УДК 681.36 DOI: 10.17587/it.25.515-521

С. А. Инютин, д-р техн. наук, проф., e-mail: inyutin_int@mail.ru,
Московский авиационный институт (национальный исследовательский университет) (МАИ)

Дробно-рациональные конструкции в компьютерной модулярной арифметике

Анализируется расширение числовых модулярных представлений на множество рациональных дробей с фиксированным знаменателем. Разработаны методы выполнения основных компьютерных операций для таких представлений в разрядной сетке вычислительной реконфигурируемой системы. Разработаны и обоснованы алгоритмы их выполнения, получены оценки временной и табличной сложностей. Доказана целесообразность применения квадратичной модулярной системы для уменьшения сложности отдельных итерационных процедур, лежащих в основе операций над введенными модулярными представлениями, что обеспечивает квадратичную сложность. Введенные модулярные представления и соответствующие компьютерные форматы применимы в модулярных реконфигурируемых вычислительных системах SIMD-архитектуры.

Ключевые слова: *многопроцессорные реконфигурируемые вычислительные системы, SIMD-архитектура, вычислительный модулярный процесс, квадратичная сложность вычислений, параллельные компьютерные форматы для рациональных дробей*

Введение

Известно биективное отображение целых числовых величин из конечного числового подмножества на множество векторов модулярного представления, являющихся теоретической базой параллельных компьютерных форматов данных, обрабатываемых в модулярных процессорах [1]:

$$A \in \left[0, \ldots \prod_{i=1}^{n} p_i\right) \leftrightarrow (\alpha'_1, \alpha'_2, \ldots, \alpha'_n), \qquad (1)$$

где $\alpha'_i = |A|_{p_i}$ — наименьший неотрицательный вычет по модулю p_i целой числовой величины $A \in \left[0, \ldots \prod_{i=1}^{n} p_i\right)$, при условии $(p_i, p_j) = 1$, $\forall i, j \in \{1, \ldots, n\}$.

Целые простые (попарно взаимно простые) модули p_i называются основаниями модулярной (параллельной) системы счисления. Произведение оснований называется модулярным числовым диапазоном $P = \prod_{i=1}^{n} p_i$, порождающим полную систему (множество) наименьших неотрицательных вычетов. Этому множеству принадлежат числовые величины, обрабатываемые в модулярном процессоре. Модулярное представление для целых чисел является вектором. Компоненты модулярных векторов могут быть классическими вычетами или нормированными вычетами.

Для векторного модулярного представления числовых величин (1) получим нормированное модулярное представление:

$$A \leftrightarrow (\alpha'_1, \alpha'_2, \ldots, \alpha'_n) \leftrightarrow (\alpha_1, \alpha_2, \ldots, \alpha_n), \qquad (2)$$

где нормированные компоненты модулярного вектора $\alpha_i = \left|\alpha'_i \left|\frac{P}{p_i}\right|_{p_i}^{-1}\right|_{p_i} < p_i$.

Прямыми скобками с модулем в правой нижней части обозначена постфиксная форма бинарной операции $f(x, p) = |x|_p : \mathbf{N} \times \mathbf{N} \to |\circ|_p$, где $|\circ|_p$ — полная система наименьших неотрицательных вычетов по модулю p; $\mathbf{N} \times \mathbf{N}$ — декартово произведение множеств натуральных чисел.

Для числовых величин, имеющих модулярное векторное представление (2), выполняется аддитивное разложение

$$A = \sum_{i=1}^{n} \frac{\alpha_i}{p_i} P - \left[\sum_{i=1}^{n} \frac{\alpha_i}{p_i}\right] P = \sum_{i=1}^{n} \alpha_i P_i - \left[\sum_{i=1}^{n} \frac{\alpha_i}{p_i}\right] P, \qquad (3)$$

где $P_i = P/p_i$.

Квадратными скобками обозначена дискретная функция — наибольшая целая часть, не превышающая числовую величину в скобках.

Позиционной характеристикой — нормированным рангом числовой величины — называют введенную В. М. Амербаевым [1] функцию от нормированных компонент вектора

$$R_A = \varphi(\alpha_1,\ldots\alpha_n) = \left[\sum_{i=1}^{n}\frac{\alpha_i}{p_i}\right].$$

Ранг необходим для выполнения ряда операций над модулярными компьютерными форматами данных. Для точного вычисления нормированного ранга модулярного вектора необходим вычислительный диапазон P, который при эмуляции модулярной арифметики на серийных компьютерах для больших значений n и p_i значительно превосходит типовой машинный, что приводит к большой сложности вычисления функции. Разработан ряд методов вычисления ранга, один из которых с линейной сложностью принадлежит автору [2].

