ИНФОРМАТИКА

2013 январь-март № 1

УДК 004.9; 004.4; 004.056

А.А. Коляда, А.Ф. Чернявский

ИНТЕГРАЛЬНО-ХАРАКТЕРИСТИЧЕСКАЯ БАЗА МОДУЛЯРНЫХ СИСТЕМ СЧИСЛЕНИЯ

Рассматривается проблематика создания интегрально-характеристической базы модулярных систем счисления, определенных на диапазонах неотрицательных целых чисел. Для решения поставленной задачи применяется аппарат интервально-модулярных форм целых чисел, ключевую роль в котором выполняют интервально-индексные характеристики – интервальный индекс и главный интервальный индекс. Приоритетные позиции данных характеристик обусловлены их существенными преимуществами над известными интегральными характеристиками модулярного кода при оптимизации алгоритмов немодульных операций.

Введение

Постоянный интерес к модулярной вычислительной технологии как к уникальному средству распараллеливания вычислений стимулирует разработки по созданию и оптимизации классов модулярных вычислительных структур, которые ориентированы на обеспечение принципиально нового уровня производительности и контроля достоверности расчетов на сложных математических моделях, таких, в частности, как множества комплексных и гиперкомплексных чисел, полиномов и т. п. [1−5]. Для модулярных вычислительных структур, определенных на диапазонах многомерного типа, вещественные модулярные системы счисления (МСС) выполняют роль систем нижнего уровня. Поэтому разработка и оптимизация алгоритмов компьютерной арифметики МСС данного класса имеют основополагающее значение.

Модулярный код явно не содержит информации о величине отвечающего ему элемента рабочего диапазона. Поэтому при выполнении в МСС операций, тем или иным образом связанных с некоторыми характеристиками местоположения целых чисел (ЦЧ) в диапазоне или за его пределами, приходится использовать формы представления ЦЧ (через цифры модулярного кода), позволяющие получить искомые характеристики. В отличие от модульных операций (сложения, вычитания, умножения без контроля переполнения), реализуемых поразрядно (параллельно), операции указанного типа в модулярной арифметике квалифицируются как немодульные. Базовые формы ЦЧ для таких операций включают одну или более интегральных характеристик модулярного кода (ИХМК) – числовых характеристик, которые рассчитываются по части или всем цифрам данного кода.

Вполне понятно, что сложность вычисления применяемых ИХМК в конечном счете определяет эффективность созданной на их основе модулярной арифметики. В свете сказанного в общей проблематике разработки модулярной арифметики ключевая роль принадлежит исследованиям по оптимизации интегрально-характеристической базы МСС, и в первую очередь МСС с вещественными (целочисленными) диапазонами. В настоящей статье излагаются теоретические основы универсальной технологии расчета ИХМК, составляющие так называемый аппарат интервально-модулярных форм (ИМФ). В рамках развиваемого подхода в качестве вспомогательного инструментария используется также и ранговая форма ЦЧ, которая наряду с полиадической формой традиционно применяется для синтеза немодульных процедур [6−8]. Преимущества, обеспечиваемые ИМФ, обусловлены модульностью базовой ИХМК – интервального индекса (ИИ). Благодаря данному свойству ИИ приведение ЦЧ к остаткам по модулю с помощью ИМФ существенно упрощается. При этом интервально-индексные характеристики связаны с другими ИХМК тривиальными соотношениями. Это относится к характеристикам не только одного и того же, но и разных порядков, а также к ИХМК элементов симметричных диапазонов. Реализация преимуществ ИМФ и связанных с ними интервально-индексных характеристик применительно к проблеме построения интегрально-характеристической базы модулярной арифметики составляет главное содержание представляемых исследований.

1. Базовые обозначения и терминология

Введем следующие обозначения:

Z – множество ЦЧ;

$\lfloor x \rfloor$ и $\lceil x \rceil$ – наибольшее и наименьшее ЦЧ соответственно, не большее и не меньшее вещественной величины x;

$\mathrm{sn}(x)$ – знаковая функция вида $\mathrm{sn}(x) = \begin{cases} 0, & \text{если } x \geq 0; \\ 1, & \text{если } x < 0; \end{cases}$

$\mathbf{X}\times\mathbf{Y}=\{\forall(x, y) \mid x \in \mathbf{X}, y \in \mathbf{Y}\}$ – декартово произведение множеств **X**, **Y**;

$\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ и $\mathbf{Z}_m^- = \{-\lfloor m/2 \rfloor, -\lfloor m/2 \rfloor+1, \ldots, \lceil m/2 \rceil -1\}$ – множества (кольца) наименьших неотрицательных и абсолютно наименьших вычетов по натуральному модулю $m>1$ соответственно;

$|x|_m$ – элемент множества $\mathbf{Z}_m$, сравнимый с x (в общем случае рациональной величиной) по модулю m;

$M_n=\prod_{j=1}^{n} m_j$, $M_{i,n}=M_n / m_i$ $(i=\overline{1,\ n})$, где $m_1, m_2, \ldots, m_n$ – натуральные модули $(n\geq 1)$;

$M_n=\prod_{j=1}^{n} m_j$, $M_{i,n}=M_n / m_i$ $(i=\overline{1, n})$, где $m_1, m_2, \ldots, m_n$ – натуральные модули $(n\geq 1)$;

$(| X |_{m_1}, | X |_{m_2}, \ldots, | X |_{m_l})$ – модулярный код числа $X\in\mathbf{Z}$ по базису $\{m_1, m_2, \ldots, m_l\}$ $(l>1)$.

