S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Том 22, № 1, стр. A62–A86 (2025) УДК 511.221
https://doi.org/10.33048/semi.2025.22.A06 MSC 11A07

РАНГ ЧИСЛА СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ И ЕГО СВОЙСТВА

М.Г. Бабенко, М.В. Валуева, Г.В. Валуев, А.С. Назаров

Посвящается 75-летию Василия Ивановича Васильева

Abstract: The residue number system is widely used in systems using addition and multiplication operations to increase their performance. However, operations such as converting numbers to and from the reside number system, the sign detection, and the numbers comparison are computationally complex in the residue number system and limit its practical application.The article presents the methods for calculating the number rank to the implementation of the reverse conversion operation of numbers from the residue number system to the positional number system. The possibility of representing the core function as an algebraic polynomial over $\mathbb{Z}_P$ for efficient calculation of the number rank is investigated. The article develops methods for calculating the number rank by an approximate method. The accuracy of calculations for the approximate method was assessed.

Keywords: residue number system, Chinese remainder theorem, number rank, core function

Babenko, M.G., Valueva, M.V., Valuev, G.V., Nazarov, A.S. The number rank of residue number system and its properties.

Работа поддержана Российским Научным Фондом, грант №23-71-30013, https://rscf.ru/project/23-71-30013/.

Поступила 4 февраля 2025 г., опубликована 30 августа 2025 г.

1 Введение

Система остаточных классов (Residue Number System – RNS) – это непозиционная система счисления, в которой числа представляются в виде остатков от деления на попарно взаимно простые модули системы. Таким образом, число $X \in \mathbb{Z}$ может быть однозначно представлено в RNS с набором модулей $(p_1,\ p_2, \ldots, p_n)$ в виде $X \xrightarrow{RNS} (x_1,\ x_2, \ldots, x_n)$, $n \in \mathbb{N}$. При этом $0 \leq X < P$ и $P = \prod_{i=1}^{n} p_i$ – динамический диапазон RNS. Операции сложения, вычитания и умножения производятся параллельно по каждому модулю RNS.

К преимуществам RNS относится возможность представления чисел большой разрядности в виде остатков от деления меньшей разрядности, что уменьшает сложность вычислений по каждому каналу, соответствующему модулям RNS. Еще одним достоинством RNS является отсутствие зависимостей между вычислительными каналами, поэтому, ошибка в одном канале не распространяется на другие, что, облегчает процесс обнаружения и исправления ошибок.

RNS широко применяется для увеличения быстродействия цифровых устройств в приложениях цифровой обработки сигналов [1, 2], в частности, при обработке и анализе изображений [3, 4, 5]. Так же RNS используется в безопасных системах хранения и обработки данных [6, 7].

Несмотря на достоинства RNS существует ряд операций, которые являются вычислительно сложными в RNS. К ним относят операцию прямого преобразования из позиционной системы счисления (Positional Number System – PNS) в RNS и обратное преобразование из RNS в PNS. Кроме того, операции определения знака числа, сравнения чисел и деления так же являются вычислительно сложными в RNS. Снижение вычислительной сложности перечисленных операций позволит расширить области применения RNS.

Одним из подходов к решению проблемы преобразования чисел из одной системы счисления в другую является использование модулей специального вида 2^α и $2^\alpha \pm 1$, $\alpha \in \mathbb{N}$ [8, 9, 10]. Данный подход позволяет заменить операцию деления по модулю операциями сложения и битового сдвига, что позволяет уменьшить вычислительную сложность.

Проблема ускорения вычислительно сложных операций в RNS, таких как определение знака числа, сравнение чисел и перевод чисел из RNS в позиционную систему счисления, может решаться за счет уменьшения вычислительной сложности алгоритма определения ранга числа. Однако, основным приложением функции ранга числа, представленного в RNS, являются алгоритмы обнаружения и исправления ошибок арифметических вычислений, и от эффективности его вычисления во многом зависит производительность указанных алгоритмов. Чтобы добиться приемлемой задержки, требуется разработать такие алгоритмы вычисления ранга числа, представленного в RNS $X \xrightarrow{RNS} (x_1, x_2, \ldots, x_n)$, которые бы позволили вычислять значение ранга за время модулярного

суммирования не более чем n вычетов по модулю q. При этом подразумевается, что величина модуля q приблизительно одного порядка с величиной модулей RNS p_i [11].

Учитывая, что в RNS можно эффективно реализовать операции сложения и умножения чисел в $\mathbb{Z}_P$, одним из способов решения проблемы эффективного вычисления ранга могло бы стать представление функции ядра в виде алгебраического многочлена над $\mathbb{Z}_P$. В данной статье показано, что функцию ядра, нормализованную функцию ядра и функцию ядра Акушского нельзя вычислить с помощью алгебраического многочлена над $\mathbb{Z}_P$.

А также в статье исследован вопрос аппроксимации функции ранга числа с помощью приближенного метода [12, 13] и доказан ряд арифметических свойств функции ранга числа. Представленный в работе приближенный подход к вычислению ранга числа может быть использован для реализации вычислительно сложных операций в RNS.

Статья организована следующим образом. В разделе 2 представлен обзор известных методов для преобразования чисел из RNS в PNS. В разделе 3 рассмотрено понятие ранга числа, а также его свойства. В разделе 4 исследована возможность представления ранга числа в виде алгебраического многочлена над $\mathbb{Z}_P$. В разделе 5 разработаны методы вычисления ранга числа с использованием приближенного метода и произведена оценка точности вычислений. Выводы о результатах исследования представлены в разделе 6.

2 Обзор известных методов обратного преобразования из RNS в PNS

Рассмотрим известные методы обратного преобразования из RNS в PNS. Основными методами для перевода чисел являются Китайская теорема об остатках, обобщенная позиционная система счисления, диагональная функция, функция ядра.

В статье [14] представлен новый алгоритм обратного преобразования RNS в PNS для произвольного набора модулей на основе функции ядра. Авторы предложили метод выбора коэффициентов функции ядра, который позволяет настраивать динамический диапазон функции ядра и упрощает сложность преобразования.

Обратное преобразование на основе Китайской теоремы об остатках требует вычисления остатка от деления на динамический диапазон системы. В статье [12] авторы предлагают приближенный метод преобразования чисел из RNS в PNS на основе Китайской теоремы об остатках, который позволяет избежать вычисления остатка от деления на динамический диапазон системы. Кроме того, авторы предложили метод замены дробных вычислений аналогичными вычислениями на основе целых чисел для дальнейшей аппаратной реализации алгоритма.

Метод преобразования чисел на основе обобщенной позиционной системы счисления требует многократного вычисления остатков от деления на модули RNS и использует в вычислениях результаты предыдущих итераций, что затрудняет распараллеливание вычислений. В работе [15] представлен подход к параллельному обратному преобразованию из RNS в обобщенную позиционную систему счисления. В предлагаемом методе вычисление цифр обобщенной позиционной системы счисления сводится к параллельному суммированию остатков в независимых модульных каналах, соответствующих модулям RNS.

В работе [16] Было показано, что преобразование RNS в PNS возможно с использованием диагональной функции. Авторы продемонстрировали связь между Китайской теоремой об остатках и диагональной функцией. Ввиду сложности оборудования преобразование RNS в двоичную систему с использованием диагональной функции может быть не привлекательным по сравнению с другими методами, но за счет возможного совместного использования ресурсов между операциями сравнения и обратного преобразования можно добиться более быстрого сравнения, жертвуя при этом временем преобразования. Поэтому диагональная функция чаще используется для реализации операции сравнения чисел [13].

Одним из подходов к уменьшению вычислительной сложности операции обратного преобразования является использование модулей специального вида. В статьях [18] и [19] авторы предлагают устройства на преобразования чисел на основе Китайской теоремы об остатках с учетом особенностей модулей специального вида 2^α и $2^\alpha \pm 1$. Авторы работы [20] предлагают обратный преобразователь на основе обобщенной позиционной системы счисления и модулей специального вида. Использование особенностей такого вида модулей позволяет уменьшить задержку и площадь устройства для перевода чисел. Тем не менее наборы модулей специального вида обычно бывают несбалансированные, что влияет на реализацию других арифметических операций.

В данной работе предлагается способ решения проблемы эффективного вычисления ранга с помощью приближенного метода. Предлагаемый подход позволяет уменьшить сложность вычисления позиционной характеристики числа, а следовательно и операции обратного преобразования из RNS в PNS.

3 Ранг числа и его свойства

Различают три формы представления Китайской теоремы об остатках, каждой из которых соответствует позиционная характеристика числа, представленного в RNS.

Первая форма

$$X = \left| \sum_{i=1}^{n} \left| P_i^{-1} \right|_{p_i} \cdot P_i \cdot x_i \right|_P = \sum_{i=1}^{n} \left| P_i^{-1} \right|_{p_i} \cdot P_i \cdot x_i - r(X) \cdot P, \tag{1}$$

где $r(X) = \left\lfloor \sum_{i=1}^{n} \frac{1}{p_i} \cdot \left| P_i^{-1} \right|_{p_i} \cdot x_i \right\rfloor$ – ранг числа.

Вторая форма

$$X = \left| \sum_{i=1}^{n} P_i \cdot \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \right|_P = \sum_{i=1}^{n} P_i \cdot \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} - \hat{r}(X) \cdot P, \tag{2}$$

где $\hat{r}(X) = \left\lfloor \sum_{i=1}^{n} \frac{1}{p_i} \cdot \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \right\rfloor$ – нормализованный ранг числа.

Третья форма

$$C(X) \equiv \left| \sum_{i=1}^{n} c_i \cdot x_i \right|_{C_P} = \sum_{i=1}^{n} c_i \cdot x_i - \check{r}(X) \cdot C_P, \tag{3}$$

где $\check{r} = \left\lfloor \frac{\sum_{i=1}^{n} c_i \cdot x_i}{C_P} \right\rfloor$ – ранг числа функции ядра Акушского.

Свойство 1. $\hat{r}(X) = -\frac{X}{P} + \sum_{i=1}^{n} \frac{\left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i}}{p_i}$.