Введем ряд понятий, опираясь на терминологию работы [4]. Одинарная модулярная система построена с использованием простых оснований, и числовую величину в ней как элемент полной системы наименьших неотрицательных вычетов по модулю запишем в классическом виде $A(\mathrm{mod}P)$. Квадратичная модулярная система построена с использованием квадратов простых оснований, и числовую величину в ней запишем в виде $A(\mathrm{mod}P^2)$. Смешанная (одинарно-квадратичная) модулярная система построена с использованием простых оснований и квадратов оснований.

Модулярная разрядная сетка вычислительной системы — аппаратно-программное устройство (модель), состоящая из n элементарных ячеек, предназначенных для размещения и обработки вычетов по модулям, являющимся компонентами вектора модулярного представления числовой величины.

Модулярное представление для правильных рациональных дробей

Для области специализированной вычислительной техники, которая опирается на модулярное представление целых числовых величин, является актуальным обобщение этого представления на множество правильных рациональных дробей, что порождает модулярный дробно-рациональный формат данных. Введем модулярное представление для правильной рациональной дроби со знаменателем, равным модулярному диапазону. Получим аддитивное разложение для правильной модулярной дроби с нормированными компонентами модулярного представления:

$$\frac{A}{P} = \sum_{i=1}^{n}\frac{\alpha_i}{p_i} - R_A. \qquad (4)$$

Для отдельных дробей из правой части равенства (4) получим:

$$\forall j \in \{1\ldots n\} : \frac{A}{p_j} = \frac{\alpha_j P_j}{p_j} +$$

$$+\frac{1}{p_j}\sum_{i=1,\ i\neq j}^{n}\frac{\alpha_i P_j p_j}{p_i} - \frac{1}{p_j}R_A P_j p_j.$$

Вычет от числителя по выбранному модулю даст соответствующую компоненту модулярного представления в виде правильной дроби.

Разрядная сетка модулярных вычислительных систем предназначена для отображения вычетов по модулям. Совокупность таких вычетов по соответствующим модулям в зависимости от поставленной задачи можно считать разрядами модулярного представления целого числа или разрядами правильной рациональной дроби. Это различие влияет на алгоритмы выполнения операций.

Оценим приближение произвольной правильной рациональной дроби $\frac{V}{U}$ модулярной дробью $\frac{A}{P}$ следующим соотношением: $\left|\frac{V}{U}-\frac{A}{P}\right| \to \min$ или $\left|\left[\frac{VP}{U}\right]-A\right| \to \min$, где прямыми скобками обозначена абсолютная величина числа. Выполняются утверждения:

— в общем случае погрешность приближения не превышает значения $\frac{1}{P}$;

— для минимизации погрешности приближения необходимо выбирать максимальное из возможных значение P;

— нулевая погрешность приближения будет получена, если P есть мультипликативное каноническое разложение числа U.

Операции с модулярными дробями

Пусть даны модулярные представления правильных дробей:

$$\frac{A}{P} \leftrightarrow (\alpha_1,\alpha_2,\ldots,\alpha_n);$$

$$\frac{B}{P} \leftrightarrow (\beta_1,\beta_2,\ldots,\beta_n).$$

Для них выполняются аддитивные разложения:

$$\frac{A}{P}=\sum_{i=1}^{n}\frac{\alpha_i}{p_i}-R_A;\ \ \frac{B}{P}=\sum_{i=1}^{n}\frac{\beta_i}{p_i}-R_B.$$

Рассмотрим операцию сложения двух правильных модулярных дробей.

В кодонезависимой записи (независимой от выбора системы счисления для представления числовых величин) получим:

$$\frac{M}{P}=\frac{A}{P}+\frac{B}{P}=\frac{A+B}{P}=\frac{|A+B|_P}{P}+0\mid 1,$$

альтернативные варианты разделены вертикальной чертой, причем единица свидетельствует о переполнении вычислительного диапазона.