2. Интегральные характеристики кода МСС с целочисленными диапазонами

На множестве **Z** ЦЧ неизбыточная МСС определяется с помощью попарно простых оснований – модулей $m_1, m_2, \ldots, m_k$ $(k>1)$ – отображением $\mathbf{Z} \to \mathbf{Z}_1\times \mathbf{Z}_2\times \ldots \times \mathbf{Z}_{m_k}$, которое каждому $X \in \mathbf{Z}$ ставит в соответствие набор $(\chi_1, \chi_2, \ldots, \chi_k)$ остатков $\chi_i = |X|_{m_i}$ от деления X на m_i $(i=\overline{1, k})$. При этом для X употребляется запись $X=(\chi_1, \chi_2, \ldots, \chi_k)$.

Модулярному коду $(\chi_1, \chi_2, \ldots, \chi_k)$ отвечает множество всех ЦЧ X, удовлетворяющих системе сравнений

$$\begin{cases} X \equiv \chi_1 (\mathrm{mod}\, m_1), \\ X \equiv \chi_2 (\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ X \equiv \chi_k (\mathrm{mod}\, m_k). \end{cases} \tag{1}$$

Справедливо следующее утверждение [9, 10].

Теорема 1 (Китайская теорема об остатках (КТО)). *Если модули $m_1, m_2, \ldots, m_k$ попарно просты, то система сравнений (1) имеет единственное решение – класс вычетов по модулю M_k, определяемый сравнением*

$$X \equiv \left(\sum_{i=1}^{k} M_{i,k}\, \chi_{i,k} \right) (\mathrm{mod}\, M_k), \tag{2}$$

где $\chi_{i,k} = | M_{i,k}^{-1} \chi_i |_{m_i}$.

Практическое применение МСС предполагает, что каждому модулярному коду $(\chi_1, \chi_2, \ldots, \chi_k)$ должно отвечать единственное ЦЧ (а не класс вычетов). Поэтому для обеспечения требуемой взаимной однозначности в качестве рабочего диапазона используются те или иные совокупности представителей классов вычетов. В компьютерных приложениях их роль выполняют множества $\mathbf{Z}_{M_k}$ или $\mathbf{Z}^{-}_{M_k}$. С учетом сказанного в первом случае модулярное кодирование определяется как отображение ν_{MCC}: $\mathbf{Z}_{M_k} \to \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \ldots \times \mathbf{Z}_{m_k}$, которое каждому $X\in \mathbf{Z}_{M_k}$ ставит в соответствие код $(\chi_1,\chi_2,\ldots,\chi_k)$. Декодирующее отображение ν^{-1}_{MCC} $\mathbf{Z}_{m_1} \times \times \mathbf{Z}_{m_2} \times \ldots \times \mathbf{Z}_{m_k} \to \mathbf{Z}_{M_k}$, базирующееся на (2), действует согласно правилу

$$X = \left|\sum_{i=1}^{k} M_{i,k}\chi_{i,k}\right| \quad (\chi_{i,k} = | M^{-1}_{i,k}\chi_i |_{m_i}) \tag{3}$$

Непосредственное применение выражения (3) в качестве базовой формы ЦЧ при синтезе немодульных процедур практически невозможно из-за сложности прямой компьютерной реализации, особенно в случае больших M_k. Вместе с тем из (3) с помощью специальных ИХМК могут быть получены параллельные формы ЦЧ, обладающие весьма хорошими реализационными свойствами.

Пусть по набору модулей m_1, m_2, ..., m_l ($2\le l\le k$) числу $X\in\mathbf{Z}$ отвечает модулярный код $(\chi_1,\chi_2,\ldots,\chi_l)$. Согласно КТО (теореме 1) по аналогии с (3) можно записать:

$$| X |_{M_l} = \left|\sum_{i=1}^{l} M_{i,l} \left| M^{-1}_{i,l}\chi_i\right|_{m_i}\right|_{M_l}. \tag{4}$$

Из (4) следует, что разность $| X |_{M_l} - \sum_{i=1}^{l} M_{i,l} \left| M^{-1}_{i,l}\chi_i\right|_{m_i}$ кратна константе M_l. Таким образом, справедливо равенство

$$\begin{aligned} | X |_{M_l} &= \sum_{i=1}^{l} M_{i,l} \left| M^{-1}_{i,l}\chi_i\right|_{m_i} - M_l\, \rho_l(X) = \\ &= \sum_{i=1}^{l} M_{i,l}\chi_{i,l} - M_l\, \rho_l(X) \; (\chi_{i,l} = \left| M^{-1}_{i,l}\chi_i\right|_{m_i}), \end{aligned} \tag{5}$$

где $\rho_l(X)$ – некоторое ЦЧ. При любом $X\in\mathbf{Z}$ числу $| X |_{M_l} \in \mathbf{Z}_{M_l}$ соответствует единственное значение ИХМК $\rho_l(X) = \rho_l\,(\chi_1,\chi_2,\ldots,\chi_l)$.

Определение 1. ИХМК $\rho_l(X)$ называется рангом числа $| X |_{M_l}$ в МСС с основаниями m_1, m_2, ..., m_l и диапазоном $\mathbf{Z}_{M_l}$ или ранговой характеристикой l-го порядка, а выражение (5) – ранговой формой ЦЧ того же порядка.

