

# Метод вычисления позиционных характеристик модулярного представления с линейной сложностью

С. А. Инютин

Московский авиационный институт (национальный исследовательский университет), Москва, Россия

**Аннотация.** Разработан метод выбора оснований - модулей для генерации модулярных систем счисления и модулярной арифметики, в которых вычисление позиционной характеристики модулярного представления числовой величины, являющейся нелинейной функцией многих переменных, выполняется с линейной сложностью от количества оснований модулярной системы счисления при вычислении в диапазоне одиночного основания модулярной системы. Это значительно уменьшает разрядность (следовательно, объем аппаратуры) дополнительных блоков модулярного процессора. В исследованиях по модулярной алгоритмике в России и за рубежом отсутствуют методы вычисления позиционных характеристик при таких параметрах. Все немодульные (не распараллеливаемые в модулярной арифметике) операции специализированного процессора с SIMD архитектурой (множество процессорных элементов для потоков данных и единый поток команд) базируются на вычислении позиционных характеристик. Применение метода позволяет выполнять все немодульные операции с минимальной линейной сложностью. Двухэтапный метод содержит выбор оснований модулярной системы счисления и вычисление позиционной характеристики и предназначен для разработчиков специализированных процессоров (сопроцессоров).

**Ключевые слова:** модулярная арифметика, модулярная система счисления, модулярные форматы данных, линейная сложность вычисления, позиционная характеристика, нелинейная функция многих переменных.

DOI 10.14357/20718632240111

EDN AYBEED

## Введение

Модулярная система счисления, известна в теории чисел и нашла применение в вычислительной технике. Главными достоинствами модулярного способа представления числовых величин и модулярной машинной арифметики являются: параллельное выполнение кольцевых операций над компонентами модулярного формата представления числовых величин, что увеличивает скорость многоразрядного вычислительного процесса, а также построение арифметических помехозащитных кодов, позволяющих контролировать вычислительный процесс [1-3, 9].

Имеются проблемы, связанные с модулярным способом представления числовых величин, сдерживающие развитие и применение модулярной арифметики и обработки модулярных форматов данных в специализированных вычислительных системах. Одна из этих проблем - нелинейная сложность вычисления в диапазоне одиночного основания позиционной характеристики (ПХ) модулярного представления числовой величины. Выполнение всех немодульных (не распараллеливаемых по векторным компонентам) операций машинной модулярной арифметики базируется на вычислении ПХ [2-4, 10].

## 1. Постановка задачи

Рассмотрим метод, имеющий линейную сложность выполнения немодульных операций в модулярной арифметике для числовых величин, заданных в модулярных форматах данных. Числовые величины принадлежат вычислительному модулярному множеству  $A \in \{0, \dots, P-1\}$ , с верхней гранью, равной  $P = \prod_{i=1}^n p_i$  - произведению оснований  $p_i; i \in \{1, \dots, n\}$  модулярной системы счисления.

Величины простых (попарно взаимно-простых) оснований предполагаются близкими для устранения эффекта «гонок» и согласования производительности процессорных элементов, выполняющих вычисления по отдельным основаниям.

Пусть целочисленная величина  $A$  задана модулярным векторным представлением:

$$A \leftrightarrow (a_1, \dots, a_i, \dots, a_n) \in W^n, \quad (1)$$

где  $\forall i \in \{1, \dots, n\}$ ,  $a_i \equiv Am_i \pmod{p_i}$ ;  $m_i \frac{P}{p_i} \equiv 1 \pmod{p_i}$ ;  $P = \prod_{i=1}^n p_i$  - верхняя грань модулярного множества (компьютерного диапазона)  $W^n$  - множество взаимно-простых оснований  $\{p_1, \dots, p_i, \dots, p_n\}$  модулярной системы счисления;  $(a_1, \dots, a_i, \dots, a_n)$  - вектор модулярного представления числовой величины  $A$ , компоненты которого наименьшие неотрицательные нормированные вычеты по модулям оснований из множества  $\{p_i\}$ , мощностью  $n$ .

Модулярный процессор обрабатывает числовые данные, заданные в виде (1), в соответствующем модулярном формате данных.

Целая числовая величина имеет аддитивное разложение, связывающее значение числовой величины с нормированными компонентами вектора модулярного представления:

$$A = \sum_{i=1}^n \alpha_i \frac{P}{p_i} R_A P, \quad (2)$$

где  $R_A$  - позиционная характеристика - нормированный ранг.

*Определение.* Позиционная характеристика - нормированный ранг есть функция:

$$R_A = \left\lfloor \sum_{i=1}^n \frac{a_i}{p_i} \right\rfloor, \quad (3)$$

зависящая от  $2n$ -переменных, принадлежащих двум множествам: множеству попарно взаимно-простых оснований  $\{p_1, \dots, p_i, \dots, p_n\}$  модулярной системы счисления и упорядоченному множеству  $(a_1, \dots, a_i, \dots, a_n)$  наименьших неотрицательных нормированных вычетов числовой величины  $A$  по модулям оснований  $p_i$  из первого множества [1, 2]; квадратными скобками здесь и в дальнейшем обозначена дискретная функция - целая часть числа, меньшая или равная ему. Назовем ранг, вычисленный по формуле (3) истинным рангом.

Для точного вычисления истинного ранга необходимо вычисление целой части от суммы правильных рациональных дробей со знаменателем  $P$ , что требует вычислений в компьютерном диапазоне с максимальным значением  $P$ , являющимся многоразрядным целым числом при большом количестве или значениях оснований. Для этого требуется большая разрядность дополнительного блока модулярного процессора, особенно в случае, когда для вычислительных приложений эмулируемой модулярной арифметики выбираются простые основания, близкие к верхней границе целочисленного вычислительного диапазона 32- или 64-разрядных серийных компьютеров.