Доказательство. По определению

$$\hat{r}(X) = \left\lfloor \sum_{i=1}^{n} \frac{\left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i}}{p_i} \right\rfloor = \left\lfloor \frac{1}{P} \sum_{i=1}^{n} \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \cdot P_i \right\rfloor.$$

Так как $\lfloor \frac{X}{P} \rfloor = \frac{X}{P} - \frac{|X|_P}{P}$, то

$$\hat{r}(X) = \frac{1}{P} \sum_{i=1}^{n} \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \cdot P_i - \frac{1}{P} \cdot \left| \sum_{i=1}^{n} \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \cdot P_i \right|_P.$$

Согласно Китайской теоремы об остатках, $\left| \sum_{i=1}^{n} \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \cdot P_i \right|_P = X$, следовательно, $\hat{r}(X) = \frac{1}{P} \sum_{i=1}^{n} \left| \left| P_i^{-1} \right|_{p_i} \cdot x_i \right|_{p_i} \cdot P_i - \frac{X}{P}$.

Свойство доказано. □

Свойство 2. $\hat{r}(1) = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left| P_i^{-1} \right|_{p_i}}{p_i}$.

Доказательство. Из Свойства 1 напрямую следует, что $\hat{r}(1) = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left| P_i^{-1} \right|_{p_i}}{p_i}$.

Свойство доказано. □

Третья форма является обобщением позиционных характеристик: диагональной функции и функции Pirlo и Impedovo[17].

Теорема 1. *Пусть заданы попарно взаимно простые модули RNS* $p_1 < p_2 < \ldots < p_n$, *число* $X \xrightarrow{RNS} (x_1, x_2, \ldots, x_n)$ *и веса функции ядра Акушского* $\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_n$ *удовлетворяющие условию* $0 \leq X < P$, *тогда*

$$\check{r}(X) = r(X) + \left\lfloor \frac{C(X)}{C_P} \right\rfloor. \tag{4}$$

Доказательство. Вычислим c_i, получим

$$c_i = C(B_i) = \sum_{j=1}^{n} \bar{w}_j \left\lfloor \frac{\left|P_i^{-1}\right|_{p_i} \cdot P_i}{p_j} \right\rfloor. \tag{5}$$

Так как $\forall i \neq j$: $\left|P_i^{-1}\right|_{p_i} \cdot P_i \equiv 0 \bmod p_j$ и $\forall i$: $\left|P_i^{-1}\right|_{p_i} \cdot P_i \equiv 1 \bmod p_i$, то для $i \neq j$: $\left\lfloor \left|P_i^{-1}\right|_{p_i} \cdot P_i / p_i \right\rfloor = \frac{\left|P_i^{-1}\right|_{p_i} \cdot P_i}{p_i}$, а для $i = j$: $\left\lfloor \left|P_i^{-1}\right|_{p_i} \cdot P_i / p_i \right\rfloor = \frac{\left|P_i^{-1}\right|_{p_i} \cdot P_i - 1}{p_i}$, следовательно, коэффициент c_i можно представить в следующем виде

$$c_i \quad = \quad \left|P_i^{-1}\right|_{p_i} \cdot P_i \cdot \sum_{j=1}^{n} \frac{\bar{w}_j}{p_j} - \frac{\bar{w}_i}{p_i}. \tag{6}$$

Учитывая, что $\sum_{j=1}^{n} \frac{\bar{w}_j}{p_j} = \frac{C_P}{P}$, то (6) преобразуется к виду

$$c_i \quad = \quad \left|P_i^{-1}\right|_{p_i} \cdot P_i \cdot \frac{C_P}{P} - \frac{\bar{w}_i}{p_i}. \tag{7}$$

Подставим (7) в (3), получим

$$\check{r}(X) = \left\lfloor \frac{\sum_{i=1}^{n} c_i \cdot x_i}{C_P} \right\rfloor = \left\lfloor \frac{1}{P} \cdot \sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} \cdot P_i \cdot x_i - \frac{1}{C_P} \cdot \sum_{i=1}^{n} \frac{x_i \cdot \bar{w}_i}{p_i} \right\rfloor. \tag{8}$$

Подставляя (1) в (8), получим

$$\check{r}(X) \quad = \quad \left\lfloor r(X) + \frac{X}{P} - \frac{1}{C_P} \cdot \sum_{i=1}^{n} \frac{x_i \cdot \bar{w}_i}{p_i} \right\rfloor. \tag{9}$$

Учитывая, что

$$\sum_{i=1}^{n} \frac{x_i \cdot \bar{w}_i}{p_i} = \sum_{i=1}^{n} \frac{\left(X - p_i \cdot \left\lfloor \frac{X}{p_i} \right\rfloor\right) \cdot \bar{w}_i}{p_i} = X \cdot \sum_{i=1}^{n} \frac{\bar{w}_i}{p_i} - \sum_{i=1}^{n} \left\lfloor \frac{X}{p_i} \right\rfloor \cdot \bar{w}_i$$
$$= X \cdot \frac{C_P}{P} - C(X). \tag{10}$$

Подставляя (10) в (9), получим

$$\check{r}(X) = \left\lfloor r(X) + \frac{C(X)}{C_P} \right\rfloor. \tag{11}$$

Так как $r(X) \in \mathbb{Z}$, а $\forall a \in \mathbb{R}, n \in \mathbb{Z}$: $\lfloor a+n \rfloor = \lfloor a \rfloor + n$, то

$$\check{r}(X) = r(X) + \left\lfloor \frac{C(X)}{C_P} \right\rfloor. \tag{12}$$

Теорема доказана. □

Следствие 1. *Пусть заданы попарно взаимно простые модули RNS* $p_1 < p_2 < \cdots < p_n$, *число* $X \in \mathbb{Z}_P$ *и функция ядра Акушского, не содержащая критических ядер, тогда* $\check{r}(X) = r(X)$.

Доказательство. Согласно Теореме 1, $\check{r}(X) = r(X) + \left\lfloor \frac{C(X)}{C_P} \right\rfloor$. Учитывая, что функция ядра Акушского не содержит критических ядер, $\forall X \in [0, P)$: $0 \le C(X) < C_P$. Отсюда $\left\lfloor \frac{C(X)}{C_P} \right\rfloor = 0$, и значит $\check{r}(X) = r(X)$.
Следствие доказано. □

4 К вопросу о представлении ранга числа в виде алгебраического многочлена над $\mathbb{Z}_P$

Возникает проблема вычисления алгебраического многочлена, интерполирующего функцию ранга числа.

Теорема 2. *Пусть заданы попарно взаимно простые модули RNS* $p_1 < p_2 < \ldots < p_n$, *число* $X \xrightarrow{RNS} (x_1, x_2, \ldots, x_n)$ *и определена функция ранга числа* $r(X) = \left\lfloor \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i} \cdot x_i}{p_i} \right\rfloor$, *тогда функцию* $r(X)$ *нельзя представить в виде алгебраического многочлена над* $\mathbb{Z}_P$.

Доказательство. Предположим противное, пусть функцию ранга числа $r(X)$ можно представить в виде многочлена степени $\phi(P) - 2$ (так как $X^{\phi(P)} \equiv X \bmod P$, $\phi(P)$ – функция Эйлера), получим

$$r(X) = \sum_{i=0}^{\phi(P)-2} a_i \cdot X^i. \tag{13}$$

Учитывая, что $r(0) = 0$, $a_0 = 0$ и формула (13) примет следующий вид

$$r(X) = \sum_{i=1}^{\phi(P)-2} a_i \cdot X^i. \tag{14}$$

Вычислим значение $|r(p_1)|_{p_1}$, используя формулу (14), получим

$$|r(p_1)|_{p_1} \equiv \left| \sum_{i=1}^{\phi(P)-2} a_i \cdot p_1^i \right|_{p_1} \equiv \sum_{i=1}^{\phi(P)-2} \left|a_i \cdot p_1^i\right|_{p_1} \equiv 0.$$

Вычислим значения $r(p_1-1)$ и $r(p_1)$, используя формулу $r(X+Y)=r(X)+r(Y)-\sum_{x_i+y_i\geq p_i}\left|P_i^{-1}\right|_{p_i}$ из работы [21], получим

$$\begin{aligned} r(p_1-1) &= (p_1-1)\cdot r(1), \\ r(p_1) &= r(p_1-1)+r(1)-\left|P_1^{-1}\right|_{p_1} \\ &= (p_1-1)\cdot r(1)+r(1)-\left|P_1^{-1}\right|_{p_1} \\ &= p_1\cdot r(1)-\left|P_1^{-1}\right|_{p_1}. \end{aligned} \tag{15}$$

Используя формулу (15), вычислим значение $|r(p_1)|_{p_1}$, получим

$$|r(p_1)|_{p_1}\equiv-\left|P_1^{-1}\right|_{p_1}. \tag{16}$$

Так как $\gcd(P_1,p_1)=1$, то $-\left|P_1^{-1}\right|_{p_1}\not\equiv 0 \bmod p_1$. Учитывая, что согласно формуле (15) $|r(p_1)|_{p_1}\equiv 0$, а согласно формуле (16) $|r(p_1)|_{p_1}\not\equiv 0$, имеет место противоречие, следовательно, функцию $r(X)$ нельзя выразить в виде алгебраического многочлена над $\mathbb{Z}_P$.

Теорема доказана. □

Следствие 2. *Пусть заданы попарно взаимно простые модули RNS $p_1<p_2<\ldots<p_n$, функция ядра Акушского, не содержащая критических ядер, и число $X\in\mathbb{Z}_P$, тогда функцию $\check{r}(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.*

Доказательство. Согласно Следствию 1 $\check{r}=r(X)$. Обратим внимание, что согласно Теореме 2 $r(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.

Следствие доказано. □

Докажем теорему о том, что функцию $\hat{r}(X)$ нельзя представить в виде алгебраического многочлена.

Теорема 3. *Пусть заданы попарно взаимно простые модули RNS $p_1<p_2<\ldots<p_n$ и число $X\in\mathbb{Z}_P$, тогда функцию $\hat{r}(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.*

Доказательство. Предположим противное, что функцию $\hat{r}(X)$ можно представить в виде алгебраического многочлена степени $\phi(P)-2$, получим

$$\hat{r}(X)=\sum_{i=0}^{\phi(P)-2}a_i\cdot X^i. \tag{17}$$

Согласно формуле (2), ранг числа $\hat{r}(0)=0$, следовательно, $a_0=0$, и формула (17) примет вид

$$\hat{r}(X)=\sum_{i=1}^{\phi(P)-2}a_i\cdot X^i. \tag{18}$$

Рассмотрим два случая.

