, 18293, 32768, 47243, 52939]
covering interval =  18884922208995639853056  < 2^ 74
bivalent defect =  0.00034707145489853986

pair [12597,52939]:
distance to middle:  20171
12597  :  [3, 13, 17, 19]
52939  :  [167, 317]

pair [18293,47243]:
distance to middle:  14475
18293  :  [11, 1663]
47243  :  [7, 17, 397]

--------------------------------
Another one best pairs set from 1000 random pairs set
[12013, 19429, 32768, 46107, 53523]
covering interval =  18873792391063879581696  < 2^ 74
bivalent defect =  0.001197573585136169

pair [12013,53523]:
distance to middle:  20755
12013  :  [41, 293]
53523  :  [3, 3, 19, 313]

pair [19429,46107]:
distance to middle:  13339
19429  :  [19429]
46107  :  [3, 3, 47, 109]
```

**Рис. 3. Пример работы программы поиска модулярных оснований, обеспечивающих минимум бивалентного эффекта**

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

В табл. 3 приведены модулярные основания, а также бивалентный эффект для различных вычислительных диапазонов.

*Таблица 3*

**Модулярные основания, обеспечивающие минимум бивалентного эффекта**

| **Вычислительный диапазон** | **Модулярные основания $p_1, p_2, \ldots, p_n$** | **Диапазон модулярной системы $P$** | **Бивалентный эффект** |
|---|---|---|---|
| $2^{45}$ | [32767, 32768, 32769] | 35184372056064 | $1.3436132206834372 \times 10^{-9}$ |
| | [32765, 32768, 32771] | 35184371793920 | $1.2092529644291972e \times 10^{-8}$ |
| $2^{50}$ | [32763, 32768, 32773] | 35184371269632 | $3.35903607151522 \times 10^{-8}$ |
| | [32755, 32768, 32781] | 35184366551040 | $2.2707086166917634e \times 10^{-7}$ |
| $2^{60}$ | [32721, 32768, 32815] | 35184299704320 | $2.9680473954130093 \times 10^{-6}$ |
| | [32741, 32768, 32795] | 35184348200960 | $9.794952724462291 \times 10^{-7}$ |
| $2^{75}$ | [32765, 32767, 32768, 32769, 32771] | 377789315111134411 16160 | $1.3436142864975409 \times 10^{-8}$ |
| | [12597, 18293, 32768, 47243, 52939] | 188849222089956398 53056 | 0.00034707145489853986 |
| $2^{90}$ | [32681, 32699, 32768, 32837, 32855] | 377784980408301343 53920 | $1.6566816317009625 \times 10^{-5}$ |
| | [32407, 32413, 32768, 33123, 33129] | 377699130280816114 72896 | 0.0003444507571259692 |

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

Можно заметить, что, чем ближе располагаются пары модулярных оснований к серединному основанию, равному степени двух, тем меньше значение бивалентного эффекта.

**ЗАКЛЮЧЕНИЕ**

В результате исследования была разработана программа поиска наилучших модулярных оснований из заданного числового диапазона. Критерием поиска служил минимум бивалентного эффекта, а также невыход требуемого вычислительного диапазона за произведение этих модулярных оснований.

Следующим этапом будет разработка программы выполнения модульных и немодульных операций в модулярной системе счисления; определение влияния различных оснований в зависимости от величины бивалентного эффекта на сложность выполнения этих операций.

Выводы:

1. Рассматриваемый способ выбора оснований модулярной арифметики позволяет сократить дополнительные расходы при выполнении модульных операций. Поясним это.

При выполнении арифметических операций сложения, вычитания и умножения мы пользуемся выражением:

$$A * B = \alpha_i * \beta_i - \left[ \frac{\alpha_i * \beta_i}{p_i} \right] \times p_i,$$

где * – арифметические операции (+, –, ×);

$A = (\alpha_1, \alpha_2, ..., \alpha_n), B = (\beta_1, \beta_2, ..., \beta_n).$

То есть необходимо реализовать следующие шаги:

а) выполнить арифметическую операцию * над числами *A* и *B*;

б) выделить целую часть $\left[ \frac{\alpha_i * \beta_i}{p_i} \right]$;