В кодозависимой записи для одинарной модулярной системы получим

$$\frac{M}{P}=\frac{|A+B|_P}{P}\leftrightarrow$$
$$\leftrightarrow(|\alpha_1+\beta_1|_{p_1},\ldots|\alpha_i+\beta_i|_{p_i},\ldots)=(\mu_1,\ldots\mu_i\ldots).$$

При суммировании двух операндов возможно переполнение вычислительного диапазона, которое устанавливается анализом нормированных рангов операндов и результата на основании следующей теоремы.

Теорема 1. Признаком переполнения одинарного вычислительного диапазона является выполнение выражения:

$$1=R_M+\sum_{i=1}^{n}\left[\frac{\alpha_i+\beta_i}{p_i}\right]-R_A-R_B. \qquad (5)$$

Доказательство.

При суммировании аддитивных разложений модулярных дробей получим

$$\frac{M}{P}=\frac{A}{P}+\frac{B}{P}=\sum_{i=1}^{n}\frac{\alpha_i}{p_i}-R_A+\sum_{i=1}^{n}\frac{\beta_i}{p_i}-R_B=$$
$$=\sum_{i=1}^{n}\frac{\alpha_i+\beta_i}{p_i}-R_A-R_B=$$
$$=\sum_{i=1}^{n}\frac{|\alpha_i+\beta_i|_{p_i}}{p_i}+\sum_{i=1}^{n}\left[\frac{\alpha_i+\beta_i}{p_i}\right]-R_A-R_B.$$

Вместе с тем выполняется соотношение

$$\frac{M}{P}=\frac{|A+B|_P}{P}=\sum_{i=1}^{n}\frac{|\alpha_i+\beta_i|_{p_i}}{p_i}-\left[\sum_{i=1}^{n}\frac{|\alpha_i+\beta_i|_{p_i}}{p_i}\right]=$$
$$=\sum_{i=1}^{n}\frac{|\alpha_i+\beta_i|_{p_i}}{p_i}-R_M.$$

Следовательно, признаком переполнения модулярного вычислительного диапазона является выполнение следующего равенства:

$$R_M+\sum_{i=1}^{n}\left[\frac{\alpha_i+\beta_i}{p_i}\right]-R_A-R_B=1.$$

Следствие. Для выполнения операции сложения с определением переполнения (5) необходимо вычисление трех позиционных характеристик — рангов числовых величин A, B, M, что при определенных условиях возможно с линейной сложностью [2].

Рассмотрим операции умножения двух дробей и дроби на целое число и выделим в них общие этапы.

Результатом операции умножения правильной рациональной дроби на целое число является неправильная дробь — целое число и правильная рациональная дробь. В кодонезависимой записи получим: $\frac{A}{P}\cdot D=\left[\frac{A\cdot D}{P}\right]+\frac{|A\cdot D|_P}{P}$.

Рассмотрим операцию умножения двух правильных модулярных дробей. Это произведение вычисляется с погрешностью из-за ограниченности разрядной сетки вычислительной системы, что требует выполнения операции деления на P в соответствии с кодонезависимым соотношением:

$$\frac{C}{P}=\frac{A}{P}\cdot\frac{B}{P}=\frac{\left[\frac{A\cdot B}{P}\right]+\frac{|A\cdot B|_P}{P}}{P}\cong\frac{\left[\frac{A\cdot B}{P}\right]}{P}.$$

Рассмотрим аналогичные соотношения в модулярной системе. Для операции умножения правильной рациональной дроби на целое число результатом является неправильная дробь в модулярном представлении:

$$\frac{|A|_p}{P}\cdot|D|_P=\frac{|A\cdot D|_{P^2}}{P}=$$
$$=\left[\frac{A\cdot D}{P}\right](\mathrm{mod}\ P\ )+\frac{A\cdot D(\mathrm{mod}\ P)}{P}. \qquad (6)$$

Для операции умножения двух правильных рациональных дробей получим соотношения, зависимые от модулярной системы счисления:

$$\frac{C(\mathrm{mod}\ P)}{P}=\frac{A(\mathrm{mod}\ P)}{P}\cdot\frac{B(\mathrm{mod}\ P)}{P}=$$
$$=\frac{A\cdot B(\mathrm{mod}\ P^2)}{P^2}= \qquad (7)$$
$$=\frac{\left[\frac{|A\cdot B|_{P^2}}{P}\right]+\frac{|A\cdot B|_P}{P}}{P}\approx\frac{\left[\frac{A\cdot B(\mathrm{mod}\ P^2)}{P}\right](\mathrm{mod}\ P)}{P}.$$

В соотношениях (6), (7) присутствует операция вычисления целой части от деления на одинарный диапазон произведения модулярных величин. Для ее выполнения можно использовать квадратичную модулярную систему. Рассмотрим алгоритм выполнения этой операции и проанализируем соотношения, лежащие в его основе.