Случай 1. Если $n = 2$. Предположим, что $\hat{r}(1) = 0$, тогда согласно Китайской теоремы об остатках, заданной уравнением во второй форме (2), получим $\left|\frac{1}{p_2}\right|_{p_1} \cdot p_2 + \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 = 1$. Так как $\gcd(p_1, p_2) = 1$, то $\left|\frac{1}{p_2}\right|_{p_1} \geq 1$ и $\left|\frac{1}{p_1}\right|_{p_2} \geq 1$, следовательно, $\left|\frac{1}{p_2}\right|_{p_1} \cdot p_2 + \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \geq p_1 + p_2$. Учитывая, что $p_1 \geq 2$ и $p_2 \geq 3$, $\left|\frac{1}{p_2}\right|_{p_1} \cdot p_2 + \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \geq 5$ и $\left|\frac{1}{p_2}\right|_{p_1} \cdot p_2 + \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \neq 1$. Таким образом, имеет место противоречие и $\hat{r}(1) \neq 0$. Учитывая, что $\forall X \in [0, P)$: $\hat{r}(X) \in \{0, 1\}$ и $\hat{r}(1) \neq 0$, $\hat{r}(1) = 1$. Следовательно, если функцию ядра $\hat{r}(X)$ можно представить в виде алгебраического многочлена над $\mathbb{Z}_P$, то его коэффициенты a_i удовлетворяют сравнению

$$\hat{r}(1) = \sum_{i=1}^{\phi(P)-2} a_i \equiv 1 \bmod P. \tag{19}$$

Вычислим значение $\hat{r}\left(\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1\right)$. Учитывая, что $\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \xrightarrow{RNS} (0, 1)$, и, используя Свойство 1, получим

$$\hat{r}\left(\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1\right) = -\frac{\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1}{P} + \frac{\left|\frac{1}{p_1}\right|_{p_2}}{p_2} = -\frac{\left|\frac{1}{p_1}\right|_{p_2}}{p_2} + \frac{\left|\frac{1}{p_1}\right|_{p_2}}{p_2} = 0. \tag{20}$$

Обратим внимание, что $\left(\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1\right)^2 \equiv \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \bmod P$, следовательно, $\forall i \in \mathbb{N}$: $\left(\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1\right)^i \equiv \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \bmod P$. Из (20) следует, что если функцию ядра $\hat{r}(X)$ можно представить в виде алгебраического многочлена над $\mathbb{Z}_P$, то его коэффициенты a_i удовлетворяют сравнению

$$\hat{r}\left(\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1\right) = \left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \cdot \sum_{i=1}^{\phi(P)-2} a_i \equiv 0 \bmod P. \tag{21}$$

Умножим (19) на $\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1$ и вычтем из результата (21), получим

$$\left|\frac{1}{p_1}\right|_{p_2} \cdot p_1 \equiv 0 \bmod P. \tag{22}$$

Таким образом, имеет место противоречие, следовательно, при $n = 2$ функцию ранга числа $\hat{r}(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.

Случай 2. Если $n \geq 3$. Используя формулу (18), вычислим значение $|\hat{r}(p_n)|_{p_n}$, получим

$$|\hat{r}(p_n)|_{p_n} = \left|\sum_{i=1}^{\phi(P)-2} a_i \cdot p_n^i\right|_{p_n} \equiv \sum_{i=1}^{\phi(P)-2} \left|a_i \cdot p_n^i\right|_{p_n} \equiv 0. \tag{23}$$

Учитывая, что $p_n \xrightarrow{RNS} \left(|p_n|_{p_1}, |p_n|_{p_2}, \ldots, |p_n|_{p_{n-1}}, 0\right)$, вычислим значение $\hat{r}(p_n)$, используя Свойство 1, получим

$$\hat{r}(p_n) = -\frac{p_n}{P} + \sum_{i=1}^{n-1} \frac{\left|\left|P_i^{-1}\right|_{p_i} \cdot |p_n|_{p_i}\right|_{p_i}}{p_i}. \tag{24}$$

Пусть $\forall i = \overline{1, n-1}$: $\hat{P}_i = \frac{P}{p_n \cdot p_i}$, тогда $\left|\left|P_i^{-1}\right|_{p_i} \cdot |p_n|_{p_i}\right|_{p_i} = \left|\hat{P}_i^{-1}\right|_{p_i}$ и $\frac{p_n}{P} = \frac{1}{P_n}$. С учетом последних соотношений получим

$$\hat{r}(p_n) = -\frac{1}{P_n} + \sum_{i=1}^{n-1} \frac{\left|\hat{P}_i^{-1}\right|_{p_i}}{p_i}. \tag{25}$$

Оценим правую часть формулы (25). Учитывая, что $\forall i = \overline{1, n-1}$: $\gcd\left(\hat{P}_i, p_i\right) = 1$, $1 \leq \left|\hat{P}_i^{-1}\right|_{p_i} \leq p_i - 1$, тогда значение $\hat{r}(p_n)$ удовлетворяет неравенству

$$-\frac{1}{P_n} + \sum_{i=1}^{n-1} \frac{1}{p_i} \leq -\frac{1}{P_n} + \sum_{i=1}^{n-1} \frac{\left|\hat{P}_i^{-1}\right|_{p_i}}{p_i} \leq -\frac{1}{P_n} + \sum_{i=1}^{n-1} \frac{p_i - 1}{p_i}. \tag{26}$$

Учитывая, что

$$\sum_{i=1}^{n-1} \frac{1}{p_i} = \frac{1}{P_n} \sum_{i=1}^{n-1} \hat{P}_i, \tag{27}$$

$$\sum_{i=1}^{n-1} \frac{p_i - 1}{p_i} = n - 1 - \sum_{i=1}^{n-1} \frac{1}{p_i} = n - 1 - \frac{1}{P_n} \sum_{i=1}^{n-1} \hat{P}_i, \tag{28}$$

неравенство (26) примет вид

$$-\frac{1}{P_n} + \frac{1}{P_n} \sum_{i=1}^{n-1} \hat{P}_i \leq -\frac{1}{P_n} + \sum_{i=1}^{n-1} \frac{\left|\hat{P}_i^{-1}\right|_{p_i}}{p_i} \leq -\frac{1}{P_n} + n - 1 - \frac{1}{P_n} \sum_{i=1}^{n-1} \hat{P}_i. \tag{29}$$

Так как $n \geq 3$, то $\hat{P}_1 \geq 3$, $-\frac{1}{P_n} + \frac{1}{P_n} \sum_{i=1}^{n-1} \hat{P}_i > 0$, $-\frac{1}{P_n} + n - 1 - \frac{1}{P_n} \sum_{i=1}^{n-1} \hat{P}_i < n - 1$, следовательно, $\hat{r}(p_n) \in (0, n-1)$. Учитывая, что $\hat{r}(p_n) \in \mathbb{Z}$, $\hat{r}(p_n) \in \{1, 2, \ldots, n-2\}$. Учитывая, что $\forall i \neq j$: $\gcd(p_i, p_j) = 1$, может существовать только две пары чисел (оснований RNS), удовлетворяющих условию $p_{i+1} - p_i = 1$, для всех остальных пар $p_{i+1} - p_i \geq 2$, значит $p_n \geq p_1 + 2 + (n-3) \cdot 2 = p_1 + 2n - 4$. Учитывая, что $p_1 \geq 2$, получим неравенство $p_n \geq 2n - 2$. Так как согласно условию теоремы $n \geq 3$, $2n - 2 > n - 2$ и $p_n > n - 2$, следовательно, $0 < \hat{r}(p_n) < p_n$, значит $|\hat{r}(p_n)|_{p_n} \not\equiv 0$. Таким образом, имеет место противоречие: с одной стороны, $|\hat{r}(p_n)|_{p_n} \equiv 0$, с другой стороны, $|\hat{r}(p_n)|_{p_n} \not\equiv 0$. Следовательно, функцию ранга $\hat{r}(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.

Объединяя результаты, полученные в первом и втором случае, делаем вывод, что функцию ранга $\hat{r}(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.

Теорема доказана. □

Свойство 3. $\check{r}(1) = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i}$.

Доказательство. Согласно Теореме 1, значение $\check{r}(1)$ равно $\check{r}(1) = r(1) + \left\lfloor \frac{C(1)}{C_P} \right\rfloor$. Учитывая, что $\forall i$: $p_i \geq 2$, $\left\lfloor \frac{1}{p_i} \right\rfloor = 0$, следовательно, $C(1) = \sum_{i=1}^{n} \bar{w}_i \left\lfloor \frac{1}{p_i} \right\rfloor = 0$, значит $\check{r}(1) = r(1)$. Вычислим значение $r(1)$, используя формулу (1), получим

$$\check{r}(1) = r(1) = \left\lfloor \frac{\sum_{i=1}^{n} P_i \cdot \left|P_i^{-1}\right|_{p_i}}{P} \right\rfloor. \tag{30}$$

Учитывая, что $\left\lfloor \frac{X}{P} \right\rfloor = \frac{X}{P} - \frac{|X|_P}{P}$, и согласно Китайской теоремы об остатках $\left| \sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} \cdot P_i \right|_P = 1$, формула (30) примет вид

$$\check{r}(1) = -\frac{1}{P} + \frac{\sum_{i=1}^{n} P_i \cdot \left|P_i^{-1}\right|_{p_i}}{P} = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i}. \tag{31}$$

Свойство доказано. □

Свойство 4. *Если модули RNS удовлетворяют условию* $p_1 < p_2 < \ldots < p_n$, *то*

$$\check{r}(p_1) = p_1 \cdot r(1) - \left|P_1^{-1}\right|_{p_1} + \left\lfloor \frac{\bar{w}_1}{C_P} \right\rfloor. \tag{32}$$

Доказательство. Используя Теорему 1, получим

$$\check{r}(p_1) = r(p_1) + \left\lfloor \frac{C(p_1)}{C_P} \right\rfloor. \tag{33}$$

Учитывая, что $r(p_1) = p_1 \cdot r(1) - \left|P_1^{-1}\right|_{p_1}$ и $C(p_1) = \bar{w}_1$, получим

$$\check{r}(p_1) = p_1 \cdot r(1) - \left|P_1^{-1}\right|_{p_1} + \left\lfloor \frac{\bar{w}_1}{C_P} \right\rfloor.$$

Свойство доказано. □

Свойство 5. *Если модули RNS удовлетворяют условию* $p_1 < p_2 < \ldots < p_n$ *и* $1 \leq t \leq n$, *то*

$$\check{r}\left(\left|P_t^{-1}\right|_{p_t} \cdot P_t\right) = 0. \tag{34}$$

Доказательство. Учитывая, что $B_t = \left|P_t^{-1}\right|_{p_t} \cdot P_t \xrightarrow{RNS} (b_1, b_2, \ldots, b_n)$, где $\forall i \neq t$: $b_i = 0$, а $b_t = 1$, вычислим $C(B_t)$ по определению

$$C(B_t) = \sum_{i=1}^{n} c_i \cdot b_i - \check{r}(B_t) \cdot C_P = c_t - \check{r}(B_t) \cdot C_P = C(B_t) - \check{r}(B_t) \cdot C_P. \quad (35)$$

Из (35) следует, что $\check{r}(B_t) \cdot C_P = 0$. Учитывая, что $C_P \neq 0$, получим, что $\check{r}(B_t) = 0$.