Значение нормированного ранга - целочисленной функции от нормированных компонент модулярного представления, принадлежит отрезку  $R_A \in [0, n-1]$ . Как правило,  $n \ll P$ , что приводит к

значительному отличию областей значений и определения нормированного ранга. Использование функций с областями определения, близкими к областям значений, значительно повышает эффективность вычисления позиционной характеристики модулярной величины – нормированный ранг  $R_A$  и, следовательно, выполнения всех немодульных операций специализированного процессора [8]. Известные методы вычисления позиционных характеристик модулярной величины имеют сложность, превышающую квадратичную  $O(n^2)$  или требуют вычислений с многоразрядными числами, значительно превышающими максимальное значение в разрядной сетке компьютера. Для вычисления функции – позиционной характеристики – важны три параметра: временная сложность вычисления, объем памяти для хранения констант, используемых при вычислении, и диапазон изменения переменных при выполнении вычислений. Значения этих параметров отражаются в объемах и разрядности дополнительных операционных блоков модулярного процессора, что отражается на сложности применения модулярной арифметики.

Разработанный метод позволяет выполнять вычисление ПХ в пределах квадрата одного основания модулярной системы (разрядность дополнительного оборудования  $2 \log_2 p_c$ , где  $p_c$  – некоторое модулярное основание). Полноразрядный метод, требует целочисленных вычислений в пределах  $P = \prod_{i=1}^n p_i$  (разрядность дополнительного оборудования  $i \cdot \log_2 p_c$ ). Для вычисления ПХ разработанным методом требуется меньшая разрядность дополнительного оборудования.

Позиционная характеристика – нормированный ранг имеет свойства:

$$1. 0 \leq R_A \leq n-1$$

$$2. \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] \leq R_A \leq \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right]$$

$$3. \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] = \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right] \Rightarrow \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] = \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right] = R_A$$

$$3. R_A = \left[ \frac{1}{p_c} \sum_{i=1}^n \left[ \frac{p_c a_i}{p_i} \right] + \frac{1}{p_c} \sum_{i=1}^n \frac{|p_c a_i|_{p_i}}{p_i} \right] = \left[ \frac{1}{p_c} \sum_{i=1}^n \left[ \frac{p_c a_i}{p_i} \right] \right] + 0 | 1, \quad (4)$$

$$4. \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] \leq R_A \leq \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right] \Rightarrow \sum_{i=1}^n \frac{a_i}{p_1} - \sum_{i=1}^n \frac{a_i}{p_n} = \sum_{i=1}^n a_i \frac{p_n - p_1}{p_1 p_n} < \varepsilon \Rightarrow \sin w \sum \sin q_i < \varepsilon$$

$$5. 0 \leq R_A - \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] < \left[ \sum_{i=1}^n \frac{a_i}{p_1} - \sum_{i=1}^n \frac{a_i}{p_n} \right]$$

где вертикальной чертой отделены альтернативные варианты,  $p_c$  – одно из модулярных оснований;  $|x|_p \equiv x(\text{mod } p)$  – обозначение операции вычисления наименьшего неотрицательного вычета по модулю;

$\sin w = \frac{p_n - p_1}{p_1}$ ,  $\sin q_i = \frac{a_i}{p_n}$ ,  $\varepsilon > 0$  – некоторая рациональная дробь. Первое слагаемое в

пункте 3 формулы (4) при произвольном целом  $p_c \geq n$  введено В. М. Амербаевым и получило название неточного нормированного ранга, вычисляемого с линейной сложностью [2].

Все немодульные (не распараллеливаемые) операции выполняются на основе вычисления позиционных характеристик. Например, операция вычисления вычета  $a_g$  (расширение на новое модулярное основание  $g$ ) модулярного представления числовой величины  $A$  определяется следующим соотношением:

$$a_g = \left| \sum_{i=1}^n a_i |p_i|_g^{-1} - |R_A|_g \left| \prod_{i=1}^n p_i \right|_g \right|.$$

Вычисление ранга при произвольной разрядности дробей дает приближенное значение ранга (неточный ранг), которое нельзя использовать в расчетах.

*Лемма 1.* Оценка абсолютного значения разности между суммой рациональных дробей и рангом. Абсолютная величина дробной части ранга, возникающая при его вычислении равна:

$$\left| R_A - \sum_{i=1}^n \frac{a_i}{p_i} \right| \leq \left[ \sum_{i=1}^n \frac{a_i}{p_i} \right] - \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right]. \quad (5)$$

*Доказательство.*

$$\left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] \leq R_A \leq \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right]$$

$$R_A - \sum_{i=1}^n \frac{a_i}{p_n} \leq \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right] - \sum_{i=1}^n \frac{a_i}{p_n}$$

Учитывая  $\sum_{i=1}^n \frac{a_i}{p_n} < \sum_{i=1}^n \frac{a_i}{p_i}$  и  $\left[ \sum_{i=1}^n \frac{a_i}{p_n} \right] \leq \sum_{i=1}^n \frac{a_i}{p_n}$ , усилим неравенство

$$R_A - \sum_{i=1}^n \frac{a_i}{p_i} \leq \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right] - \sum_{i=1}^n \frac{a_i}{p_n} \text{ или}$$

$$\left| R_A - \sum_{i=1}^n \frac{a_i}{p_i} \right| \leq \left[ \sum_{i=1}^n \frac{a_i}{p_1} \right] - \left[ \sum_{i=1}^n \frac{a_i}{p_n} \right]. \text{ Лемма доказана.}$$

## 2. Обоснование метода

Опишем разработанный двухэтапный метод вычисления позиционной характеристики числовой величины вычислением дискретной функции - целой части от суммы правильных рациональных дробей, используя вычисления в пределах квадрата одиночного основания модулярной системы счисления. Первый этап - выбор медианного основания и рабочих симметричных оснований, равноудаленных от медианного основания. Второй этап - выбор номера шага, после которого при вычислении целой части от суммы правильных дробей последующие слагаемые не влияют на вычисление позиционной характеристики.

Рассмотрим медианный метод вычисления позиционной характеристики  $R_A \in [0, n-1]$  с использованием среднего (медианного) основания модулярной системы счисления.

Основания модулярной системы счисления  $\forall i \in \{1, \dots, n\} = W = U \cup V, \delta_i = p_i - p_c$  связаны невязками с медианным основанием  $p_c \in \{p_1, \dots, p_n\}$ . Для них выполняется одно из двух неравенств. Назовем положительными те невязки, для которых выполняется неравенство

$\forall l \in U, \delta_l = p_l - p_c \geq 0$  и отрицательными - для которых выполняется неравенство  $\forall t \in V, \delta'_t = p_c - p_t > 0$ .