Теорема 2. Произведение двух целых модулярных величин, заданных в одинарной модулярной системе, в квадратичной модулярной системе имеет вид

$$C = A \cdot B (\mathrm{mod}\, P^2) = \left(|A \cdot B|_P + \left[\frac{A \cdot B}{P} \right] P \right) (\mathrm{mod}\, P^2);$$

$$C = A (\mathrm{mod}\, P) \cdot B (\mathrm{mod}\, P) =$$

$$= A \cdot B (\mathrm{mod}\, P^2) \leftrightarrow \left(\tilde{s}_1 (\mathrm{mod}\, p_1^2) \ldots \tilde{s}_i (\mathrm{mod}\, p_i^2) \ldots \right) =$$

$$= (s_i + k_i p_i (\mathrm{mod}\, p_i^2), \ldots s_i + k_i p_i (\mathrm{mod}\, p_i^2), \ldots),$$

где для числовых коэффициентов выполняются неравенства $s_i, k_i < p_i$; $\tilde{s}_i < p_i^2$.

Доказательство.

Пусть две величины представлены ненормированными вычетами в одинарной модулярной системе. Запишем их аддитивные разложения:

$$A = \sum_{i=1}^{n} \frac{\alpha'_i m_i P}{p_i} - \left[\sum_{i=1}^{n} \frac{\alpha'_i m_i}{p_i} \right] P =$$

$$= \frac{\alpha'_j m_j P}{p_j} + \sum_{i \neq j}^{n} \frac{\alpha_i m_i P}{p_i} - \left[\sum_{i=1}^{n} \frac{\alpha'_i m_i}{p_i} \right] P;$$

$$B = \sum_{i=1}^{n} \frac{\beta'_i m_i P}{p_i} - \left[\sum_{i=1}^{n} \frac{\beta'_i m_i}{p_i} \right] P =$$

$$= \frac{\beta'_j m_j P}{p_j} + \sum_{i \neq j}^{n} \frac{\beta'_i m_i P}{p_i} - \left[\sum_{i=1}^{n} \frac{\beta'_i m_i}{p_i} \right] P.$$

Результат произведения $A \cdot B (\mathrm{mod} P)$ в квадратичной модулярной системе имеет вид:

$$|A \cdot B|_{P^2} \leftrightarrow (\alpha'_1 \beta'_1 m_1 m_1 (\mathrm{mod}\, p_1^2), \ldots$$

$$\ldots \alpha'_i \beta'_i m_i m_i (\mathrm{mod}\, p_i^2) \ldots) =$$

$$= ((\tilde{\alpha}_1 + k_1 p_1) \cdot (\tilde{\beta}_1 + d_1 p_1) (\mathrm{mod}\, p_1^2), \ldots$$

$$\ldots (\tilde{\alpha}_i + k_i p_i) \cdot (\tilde{\beta}_i + d_i p_i) (\mathrm{mod}\, p_i^2) \ldots) =$$

$$= (x_1 + y_1 p_1 (\mathrm{mod}\, p_1^2), \ldots x_i + y_i p_i (\mathrm{mod}\, p_i^2) \ldots).$$

Для векторных компонент, возникающих на промежуточных этапах, выполняются соотношения $\tilde{\alpha}_i, \tilde{\beta}_i, x_1, k_i, d_i, y_i < p_i$.

Найдем произведение аддитивных разложений числовых величин:

$$A \cdot B = \frac{\alpha'_j \beta'_j m_j^2 P_j^2}{p_j^2} + \left(\sum_{i \neq j}^{n} \frac{\alpha'_i m_i P_j}{p_i} \cdot \sum_{i \neq j}^{n} \frac{\beta'_i m_i P_j}{p_i} \ldots \right) p_j +$$

$$+ \left[\sum_{i=1}^{n} \frac{\beta'_i m_i}{p_i} \right] \cdot \left[\sum_{i=1}^{n} \frac{\alpha'_i m_i}{p_i} \right] P^2.$$