Свойство доказано. □

Теорема 4. *Пусть заданы попарно взаимно простые модули RNS* $p_1 < p_2 < \ldots < p_n$ *и число* $X \in \mathbb{Z}_P$, *тогда функцию* $\check{r}(X)$ *нельзя представить в виде алгебраического многочлена над* $\mathbb{Z}_P$.

Доказательство. Предположим, что над $\mathbb{Z}_P$ существует алгебраический многочлен

$$\check{r}(X) = \sum_{i=0}^{\phi(P)-2} a_i \cdot X^i. \quad (36)$$

Вычислим $\check{r}(0)$ с использованием формулы (36), получим, что $\check{r}(0) = a_0 = 0$, следовательно, (36) преобразуется к виду

$$\check{r}(X) = \sum_{i=1}^{\phi(P)-2} a_i \cdot X^i. \quad (37)$$

Используя формулу (37) вычислим значения $\check{r}(1)$ и $\check{r}(B_n)$, получим

$$\check{r}(1) = \sum_{i=1}^{\phi(P)-2} a_i, \quad (38)$$

$$\check{r}(B_n) = \sum_{i=1}^{\phi(P)-2} a_i \cdot B_n^i. \quad (39)$$

Учитывая, что $\forall i \in \mathbb{N}$: $B_n^i \equiv B_n \bmod P$, формула (39) преобразуется к виду

$$\check{r}(B_n) \equiv B_n \cdot \sum_{i=1}^{\phi(P)-2} a_i \bmod P. \quad (40)$$

С другой стороны, согласно Свойству 5

$$\check{r}(B_n) = 0.$$

Составим систему сравнений над $\mathbb{Z}_P$

$$\begin{cases} \sum_{i=1}^{\phi(P)-2} a_i & \equiv \check{r}(1) \bmod P, \\ B_n \cdot \sum_{i=1}^{\phi(P)-2} a_i & \equiv 0 \bmod P. \end{cases} \quad (41)$$

Система сравнений (41) равносильна сравнению

$$B_n \cdot \check{r}(1) \equiv 0 \bmod P. \quad (42)$$

Так как $B_n = P_n \cdot \left|P_n^{-1}\right|_{p_n}$, то $\gcd(B_n, P) = P_n$, тогда (42) равносильно сравнению

$$\left|P_n^{-1}\right|_{p_n} \cdot \check{r}(1) \equiv 0 \bmod p_n. \tag{43}$$

Так как $\gcd\left(\left|P_n^{-1}\right|_{p_n}, p_n\right) = 1$, то (43) равносильно сравнению

$$\check{r}(1) \equiv 0 \bmod p_n. \tag{44}$$

Из (44) следует, что чтобы прийти к противоречию необходимо и достаточно показать, что сравнение не имеет решений.

Для начала покажем, что $\check{r}(1)$ не равно нулю. Согласно Свойству 3, значение $\check{r}(1)$ вычисляется по формуле $\check{r}(1) = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i}$ и $\check{r}(1) \in \mathbb{Z}$.

Так как $n \geq 2$, то $P_1 \geq 2$, $P_2 \geq 3$, следовательно, $\sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} \cdot P_i \geq \left|P_1^{-1}\right|_{p_1} \cdot P_1 + \left|P_2^{-1}\right|_{p_2} \cdot P_2 \geq 2 \cdot \left|P_1^{-1}\right|_{p_1} + 3 \cdot \left|P_2^{-1}\right|_{p_2}$. Учитывая, что $\gcd(P_1, p_1) = 1$ и $\gcd(P_2, p_2) = 1$, $\left|P_1^{-1}\right|_{p_1} \geq 1$ и $\left|P_2^{-2}\right|_{p_2} \geq 1$. Значит, $\sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} \cdot P_i \geq 5$. Подставим полученный результат в $\check{r}(1)$

$$\check{r}(1) = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} = -\frac{1}{P} + \frac{1}{P} \cdot \sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} \cdot P_i \geq -\frac{1}{P} + \frac{5}{P} = \frac{4}{P} \tag{45}$$

Учитывая, что $\check{r}(1) \in \mathbb{Z}$ и $\check{r}(1) \geq \frac{4}{P} > 0$, то $\check{r}(1) \geq 1$. Таким образом, $\check{r}(1) \neq 1$.

Покажем, что $\check{r}(1) < p_n$. Для этого найдем верхнюю границу значения $\check{r}(1)$. Учитывая, что $\forall i \in \overline{1,n}$: $\left|P_i^{-1}\right|_{p_i} \leq p_i - 1$, получим

$$\check{r}(1) = -\frac{1}{P} + \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|}{p_i} \leq -\frac{1}{P} + \sum_{i=1}^{n} \frac{p_i - 1}{p_i} = n - \frac{1}{P} - \frac{1}{P} \sum_{i=1}^{n} P_i = n - \frac{1}{P} - \frac{SQ}{P} \leq n.$$

Учитывая, что $\check{r}(1) < n$ и $\check{r}(1) \in \mathbb{Z}$, $\check{r}(1) \leq n-1$. Ранее было показано, что $p_n \geq 2n - 2$, следовательно, $p_n > n - 1$ и $\check{r}(1) < p_n$.

Таким образом, $0 < \check{r}(1) < p_n$, следовательно, сравнение (44) решений не имеет. Значит функцию ранга числа ядра Акушского $\check{r}(X)$ нельзя представить в виде алгебраического многочлена над $\mathbb{Z}_P$.

Теорема доказана. □

5 Разработка методов вычисления ранга числа с использованием приближенного метода

Теорема 5. *Если для фиксированного N, $\forall i \in \overline{1,n}$ и $x_i \in [1, p_i - 1]$ выполняется условие*

$$2^N \geq \frac{x_i \cdot \left|\left|P_i^{-1}\right|_{p_i} \cdot 2^N\right|_{p_i}}{\left|x_i \cdot \left|P_i^{-1}\right|_{p_i}\right|_{p_i}}, \tag{46}$$

то

$$\sum_{i=1}^{n}\left\lfloor\frac{\left|P_i^{-1}\right|_{p_i}\cdot x_i}{p_i}\right\rfloor=\sum_{i=1}^{n}\left\lfloor\frac{k_i\cdot x_i}{2^N}\right\rfloor, \tag{47}$$

где $k_i=\left\lfloor\frac{\left|P_i^{-1}\right|_{p_i}\cdot 2^N}{p_i}\right\rfloor$.

Доказательство. Подставим $k_i=\left\lfloor\frac{1}{p_i}\cdot\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right\rfloor$ в $\left\lfloor\frac{k_i\cdot x_i}{p_i}\right\rfloor$, получим

$$\left\lfloor\frac{k_i\cdot x_i}{2^N}\right\rfloor=\left\lfloor\left\lfloor\frac{1}{p_i}\cdot\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right\rfloor\cdot\frac{x_i}{2^N}\right\rfloor. \tag{48}$$

Так как $\left\lfloor\frac{\left|P_i^{-1}\right|_{p_i}\cdot 2^N}{p_i}\right\rfloor=\frac{1}{p_i}\cdot\left(\left|P_i^{-1}\right|_{p_i}\cdot 2^N-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\right)$, то (48) примет вид

$$\begin{aligned}\left\lfloor\frac{k_i\cdot x_i}{2^N}\right\rfloor &= \left\lfloor\frac{1}{p_i}\cdot\left(\left|P_i^{-1}\right|_{p_i}\cdot 2^N-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\right)\cdot\frac{x_i}{2^N}\right\rfloor\\ &= \left\lfloor\frac{\left|P_i^{-1}\right|_{p_i}\cdot x_i}{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\cdot\frac{x_i}{2^N\cdot p_i}\right\rfloor.\end{aligned} \tag{49}$$

Учитывая, что $\forall a\in\mathbb{Z},b\in\mathbb{N}$: $\frac{a}{b}=\lfloor\frac{a}{b}\rfloor+\{\frac{a}{b}\}=\lfloor\frac{a}{b}\rfloor+\frac{|a|_b}{b}$, и $\forall c\in\mathbb{R},d\in\mathbb{Z}$: $\lfloor c+d\rfloor=\lfloor c\rfloor+d$, (49) преобразуется к виду

$$\begin{aligned}\left\lfloor\frac{k_i\cdot x_i}{2^N}\right\rfloor=&\left\lfloor\frac{\left|P_i^{-1}\right|_{p_i}\cdot x_i}{p_i}\right\rfloor\\ &+\left\lfloor\frac{1}{p_i}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\frac{x_i}{2^N\cdot p_i}\right\rfloor.\end{aligned} \tag{50}$$

Из формулы (50) следует, что $\left\lfloor\frac{k_i\cdot x_i}{2^N}\right\rfloor=\left\lfloor\frac{\left|P_i^{-1}\right|_{p_i}\cdot x_i}{p_i}\right\rfloor$, тогда и только тогда, когда $\left\lfloor\frac{1}{p_i}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\frac{x_i}{2^N\cdot p_i}\right\rfloor=0$. Условие $\left\lfloor\frac{1}{p_i}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\frac{x_i}{2^N\cdot p_i}\right\rfloor=0$ выполняется, если

$$0\le\frac{1}{p_i}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\frac{x_i}{2^N\cdot p_i}<1. \tag{51}$$

Умножим (51) на $p_i\cdot 2^N>0$, получим

$$0\le 2^N\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\cdot x_i<2^N\cdot p_i. \tag{52}$$

Так как $\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}\le p_i-1$ и $\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\ge 0$, то $\forall N\in\mathbb{N}$: $2^N\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_{p_i}-\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\cdot x_i<2^N\cdot(p_i-1)$. Следовательно,

правая часть неравенства (52) выполняется при любом N. Таким образом, $\left\lfloor \frac{1}{p_i} \cdot \left| \left|P_i^{-1}\right|_{p_i} \cdot x_i \right|_{p_i} - \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i} \frac{x_i}{2^N \cdot p_i} \right\rfloor = 0$, если выполняется неравенство

$$0 \le 2^N \cdot \left| \left|P_i^{-1}\right|_{p_i} \cdot x_i \right|_{p_i} - \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i} \cdot x_i. \tag{53}$$

Рассмотрим два случая.