Согласно КТО, применяемой к системе сравнений

$$\begin{cases} X \equiv \chi_1 (\mathrm{mod}\, m_1), \\ X \equiv \chi_2 (\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ X \equiv \chi_{l-1} (\mathrm{mod}\, m_{l-1}), \end{cases}$$

имеем $X \equiv (\sum_{i=1}^{l-1} M_{i,l-1} \left| M_{i,l-1}^{-1} \chi_i \right|_{m_i})$ (mod M_{l-1}). Следовательно, для X существует единственное ЦЧ (обозначим его через $I_l(X)$), такое, что

$$X = \sum_{i=1}^{l-1} M_{i,l-1} \left| M_{i,l-1}^{-1} \chi_i \right|_{m_i} + M_{l-1} I_l(X) = \\ = \sum_{i=1}^{l-1} M_{i,l-1} \chi_{i,l-1} + M_{l-1} I_l(X) \ (\chi_{i,l-1} = \left| M_{i,l-1}^{-1} \chi_i \right|_{m_i}). \quad (6)$$

Определение 2. ИХМК $I_l(X)$ называется ИИ ЦЧ X относительно модулей $m_1, m_2, ..., m_l$, а выражение вида (6) – ИМФ ЦЧ.

При $l=k$ для введенных ИХМК $\rho_l(X)$ и $I_l(X)$ будем использовать также обозначения $\rho(X)$ и $I(X)$.

Определение 3. Компоненты $\hat{I}_l(X) = |I_l(X)|_{m_l}$ и $J_1(X)=\lfloor I_l(X)/m_l \rfloor$ представления ИИ $I_1(X)$ вида

$$I_l(X) = \hat{I}_l(X) + m_l J_l(X) \quad (7)$$

назовем соответственно компьютерным и главным ИИ ЦЧ X относительно модулей $m_1, m_2, ..., m_l$.

С помощью ранговой и интервально-индексной характеристик, а также связанных с ними форм ЦЧ могут быть реализованы все немодульные операции. Наряду с ранговой и интервально-индексной версиями модулярной арифметики на практике часто применяется версия, использующая полиадическую форму ЦЧ [6, 11, 12], которая имеет вид

$$|X|_{M_l} = \sum_{i=1}^{l} M_{i-1} x_i \ (X \in \mathbf{Z};\ M_0 = 1;\ \ x_i \in \mathbf{Z}_{m_i}). \quad (8)$$

В модулярной арифметике, построенной на основе (8), коэффициенты $x_1, x_2, ..., x_l$ выполняют роль ИХМК.

Определение 4. Систему счисления (СС), в которой ЦЧ из диапазона $\mathbf{Z}_{M_l}$ представляется в форме (8), называют обобщенной позиционной СС, полиадической СС или СС со смешанным основанием. При этом для $|X|_{M_l}$ употребляется запись $|X|_{M_l} = \langle x_l x_{l-1} ... x_1 \rangle_{m_1, m_2, ..., m_l}$ или $|X|_{M_l} = \langle x_l x_{l-1} ... x_1 \rangle$.

Определение 5. Величину $N_l(X) = \lfloor X / M_l \rfloor$ назовем интервальным номером ЦЧ X относительно модулей $m_1, m_2, ..., m_l$ ($l \geq 1$).

3. Вычислительная структура интегральных характеристик кода неизбыточных МСС с целочисленными диапазонами

Для введенных ИХМК верны приводимые ниже утверждения.

Теорема 2. *Максимальное значение* $\rho_{l,\max}$ *ранга* $\rho_l(X)=\rho_l(|X|_{M_l})$ *числа* $|X|_{M_l} = (\chi_1, \chi_2, ..., \chi_l)$ ($X \in Z$; $l>1$) *в МСС с основаниями* $m_1, m_2, ..., m_l$ *не превышает* $l-1$, *т. е.*

$$\rho_1(X) \leq \rho_{l,\max} = \max\{\rho_l(A) \mid A \in \mathbf{Z}_{M_l}\} \leq l-1. \quad (9)$$

Доказательство. Согласно (5)

$$|X|_{M_l} = \sum_{i=1}^{l} M_{i,l} - M_l \rho_l(X) \ (X \in \mathbf{Z};\ \chi_{i,l} = \left| M_{i,l}^{-1} \chi_i \right|_{m_i}). \quad (10)$$

Деление (10) M_l с последующим переходом в обеих частях полученного равенства к антье $\lfloor |X|_{M_l}/M_l \rfloor = 0$ дает

$$\rho_l(X) = \left\lfloor \sum_{i=1}^{l} \frac{\chi_{i,l}}{m_i} \right\rfloor. \qquad (11)$$

Пусть $m_{\max,l} = \max\{m_1, m_2, ..., m_l\}$. Так как $m_{\max,l} > l$ при любом $l > 1$, из (11) с учетом взаимной однозначности отображений $\chi_i \to \chi_{i,l}$ на $\mathbf{Z}_{m_i}$ $(i = \overline{1,l})$ для $\rho_l(X)$ вытекает оценка

$$\rho_l(X) \le \left\lfloor \sum_{i=1}^{l} \frac{m_i - 1}{m_i} \right\rfloor = l + \left\lfloor -\sum_{i=1}^{l} \frac{1}{m_i} \right\rfloor = l - \left\lceil \sum_{i=1}^{l} \frac{1}{m_i} \right\rceil \le l - \left\lceil \sum_{i=1}^{l} \frac{1}{m_{\max,l}} \right\rceil = l - \left\lceil \frac{l}{m_{\max,l}} \right\rceil = l - 1. \blacksquare$$

Теорема 3 (о ранге числа). *В МСС с основаниями* $m_1, m_2, ..., m_{l-1}$, $m_l \ge l - 2$ $(l > 1)$ *и диапазоном* $\mathbf{Z}_{M_l}$ *ранг* $\rho_l(X) = \rho_l(|X|_{M_l})$ *числа* $|X|_{M_l} = (\chi_1, \chi_2, ..., \chi_l)$ $(X \in \mathbf{Z})$ *представим в виде*

$$\rho_l(X) = \hat{\rho}_l(X) + \Theta_l(X), \qquad (12)$$

где

$$\hat{\rho}_l(X) = \left\lfloor m_l^{-1} \sum_{i=1}^{l} R_{i,l}(\chi_i) \right\rfloor; \qquad (13)$$

$$R_{i,l}(\chi_i) = \left\lfloor \frac{m_l}{m_i} |M_{i,l}^{-1}\chi_i|_{m_i} \right\rfloor = |-m_i^{-1} |M_{i,l-1}^{-1}\chi_i|_{m_i}|_{m_l} \quad (i = \overline{1, l-1});$$

$$R_{l,l}(\chi_l) = \left| \frac{\chi_l}{M_{l-1}} \right|_{m_l}; \qquad (14)$$

$\Theta_l(X)$ – *двузначная величина, принимающая значения* 0 *или* 1.