в) выполнить умножение $\left[ \frac{\alpha_i * \beta_i}{p_i} \right] \times p_i$;

г) выполнить итоговое вычитание.

Если в качестве оснований модулярной арифметики мы будем выбирать простые или взаимно простые пары чисел, симметричных относительно среднего основания, то шаги б), в) и г) можно опустить. В этом случае достаточно оперировать только с остатками чисел *A* и *B*.

2. Для уменьшения бивалентного эффекта в качестве оснований модулярной арифметики следует выбирать простые или взаимно простые пары чисел, симметричных относительно среднего основания, являющегося некоторой степенью двойки.

3. При переводе числа в модулярную систему счисления, используя модулярные основания, с бивалентным эффектом, равным нулю, получим малоразрядные остатки, симметричные относительно нуля, то есть при переводе числа $A = 2^{32} = 4294967296$ из десятичной системы счисления в модулярную систему счисления получим число *A* в виде остатков (36, 4, 0, 4, 6), симметричных относительно нуля.

4. Бивалентный эффект позволяет осуществлять гибкий выбор оснований модулярной арифметики в зависимости от поставленных технологических целей.

**Список источников**

1. Коптенок Е. В., Кузин А. В., Шумилин Т. Б., Соколов М. Д. Разработка способа представления длинных чисел в памяти компьютера // Молод. ученый. 2017. № 46 (180). С. 26–30.
2. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. М. : Совет. радио, 1968. 439 с.
3. Амербаев В. М. Теоретические основы машинной арифметики. Алма-Ата : Наука, 1986. 224 с.
4. Лавриненко А. Н., Червяков Н. И. Исследование немодульных операций в системе остаточных классов // Науч. вед. компьютер. моделирование 2012. № 1 (120), Вып. 21/1. С. 110–122.

**References**

1. Koptenok E. V., Kuzin A. V., Shumilin T. B., Sokolov M. D. Razrabotka sposoba predstavleniia dlinnykh chisel v pamiati kompiutera // Molod. uchenyi. 2017. No. 46 (180). P. 26–30. (In Russian).
2. Akushsky I. Ya., Yuditsky D. I. Mashinnaia arifmetika v ostatochnykh klassakh. Moscow : Sovet. radio, 1968. 439 p. (In Russian).
3. Amerbaev V. M. Teoreticheskie osnovy mashinnoi arifmetiki. Alma-Ata : Nauka, 1986. 224 p. (In Russian).
4. Lavrinenko A. N., Chervyakov N. I. Issledovanie nemodulnykh operatsii v sisteme ostatochnykh klassov // Nauch. ved. kompiuter. modelirovanie. 2012. No. 1 (120), Is. 21/1. P. 110–122. (In Russian).

5. Юдитский Д. И. Создатели отечественной электроники : сер. сб / под ред. Б. М. Малашевича. М. : РИЦ «Техносфера», 2011. 320 с.
6. Малашевич Б. М. Краткие основы и история создания отечественных модулярных ЭВМ. Истоки модулярной арифметики // Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы (SoRuCom-2017) : сб. тр. IV Междунар. конф., 3–5 октября 2017 г., Зеленоград / под ред. д. ф.-м. н. А. Н. Томилина. М. : ФГБОУВО «РЭУ им. Г. В. Плеханова», 2017. С. 193–207.
7. Инютин С. А. Модулярные процессоры – оценки, история борьбы и победы над бивалентным дефектом // Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы (SoRuCom-2017) : сб. тр. IV Междунар. конф., 3–5 октября 2017 г., Зеленоград / под ред. д. ф.-м. н. А. Н. Томилина. М. : ФГБОУВО «РЭУ им. Г. В. Плеханова», 2017. С. 72–77.
8. Золотарева Н. С., Инютин С. А. Методы выбора оснований, понижающих бивалентный дефект в системе остаточных классов // Вестник кибернетики. 2020. № 2 (38). С. 6–11.
9. Амербаев В. М., Тельпухов Д. В., Константинов А. В. Бивалентный эффект модулярных кодов // Проблемы разработки перспективных микро- и наноэлектронных систем : сб. тр. ИППМ РАН / под общ. ред. А. Л. Стемпковского. М. : ИППМ-МЕС, 2008. С. 492–496.