Случай 1. Если $x_i = 0$, то $\left| \left|P_i^{-1}\right|_{p_i} \cdot x_i \right|_{p_i} - \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i} \cdot x_i = 0$, и неравенство (53) выполняется при любом N.

Случай 2. Если $x_i \neq 0$, то неравенство (53) примет вид

$$2^N \ge \frac{x_i \cdot \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i}}{\left| x_i \cdot \left|P_i^{-1}\right|_{p_i} \right|_{p_i}}.$$

Теорема доказана. □

Следствие 3 (верхняя граница)**.** *Пусть модули RNS – попарно взаимно простые числа $p_1 < p_2 < \ldots < p_n$, тогда существует хотя бы одно значение $N \le \lceil 2 \log_2 (p_n - 1) \rceil$, удовлетворяющее условию Теоремы 5.*

Доказательство. Так как $1 \le x_i \le p_i - 1$, $\left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i} \le p_i - 1$ и $\left| x_i \cdot \left|P_i^{-1}\right|_{p_i} \right|_{p_i} \ge 1$, то

$$\frac{x_i \cdot \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i}}{\left| x_i \cdot \left|P_i^{-1}\right|_{p_i} \right|_{p_i}} \le \frac{(p_i - 1)^2}{1} \le (p_n - 1)^2 .$$

Следовательно, если $2^N \ge (p_n - 1)^2$, то условие Теоремы 5 выполняется. Таким образом, при выборе $N = \lceil 2 \log_2 (p_n - 1) \rceil$, условие Теоремы 5 выполняется. Значит существует хотя бы одно $N \le \lceil 2 \log_2 (p_n - 1) \rceil$, удовлетворяющее условию Теоремы 5.

Следствие доказано. □

Следствие 4 (нижняя граница)**.** *Для любого $N < \log_2 U$ условие Теоремы 5 не выполняется, где $U = \max_{i=\overline{1,n}, \gcd(p_i,2)=1} |P_i|_{p_i}$.*

Доказательство. Так как $x_i \neq 0$, то его можно представить в виде $x_i = |a \cdot P_i|_{p_i}$, где $a \in [1, p_i - 1]$ и $a = \left| x_i \cdot P_i^{-1} \right|_{p_i}$. Вычислим значения правой части неравенства (46) в точках x_i, получим

$$\frac{x_i \cdot \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i}}{\left| x_i \cdot \left|P_i^{-1}\right|_{p_i} \right|_{p_i}} = \frac{|a \cdot P_i|_{p_i} \cdot \left| \left|P_i^{-1}\right|_{p_i} \cdot 2^N \right|_{p_i}}{\left| |a \cdot P_i|_{p_i} \cdot \left|P_i^{-1}\right|_{p_i} \right|_{p_i}}. \tag{54}$$

Так как $\left||a\cdot P_i|_{p_i}\cdot\left|P_i^{-1}\right|_{p_i}\right|_{p_i}=a$, то формула (54) примет вид

$$\frac{x_i\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}}{\left|x_i\cdot\left|P_i^{-1}\right|_{p_i}\right|_{p_i}}=\frac{|a\cdot P_i|_{p_i}}{a}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}. \tag{55}$$

Покажем, что $\frac{|a\cdot P_i|_{p_i}}{a}\le|P_i|_{p_i}$, для этого представим $|a\cdot P_i|_{p_i}$ в виде $|a\cdot P_i|_{p_i}=\left|a\cdot|P_i|_{p_i}\right|_{p_i}=a\cdot|P_i|_{p_i}-p_i\cdot\left\lfloor\frac{a\cdot|P_i|_{p_i}}{p_i}\right\rfloor$. Так как $a\cdot|P_i|_{p_i}\ge 1$, то $\left\lfloor\frac{a\cdot|P_i|_{p_i}}{p_i}\right\rfloor\ge 0$, следовательно, $|a\cdot P_i|_{p_i}\le a\cdot|P_i|_{p_i}$, значит $\frac{|a\cdot P_i|_{p_i}}{a}\le\frac{a\cdot|P_i|_{p_i}}{a}\le|P_i|_{p_i}$. Обратим внимание на тот факт, что в неравенстве $\frac{|a\cdot P_i|_{p_i}}{a}\le|P_i|_{p_i}$ равенство достигается при $a=1$. Подставляя полученный результат в (55), получим

$$\frac{x_i\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}}{\left|x_i\cdot\left|P_i^{-1}\right|_{p_i}\right|_{p_i}}\le|P_i|_{p_i}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}. \tag{56}$$

Равенство в неравенстве (56) достигается в точке $x_i=|P_i|_{p_i}$.

Если $\gcd(p_i,2)=1$, то $\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}\ge 1$, следовательно, если $2^N<U$, то условие Теоремы 5 не будет выполнено хотя бы в одной точке $x_t=U$, где t – индекс, при котором $U=|P_t|_{p_t}$.

Следствие доказано. □

Из формулы (56) следует, что для того, чтобы найти минимальное N, для которого бы выполнялось условие Теоремы 5, необходимо и достаточно проверить условие $\forall i=\overline{1,n}$: $2^N\ge|P_i|_{p_i}\cdot\left|\left|P_i^{-1}\right|_{p_i}\cdot 2^N\right|_{p_i}$.

Пример 1. *Пусть задана RNS с модулями* $p_1=23,p_2=25,p_3=27,p_4=29$. *Вычислим наименьшее* N, *удовлетворяющее условиям Теоремы 5.*

Вычислим диапазон RNS: $P=\prod_{i=1}^n p_i=23\cdot 25\cdot 27\cdot 29=450225$.

Вычислим P_i: $P_1=\frac{P}{p_1}=\frac{450225}{23}=19575$, $P_2=\frac{P}{p_2}=\frac{450225}{25}=18009$, $P_3=\frac{P}{p_3}=\frac{450225}{27}=16675$, $P_4=\frac{P}{p_4}=\frac{450225}{29}=15525$.

Вычислим $|P_i|_{p_i}$: $|P_1|_{p_1}=|19575|_{23}=2$, $|P_2|_{p_2}=|18009|_{25}=9$, $|P_3|_{p_3}=|16675|_{27}=16$, $|P_4|_{p_4}=|15525|_{29}=10$.

Следовательно, $U=\max_{i=\overline{1,n},\gcd(p_i,2)=1}|P_i|_{p_i}=\max(2,9,16,10)=16$, *значит* $N\ge\log_2 U=4$. *С другой стороны,* $N\le\lceil 2\log_2(p_n-1)\rceil=\lceil 2\log_2 28\rceil=10$.

Таким образом, минимальное N, *удовлетворяющее условиям Теоремы 5, принадлежит отрезку* $4\le N\le 10$.

Таблица 1. Значения $|P_i|_{p_i} \cdot \left|\left|P_i^{-1}\right|_{p_i} \cdot 2^N\right|_{p_i}$ для $i = \overline{1,4}$ и $N = \overline{4,10}$

N	4	5	6	7	8	9	10
$b_{1,N} = \|P_1\|_{p_1} \cdot \left\|\left\|P_1^{-1}\right\|_{p_1} \cdot 2^N\right\|_{p_1}$	16	32	18	36	26	6	12
$b_{2,N} = \|P_2\|_{p_2} \cdot \left\|\left\|P_2^{-1}\right\|_{p_2} \cdot 2^N\right\|_{p_2}$	216	207	189	153	81	162	99
$b_{3,N} = \|P_3\|_{p_3} \cdot \left\|\left\|P_3^{-1}\right\|_{p_3} \cdot 2^N\right\|_{p_3}$	16	32	64	128	256	80	160
$b_{4,N} = \|P_4\|_{p_4} \cdot \left\|\left\|P_4^{-1}\right\|_{p_4} \cdot 2^N\right\|_{p_4}$	190	90	180	70	140	280	270
$b_{max,N} = \max(b_{1,N}, b_{2,N}, b_{3,N}, b_{4,N})$	216	207	189	153	**256**	280	270
2^N	16	32	64	128	**256**	512	1024

Найдем минимальное N, удовлетворяющее условию Теоремы 5. Для этого вычислим значения $|P_i|_{p_i} \cdot \left|\left|P_i^{-1}\right|_{p_i} \cdot 2^N\right|_{p_i}$, результаты вычислений занесем в таблицу 1. Исходя из полученных результатов (табл. 1) делаем вывод, что минимальное N, при котором выполняются условия Теоремы 5, равно $N = 8$.

Из результатов, полученных в примере 1, можно сделать вывод, что при выборе 5-битных модулей RNS необходимо использовать $N = 8$ бит, что в 1.6 раза превышает размер модулей. Возникает задача: выбрать модули RNS так, чтобы N максимально приблизилось к нижней границе. Одним из путей решения данной задачи является наложение дополнительных условий на модули RNS, например, если $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$, тогда $N \leq \lceil \log_2 p_n \rceil$. Исследуем вопрос о количестве наборов модулей, удовлетворяющих указанному условию, для $n \leq 10$. Для этого докажем следующие утверждения.

Лемма 1. *Если модули RNS $\{p_1, p_2, \ldots, p_n\}$ удовлетворяют условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$, то $n \geq 3$.*

Доказательство. Покажем, что не существует двухмодульной RNS, удовлетворяющей условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$. Без потери общности будем считать, что выполняется неравенство $p_1 < p_2$. Предположим, что существует двухмодульная RNS, удовлетворяющая условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$. Следовательно, $|p_1|_{p_2} = 1$ и $|p_2|_{p_1} = 1$. Из условия $|p_1|_{p_2} = 1$ следует, что p_1 можно представить в виде $p_1 = b \cdot p_2 + 1$, где $b \in \mathbb{Z}$. Учитывая, что $p_1 < p_2$, $b \cdot p_2 + 1 < p_2$, следовательно, $b < 1 - \frac{1}{p_2}$, значит $b \leq 0$. Обращая внимание на то, что, с одной стороны, $p_1 \geq 2$, с другой стороны, $p_1 \leq 1$, обнаружим противоречие. Следовательно, двухмодульной RNS, удовлетворяющей условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$, не существует.