*Лемма 2.* Знакопеременный ряд с параметрами  $\delta < p; \mu = \frac{\delta}{p} < 1$ :

$$\sum_{j=0}^{\infty} (-1)^j \mu^j = 1 - \mu + \mu^2 - \mu^3 + \dots (-1)^j \mu^j + \dots = \frac{1}{1 + \mu} = \frac{p}{p + \delta} \quad (6)$$

$$\text{или } \sum_{j=0}^{\infty} (-1)^j \mu^j = 1 - (\mu - (\mu^2 - (\mu^3 - (\mu^j - \dots) \dots)) = \frac{p}{p + \delta}$$

является абсолютно сходящимся. *Примечание:*  $\delta < p; \mu = \frac{\delta}{p} < 1; \delta < 0 \mid \delta > 0$

*Доказательство.*

Частичные суммы ряда имеют вид:

$$S_k = \frac{1 + (-1)^k \mu^k}{1 + \mu}; \delta < p; \mu = \frac{\delta}{p} < 1$$

$$\text{Предел частичных сумм ряда: } \lim_{k \rightarrow \infty} S_k = \lim_{k \rightarrow \infty} \frac{1 + (-1)^k \mu^k}{1 + \mu} = \frac{1}{1 + \mu} = \frac{p}{p + \delta}$$

Сумма ряда равна

$$\sum_{j=0}^{\infty} (-1)^j \mu^j = 1 - \mu + \mu^2 - \mu^3 + \dots (-1)^j \mu^j + \dots = \frac{p}{p + \delta}$$

Для знакопеременного ряда при условии  $\mu = \frac{\delta}{p} < 1$  необходимое условие сходимости выполняется. По признаку Даламбера знакопеременный ряд сходится. При отрицательных значениях величин  $\mu$  аналогично будет получен положительно определенный сходящийся ряд.

*Следствие 1.* Для некоторого целого  $x_i < p_i, i \in \{1, \dots, n\}$  итерационная процедура (6) при  $\mu_i = \frac{\delta_i}{p_c}$

позволяет получить разложение в ряд (6) правильной рациональной дроби  $\frac{x_i}{p_c + \delta_i} = \frac{x_i}{p_i}$ :

$$\begin{aligned} x_i^0 &= x_i; x_i^1 = x_i(1 - \mu_i); \dots \\ x_i^{j+1} &= x_i - \frac{\delta_i}{p_c} x_i^j = x_i - \mu_i x_i^j \\ x_i^k &= x_i(1 - \mu_i + \mu_i^2 - \mu_i^3 + \dots (-1)^k \mu_i^k) \\ &\dots \end{aligned} \quad (7)$$

Процедура генерирует знакопеременный ряд, т.к. в соотношениях (6) на разных шагах степени переменных  $\mu_i$  принимают различные знаки,

*Следствие 2.* Для некоторого целого  $0 \leq x_i < p_i$  выполняется:

$$\frac{x_i}{p_i} = \frac{x_i}{p_c + \delta_i} = \frac{1}{p_c} x_i \sum_{j=0}^{\infty} (-1)^j \mu^j = \frac{x_i}{p_c} (1 - \mu + \mu^2 - \mu^3 + \dots (-1)^j \mu^j + \dots) \quad (8)$$

Выберем медианное модулярное основание. По аналогии с функцией  $\pi(x)$  – оценкой количества простых чисел меньших  $x$  – введем функцию выбора  $p_c = \psi(x)$ , ближайшего к  $x$  простого числа большего  $x$ . Установим ее элементарные свойства:

1.  $p_{\tilde{n}} = \psi(p_c)$  для простого числа  $p_c$ ;
2.  $\psi(\dots(\psi(x)\dots)) = \psi(x)$ ;
3.  $p_c - x = \psi(x) - x \geq 1$ ;
4.  $1 \leq |\psi(x) - x| \leq \delta$ .

На основе оценки Чебышева  $\pi(x) \approx \frac{x}{\ln x - 1}$  количества простых чисел меньших  $x$ , учитывая медленный рост логарифмической функции при больших значениях аргументов, получим приближенную оценку верхней границы:  $\pi(x + \delta) - \pi(x) = 1, \Rightarrow \delta \approx \ln x - 1 \leq \ln(x + \delta) - 1$ .

Аналогичным образом определяется функция выбора простого числа меньшего  $x$ .

Введенная функция позволяет выделить медианное модулярное основание, с последующим включением его в общее множество оснований модулярной системы счисления  $p_c \in \{p_1, \dots, p_n\}$ . Например, выберем основание являющееся средним значением других оснований модулярной системы счисления:  $p_c = \psi\left(\frac{1}{n-1} \sum_{i=1}^{n-1} p_i\right)$ .

При анализе последующих двойных сумм первая сумма индексируется символом  $i$ , а вторая сумма, индексируется символом  $j$ , который определяет номер шага процесса вычисления позиционной характеристики.

*Лемма 3.* Позиционная характеристика – нормированный ранг равна:

$$R_A = \left[ \sum_{i=1}^n \sum_{j=0}^{\infty} \frac{a_i (-1)^j \mu_i^j}{p_c} \right] = \left[ \sum_{i=1}^n \frac{a_i}{p_c} (\mu_i^0 - \mu_i^1 + \mu_i^2 - \dots - \mu_i^j \dots (-1)^t \mu_i^t \dots) \right] \quad (9)$$

Доказательство.

Введем вспомогательную функцию  $T_j = \sum_{i=1}^n a_i \delta_i^j$ , где  $\mu_i = \frac{\delta_i}{p_c}$

Формула (9) содержит следующие соотношения:

$$R_A = \left[ \frac{1}{p_c} \left( T_0 - \frac{1}{p_c} \left( T_1 - \frac{1}{p_c} \left( T_2 - \frac{1}{p_c} (T_3 - \dots) \right) \right) \right) \right] \quad (10)$$

На основе следствий леммы 1 при бесконечной второй сумме будет получено значение позиционной характеристики.