Доказательство. Применяя лемму Евклида [9], можно записать

$$m_l\chi_{i,l} = |m_l\chi_{i,l}|_{m_i} + m_i \left\lfloor \frac{m_l}{m_i}\chi_{i,l} \right\rfloor = \left| m_l \left| M_{i,l}^{-1}\chi_i \right|_{m_i} \right|_{m_i} + m_i \left\lfloor \frac{m_l}{m_i} \left| M_{i,l}^{-1}\chi_i \right|_{m_i} \right\rfloor =$$
$$= \chi_{i,l-1} + m_i R_{i,l}(\chi_i) \ (i = \overline{1, l-1}). \qquad (15)$$

Фигурирующая в (15) величина $R_{i,l}(\chi_i) = \left\lfloor \frac{m_l}{m_i} \left| M_{i,l}^{-1}\chi_i \right|_{m_i} \right\rfloor \in \mathbf{Z}_{m_l}$. Поэтому переход в (15) к остаткам по модулю m_l позволяет получить $R_{i,l}(\chi_i)$ в следующей эквивалентной форме: $R_{i,l}(\chi_i) = |(m_l\chi_{i,l} - \chi_{i,l-1})/m_i|_{m_l} = |-m_i^{-1} |M_{i,l-1}^{-1}\chi_i|_{m_i}|_{m_l}$.

Используя (15) и обозначения (14), выполним над ранговой формой ЦЧ $|X|_{M_l}$ (см. (5)) преобразование

$$|X|_{M_l} = \sum_{i=1}^{l} M_{i,l}\chi_{i,l} - M_l\rho_l(X) = \sum_{i=1}^{l-1} M_{i,l-1} m_l \chi_{i,l} + M_{l,l}\chi_{l,l} - M_l\rho_l(X) =$$
$$= \sum_{i=1}^{l-1} M_{i,l-1}\chi_{i,l-1} + M_{l-1}\Big(\sum_{i=1}^{l} R_{i,l}(\chi_i) - m_l\rho_l(X)\Big) = \sum_{i=1}^{l-1} M_{i,l-1}\chi_{i,l-1} - M_{l-1}\rho_{l-1}(X) + \qquad (16)$$
$$+ M_{l-1}\rho_{l-1}(X) + M_{l-1}\Big(\sum_{i=1}^{l} R_{i,l}(\chi_i) - m_l\rho_l(X)\Big).$$

Для МСС с основаниями m_1, m_2, ..., m_{l-1} и диапазоном $\mathbf{Z}_{M_{l-1}}$ аналог равенства (5) (ранговая форма ЦЧ ($l-1$)-го порядка) имеет вид

$$|X|_{M_l-1} = \sum_{i=1}^{l-1} M_{i,\,l-1}\chi_{i,l-1} - M_{l-1}\rho_{l-1}(X). \tag{17}$$

Благодаря (17) из (16) вытекает соотношение

$$|X|_{M_l} = |X|_{M_{l-1}} + M_{l-1}(\rho_{l-1}(X) + \sum_{i=1}^{l} R_{i,l}(\chi_i) - m_l\rho_l(X)).$$

В соответствии с леммой Евклида отсюда следует, что

$$N_{l-1}(|X|_{M_{l-1}}) = \lfloor |X|_{M_l} / M_{l-1} \rfloor = \rho_{l-1}(X) + \sum_{i=1}^{l} R_{i,l}(\chi_i) - m_l\rho_l(X)$$

или

$$\rho_l(X) + (N_{l-1}(|X|_{M_l}) - \rho_{l-1}(X))/m_l = m_l^{-1}\sum_{i=1}^{l} R_{i,l}(\chi_i). \tag{18}$$

Теперь для получения искомого результата − формулы (12) – достаточно в (18) перейти к антье, приняв при этом во внимание (13), а также обозначение

$$\Theta_l(X) = -\lfloor (N_{l-1}(|X|_{M_l}) - \rho_{l-1}(X))/m_l \rfloor = \lceil (\rho_{l-1}(X) - N_{l-1}(|X|_{M_l}))/m_l \rceil. \tag{19}$$

Согласно теореме 2, применяемой к МСС с основаниями m_1, m_2, ..., m_{l-1}, для ранговой характеристики $\rho_{l-1}(X)$ верна оценка $\rho_{l-1}(X) \le l-2$. Поэтому благодаря условию $m_l > l-2$ ввиду $N_{l-1}(|X|_{M_l}) \in \mathbf{Z}_{m_l}$ справедливо неравенство $-1 < -\frac{m_l-1}{m_l} \le (\rho_{l-1}(X) - N_{l-1}(|X|_{M_l}))/m_l \le \frac{l-2}{m_l} \le 1$, из которого вытекает двузначность величины (19): $\Theta_l(X) \in \{0, 1\}$. ■

Определение 6. Величину $\Theta_l(X)$, определяемую формулой (19), назовем минимальной ИХМК l-го порядка, отвечающей ЦЧ X в МСС с основаниями m_1, m_2, ..., m_{l-1} и диапазоном $\mathbf{Z}_{M_l}$ ($l > 1$).