Лемма доказана. □

Пример 2. *Пусть RNS задана модулями* $\{2,3,5\}$*, тогда* $P = p_1 \cdot p_2 \cdot p_3 = 30$*,* $P_1 = \frac{P}{p_1} = 15$*,* $P_2 = \frac{P}{p_2} = 10$*,* $P_3 = \frac{P}{p_3} = 6$*, следовательно,* $|P_1|_{p_1} = |15|_2 = 1$*,* $|P_2|_{p_2} = |10|_3 = 1$ *и* $|P_3|_{p_3} = |6|_5 = 1$*. Значит для данного набора модулей выполняется условие* $\forall i = \overline{1,n}$*:* $|P_i|_{p_i} = 1$*.*

Лемма 2. *Модули RNS* $\{p_1, p_2, \ldots, p_n\}$ *удовлетворяют условию* $\forall i = \overline{1,n}$*:* $|P_i|_{p_i} = 1$ *тогда и только тогда, когда*

$$P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P + 1. \tag{57}$$

Доказательство. Так как $|P_n|_{p_n} = 1$, P_n можно представить в виде $P_n = a \cdot p_n + 1$, где $a \in \mathbb{Z}_{P_n}$. Учитывая, что $\forall i = \overline{1,n-1}$: $|P_n|_{p_i} = 1$, то $\forall i = \overline{1,n-1}$: $|a \cdot p_n + 1|_{p_i} = 0$, следовательно, $a \equiv \left|-\frac{1}{p_n}\right|_{p_i}$. Вычислим значение a, используя Китайскую теорему об остатках, получим $a = \left|\sum_{i=1}^{n-1} \left|\left|\hat{P}_i^{-1}\right|_{p_i} \cdot \left|-\frac{1}{p_n}\right|_{p_i}\right|_{p_i} \cdot \hat{P}_i\right|_{P_n}$. Заметим, что $\forall i = \overline{1,n-1}$: $\left|\left|\hat{P}_i^{-1}\right|_{p_i} \cdot \left|-\frac{1}{p_n}\right|_{p_i}\right|_{p_i} = \left|-\frac{1}{P_i}\right|_{p_i}$. Из условия теоремы следует, что $|P_i|_{p_i} = 1$, значит $\left|-\frac{1}{P_i}\right|_{p_i} = p_i - 1$. Таким образом, $a = \left|\sum_{i=1}^{n-1} (p_i - 1) \cdot \hat{P}_i\right|_{P_n}$. Так как $\hat{P}_i \cdot p_i = P_n$, то

$$a = \left|\sum_{i=1}^{n-1} (p_i - 1) \cdot \hat{P}_i\right|_{P_n} = \left|\sum_{i=1}^{n-1} P_n - \sum_{i=1}^{n-1} \hat{P}_i\right|_{P_n} = P_n - \left|\sum_{i=1}^{n-1} \hat{P}_i\right|_{P_n}. \tag{58}$$

Учитывая, что $a = P_n - \left|\sum_{i=1}^{n-1} \hat{P}_i\right|_{P_n}$, получим

$$P_n = a \cdot p_n + 1 = p_n \cdot \left(P_n - \left|\sum_{i=1}^{n-1} \hat{P}_i\right|_{P_n}\right) + 1 = P - p_n \cdot \left|\sum_{i=1}^{n-1} \hat{P}_i\right|_{P_n} + 1. \tag{59}$$

Так как

$$p_n \cdot \left|\sum_{i=1}^{n-1} \hat{P}_i\right|_{P_n} = p_n \cdot \left(\sum_{i=1}^{n-1} \hat{P}_i - P_n \cdot \left\lfloor \frac{\sum_{i=1}^{n-1} \hat{P}_i}{P_n} \right\rfloor\right)$$
$$= \sum_{i=1}^{n-1} P_i - P \cdot \left\lfloor \frac{\sum_{i=1}^{n-1} P_i}{P} \right\rfloor = \left|\sum_{i=1}^{n-1} P_i\right|_P. \tag{60}$$

Следовательно, $P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P + 1$.

Докажем, что если $P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P+1$, то $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$. Так как $P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P+1$, то, следовательно, выполняется сравнение

$$P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P + 1 \bmod p_i.$$

Учитывая, что $\forall i = \overline{1,n}$: $P \equiv 0 \bmod p_i$ и $P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P \equiv P_i \bmod p_i$, получим $\forall i = \overline{1,n}$: $P_i \equiv 1 \bmod p_i$.

Лемма доказана. □

Лемма 3. *Если модули RNS $p_1 < p_2 < \ldots < p_n$ удовлетворяют условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$ и $2 \le n \le 58$, то $\sum_{i=1}^{n} P_i = P + 1$.*

Доказательство. Заметим, что $\forall i \in \overline{1,n}$: $\left|\sum_{i=1}^{n} P_i\right|_{p_i} = |P_i|_{p_i}$. Согласно условию леммы, $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$, следовательно, $\forall i \in \overline{1,n}$: $\left|\sum_{i=1}^{n} P_i\right|_{p_i} = 1$, значит, согласно Китайской теореме об остатках, $\left|\sum_{i=1}^{n} P_i\right|_P = 1$. Из равенства $\left|\sum_{i=1}^{n} P_i\right|_P = 1$ следует, что $\sum_{i=1}^{n} P_i = 1 + a \cdot P$, где $a \in \mathbb{Z}$. Так как $n \ge 2$, то $P_{n-1} \ge 2$, $P_n \ge 3$ и $\sum_{i=1}^{n} P_i \ge 5$. Следовательно, $a \ge \frac{4}{P}$. Учитывая, что $a \in \mathbb{Z}$, получим $a \ge 1$. С другой стороны, $\sum_{i=1}^{n} P_i = P \sum_{i=1}^{n} \frac{1}{p_i}$. Так как $p_1 \ge 2$, $p_2 \ge 3$, и так далее, $p_n \ge pr_n$, где pr_i – последовательность простых чисел, то $\sum_{i=1}^{n} \frac{1}{p_i} \le \sum_{i=1}^{n} \frac{1}{pr_i}$. Учитывая, что $\sum_{i=1}^{58} \frac{1}{pr_i} \approx 1.998$ и $\sum_{i=1}^{59} \frac{1}{pr_i} \approx 2.002$, получим, если $n \le 58$, то справедливо неравенство $1 + a \cdot P < 2 \cdot P$, следовательно, $a < 2 - \frac{1}{P} < 2$. Так как $a \in \mathbb{Z}$, $a \ge 1$ и $a < 2$, получим $a = 1$, следовательно, если $n \le 58$, то $\sum_{i=1}^{n} P_i = 1 + P$.

Лемма доказана. □

Из Леммы 3 следует, что если $2 \le n \le 58$ и выполнены условия Леммы 2, то $SQ = P + 1$.

Исследуем подробнее вопрос существования трех-, четырех- и пятимодульных RNS, удовлетворяющих условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$.

Теорема 6. *Пусть модули RNS – попарно взаимно простые числа $p_1 < p_2 < \ldots < p_n$, удовлетворяющие условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$, тогда справедливы следующие утверждения*

1. *Если $n = 3$, то модули RNS $\{2, 3, 5\}$.*
2. *Если $n = 4$, то модули RNS $\{2, 3, 7, 41\}$ или $\{2, 3, 11, 13\}$.*
3. *Если $n = 5$, то модули RNS $\{2, 3, 7, 43, 1805\}$, $\{2, 3, 7, 83, 85\}$ или $\{2, 3, 11, 17, 59\}$.*

Доказательство. Рассмотрим первое утверждение, когда $n = 3$. Для начала покажем, что условие теоремы выполняется только тогда, когда $p_1 = 2$, для этого предположим противное. Пусть существует трехмодульная RNS, удовлетворяющая условию теоремы, для которой $p_1 \ge 3$.

Так как $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$ и $n = 3 \leq 58$, то согласно Лемме 3, выполняется равенство $SQ = P + 1$. Разделим $SQ = P + 1$ на P, получим $\sum_{i=1}^{3} \frac{1}{p_i} = 1 + \frac{1}{P}$, т.е. $\sum_{i=1}^{3} \frac{1}{p_i} > 1$. С другой стороны, так как $p_1 \geq 3$, то $\sum_{i=1}^{3} \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{47}{60} < 1$, следовательно, имеет место противоречие, значит $p_1 = 2$.

Подставляя $p_1 = 2$ в $SQ = P+1$, получим $2 \cdot p_2 + 2 \cdot p_3 + p_2 \cdot p_3 = 2 \cdot p_2 \cdot p_3 + 1$, следовательно,

$$p_3 = \frac{2 \cdot p_2 - 1}{p_2 - 2} = 2 + \frac{3}{p_2 - 2}. \tag{61}$$

Учитывая, что $p_3 \in \mathbb{N}$, из формулы (61) следует, что $\frac{3}{p_2-2} \in \mathbb{N}$, значит $p_2 - 2 = 1$ или $p_2 - 2 = 3$. Решая уравнения, получим $p_2 = 3$ или $p_2 = 5$. Подставляя в формулу (61) $p_2 = 3$, получим $p_3 = 5$, а подставив $p_2 = 5$, получим $p_3 = 3$. Учитывая, что $p_1 < p_2 < p_3$, существует единственный набор трехмодульной RNS, удовлетворяющий условию теоремы, – $\{2, 3, 5\}$.

Докажем второе утверждение, для $n = 4$. Если $p_1 \geq 3$, то $\sum_{i=1}^{4} \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{7} = \frac{389}{420} < 1$, следовательно, аналогично случаю при $n = 3$, получаем, что $p_1 = 2$. Предположим, что существует набор модулей RNS, удовлетворяющий условию теоремы, для которого $p_2 > 3$, следовательно, $p_2 \geq 5$. Тогда $\frac{1}{2} + \frac{1}{p_2} + \frac{1}{p_3} + \frac{1}{p_4} > 1$, откуда $\frac{1}{p_2} + \frac{1}{p_3} + \frac{1}{p_4} > \frac{1}{2}$. Так как $5 \leq p_2 < p_3 < p_4$ и $\forall i = \overline{2,4}$: $\gcd(2, p_i) = 1$, $\frac{1}{p_2} + \frac{1}{p_3} + \frac{1}{p_4} \leq \frac{1}{5} + \frac{1}{7} + \frac{1}{9} = \frac{143}{315} < \frac{1}{2}$. Следовательно, имеет место противоречие и $p_2 = 3$. Подставляя $p_1 = 2$ и $p_2 = 3$ в уравнение $SQ = P + 1$, и выражая p_4 через p_3, получим

$$p_4 = \frac{6 \cdot p_3 - 1}{p_3 - 6} = 6 + \frac{35}{p_3 - 6}. \tag{62}$$

Так как $p_3, p_4 \in \mathbb{N}$ и $3 < p_3 < p_4$, то $p_3 - 6 = 1$ или $p_3 - 6 = 5$. Следовательно, $p_3 = 7$ или 11, а $p_4 = 41$ или 13 соответственно. Значит, существует два набора четырехмодульных RNS, удовлетворяющих условию теоремы, – $\{2, 3, 7, 41\}$ и $\{2, 3, 11, 13\}$.