Лемма доказана.

Для технических приложений учет соотношений между основаниями  $\{p_1, \dots, p_i, \dots, p_n\}, p_c$  позволяет в формулах (8) и (9) прерывать вычисления на шаге, когда последующие слагаемые не влияют на вычисляемое выражение.

Формулы (8) и (9) определяют требования к конечному вычислительному процессу вычисления. При минимально необходимом количестве шагов процесса повышается скорость вычисления позиционной характеристики – ранг. Необходимо более двух шагов вычислительного процесса, который должен прерываться на четном шаге, что позволяет учесть различные знаки слагаемых первой суммы на последующем шаге. Необходимо, чтобы расчетный ранг, вычисленный на основе неточного ранга, был равен истинному рангу.

Рассмотрим вариант первичной оценки количества шагов процедуры вычисления позиционной характеристики – ранг.

*Теорема Т-1.* Позиционная характеристика – нормированный ранг для трех шагов при условии  $\sum_{i=1}^n (-1)^i \delta_i^3 < p_c$  вычисляется по формуле:

$$R_A = \left[ \sum_{i=1}^n \frac{a_i}{p_i} \right] = \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i + \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i (-1)^i \delta_i + \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i \delta_i^2 + \dots \right) \right] \right) \right] \right) \right] \quad (11)$$

*Доказательство.*

Используем для замены правильной рациональной дроби гладкую монотонно возрастающую функцию синус в диапазоне  $(-\pi/2; \pi/2)$ , что позволяет рассматривать позиционную характеристику как тригонометрическую сумму синусов некоторых углов. Уменьшая знаменатель, что увеличивает значение функции и в конечном случае увеличивается абсолютное значение невязок. Задав пределы изменения последней, можем установить соотношения, при которых прерывается процесс вычисления позиционной характеристики. Целое число  $\psi$  позволяет учесть, что при положительных невязках в отдельных дробях могут возникнуть вычеты, большие  $p_c$ .

Учтем близость величин оснований  $p_i$ , а неравенство  $p_c \geq \delta_i$  приравняем единице отношения компонент модулярного представления к медианному основанию, что даст первичную оценку формулы вычисления ранга для произвольных компонент модулярного представления числовой величины.

Полагая синусы всех углов равными единице, получим:

$$R_A \approx \dots + \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i \delta_i^2 + \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i (-1)^i \delta_i^3 \right) \right] \right) \right] = \dots + \left[ \left( \sum_{i=1}^n \sin \gamma_i \delta_i^2 + \frac{1}{p_c} \left[ \left( \sum_{i=1}^n \sin((-1)^i \gamma_i) \delta_i^3 \right) + \psi \right] \right) \right]$$

$$R_A \approx \left[ \sum_{i=1}^n \delta_i^0 + \frac{1}{p_c} \sum_{i=1}^n (-1)^i \delta_i^1 + \frac{1}{p_c^2} \sum_{i=1}^n \delta_i^2 + \frac{1}{p_c^3} \sum_{i=1}^n (-1)^i \delta_i^3 + \dots \right] \quad (12)$$

Анализ формулы (12), где  $\frac{1}{1+\mu_i} = \frac{p_c}{p_c + \delta_i}$ ;  $\mu_i = \frac{\delta_i}{p_c} < 1$ , показывает что:

- в третьем слагаемом дробная часть лежит между  $\frac{1}{p_c^2}$  и  $\frac{p_c^2 - 1}{p_c^2}$

- если четвертое слагаемое ограничено  $< \frac{1}{p_c^2}$ , то процесс вычисления позиционной характеристики прерывается, т.к. четвертое слагаемое не влияет на третье слагаемое и общий результат.

Если выполняется условие  $\sum_{i=1}^n (-1)^i \delta_i^3 < p_c$ , то  $\left| \frac{1}{p_c^3} \sum_{i=1}^n (-1)^i \delta_i^3 \right| < \frac{1}{p_c^2} = \frac{\gamma}{p_c^2}$  ( $\gamma < 1$ ), добавка к сумме четвертого слагаемого, меньшая  $\frac{1}{p_c^2}$ , не влияет на третье и на результат в формуле (12).

Условие  $\sum_{i=1}^n (-1)^i \delta_i^3 < p_c$  выдвигает требования к параметрам  $n$ ,  $p_c$ ,  $\{\delta_i, \dots\}$ . Требования уменьшают множество модулярных систем счисления, для которых уменьшается сложность вычисления позиционной характеристики, а результаты моделирования в Табл. 1 показывают, что множество таких систем не пусто. Теорема доказана.

Анализ формулы (12) показывает:

- четвертое слагаемое уменьшается суммированием слагаемых с разными знаками  $\delta_i$ ;
- для оснований с положительной невязкой возможно  $a_i > p_c$ . Тогда дробь записывается в виде

$$\frac{a_i}{p_c} = \left\lfloor \frac{a_i}{p_c} \right\rfloor + \frac{|a_i|_{p_c}}{p_c} = 1 + \sin \gamma_i;$$

- приравнивание единице отношения произвольной компоненты модулярного представления числовой величины к серединному основанию  $p_c \geq 0$  дает погрешность для положительных невязок, которая частично компенсируется встречной погрешностью для отрицательных невязок. Для положительных невязок выполняются неравенства  $\forall l \in U, \delta_l = p_l - p_c \geq 0$ , а для отрицательных выполняются неравенства  $\forall t \in V, \delta'_t = p_c - p_t > 0$ .

Оценим максимальное значение третьего слагаемого второй суммы, на котором можно прервать процесс вычисления позиционной характеристики. Пусть для некоторой числовой величины все вычеты равны нулю по основаниям, для которых невязки меньше нуля, и вычеты принимают максимальные значения по основаниям, для которых невязки больше нуля. В этом случае для прерывания процесса вычисления позиционной характеристики на третьем шаге должно выполняться неравенство:

$$\frac{1}{p_c^3} \sum_{i=1}^n x_i \delta_i^3 \leq \frac{1}{p_c^3} \sum_{i=1}^n (p_c + \delta_i - 1) \delta_i^3 = \frac{1}{p_c^3} \sum_{i=1}^n ((p_c - 1) \delta_i^3 + \delta_i^4) < 1. \quad (13)$$

Неравенство (13) может быть получено для всех числовых величин из вычислительного модулярного диапазона ограничением  $n$  и выбором параметров  $\{\delta_1, \dots, \delta_i, \dots, \delta_n\}, p_c$ , это показано на числовом примере в Табл. 1.