Приведенное доказательство теоремы 3 позволяет сформулировать следующее утверждение.

Теорема 4. *Минимальная ИХМК $\Theta_l(X)$, отвечающая произвольному ЦЧ X в МСС с основаниями m_1, m_2, ..., m_{l-1}, $m_l \ge l-2$ ($l>1$), является двузначной величиной:* $\Theta_l(X) \in \{0, 1\}$.

Теорема 5 (об интервальном индексе ЦЧ). *Для ИИ $I_l(X)$ произвольного элемента $X=(\chi_1, \chi_2, ..., \chi_l)$ диапазона $\mathbf{Z}_{M_l}$ МСС с основаниями m_1, m_2, ..., m_{l-1}, $m_l \ge l-2$ ($l>1$) справедлива формула*

$$I_l(X) = \hat{I}_l(X) - m_l\,\Theta_l(X), \tag{20}$$

где

$$\hat{I}_l(X) = \left| \sum_{i=1}^{l} R_{i,l}(\chi_i) \right|_{m_l}; \tag{21}$$

вычеты $R_{i,l}(\chi_i)$ вычисляются по (14); $\Theta_l(X)$ – минимальная ИХМК l-го порядка вида (19) ($\Theta_l(X) \in \{0, 1\}$).

Доказательство. Используя (6) и (17), представим ЦЧ X следующим образом: $X=\sum_{i=1}^{l-1} M_{i,l-1}\chi_{i,l-1}+M_{l-1}I_l(X)=\sum_{i=1}^{l-1} M_{i,l-1}\chi_{i,l-1}-M_{l-1}\rho_{l-1}(X)+M_{l-1}I_l(X)=|X|_{M_{l-1}}+M_{l-1}\ (\rho_{l-1}(X)+I_l(X))$.
Отсюда согласно лемме Евклида вытекает равенство $N_{l-1}(X)=\lfloor X/M_{l-1}\rfloor=\rho_{l-1}(X)+I_l(X)$, из которого находим

$$\lfloor I_l(X)/m_l\rfloor=\lfloor (N_{l-1}(X)-\rho_{l-1}(X))/m_l\rfloor=-\lceil(\rho_{l-1}(X)-N_{l-1}(X))/m_l\rceil. \tag{22}$$

Принимая во внимание (19) и определение (18), на основании (22) заключаем, что для главного ИИ $G_l(X)$ ЦЧ $X\in\mathbf{Z}_{M_l}$ в заданной МСС верна формула

$$G_l(X)=-\Theta_l(X). \tag{23}$$

Подстановка (23) в (7) доказывает справедливость (20).

Расчетное соотношение (21) для компьютерного ИИ $\hat{I}_l(X)$ ЦЧ X вытекает из (6):

$$\hat{I}_l(X)=|I_l(X)|_{m_l}=\left|-\sum_{i=1}^{l-1}\frac{\chi_{i,l-1}}{m_i}+\frac{X}{M_{l-1}}\right|_{m_l}=\left|\sum_{i=1}^{l-1}\left|-m_i^{-1}\,|M_{i,l-1}^{-1}\chi_i|_{m_i}\right|_{m_l}+|M_{l-1}^{-1}\chi_l|_{m_l}\right|_{m_l}=\left|\sum_{i=1}^{l}R_{i,l}(\chi_i)\right|_{m_l}$$

(см. (14)). ■

***Теорема 6* (*об интервальном номере ЦЧ*).** *Для интервального номера* $N_l(X)=\lfloor X/M_l\rfloor$ *произвольного ЦЧ X относительно* $m_1, m_2, ..., m_{l-1}, m_l\geq l-2$ *имеет место равенство* $N_l(X)=J_l(X)+$ $+\,\Theta_l(X)$, *где* $J_l(X)$ *– главный ИИ числа X, а* $\Theta_l(X)$ *– отвечающая ему минимальная ИХМК l-го порядка* ($\Theta_l(X)\in\{0,1\}$).

Доказательство. Пусть числу X в МСС с основаниями $m_1, m_2, ..., m_l$ и диапазоном $\mathbf{Z}_{M_l}$ отвечает модулярный код $(\chi_1,\chi_2,...,\chi_l)$. Используя (7) и (20), выполним над ИМФ ЦЧ X l-го порядка (см. (6)) преобразование

$$X=\sum_{i=1}^{l-1}M_{i,l-1}\chi_{i,l-1}+M_{l-1}I_l(X)=\sum_{i=1}^{l-1}M_{i,l-1}\chi_{i,l-1}+M_{l-1}(\hat{I}_l(X)+m_lJ_l(X))=$$
$$=\sum_{i=1}^{l-1}M_{i,l-1}\chi_{i,l-1}+M_{l-1}(\hat{I}_l(X)-m_l\Theta_l(X)+m_l\Theta_l(X)+m_lJ_l(X))=$$
$$=\sum_{i=1}^{l-1}M_{i,l-1}\chi_{i,l-1}+M_{l-1}I_l(|X|_{M_l})+M_l(J_l(X)+\Theta_l(X))=|X|_{M_l}+M_l(J_l(X)+\Theta_l(X)).$$

Таким образом, $X=|X|_{M_l}+M_l(J_l(X)+\Theta_l(X))$. Отсюда в соответствии с леммой Евклида, а также определением 5 и вытекает искомый результат: $\lfloor X/M_l\rfloor=N_l(X)=J_l(X)+\Theta_l(X)$. ■