Рассмотрим третье утверждение, для $n = 5$. Так как если $p_1 \geq 4$, то $\sum_{i=1}^{5} \frac{1}{p_i} \leq \frac{1}{4} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} = \frac{11017}{13860} < 1$, $p_1 = 2$ или $p_1 = 3$.

Пусть $p_1 = 2$. Предположим, что $p_2 \geq 7$, тогда $\sum_{i=2}^{5} \frac{1}{p_i} \leq \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{13} = \frac{3800}{9009} < \frac{1}{2}$. С другой стороны, $\sum_{i=2}^{5} \frac{1}{p_i} = \frac{1}{2} + \frac{1}{P}$, имеет место противоречие, следовательно, $3 \leq p_2 < 7$. Значит, если $p_1 = 2$, то $p_2 = 3$ или $p_2 = 5$.

Рассмотрим случай, когда $p_1 = 2$ и $p_2 = 3$, тогда

$$\sum_{i=3}^{5} \frac{1}{p_i} = 1 - \frac{1}{2} - \frac{1}{6} + \frac{1}{P} = \frac{1}{6} + \frac{1}{P}. \tag{63}$$

Если $p_3 \geq 17$, то левая часть равенства (63) удовлетворяет неравенству $\sum_{i=3}^{5} \frac{1}{p_i} \leq \frac{1}{17} + \frac{1}{19} + \frac{1}{23} = \frac{1151}{7429} < \frac{1}{6}$, при этом правая часть равенства (63) больше $\frac{1}{6}$. Следовательно, $p_3 \leq 16$ и $\gcd(p_3, 6) = 1$, отсюда $p_3 = 7$, 11 или 13.

Если $p_1 = 2$, $p_2 = 3$ и $p_3 = 7$, то

$$p_5 = \frac{42 \cdot p_4 - 1}{p_4 - 42} = 42 + \frac{1763}{p_4 - 42}. \tag{64}$$

Учитывая, что $1763 = 41 \cdot 43$, получим, $p_4 - 42 = 1$ или $p_4 - 42 = 41$. Следовательно, $p_4 = 43$ или 83, а $p_5 = 1805$ или 85 соответственно. Таким образом, основания RNS, удовлетворяющие условию теоремы, – $\{2, 3, 7, 43, 1805\}$ и $\{2, 3, 7, 83, 85\}$.

Если $p_1 = 2$, $p_2 = 3$ и $p_3 = 11$, то

$$p_5 = \frac{66 \cdot p_4 - 1}{5 \cdot p_4 - 66} = 13 + \frac{p_4 + 857}{5 \cdot p_4 - 66}. \tag{65}$$

Так как $\frac{p_4+857}{5 \cdot p_4 - 66} \in \mathbb{N}$, то $\frac{p_4+857}{5 \cdot p_4 - 66} \geq 1$, следовательно, $p_4 + 857 \geq 5 \cdot p_4 - 66$, значит $p_4 \leq \frac{923}{4}$. Проверив все возможные варианты, получим что для $p_4 \in [14, 230]$: $\frac{p_4+857}{5 \cdot p_4 - 66} \in \mathbb{N}$, $p_4 = 17$ или 59, следовательно, $p_5 = 59$ или 4, соответственно. Учитывая, что $p_1 < p_2 < p_3 < p_4 < p_5$, получим, что условию теоремы в этом случае удовлетворяют основания RNS $\{2, 3, 11, 17, 59\}$.

Если $p_1 = 2$, $p_2 = 3$ и $p_3 = 13$, то

$$p_5 = \frac{78 \cdot p_4 - 1}{7 \cdot p_4 - 78} = 11 + \frac{p_4 + 857}{7 \cdot p_4 - 78}. \tag{66}$$

Учитывая, что $\frac{p_4+857}{7 \cdot p_4 - 78} \in \mathbb{N}$, $\frac{p_4+857}{7 \cdot p_4 - 78} \geq 1$, следовательно, $p_4 + 857 \geq 7 \cdot p_4 - 78$, значит $p_4 \in [14, 155]$. Проверяем, все возможные значения получаем, что при указанных условиях уравнение в целых числах решения не имеет.

Рассмотрим случай, когда $p_1 = 2$ и $p_2 = 5$. Для таких RNS $\sum_{i=3}^{5} \frac{1}{p_i} = 1 - \frac{1}{2} - \frac{1}{5} - \frac{1}{P} = \frac{3}{10} + \frac{1}{P}$. Если $p_3 \geq 9$, то $\sum_{i=3}^{5} \frac{1}{p_i} \leq \frac{1}{9} + \frac{1}{11} + \frac{1}{13} = \frac{359}{1287} < \frac{3}{10}$. С другой стороны, $\sum_{i=3}^{5} \frac{1}{p_i} = \frac{3}{10} + \frac{1}{P} > \frac{3}{10}$, следовательно, $5 < p_3 < 9$ и $\gcd(p_3, 10) = 1$, значит $p_3 = 7$.

Подставим $p_1 = 2$, $p_2 = 5$ и $p_3 = 7$ в равенство $SQ = P + 1$, получим

$$p_5 = \frac{70 \cdot p_4 - 1}{11 \cdot p_4 - 70} = 6 + \frac{4 \cdot p_4 + 419}{11 \cdot p_4 - 70}. \tag{67}$$

Учитывая, что $7 < p_4 < p_5$ и $p_5 \in \mathbb{N}$, $\frac{4 \cdot p_4 + 419}{11 \cdot p_4 - 70} \in \mathbb{N}$, следовательно,

$$\begin{cases} p_4 & > 7, \\ 11 \cdot p_4 - 70 & > 0, \\ \frac{4 \cdot p_4 + 419}{11 \cdot p_4 - 70} & \geq 3. \end{cases} \tag{68}$$

Решая систему неравенств получим, что $7 < p_4 \leq \frac{629}{29}$. Учитывая, что $p_4 \in \mathbb{N}$ и $\gcd(p_4, 70) = 1$, возможными решениями являются $p_4 \in \{9, 11, 13, 17, 19\}$. Проверим какие из чисел $\{9, 11, 13, 17, 19\}$ при подстановке в $f(p_4) = \frac{4 \cdot p_4 + 419}{11 \cdot p_4 - 70}$ удовлетворяют условию $f(p_4) \in \mathbb{N}$, получим $f(9) = \frac{455}{29} \notin \mathbb{N}$, $f(11) = \frac{463}{51} \notin \mathbb{N}$, $f(13) = \frac{471}{73} \notin \mathbb{N}$, $f(17) = \frac{487}{117} \notin \mathbb{N}$ и $f(19) = \frac{495}{139} \notin \mathbb{N}$. Значит не существует пятимодульных RNS с модулями $p_1 = 2$ и $p_2 = 5$, удовлетворяющих условию $\forall i = \overline{1, n}$: $|P_i|_{p_i} = 1$.

Рассмотрим случай, когда $p_1 = 3$, тогда $\sum_{i=2}^{5} \frac{1}{p_i} = 1 - \frac{1}{3} + \frac{1}{P} = \frac{2}{3} + \frac{1}{P} > \frac{2}{3}$. Если $p_2 \geq 5$, то $\sum_{i=2}^{5} \frac{1}{p_i} \leq \frac{1}{5} + \frac{1}{7} + \frac{1}{8} + \frac{1}{11} = \frac{1721}{3080} < \frac{2}{3}$, таким образом, имеет место противоречие, следовательно, $3 < p_2 < 5$, значит $p_2 = 4$.

Оценим значения, которые может принимать p_3. $\sum_{i=3}^{5} \frac{1}{p_i} = 1 - \frac{1}{3} - \frac{1}{4} + \frac{1}{P} = \frac{5}{12} + \frac{1}{P} > \frac{5}{12}$. Если $p_3 \geq 7$, то $\sum_{i=3}^{5} \frac{1}{p_i} \leq \frac{1}{7} + \frac{1}{11} + \frac{1}{13} = \frac{311}{1001} < \frac{5}{12}$, следовательно, имеет место противоречие, и p_3 удовлетворяет условиям $4 < p_3 < 7$ и $\gcd(p_3, 12) = 1$, значит $p_3 = 5$.

Подставим $p_1 = 3$, $p_2 = 4$ и $p_3 = 5$ в $SQ = P + 1$, получим

$$p_5 = \frac{60 \cdot p_4 - 1}{13 \cdot p_4 - 60} = 4 + \frac{8 \cdot p_4 + 239}{13 \cdot p_4 - 60}. \tag{69}$$

Учитывая, что $5 < p_4 < p_5$, $\gcd(p_5, 60) = 1$ и $p_5 \in \mathbb{N}$, $p_4 \geq 7$, $p_5 \geq 11$, $\frac{8 \cdot p_4 + 239}{13 \cdot p_4 - 60} \geq 7$ и $\frac{8 \cdot p_4 + 239}{13 \cdot p_4 - 60} \in \mathbb{N}$, следовательно

$$\begin{cases} p_4 & \geq 7, \\ 13 \cdot p_4 - 60 & > 0, \\ \frac{8 \cdot p_4 + 239}{13 \cdot p_4 - 60} & \geq 7. \end{cases} \tag{70}$$

Учитывая, что $p_4 \in \mathbb{N}$, $p_4 = 7$ – единственное решение, удовлетворяющее системе неравенств (70). Проверим является, ли натуральным числом $g(p_4) = \frac{8 \cdot p_4 + 239}{13 \cdot p_4 - 60}$ в точке $p_4 = 7$, получим $g(7) = \frac{295}{31} \notin \mathbb{N}$. Следовательно, не существует пятимодульных RNS, для которых выполнялись бы условия $p_1 = 3$ и $\forall i = \overline{1, n}$: $|P_i|_{p_i} = 1$.