Рассмотрим выражения для  $T_2, T_3$ , где  $\xi < 1$ :

$$T_2 = \left\lfloor \frac{1}{p_c} \left( \sum_{i=1}^n a_i \delta_i^2 + \xi \right) \right\rfloor = \left\lfloor \frac{1}{p_c} \left( \sum_{i=1}^n a_i \delta_i^2 \right) \right\rfloor; T_3 = \left\lfloor \frac{1}{p_c} \sum_{i=1}^n a_i (-1) \delta_i^3 \right\rfloor < 1.$$

Невязки в  $T_3$  имеют разные знаки, что позволяет получить  $\left| \sum_{i=1}^n (-1) \delta_i^3 \right| < p_c$  и

$$\left\lfloor \frac{1}{p_c} \sum_{i=1}^n (-1) \delta_i^3 \right\rfloor = 0, \text{ следовательно: } R_A = \left\lfloor \sum_{i=1}^n \delta_i^0 + \frac{1}{p_c} \left[ \left( \sum_{i=1}^n (-1) \delta_i^1 + \left\lfloor \frac{1}{p_c} \left( \sum_{i=1}^n \delta_i^2 + 0 \right) \right\rfloor \right) \right] \right\rfloor.$$

**Теорема T-2.** Истинный нормированный ранг числовой величины, с использованием вспомогательных функций  $T_j = \sum_{i=1}^n a_i \delta_i^j$  вычисляется по формуле:

$$R_A = \left\lfloor \sum_{i=1}^n \frac{a_i}{p_i} \right\rfloor = \left\lfloor \frac{1}{p_c} \left( T_0 - \left\lfloor \frac{1}{p_c} \left( T_1 - \left\lfloor \frac{1}{p_c} T_2 \right\rfloor \right) \right\rfloor \right) \right\rfloor \quad (14)$$

*Доказательство.*

Введем вспомогательную функцию  $T_j = \sum_{i=1}^n a_i \delta_i^j$ . На основе леммы 3 при бесконечной второй сумме будет получено значение позиционной характеристики.

Вычисления в формуле (10) должны прерываться на некотором шаге, когда последующие слагаемые не влияют на вычисляемое выражение. Это достигается учетом соотношений между основаниями  $\{p_1, \dots, p_i, \dots, p_n\}, p_c$

Формула (10) содержит следующие соотношения:

$$R_A = \left[ \frac{1}{p_c} \left( T_0 - \frac{1}{p_c} \left( T_1 - \frac{1}{p_c} \left( T_2 - \frac{1}{p_c} (T_3 - \dots) \right) \right) \right) \right] \quad (15)$$

Для трех итераций получим:

$$R_A = \left[ \frac{1}{p_c} \left( T_0 - \frac{1}{p_c} \left( T_1 - \frac{1}{p_c} (T_2) \right) \right) \right] \quad (16)$$

Учитывая соотношение Виноградова-Бухштаба  $\left[ \frac{a}{p} \right] = \left[ \frac{[a]}{p} \right]$  для целого  $p$  и вещественного (рационального)  $a$ , а также, что отбрасываемые на каждом шаге дробные части меньше  $\frac{1}{p_c}$ , получим:

$$R_A = \left[ \sum_{i=1}^n \frac{a_i}{p_i} \right] \approx \left[ \frac{1}{p_c} \left( T_0 - \left[ \frac{1}{p_c} \left( T_1 - \left[ \frac{1}{p_c} T_2 - \left[ \frac{1}{p_c} (\dots) \right] \right) \right] \right) \right] \right] \quad (17)$$

Для трех итераций получим:

$$R_A = \left[ \sum_{i=1}^n \frac{a_i}{p_i} \right] \approx \left[ \frac{1}{p_c} \left( T_0 - \left[ \frac{1}{p_c} \left( T_1 - \left[ \frac{1}{p_c} T_2 \right] \right) \right] \right) \right] \quad (18)$$

Окончательно получим:

$$R_A \approx \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i \delta_i^0 + \frac{1}{p_c} \left( \sum_{i=1}^n a_i (-1) \delta_i^1 + \left[ \frac{1}{p_c} \left( \sum_{i=1}^n a_i \delta_i^2 \right) \right] \right) \right) \right] + \dots \quad (19)$$

*Следствие 1.* Случай равенства сумм абсолютных значений положительных и отрицательных разностей модулярных оснований с медианным основанием  $\sum_{l=1}^q |\delta_l| = \sum_{t=1}^z |\delta'_t|$  максимально учитывает разные знаки слагаемых первой суммы в отброшенном слагаемом с нечетной степенью по параметру  $j$ .

*Следствие 2.* Вычисление позиционной характеристики - истинный нормированный ранг  $R_A$  на основе приведенной теоремы содержит вычисление конечных сумм с  $n$  слагаемыми и имеет линейную сложность  $O(n)$  при последовательном выполнении и логарифмическую сложность  $O(\log n)$  при параллельном выполнении.