Вычислим ненормированные вычеты произведения в квадратичной модулярной системе на примере вычисления одной компоненты вектора представления:

$$|A \cdot B|_{p^2} = \left| \alpha'_j \beta'_j \right|_{p^2} + k_j p_j (\mathrm{mod}\, p_j^2) =$$

$$= \left| \alpha'_j \beta'_j \right|_{p_j} + \left[\frac{\alpha'_j \beta'_j}{p_j} \right] p_j + k_j p_j (\mathrm{mod}\, p_j^2) =$$

$$= \left| \alpha'_j \beta'_j \right|_{p_j} + \left| \left[\frac{\alpha'_j \beta'_j}{p_j} \right] + k_j \right|_{p_j} p_j (\mathrm{mod}\, p_j^2),$$

где для числового коэффициента выполняется соотношение $k_j < p_j$.

Теорема доказана.

Рассмотрим операцию отображения в квадратичный модулярный диапазон числовой величины, заданной в одинарном модулярном диапазоне:

$$|A|_{P^2} = \left| \sum_{i=1}^{n} \frac{\alpha_i}{p_i} P - R_A P \right|_{P^2}.$$

Вычислим компоненты вектора представления в квадратичном диапазоне на примере вычисления одной компоненты:

$$|A|_{p_j^2} = \left| \sum_{i=1}^{n} \frac{\alpha_i}{p_i} P - R_A P \right|_{p_j^2} =$$

$$= \left| \alpha_j P_j + \sum_{i=1, i \neq j}^{n-1} \alpha_i P_i - R_A P \right|_{p_j^2} = \left| \alpha_j P_j \right|_{p_j^2} + x_j p_j =$$

$$= \left| \alpha_j P_j \right|_{p_j} + \left| \left[\frac{\left| \alpha_j P_j \right|_{p_j^2}}{p_j} \right] + x_j \right|_{p_j} p_j (\mathrm{mod}\, p_j^2),$$

где выполняется условие $x_j < p_j$ для числа, полученного при промежуточных вычислениях.

Рассмотрим алгоритм деления числовой величины на числовой диапазон одинарной модулярной системы в модулярной системе квадратичного диапазона:

$$C = A \cdot B (\mathrm{mod}\, P^2) = |A \cdot B|_P + \left[\frac{A \cdot B}{P} \right] P (\mathrm{mod}\, P^2).$$

На входе алгоритма дано произведение модулярных представлений числовых величин в квадратичной модулярной системе:

$$C = A(\mathrm{mod}\, P)\cdot B(\mathrm{mod}\, P) = A\cdot B(\mathrm{mod}\, P^2) \leftrightarrow$$
$$\leftrightarrow (\tilde{s}_1(\mathrm{mod}\, p_1^2)\ldots\tilde{s}_i(\mathrm{mod}\, p_i^2)\ldots) =$$
$$= (s_1 + d_1 p_1(\mathrm{mod}\, p_1^2),\ldots s_i + d_i p_i(\mathrm{mod}\, p_i^2),\ldots)$$
$$\forall i \in \{1,\ldots n\}; s_i, d_i < p, \tilde{s}_i < p_i^2.$$

Обозначим

$$C = C^1 \leftrightarrow$$
$$\leftrightarrow (s_1^1 + d_1^1 p_1(\mathrm{mod}\, p_1^2),\ldots s_i^1 + d_i^1 p_i(\mathrm{mod}\, p_i^2),\ldots),$$

где верхний индекс в векторных компонентах означает номер итерации в алгоритме.

Алгоритм деления.

1. Вычитание элемента компоненты s_1^1 и деление на основание p_1 в каждой векторной компоненте модулярного представления числовой величины:

$$\frac{C^1 - s_1^1}{p_1} \leftrightarrow$$
$$\leftrightarrow (d_1^1(\mathrm{mod}\, p_1),\ldots(s_i^1 + d_i^1 p_i - s_1^1)|p_1|_{p_i^2}^{-1}(\mathrm{mod}\, p_i^2),\ldots) =$$
$$= (d_1^1(\mathrm{mod}\, p_1),\ldots(s_i^2 + d_i^2 p_i)(\mathrm{mod}\, p_i^2),\ldots) =$$
$$= (d_1^2(\mathrm{mod}\, p_1),\ldots(s_i^2 + d_i^2 p_i)(\mathrm{mod}\, p_i^2),\ldots) = C^2.$$