Теорема доказана. □

Теорема 7. *Не существует попарно взаимно простых чисел (оснований RNS)* $p_1 < p_2 < \ldots < p_n < 2 \cdot p_1$, *удовлетворяющих условиям* $\forall i = \overline{1, n}$: $|P_i|_{p_i} = 1$.

Доказательство. Покажем, что если $\forall i = \overline{1, n}$: $|P_i|_{p_i} = 1$, то $p_1 < n$. Предположим противное, что существует набор модулей RNS, для которых выполняются условия $\forall i = \overline{1, n}$: $|P_i|_{p_i} = 1$ и $p_1 \geq n$. Так как выполняются условия $\forall i = \overline{1, n}$: $|P_i|_{p_i} = 1$, то, следовательно, выполняются условия Леммы 2, и $P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P + 1$. Разделим равенство

$P_n + \left|\sum_{i=1}^{n-1} P_i\right|_P = P + 1$ на P, получим

$$\frac{1}{p_n} + \left\{\sum_{i=1}^{n-1} \frac{1}{p_i}\right\} = 1 + \frac{1}{P}, \tag{71}$$

где $\{x\}$ – дробная часть вещественного числа x.

Так как $n \le p_1 < p_2 < \ldots < p_n$, то $\sum_{i=1}^{n-1} \frac{1}{p_i} \le \sum_{i=1}^{n-1} \frac{1}{n} = \frac{n-1}{n} < 1$, следовательно, $\left\{\sum_{i=1}^{n-1} \frac{1}{p_i}\right\} = \sum_{i=1}^{n-1} \frac{1}{p_i}$, тогда формула (71) примет вид

$$\sum_{i=1}^{n} \frac{1}{p_i} = 1 + \frac{1}{P}. \tag{72}$$

Учитывая, что $n \le p_1 < p_2 < \ldots < p_n$, левая часть равенства (72) удовлетворяет условию $\sum_{i=1}^{n} \frac{1}{p_i} \le \sum_{i=1}^{n} \frac{1}{n} = 1$, а правая часть $1 + \frac{1}{P} > 1$, следовательно, если $p_1 \ge n$, то имеет место противоречие. Таким образом, не существует RNS с модулями, удовлетворяющими условиям $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$ и $p_1 \ge n$. Значит условием $p_1 < n$ является необходимым.

С другой стороны, ранее было показано, что $p_n \ge p_1 + 2 \cdot n - 4$. Учитывая, что согласно условию теоремы $p_n < 2 \cdot p_1$, $p_n < 2 \cdot n$. Решая неравенство $p_1 + 2 \cdot n - 4 < 2 \cdot n$, получим, что условию $p_1 < p_2 < \ldots < p_n < 2 \cdot p_1$ могут удовлетворять значения $p_1 < 4$, т.е. $p_1 = 2$ и $p_1 = 3$. Если $p_1 = 2$, то $p_n < 4$, следовательно, если и существуют подходящие RNS, то только двухмодульная RNS $\{2, 3\}$, что противоречит Лемме 1, согласно которой $n \ge 3$ при указанных в формулировке теоремы условиях. Рассмотрим случай, если $p_1 = 3$. Тогда $p_n < 6$, следовательно, возможен только один вариант, при условии что $n \ge 3$, равный $\{3, 4, 5\}$, но он не удовлетворяет условию $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$. Следовательно, не существует модулей RNS, удовлетворяющих условиям: $p_1 < p_2 < \ldots < p_n < 2 \cdot p_1$ и $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$.

Теорема доказана. □

Из Теоремы 7 следует, что если модули RNS удовлетворяют условиям $\forall i = \overline{1,n}$: $|P_i|_{p_i} = 1$, то они не являются компактной или сбалансированной последовательностью.

6 Заключение

В статье рассмотрена проблема вычисления ранга числа для реализации операции обратного преобразования чисел из RNS в PNS. Выдвинуто предположение, что одним из способов решения проблемы эффективного вычисления ранга числа могло бы стать представление функции ядра в виде алгебраического многочлена над $\mathbb{Z}_P$. Показано, что функцию ядра нельзя вычислить с помощью алгебраического многочлена над $\mathbb{Z}_P$. В статье разработаны методы вычисления ранга числа с использованием приближенного метода. Произведена оценка точности вычислений для

приближенного метода. Рассчитана верхняя и нижняя граница N, для гарантированного точного перевода чисел. Исследована задача выбора модулей RNS так, чтобы N максимально приблизилось к нижней границе.

Результаты представленного в статье исследования могут использоваться для реализации вычислительно сложных операций в RNS, что позволит расширить область применения RNS на практике.

References

[1] C.H. Chang, A.S. Molahosseini, A.A.E. Zarandi, T.F. Tay, *Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications*, IEEE Circuits Systems Magazine, **15**:4 (2015), 26–44.

[2] G.C. Cardarilli, A. Nannarelli, M. Re, *RNS applications in digital signal processing*, In Molahosseini, A., de Sousa, L., Chang, CH. (eds), *Embedded systems design with special arithmetic and number systems*, Springer, Cham, 2017, 181–215.

[3] R. Reddy, B. Rajesh, A. Nandini, P. Kumar, K.S. Chakradhar, *Design of RNS-KSA based 2D FIR filter*, 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS), (2024), 1–5.

[4] Y. Yao, J. Zhou, B. Yan, Y. Li, *RNS-Based embedding scheme for data hiding in digital images*, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), (2018), 1480–1483.

[5] G.K. Armah, E. Ahene, *Application of residue number system (RNS) to image processing using orthogonal transformation*, 2015 IEEE International Conference on Communication Software and Networks (ICCSN), (2015), 322–328.

[6] J.B. Eseyin, K.A. Gbolagade, *A residue number system based data hiding using steganography and cryptography*, NIU J. Social Sci., **5**:2 (2019), 345–351.

[7] J.H. Cheon, K. Han, A. Kim, M. Kim, Y. Song, *A full RNS variant of approximate homomorphic encryption*, in Cid, Carlos (ed.) et al., *Selected areas in cryptography – SAC 2018*, Lect. Notes Comput. Sci., **11349**, Springer, Cham, 2018, 347–368. Zbl 1447.94026

[8] H.T. Vergos, G. Dimitrakopoulos, *On modulo $2^n + 1$ adder design*, IEEE Trans. Comput., **61**:2 (2012), 173–186. Zbl 1365.65320

[9] P.V.A. Mohan, *RNS-to-binary converter for a new three-moduli set $\{2^{n+1}-1, 2^n, 2^n-1\}$* , IEEE Trans. Circuits Syst. I: Express Briefs, **54**:9 (2007), 775–779.

[10] P. Patronik, S.J. Piestrak, *Design of reverse converters for the general RNS 3-moduli set $\{2^k,\ 2^n-1,\ 2^n+1\}$* , EURASIP J. Adv. Signal Process, **92** (2023).

[11] V.M. Amerbaev *Theoretical foundations of machine arithmetic*, Nauka, Alma-Ata, 1976. Zbl 0401.68047

[12] N.I. Chervyakov, A.S. Molahosseini, P.A. Lyakhov, M.G. Babenko, M.A. Deryabin, *Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem*, Int. J. Comput. Math., **94**:9 (2017), 1833–1849. Zbl 6905133

[13] M. Babenko, M. Deryabin, S. Piestrak, P. Patronik, N. Chervyakov, A. Tchernykh, A. Avetisyan, *RNS number comparator based on a modified diagonal function*, Electronics, **9**:11 (2020), Article ID 1784.

[14] V. Ryabchikova, R. Kurmaev, E. Martirosyan, V. Slobodskoy, *Novel RNS reverse conversion algorithm based on core function*, 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2022, 42–46.

[15] M. Selianinau, Y. Povstenko, *An efficient parallel reverse conversion of residue code to mixed-radix representation based on the Chinese remainder theorem*, Entropy, **24**:2 (2022), Paper No. 242. MR4386730

[16] P.V.A. Mohan, *RNS to binary conversion using diagonal function and Pirlo and Impedovo monotonic function*, Circuits Syst Signal Process, **35**:3 (2016), 1063–1076. MR3459148

[17] G. Pirlo, D. Impedovo, *A new class of monotone functions of the residue number system*, Int. J. Math. Models Methods Appl. Sci., **7**:9 (2013), 802–809.

[18] K.A. Gbolagade, R. Chaves, L. Sousa, S.D. Cotofana, *An improved RNS reverse converter for the* $\{2^{2n+1}-1,\ 2^n,\ 2^n-1\}$, Proceedings of 2010 IEEE International Symposium on Circuits and Systems, 2010, 2103–2106.

[19] H. Pettenghi, R. de Matos, A. Molahosseini, *RNS reverse converters for moduli sets with dynamic ranges of 9n-bit*, 2016 IEEE 7th Latin American Symposium on Circuits & Systems (LASCAS), 2016, 143–146.

[20] P. Patronik, S.J. Piestrak, *Design of reverse converters for a new flexible RNS five-moduli set* $\{2^k, 2^n-1, 2^n+1, 2^{n+1}-1, 2^{n-1}-1\}$ *(n even)*, Circuits Syst. Signal Process, **36**:11 (2017), 4593–4614. Zbl 1373.94680

[21] N. Chervyakov, M. Babenko, A. Tchernykh, N. Kucherov, V. Miranda-López, J. M. Cortés-Mendoza, *AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security*, Computation, **92** (2019), 1080–1092.

Babenko Mikhail Grigorevich
Federal State Autonomous Educational Institution for Higher Education "North-Caucasus Federal University",
1 Pushkin str,
355017, Stavropol, Russia
Email address: mgbabenko@ncfu.ru

Valueva Maria Vasilyevna
FSAE HE "M. K. Ammosov North-Eastern Federal University",
58 Belinsky str,
677027, Yakutsk, Republic of Sakha (Yakutia), Russia,
Email address: mriya.valueva@mail.ru

Valuev Georgii Vyacheslavovich
Federal State Autonomous Educational Institution for Higher Education "North-Caucasus Federal University",
1 Pushkin str,
355017, Stavropol, Russia
Email address: mail@gvvaluev.ru

Anton Sergeevich Nazarov
Federal State Autonomous Educational Institution for Higher Education "North-Caucasus Federal University",
1 Pushkin str,
355017, Stavropol, Russia
Email address: anazarov@ncfu.ru