*Следствие 3.* Для вычислений  $R_A$  применимы формулы:

$$R_A = \left[ \sum_{i=1}^n \frac{a_i}{p_i} \right] = \left[ \frac{1}{p_c} \sum_{i=1}^n \left[ \frac{p_c a_i}{p_i} \right] + \frac{1}{p_c} \sum_{i=1}^n \frac{|p_c a_i|_{p_i}}{p_i} \right] = \left[ \frac{1}{p_c} \left( \sum_{i=1}^n \left[ \frac{p_c a_i}{p_i} \right] + \sum_{i=1}^n \frac{d_i}{p_i} \right) \right], \quad (20)$$

$$R_A = \left[ \sum_{i=1}^n \frac{a_i}{p_i} \right] = \left[ \frac{1}{p_c} \left( \sum_{i=1}^n \left[ \frac{p_c a_i}{p_i} \right] + \left[ \frac{1}{p_c} \left( T_0 - \left[ \frac{1}{p_c} \left( T_1 - \left[ \frac{1}{p_c} (T_2) \right] \right) \right) \right] \right) \right] \right], \quad (21)$$

где:  $d_i = |p_c a_i|_{p_i}$ ,  $T_0 = \sum_{i=1}^n d_i \delta_i^0$ ,  $T_1 = \sum_{i=1}^n d_i \delta_i^1$ ,  $T_2 = \sum_{i=1}^n d_i \delta_i^2$ .

*Следствие 4.* Для хранения разностей модулярных оснований с медианным основанием  $\delta_i \forall i \in \{1, \dots, n\}$  для модулярных оснований  $p_i \forall i \in \{1, \dots, n\}$  требуются линейные объемы памяти [3].

### 3. Экспериментальная проверка метода и примеры применения

Была выполнена полная числовая проверка метода, чтобы убедиться, что не учитываемые слагаемые второй суммы после третьего шага не влияют на значение позиционной характеристики. Проверка подтвердила, что вышеприведенные соотношения позволяют генерировать модулярные системы счисления и модулярные арифметики, в которых позиционные характеристики вычисляются линейно при указанных ограничениях. Метод вычисления позиционной характеристики приведен в теоремах 1, 2. Все ранее разработанные методы вычисления в ограниченном диапазоне одиночного основания для позиционных характеристик модулярного представления числовых величин имеют сложность, превышающую линейную, возможно для части числовых величин из полного вычислительного модулярного множества [4, 5, 9].

Соотношения, приведенные в теореме Т-2 и следствии 3 дают метод генерации модулярных систем счисления, имеющих линейную сложность вычисления в ограниченном диапазоне одиночного основания позиционной характеристики – истинный нормированный ранг числовой величины. Следовательно, линейную сложность вычисления имеют немодульные (не распараллеливаемые) операции модулярной арифметики, опирающиеся на вычисление позиционной характеристики [6, 7, 10].

В Табл. 1 приведен числовой пример вычисления позиционной характеристики.

Табл. 1. Пример вычисления позиционной характеристики – ранг числовой величины  $A$

| $p_i$                                                                               | $p_1=253$        | $p_2=255$        | $p_{\bar{n}} = p_3=256$ | $p_4=257$       | $p_5=259$       |
|-------------------------------------------------------------------------------------|------------------|------------------|-------------------------|-----------------|-----------------|
| $a_i$                                                                               | 98               | 38               | 14                      | 242             | 16              |
| $d_i =  p_c a_i _{p_i}$                                                             | 41               | 38               | 0                       | 15              | 211             |
| $\delta_i$                                                                          | -3               | -1               | 0                       | 1               | 3               |
| $\mu_i$                                                                             | $\frac{-3}{p_c}$ | $\frac{-1}{p_c}$ | 0                       | $\frac{1}{p_c}$ | $\frac{3}{p_c}$ |
| $\left[ \frac{p_c a_i}{p_i} \right]$                                                | 99               | 38               | 14                      | 241             | 15              |
| $D = \sum_{i=1}^5 \left[ \frac{p_c a_i}{p_i} \right]$                               | 407              |                  |                         |                 |                 |
| $T_2 = \left[ \frac{1}{p_c} \sum_{i=1}^5 d_i \delta_i^2 \right]$                    | 9                |                  |                         |                 |                 |
| $T_1 = \left[ \frac{1}{p_c} \left( \sum_{i=1}^5 d_i \delta_i - T_2 \right) \right]$ | 1                |                  |                         |                 |                 |
| $T_0 = \left[ \frac{1}{p_c} \left( \sum_{i=1}^5 d_i - T_1 \right) \right]$          | 1                |                  |                         |                 |                 |
| $R_A = \left[ \frac{1}{p_c} (D + T_0) \right]$                                      | 1                |                  |                         |                 |                 |

От датчика псевдослучайных чисел получена числовая величина  $A=194738406158$ . Точный ранг, вычисленный суммированием дробей со знаменателем  $P$  (полноразрядным методом), равен:

$$R_A = \left[ \sum_{i=1}^5 \frac{a_i}{p_i} \right] = \left[ \frac{1}{P} \sum D_i a_i \right] = 1, \text{ где } D_i = \frac{P}{p_i}. \text{ Для этого необходимы целочисленные вычисления в}$$

вычислительном диапазоне с верхней гранью  $P = \prod_{i=1}^n p_i$ . Применяя разработанный метод,  $R_A$  вычисляется на основе теоремы 2 по формулам (18) и (19). Промежуточные вычисления, для которых достаточен вычислительный диапазон с верхней гранью  $5p_c^2$ , представлены в Табл. 1.

Приведем примеры выбора модулярных оснований, ориентируясь на разрядности модулярных ЦВМ, разработанных в Специализированном вычислительном центре Министерства электронной промышленности (Зеленоградский научный центр микроэлектроники, главный конструктор Д.И. Юдицкий, научный руководитель проекта И. Я. Акушский). Разработанные специализированные ЦВМ 5Э53 (1971) и проекта 41-50 «Лидер» (1973) имели 40-разрядную бинарную сетку модулярного процессора и предназначались для замены в специализированных системах управляющего 32 разрядного компьютера с форматами данных на основе позиционного представления. Модулярные ЦВМ выпускались серийно и имели очень высокое быстродействие для своего времени [1, 2]. Используя соотношения разработанного метода для 42 битовой разрядной сетки модулярного процессора,  $n=5$ , содержащего три 8-битовых и два 9-битовых регистров, выберем взаимно-простые модули - основания модулярной системы:  $\{p_1, p_2, p_3, p_4, p_5\} = \{253, 255, 256, 257, 259\}$ . Для модулей выполняются соотношения: модуль 257 – простой; для трех модулей мультипликативные канонические разложения имеют вид:  $253=11 \cdot 23$ ;  $255=3 \cdot 5 \cdot 17$ ;  $259=7 \cdot 37$ ;  $256=2^8$ . Сформируем две группы взаимно-простых модулей, для которых выполняются следующие соотношения:

$$p_c = p_3 = 256 = 2^8 + 0;$$

$$p_1 = p_c - \delta'_1 = 253 = 2^8 - 3; \quad p_5 = p_c + \delta_1 = 259 = 2^8 + 3; \quad \delta_1 = 3;$$

$$p_2 = p_c - \delta'_2 = 255 = 2^8 - 1; \quad p_4 = p_c + \delta_2 = 257 = 2^8 + 1; \quad \delta_2 = 1;$$

$$\log_2 p_3 = \log_2 2^8 = 8 = 8.$$

$$\{p_1, p_2, p_3, p_4, p_5\} = \{253, 255, 256, 257, 259\} = \{11 \cdot 23, 3 \cdot 5 \cdot 17, 2^8, 257, 7 \cdot 37\}$$

$$\{\delta'_1, \delta'_2, \delta_3, \delta_4, \delta_5\} = \{-3, -1, 0, +1, +3\}.$$

При таком выборе модулярных оснований позиционная характеристика - нормированный ранг числовой величины, заданной модулярным представлением, последовательно вычисляется с линейной сложностью на 16 разрядном дополнительном операционном оборудовании. Вычислительный

диапазон 42 разрядного модулярного процессора равен  $P = \prod_{i=1}^5 p_i = 1'099'343'857'920$ , что превышает

целочисленный вычислительный диапазон  $4'294'967'296 = 2^{32}$  для 32-разрядной ЦВМ традиционной архитектуры на основе позиционной системы счисления.

Результаты моделирования показывают, что для вычисления в диапазоне меньшем квадрата однократного основания точного нормированного ранга по формуле (12) для всех чисел из модулярного вычислительного диапазона достаточно трех шагов вычислительного процесса.

Рассмотрим модулярный аналог 64-разрядного серийного компьютера, использующего позиционное представление числовых величин. Для разрядной сетки модулярного процессора 82 бит,  $n=5$ , содержащего три двоичных регистра по 16 бит и два двоичных регистра по 17 бит, выберем взаимно-простые модули - основания модулярной системы:  $\{p_1, p_2, p_3, p_4, p_5\} = \{65533, 65535, 65536, 65537, 65539\}$ , учитывая стандартный размер удвоенного двоичного байта. Для модулей выполняются

соотношения: модули 65537, 65539 – простые; для трех модулей мультипликативные канонические разложения имеют вид:  $65533=13 \cdot 71^2$ ;  $65535=3 \cdot 5 \cdot 17 \cdot 257$ ;  $65536=2^{16}$ . Сформируем две группы взаимно-простых модулей, для которых выполняются следующие соотношения:

$$p_c = p_3 = 65536 = 2^{16};$$

$$p_1 = p_c - \delta'_1 = 65533 = 2^{16} - 3; \quad p_5 = p_c + \delta_1 = 65539 = 2^{16} + 3; \quad \delta_1 = 3;$$

$$p_2 = p_c - \delta'_2 = 65535 = 2^{16} - 1; \quad p_4 = p_c + \delta_2 = 65537 = 2^{16} + 1; \quad \delta_2 = 1;$$

$$\log_2 p_c = \log_2 2^{16} = 16.$$

Вычислительный диапазон модулярного процессора равен

$$P = \prod_{i=1}^5 p_i = 1'208'925'816'799'879'408'189'440.$$

Процесс формирования оснований для модулярных компьютеров можно продолжить. Модулярный компьютер – аналог 128-разрядного позиционного компьютера – это 115-разрядный модулярный компьютер с основаниями: 65551 ( $\delta_1 = +15$ ), 65539 ( $\delta_2 = +3$ ), 65537 ( $\delta_3 = +1$ ), 65536 ( $\delta_4 = +0$ ), 65535 ( $\delta'_5 = -1$ ), 65533 ( $\delta'_6 = -3$ ), 65521 ( $\delta'_7 = -15$ ).

$$\{p_1, p_2, p_3, p_4, p_5, p_6, p_7\} = \{65521, 65533, 65535, 65536, 65537, 65539, 65551\}$$

$$\{\delta'_1, \delta'_2, \delta'_3, \delta_4, \delta_5, \delta_6, \delta_7\} = \{-15, -3, -1, 0, +1, +3, +15\}.$$

Вычислительная проверка медианного метода вычисления позиционной характеристика – ранг выполнена с использованием программы на а/я Python для всех числовых величин в модулярном представлении, из полного вычислительного диапазона для первого (байтного) набора оснований, при 10 разрядной точности вычислений показала 100% результат. Проверка потребовала более 38 часов работы персонального компьютера HP с параметрами: оперативная память 4 Гб, тактовая частота 3.9 ГГц под управлением ОС Windows 10.

Вычислительная проверка медианного метода вычисления позиционной характеристика – ранг выполнена с использованием универсального математического пакета Maple-8 для числовых величин в модулярном представлении, из полного вычислительного диапазона для первого (байтного) набора оснований, при 10 разрядной точности вычислений показала 100% результат. Проверка потребовала более 40 часов работы персонального компьютера HP с параметрами: оперативная память 4 Гб, тактовая частота 3.9 ГГц под управлением ОС Windows 10.

## Заключение

Разработанный метод выбора модулярных оснований и вычисления позиционной характеристики позволяет генерировать модулярные системы счисления и модулярную машинную арифметику, в которых позиционная характеристика – нормированный ранг (и аналогичные) вычисляются в диапазоне, меньшем квадрата одиночного основания, с линейной сложностью при последовательном выполнении вычислительного процесса, что при распараллеливании вычислительного процесса вычисления ПХ позволяет достичь логарифмической сложности. В таких модулярных арифметиках уменьшается сложность выполнения всех немодульных операций модулярной арифметики, так как в их основе лежит вычисление позиционной характеристики. Применение метода позволяет выполнять все немодульные операции с минимальной линейной сложностью. В исследованиях по модулярной алгоритмике в России и за рубежом отсутствуют методы вычисления позиционных характеристик при таких параметрах.