2. Вычитание элемента s_2^2 следующей компоненты и деление на основание p_2 в каждой компоненте представления числовой величины:

$$\frac{C^2 - s_2^2}{p_2} \leftrightarrow ((d_1^2 - s_2^2)|p_2|_{p_1}^{-1}(\mathrm{mod}\, p_1),\ldots$$
$$\ldots(s_i^2 + d_i^2 p_i - s_2^2)|p_2|_{p_i^2}^{-1}(\mathrm{mod}\, p_i^2),\ldots) =$$
$$= (s_1^3(\mathrm{mod}\, p_1),\ldots s_i^3 + d_i^3 p_i(\mathrm{mod}\, p_i^2),\ldots) = C^3.$$

3. Операции из пунктов 1—2 выполняются для всех остальных оснований модулярной системы.

Выражения на различных этапах алгоритма представлены в смешанных одинарно-квадратичных модулярных системах.

На выходе алгоритма после выполнения n этапов получен результат в одинарной модулярной системе $\dfrac{C - |A\cdot B|_P}{P} \equiv \left[\dfrac{A\cdot B}{P}\right](\mathrm{mod}\, P)$.

Одинарный диапазон в квадратичной модулярной системе имеет представление:

$$P(\mathrm{mod}\, P^2) \leftrightarrow$$
$$\leftrightarrow (|P_1|_{p_1} p_1(\mathrm{mod}\, p_1^2);\ldots.|P_i|_{p_i} p_i(\mathrm{mod}\, p_i^2),\ldots).$$

Это позволяет получить представление модулярной величины в квадратичном диапазоне:

$$|A\cdot B|_P = C - \left[\frac{A\cdot B}{P}\right] P(\mathrm{mod}\, P^2).$$

Запишем преобразование, выполняемое на каждом шаге приведенного алгоритма деления, на алгоритмическом псевдоязыке в нотации работы [3]. Такой подход позволяет получить компактную запись сложных алгоритмов, выделив повторяющиеся последовательности преобразований в отдельные процедуры, вызываемые в последующих этапах и алгоритмах.

Algorithm SD

На входе задан одномерный массив, элементами которого являются вычеты по модулям — квадратам оснований $C(1:n) \leftrightarrow (\ldots\tilde{s}_i\ldots)$.

1. $i \leftarrow 1$
2. $\tilde{s}_i \leftarrow \left(\tilde{s}_i - |\tilde{s}_j|_{p_j}\right)\cdot |p_j|_{p_i}^{-1}$
3. $s_i \leftarrow |\tilde{s}_i|_{p_i}$
4. $d_i \leftarrow \left[\dfrac{\tilde{s}_i - s_i}{p_i}\right]$
5. $\tilde{C}(i) \leftarrow (s_i, d_i)$
6. $i \leftarrow i + 1$
7. *if* $i \leqslant n$ *then goto* 2 *else exit*
8. *exit* : $\tilde{C}(1:n)$
9. *comment*: $\tilde{C}(1:n) \leftrightarrow (\ldots(s_i, d_i)\ldots)$

Для оценки сложности запишем алгоритм деления на алгоритмическом псевдоязыке.

Algorithm Division

$$C^1 \leftrightarrow (\ldots(s_i^1, d_i^1)\ldots) \leftarrow C \leftrightarrow (\ldots(s_i, d_i)\ldots)$$

1. $j \leftarrow 1$
2. $C^{j+1} \leftarrow call\ SD(C^j)$
3. *comment* $C^{j+1} \leftarrow \left[\dfrac{C^j - s^j}{p^j}\right]$
4. $C^{j+1} \leftrightarrow (\ldots(s_i^{j+1}, d_i^{j+1})\ldots)$
5. $j \leftarrow j + 1$
6. *if* $j \leqslant n$ *then goto* 2 *else exit*
7. *exit*: C^{n+1}
8. *comment*: $C^{n+1} = \left[\dfrac{A\cdot B(\mathrm{mod}\, P^2)}{P}\right](\mathrm{mod}\, P);$
$|A\cdot B|_P(\mathrm{mod}\, P^2) = C^1 - C^{j+1}P(\mathrm{mod}\, P^2)$

Для n-разрядного модулярного процессора (*n-modular processor*) найдем оценки сложности. Временная сложность алгоритма $time = O(n^2)$. Таблицы констант $\left|p_i\right|_j^{-1}$, используемых на n этапах алгоритма, имеют квадратичную размерность (оба индекса принадлежат одному множеству $\forall i, j \in \{1,\ldots n\}$). Назовем оценку их объема табличной сложностью алгоритма $const = O(n^2)$ [4]. Таблицы с константами целесообразно хранить в дополнительной машинной памяти и загружать оперативно по мере необходимости в процессе вычислений [5].