***Теорема 7* (*о полиадическом коде числа*).** *Пусть в МСС с основаниями* $m_1, m_2, ..., m_k$ *задан произвольный элемент* $X=(\chi_1,\chi_2,...,\chi_k)$ *диапазона* $\mathbf{Z}_{M_k}$ *и пусть*

$$L_l(X)=\sum_{i=1}^{l-1}M_{i,l-1}\,\chi_{i,l-1}+M_{l-1}\hat{I}_l(X)\quad(\chi_{i,l-1}=|M_{i,l-1}^{-1}\chi_i|_{m_i};\ 2\leq l\leq k), \tag{24}$$

$\hat{I}_l(X)$ *определяется по (21) с использованием (14). Тогда для коэффициентов полиадической формы числа X (определение 4)*

$$X=\sum_{i=1}^{k}M_{i-1}x_i\ \ (M_0=1;\ x_i\in\mathbf{Z}_{m_i}) \tag{25}$$

верны формулы

$$x_1 = \chi_1,\ x_2 = \hat{I}_2(X),\ x_3 = \hat{x}_3,\ x_l = \ |\hat{x}_l + \Theta_{l-1}(X)|_{m_l}\ (l = \overline{4, k}), \tag{26}$$

где

$$\hat{x}_l = \left| J_{l-1}(L_l(X)) \right|_{m_l}\ (l = \overline{3, k}); \tag{27}$$

$J_{l-1}(L_l(X))$ *– главный ИИ ЦЧ* $L_l(X)$ *в МСС с основаниями* $m_1, m_2, ..., m_{l-1}$, *вычисляемый по правилу*

$$J_{l-1}(L_l(X)) = \hat{\rho}_{l-1}(X) + \hat{I}_l(X); \tag{28}$$

$$\hat{\rho}_{l-1}(X) = \left\lfloor m_{l-1}^{-1} \sum_{i=1}^{l-1} R_{i,l-1}(\chi_i) \right\rfloor; \tag{29}$$

вычеты $R_{i,l-1}(\chi_i)$ *определяются по (14) с заменой* l *на* $l-1$; $\Theta_{l-1}(X)$ *– минимальная ИХМК* $(l-1)$*-го порядка, которая при* $m_{l-1} \geq l-3$ *принимает значения* 0 *или* 1 (*см. теорему* 4).

Доказательство. Из (25) следует, что при $l = \overline{1, k-1}$ выполняется равенство $|X|_{M_l} = \sum_{i=1}^{l} M_{i-1} x_i$, в результате чего

$$N_{l-1}(|X|_{M_l}) = \lfloor |X|_{M_l} / M_{l-1} \rfloor = x_l. \tag{30}$$

Согласно (6), (7) и (24)

$$X = \sum_{i=1}^{l-1} M_{l-1}\chi_{i,l-1} + M_{l-1}\ \ (\hat{I}_l(X) + m_l J_l(X)) = L_l(X) + M_l J_l(X).$$

Поэтому $|X|_{M_l} = \ |L_l(X)|_{M_l}$ и (30) можно записать в следующей эквивалентной форме:

$$x_l = N_{l-1}(|L_l(X)|_{M_l}). \tag{31}$$

Поскольку по лемме Евклида $L_l(X) = \ |L_l(X)|_{M_l} + M_l N_l(L_l(X))$, то $N_{l-1}(L_l(X)) =$ $= N_{l-1}(|L_l(X)|_{M_l}) + m_l N_l(L_l(X))$. Отсюда ввиду (31) заключаем, что

$$x_l = \ |N_{l-1}(L_l(X))|_{m_l}. \tag{32}$$

Применяя к интервальному номеру $N_l(L_l(X))$ теорему 6 из (32), находим

$$x_l = \ |J_{l-1}(L_l(X)) + \Theta_{l-1}(X)|_{m_l}. \tag{33}$$

С учетом обозначения (27) равенство (33) совпадает с искомым соотношением для x_l при $l = \overline{4, k}$ (см. (26)).

Как видно из (5), в одномодульном (вырожденном) случае (в случае $l = 1$) для любого ЦЧ X ранг $\rho_1(X) = 0$, вследствие чего и $\Theta_2(X) = 0$ (см. (19)). Поэтому при $l = 3$ (33) дает $x_3 = \ |J_2(L_3(X))|_{m_3}$. Искомые равенства для коэффициентов x_1 и x_2 вытекают соответственно из (30) и (32):

$$x_1 = N_0(|X|_{M_1}) = \lfloor\ |X|_{M_1} / M_0 \rfloor = \ |X|_{M_1} = \chi_1;$$

$$x_2 = \left| N_1(L_2(X)) \right|_{m_2} \left| \left\lfloor \frac{1}{m_1}(\chi_1 + m_1 \hat{I}_2(X)) \right\rfloor \right|_{m_2} = \hat{I}_2(X).$$

Что касается расчетных соотношений (28), (29), то для их вывода воспользуемся процедурой сужения ИМФ ЦЧ. Необходимая процедура состоит в получении ИМФ ($l-1$)-го порядка числа по его ИМФ l-го порядка. Осуществляемое сужение базируется на соотношении типа (15). Замена в (15) l на $l-1$ приводит к равенствам

$$m_{l-1}\, \chi_{i,l-1} = \chi_{i,l-2} + m_{l-1} R_{i,l-1}(\chi_i) \; (i = \overline{1,\, l-2}) \; . \tag{34}$$

Применяя (34), выполним над (24) преобразование

$$\begin{aligned} L_l(X) &= \sum_{i=1}^{l-2} M_{i,l-2}\, m_{l-1} \chi_{i,l-1} + M_{l-1,l-1} \chi_{l-1,l-1} + M_{l-1} \hat{I}_l(X) = \\ &= \sum_{i=1}^{l-2} M_{i,l-2}\, \chi_{i,l-2} + M_{l-2} \Big(\sum_{i=1}^{l-1} R_{i,l-1}(\chi_i) + m_{l-1} \hat{I}_l(X) \Big). \end{aligned} \tag{35}$$

В соответствии с (6) из (35) находим

$$I_{l-1}(L_l(X)) = \sum_{i=1}^{l-1} R_{i,l-1}(\chi_i) + m_{l-1} \hat{I}_l(X)). \tag{36}$$

Деление (36) на m_{l-1} с последующим переходом в обеих частях полученного равенства к антье дает искомый результат – расчетные соотношения (28), (29).