Все немодульные (не распараллеливаемые в модулярной арифметике) операции специализированного процессора с SIMD архитектурой (множество процессорных элементов для потоков данных и единый поток команд) базируются на вычислении позиционных характеристик. Метод содержит два этапа: выбор оснований модулярной системы счисления и итерационное вычисление позиционной

характеристики и предназначен для инженеров и разработчиков специализированных процессоров (сопроцессоров), обрабатывающих модулярные форматы данных. На основе модулярных систем счисления с наборами оснований, полученных разработанным методом, целесообразно создание специализированных модулярных процессоров SIMD-архитектуры.

## Литература

1. Акушкин И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Советское радио, 1968. 440 с.
2. Амербаев В.М. Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 320с.
3. Инютин С.А. Модулярная алгоритмика многообразных вычислений. М.: Из-во МАИ, 2020. 160 с.
4. Mandelbaum D. Further Results Decoding Arithmetic Residue Codes. // Transaction on Information Theory, 1998, vol. IT – 24, N 5. -P. 36-41.
5. Амербаев В. М., Стемпковский А.Л., Соловьев Р.А. Принципы рекурсивных модулярных вычислений // Информационные технологии. 2013. № 2. С. 22-27
6. David A. Patterson J., Hennessy L. Computer Organization and Design (Second Edition). London: Morgan Kaufmann Publishers, 2009. 715 p. ISBN 1-55860-428-6.
7. Инютин С.А. Метод вычисления количественной характеристики модулярной величины // Информационные технологии. 2016. Том 22. № 5. С. 343-347.
8. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. Под редакцией Червякова Н.И. М.: ФизМатЛит, 2016. 395с.
9. Munro I. The Computational Complexity of Algebraic and Numeric Problems (Second edition). New-York: American Elsevier pub. Co; 1986. 174p. ISBN 13: 9780444001566.
10. Инютин С.А. Метод вычисления характеристики отношения порядка для параллельных форматов данных // Информационные технологии. 2017. Том 23. № 8. С. 569-574.

**Инютин Сергей Арнольдович.** ФГБОУ ВО НИУ Московский авиационный институт (национальный исследовательский университет), Москва, Россия. Профессор кафедры, доктор технических наук, профессор. Область научных интересов: высокопроизводительные вычислительные системы, параллельные вычислительные процессы в больших компьютерных диапазонах, сложность алгоритмов, модулярные компьютеры, модулярная арифметика и алгоритмика, помехозащитное и криптографическое кодирование дискретной информации, анализ эффективности АСУ специального назначения. E-mail: inyutin\_sa@mail.ru

## A method for Calculating the Positional Characteristics of a Modular Representation with Linear Complexity

S. A. Inyutin

Moscow Aviation Institute (National Research University), Moscow, Russia

**Abstract.** A method has been developed for selecting base modules for generating modular number systems and modular arithmetic, in which the calculation of the positional characteristic of the modular representation of a numerical quantity, which is a nonlinear function of many variables, is performed with linear complexity from the number of bases of the modular number system when calculated in the range of a single base of the modular system. This significantly reduces the bit depth (hence the amount of hardware) of additional modular processor blocks. Modular algorithmics previously lacked methods for calculating positional characteristics for such parameters. All non-modular (not parallelizable in modular arithmetic) operations of a specialized processor with multiple processor elements (data streams) and a single instruction stream are based on the calculation of positional characteristics. For numerical quantities in modular data formats, the method allows them to be performed with minimal linear complexity. The article substantiates the formulation of the problem and the goal of fast calculation of positional features in modular data encoding. A new method is described and justified. The results of numerical modeling of the method and examples of modular number systems allowing its use are presented. The analysis is given the obtained of new results.

**Keywords:** modular arithmetic, modular number system, modular data formats, linear calculation complexity, positional characteristic, nonlinear function of many variables.

DOI 10.14357/20718632240111

EDN AYBEED

## References

1. Akushsky I.Ya., Yuditsky D.I. Machine arithmetic in residual classes. Sovetskoe radio; 1968. 440p. (In Russ.)
2. Amerbaev V.M. Theoretical foundations of machine arithmetic. Nauka; 1976. 320p. (In Russ.).
3. Inyutin S.A. Modular algorithmics of multi-bit computing. Moscow: Izdatel'stvo MAI; 2020. 160 p. (In Russ.).
4. Mandelbaum D. Further Results Decoding Arithmetic Residue Codes. // Transaction on Information Theory, 1998, vol. IT – 24, N 5. P. 36-41.
5. Amerbaev V. M., Stempkovsky A.L., Soloviev R.A. Principles of recursive modular computing // Informacionnye tekhnologii. 2013. No. 2. pp. 22-27. (In Russ.).
6. David A., Patterson J., Hennessy L. Computer Organization and Design (Second Edition). London: Morgan Kaufmann Publishers; 2009. ISBN 1-55860-428-6, pp. 715.
7. Inyutin S.A. Method of calculating the quantitative characteristics of a modular quantity. Informacionnye tekhnologii. 2016; 22(5): pp. 343-347. (In Russ.).
8. Chervyakov N.I. Modular arithmetic and its applications in infocommunication technologies. FizMatLit. 2016; 395 p. (In Russ.).
9. Munro I. The Computational Complexity of Algebraic and Numeric Problems. New-York: American Elsevier pub. Co; 1986. 174 p.
10. Inyutin S.A. Method of calculating the characteristics of the order ratio for parallel data formats // Informacionnye tekhnologii. 2017; 23(8): pp. 569-574. (In Russ.).

**Inyutin Sergey A.** Full professor, Doctor technical science. Nation Research University «Moscow Aviation Institute (MAI)», bl. 4, Volokolamsk road, Moscow, 125993, Russia. Area of scientific interests: high-performance computing systems, parallel computing processes in large computer ranges, complexity of algorithms, modular computers, modular arithmetic and algorithmic, algorithm interference-proof and cryptographic coding of discrete information, analysis of the effectiveness of special-purpose automated control systems. E-mail: inyutin\_sa@mail.ru