10. Инютин С. А. Модулярные процессоры – история и оценки тривалентного эффекта // Развитие вычислительной техники в России, странах бывшего СССР и СЭВ: история и перспективы (SoRuCom-2020) : сб. тр. V Междунар. конф. 6–7 октября 2020 г., Москва, Россия / под ред. А. Н. Томилина. М., 2020. С. 138–142.
11. Инютин С. А. Методы организации многоразрядных вычислений // Вестник кибернетики. 2013. № 12. С. 89–93.
12. Инютин С. А. Способ и устройство размещения групп чисел в однородных блоках цифрового регистра : патент на изобретение РФ № 2591009 зарегистрирован 17.06.2016.
13. Инютин С. А. Теория и методы моделирования вычислительных структур с параллелизмом машинных операций : дис. … д-ра техн. наук. М., 2001. 272 с.
14. Эрдниева Н. С. Использование специальных модулей системы остаточных классов для избыточного представления // Вестн. АГТУ. Сер. Управление, вычислительная техника и информатика. 2013. № 2. С. 75–84.

5. Yuditsky D. I. Series “Inventors of Locally-Produced Electronics” / Ed. B. M. Malashevich. Moscow : RITs “Tekhnosfera”, 2011. 320 p. (In Russian).
6. Malashevich B. M. Kratkie osnovy i itsoriia sozdaniia otechestvennykh moduliarnykh EVM. Istoki moduliarnoi arifmetiki // Computer Technology in Russia and in the Former Soviet Union : Proceedings of the SoRuCom-2017. IV International Conference, October 3–5, 2017, Zelenograd / Ed. Doctor of Sciences (Physics and Mathematics) A. N. Tomilin. Moscow : Plekhanov Russian University of Economics, 2017. P. 193–207. (In Russian).
7. Inyutin S. A. Moduliarnye protsessory – otsenki, istoriia borby i pobedy nad bivalentnym defektom // Computer Technology in Russia and in the Former Soviet Union : Proceedings of the SoRuCom-2017. IV International Conference, October 3–5, 2017, Zelenograd / Ed. Doctor of Sciences (Physics and Mathematics) A. N. Tomilin. Moscow : Plekhanov Russian University of Economics, 2017. P. 72–77. (In Russian).
8. Zolotareva N. S., Inyutin S. A. Methods for Selection of Bases Reducing Bivalent Defect in Residue Number System // Proceedings in Cybernetics. 2020. No. 2 (38). P. 6–11. (In Russian).
9. Amerbaev V. M., Telpukhov D. V., Konstantinov A. V. Bivalentnyi effekt moduliarnykh kodov // Problems of Advanced Micro and Nanoelectronic Systems Development : Proceedings of the Institute for Design Problems in Microelectronics of the Russian Academy of Sciences / Ed. A. L. Stempkovsky. Moscow : IPPM-MES, 2008. P. 492–496. (In Russian).
10. Inyutin S. A. Moduliarnye protsessory – istoriia i otsenki trivalentnogo effekta // History of Computing in the Russia, Former Soviet Union and Council for Mutual Economic Assistance Countries : Proceedings of the SoRuCom-2020. V International Conference, October 6–7, 2020, Moscow, Russia / Ed. A. N. Tomilin. Moscow, 2020. P. 138–142. (In Russian).
11. Inyutin S. A. Organization Methods for Multi-Digit Calculations // Proceedings in Cybernetics. 2013. No. 12. P. 89–93. (In Russian).
12. Inyutin S. A. Method and Device for Arrangement of Groups of Numbers in Homogeneous Units of Digital Register : Patent No. 2591009, Russian Federation, Registered 17.06.2016. (In Russian).
13. Inyutin S. A. Teoriia i metody modelirovaniia vychislitelnykh struktur s parallelizmom mashinnykh operatsii : Doctoral Dissertation (Engineering). Moscow, 2001. 272 p. (In Russian).
14. Erdnieva N. S. Use of Special Modules of the Residue Number System for Redundant Representation // Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics. 2013. No. 2. P. 75–84. (In Russian).

**Информация об авторе**

**Н. С. Золотарева** – аспирант.

**Information about the author**

**N. S. Zolotareva –** Postgraduate.