Запишем на алгоритмическом псевдоязыке алгоритмы и получим оценки временной и табличной сложностей рассмотренных операций сложения и умножения модулярных рациональных дробей, учитывая оценки сложности алгоритма деления. В рассматриваемых операциях используется единый набор констант.

Algorithm Addition

На входе алгоритма модулярные представления дробей $\frac{A}{P} \leftrightarrow (\ldots\alpha_i\ldots); \frac{B}{P} \leftrightarrow (\ldots\beta_i\ldots)$.

1. $i \leftarrow 1; m \leftarrow 0$
2. $\mu_i \leftarrow \left|\alpha_i + \beta_i\right|_{p_i}$
3. $M(i) \leftarrow \mu_i$
4. $m \leftarrow m + \left[\frac{\alpha_i + \beta_i}{p_i}\right]$
5. $i \leftarrow i + 1$
6. *if* $i \leqslant n$ *then goto* 2 *else* 7
7. $rang(A) \leftarrow Call\ \ Rang(A)$
8. $rang(B) \leftarrow Call\ \ Rang(B)$
9. $rang(M) \leftarrow Call\ \ Rang(M)$
10. $priznak \leftarrow rang(A) + rang(B) - rang(M) - m$
11. *exit*: $M(1:n); priznak$
12. *comment*: $\frac{M(1:n)}{P} \leftrightarrow (\ldots\mu_i\ldots);$
    $priznak = rang(A) + rang(B) - rang(M) - m$

Сложность операции сложения с определением переполнения

$$time = 3T_{rang} + O(1),\ const = O(n^2),$$

где T_{rang} — временная сложность операции вычисления ранга — позиционной характеристики модулярной числовой величины. При определенных условиях операция вычисления ранга имеет линейную сложность, получим $time = O(n) + O(1)$, $const = O(n^2)$.

Algorithm Multiplication (for fraction)

На входе алгоритма

$$\frac{A}{P} \leftrightarrow (\alpha_1,\ldots\alpha_i\ldots); \frac{B}{P} \leftrightarrow (\beta_1,\ldots\beta_i\ldots)$$

1. $i \leftarrow 1$
2. $\mu_i \leftarrow \left|\alpha_i \cdot \beta_i\right|_{p_i^2}$
3. $C(i) \leftarrow \mu_i$
4. $i \leftarrow i + 1$
5. *if* $i \leqslant n$ *then goto* 2 *else* 6
6. $W = Call\ \ Division(C)$
7. *exit*: $W(1:n)$
8. *comment*: $W(1:n) \leftrightarrow (\ldots\omega_i\ldots)(\mathrm{mod}\ P)$

Найдем сложность операции умножения с округлением результата до дроби со знаменателем — одинарным модулярным диапазоном $time = O(n^2) + O(1)$; $const = O(n^2)$.

Рассмотрим модулярные рациональные дроби с произвольным знаменателем. Определим вычет от рационального числа по простому модулю p следующим образом:

$$\left|\frac{a}{b}\right|_P = \left|a \cdot \left|b\right|_P^{-1}\right|_P = n \in \{0,1,\ldots p-1\} \subset \mathbf{N};\ (b,p) = 1.$$

При условии $p > \max\{a, b\}$ однозначно восстанавливается числитель рациональной дроби при известном знаменателе, что обеспечивает биективность отображения.

В операции сложения вычетов для однозначности восстановления результата, т.е. перехода от вычетов к рациональным дробям, условием изоморфизма отображения является неравенство $p > \max\{ad + cb, bd\}$:

$$\left|\left|\frac{a}{b}\right|_P + \left|\frac{c}{d}\right|_P\right|_p = \left|(ad + cb)\left|d\right|_P^{-1}\left|b\right|_P^{-1}\right|_P =$$

$$= \left|(a\left|b\right|_P^{-1} + c\left|d\right|_P^{-1})\right|_P = \left|\frac{ad + cb}{bd}\right|_P =$$

$$= \left|n_1 + n_2\right|_P = n \in \{0,1,\ldots p-1\} \subset \mathbf{N}.$$

Условие изоморфизма для дробно-рационального модулярного представления имеет вид $\tilde{P} \geqslant \max\left\{\sum_{i=1}^{n} \frac{\alpha_i}{p_i} P, P\right\}$ или $\tilde{P} \geqslant nP$, что соответствует условию точного вычисления нормированного ранга [6].