4. Метод сужения ИМФ ЦЧ для определения минимальных ИХМК

Основой для расчета минимальных ИХМК по разработанной интервально-индексной технологии служат приводимые ниже теоремы, а также операция сужения ИМФ ЦЧ.

Теорема 8. *Для минимальной ИХМК* $\Theta_l(X)$, *отвечающей числу* $X \in Z$ *в МСС с основаниями* $m_1, m_2, ..., m_{l-1}, m_l \geq l-2$ $(l>1)$, *справедлива формула*

$$\Theta_l(X) = 1 - \mathrm{sn}\,(Z_l(X)), \tag{37}$$

где

$$Z_l(X) = L_l(X) - M_l; \tag{38}$$

ЦЧ $L_l(X)$ *определяется соотношением* (24) *с использованием модулярного кода* $(\chi_1, \chi_2, ..., \chi_l)$ $(\chi_i = |X|_{m_i}\ (i = \overline{1,l}))$ *и интервально-индексной характеристики* $\hat{I}_l(X)$ *(см. (21)); через* $\mathrm{sn}(x)$ *обозначается знаковая функция вида*

$$\mathrm{sn}(x) = \begin{cases} 0, & \text{если } x \geq 0; \\ 1, & \text{если } x < 0. \end{cases}$$

Доказательство. Подставляя (24) в (38) и применяя (6), а также теорему 5, получим

$$\begin{aligned} Z_l(X) &= \sum_{i=1}^{l-1} M_{i,l-1} \chi_{i,l-1} + M_{l-1} \hat{I}_l(X) - M_l = \sum_{i=1}^{l-1} M_{i,l-1} \chi_{i,l-1} + M_{l-1} (\hat{I}_l(X) - \\ &- m_l \Theta_l(X) + m_l \Theta_l(X)) - M_l = \sum_{i=1}^{l-1} M_{i,l-1} \chi_{i,l-1} + M_{l-1} I_l(|X|_{M_l}) + M_l(\Theta_l(X) - 1) = \\ &= |X|_{M_l} + M_l(\Theta_l(X) - 1). \end{aligned} \tag{39}$$

По теореме 4 $\Theta_l(X) \in \{0, 1\}$. При этом из (39) ввиду $0 \le |X|_{M_l} < M_l$ следует, что значению $\Theta_l(X)=0$ ИХМК $\Theta_l(X)$ соответствует $Z_l(X)<0$, а значению $\Theta_l(X)=1$ − $Z_l(X)\ge 0$. Таким образом, формула (37) верна. ■

Теорема 9. *Пусть числу $X\in Z$ по набору модулей $m_1, m_2, ..., m_k$ отвечает модулярный код $(\chi_1,\chi_2,...,\chi_k)$ и пусть $J_l(X)$ – главный ИИ ЦЧ X относительно $m_1, m_2, ..., m_{l-1}$, $m_l \ge l-2$ $(2\le l\le k)$. Знаки чисел X и $J_l(X)$ совпадают при $l=2$, а также при $l>2$, если $J_l(X)\ne -1$.*

Доказательство. Согласно лемме Евклида и теореме 6 об интервальном номере ЦЧ выполняется равенство

$$X = |X|_{M_l} + M_l N_l(X) = |X|_{M_l} + M_l(J_l(X)+\Theta_l(X)), \tag{40}$$

где $\Theta_l(X)$ − минимальная ИХМК, отвечающая X в МСС с базисом $\{m_1, m_2, ..., m_l\}$, причем $\Theta_l(X) \in \{0, 1\}$. Как отмечалось в ходе доказательства теоремы 7, ИХМК $\Theta_2(X) = 0$, поэтому из (40) следует, что $\mathrm{sn}(X) = \mathrm{sn}(J_2(X))$. При $l>2$ формирование $\mathrm{sn}(X)$ числа X по его главному ИИ $J_l(X)$ невозможно только тогда, когда $J_l(X) = -1$. В этом случае возникает неопределенная ситуация, обусловленная тем, что знак $\mathrm{sn}(N_l(X))$ интервального номера $N_l(X) = \Theta_l(X) - 1$ ввиду $\Theta_l(X) = 0$ или 1 неоднозначен: $\mathrm{sn}(\Theta_l(X) -1) \in \{0, 1\}$. Если $J_l(X) \ne -1$, то $\mathrm{sn}(X) = \mathrm{sn}(N_l(X)) = \mathrm{sn}(J_l(X) + \Theta_l(X)) = \mathrm{sn}(J_l(X))$ при любом $\Theta_l(X) \in \{0, 1\}$. ■

Непосредственное применение теоремы 9 к числу (38) для получения в сответствии с теоремой 8 минимальной ИХМК $\Theta_l(X)$ по (37) к цели не приводит из-за имеющейся неопределенности: $J_l(Z_l(X))=-1$. В рамках предлагаемой методологии критическая ситуация устраняется с помощью процедуры сужения ИМФ ЦЧ. Эта процедура состоит в преобразовании ИМФ числа $Z_l(X)$ относительно модулей $m_1, m_2, ..., m_l$:

$$Z_l(X)= \sum_{i=1}^{l-1} M_{i,l-1}\chi_{i,l-1} + M_{l-1}\hat{I}_l(X) - M_l \tag{41}$$