Заключение

В классах вычислительных процессов, в которых операнды и результаты операций являются рациональными дробями, модулярные представления для правильных и неправильных рациональных дробей позволяют организовать высокопроизводительный параллельный вычислительный процесс на системах с SIMD-архитектурой. Такие вычислительные архитектуры в явном или латентном виде используются в современных многопроцессорных системах. Эти системы содержат в своем составе множество центральных процессоров CPU и графических ускорителей GPU, что позволяет эффективно организовать параллельные многоядерные вычислительные процессы с данными в целочисленных и дробно-рациональных модулярных форматах.

Введенные соотношения показывают непосредственную связь дробно-рационального модулярного представления числовых величин с вычетами по модулю от правильных рациональных дробей. Использование квадратичной модулярной системы для отдельных операций в модулярной арифметике позволяет ряд вычислительно-сложных процедур выполнять с квадратичной временной и табличной сложностью, что удовлетворяет требованиям, предъявляемым к аппаратным и программным реализациям модулярной арифметики [7].

Список литературы

1. **Амербаев В. М.** Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 320 с.
2. **Инютин С. А.** Метод вычисления характеристики отношения порядка для параллельных форматов данных // Информационные технологии. Т. 24, № 7. 2017. С. 343—347.
3. **Ноден П., Китте К.** Алгебраическая алгоритмика. М.: Мир, 1999. 720 с.
4. **Инютин С. А.** Основы модулярной алгоритмики. Ханты-Мансийск: Полиграфист, 2009. 237 с.
5. **Столярский Е. З., Шилов В. В.** Организация и работа кэш-памяти // Информационные технологии. 2000. № 7. С. 2—8.
6. **Инютин С. А.** Анализ сложности многоразрядных вычислительных процессов // Научные труды МАТИ. 2014. Вып. 22 (94). С. 154—159.
7. **Амербаев В. М., Стемпковский А. Л., Соловьев Р. А.** Принципы рекурсивных модулярных вычислений // Информационные технологии. 2013. № 2. С. 22—27.

S. A. Inyutin, Dr. Tech. Sc. (PhD), Full Professor, e-mail: inyutin_int@mail.ru,
Moscow Aviation Institute (Nation Research University) (MAI)

Fraction-Rational Constructions in Computer Modular Arithmetic

The expansion of modular representations to a set of rational fractions with a fixed denominator is analyzed. Methods have been developed for performing basic computer operations for such representations in the bit grid of a computational reconfigurable system. Given in pseudo-language and justified algorithms for their implementation, obtained estimates of their temporal and tabular complexities. The expediency of using a quadratic modular system to reduce the complexity of individual iterative procedures that underlie operations on the introduced modular representations and which have quadratic complexity has been proved. The representations introduced are intended for use in modular reconfigurable computing SIMD systems.

Keywords: *multiprocessor reconfigurable calculation systems SIMD architecture, modular computational process, quadratic computational complexity, parallel computer formats for rational fractions*

DOI: 10.17587/it.25.515-521

References

1. **Amerbaev V. M.** Theoretic base computer arithmetic, Alma-Ata, Nauka, 1976, 320 p. (in Russian).
2. **Inyutin S. A.** *Informatsionnyie Tehnologii*, 2017, no. 7, vol. 24, pp. 343—347 (in Russian).
3. **Noden P., Kitte K.** Algebra algorithmic, Moscow, Mir, 1999, 720 p. (in Russian).
4. **Inyutin S. A.** Base at modular algorithmic, Hantyi-Mansiysk, Poligrafist, 2009, 237 p. (in Russian).
5. **Shilov V. V., Stolyarskiy E. Z.** *Informatsionnyie Tehnologii*, 2000, no. 7, pp. 2—8 (in Russian).
6. **Inyutin S. A**. *Nauchnyie Trudyi MATI*, 2014, vol. 22 (94), pp. 154—159 (in Russian).
7. **Amerbaev V. M., Stempkovsky A. L., Solovjev R. A.** Informatsionnyie tehnologii, 2013, no. 2, vol. 5, pp. 22—27 (in Russian).