к его ИМФ относительно модулей $m_1, m_2, ..., m_{l-1}$, т. е. к виду

$$Z_l(X)=\sum_{i=1}^{l-2} M_{i,l-2}\chi_{i,l-2} + M_{l-2}\hat{I}_{l-1}(X) + M_{l-1}J_{l-1}(Z_l(X)) \ (l \in \{3,4,...,k\}). \tag{42}$$

Осуществляемое преобразование базируется на соотношениях (34). Как следует из (35) и (38), ИМФ (41) с помощью (34) приводится к выражению

$$Z_l(X)= \sum_{i=1}^{l-2} M_{i,l-2}\chi_{i,l-2} + M_{l-2}\Big(\sum_{i=1}^{l-1} R_{i,l-1}(\chi_i) + m_{l-1}\hat{I}_l(X) - m_{l-1}m_l\Big). \tag{43}$$

В соответствии с (6) из (43) для ИИ $I_{l-1}(Z_l(X))$ ЦЧ $Z_l(X)$ относительно модулей $m_1, m_2, ..., m_{l-1}$ вытекает формула $I_{l-1}(Z_l(X)) = \sum_{i=1}^{l-1} R_{i,l-1}(\chi_i) + m_{l-1}\hat{I}_l(X) - m_{l-1}m_l$. Отсюда согласно определению (18) для интервально-индексных характеристик, входящих в состав ИМФ (42), получаем выражения

$$\hat{I}_{l-1}(Z_l(X)) = |I_{l-1}(Z_l(X))|_{m_{l-1}} = \left|\sum_{i=1}^{l-1} R_{i,l-1}(\chi_i)\right|_{m_{l-1}}; \tag{44}$$

$$J_{l-1}(Z_l(X)) = \lfloor I_{l-1}(Z_l(X))/m_{l-1} \rfloor = \hat{\rho}_{l-1}(X) + \hat{I}_l(X) - m_l, \tag{45}$$

где $\hat{\rho}_{l-1}(X) = \left\lfloor m_{l-1}^{-1} \sum_{i=1}^{l-1} R_{i,l-1}(\chi_i) \right\rfloor$; вычеты $R_{i,l-1}(\chi_i)$ вычисляются по формулам типа (14) с заменой l на $l-1$.

Если в результате сужения ИМФ (41), осуществляемого по расчетным соотношениям (44), (45), для всех $i=i_l+1, i_l+2, \ldots, l$, где i_l – натуральное число, такое, что $2<i_l\le l$, выполняется $J_{i-1}(Z_i(X)) = -1$, а $J_{i_l-1}(Z_{i_l}(X)) \ne -1$ (существование для каждого $l=\overline{3, k}$ указанного i_l гарантируется теоремой 9), то числа $Z_{i_l}(X)$, $Z_{i_l+1}(X)$, …, $Z_l(X)$ совпадают, причем согласно теоремам 8 и 9 sn($Z_{i_l}(X)$) = sn($J_{i_l-1}(Z_{i_l}(X))$), а $\Theta_j(X) = 1-$ sn($Z_{i_l}(X)$) ($j=i_l, i_l+1, \ldots, l$).

Согласно теоремам 2 и 3 $\rho_{l-1}(X) = \hat{\rho}_{l-1}(X) + \Theta_{l-1}(X) \le l-2$. Следовательно, при $m_l \ge l-2$ верна оценка $\hat{\rho}_{l-1}(X) \le l-2$. Поэтому ввиду

$$0 \le \hat{\rho}_{l-1}(X) + \hat{I}_l(X) \le l-2+m_l-1 \le 2m_l-1 \tag{46}$$

детектирование знака главного ИИ (45) равносильно формированию признака

$$\omega_l = \left\lfloor (\hat{\rho}_{l-1}(X) + \hat{I}_l(X)) / m_l \right\rfloor \tag{47}$$

переполнения при выполнении операции $\hat{x}_l = |\hat{\rho}_{l-1}(X) + \hat{I}_l(X)|_{m_l}$ сумматором по модулю m_l. При этом на неопределенную ситуацию в процедуре сужения ИМФ ЦЧ $Z_i(X)$ указывает единичное значение булевой величины

$$\delta_l = \begin{cases} 0, & \text{если } \hat{x}_l \ne m_l-1; \\ 1, & \text{если } \hat{x}_l = m_l-1. \end{cases} \tag{48}$$

Из (46) следует, что в случае, когда $m_l = m_{l-2}$, величина (48) может принимать значение $\delta_l = 1$ не только при $J_{l-1}(Z_l(X)) = -1$ $(\omega_l = 0)$, но и при $J_{l-1}(Z_l(X)) = m_l - 1$ $(\omega_l = 1)$. Видно, что вторая из указанных ситуаций не возникает, если m_l ограничить снизу порогом $l-1$ (см. (45)–(48)).

На основании изложенных базовых теоретических положений арифметики неизбыточных МСС с диапазонами неотрицательных ЦЧ синтезирован алгоритм расчета ИХМК, который допускает как параллельную, так и последовательную реализации.

Приведем числовые примеры, демонстрирующие реализационные свойства различных форм представления ЦЧ (см. (5), (6), (8)). При этом в качестве базовой будем использовать МСС с четырьмя основаниями (k=4): m_1=2, m_2=3, m_3=5, m_4=7. Найдем необходимые системные константы:

$M_4 = 2\cdot 3\cdot 5\cdot 7 = 210$;

$M_{1,4} = M_4/m_1 = 105$, $M_{2,4} = M_4/m_2 = 70$, $M_{3,4} = M_4/m_3 = 42$, $M_{4,4} = M_4/m_4 = M_3 = 30$;

$M_{1,3} = M_3/m_1 = 15$, $M_{2,3} = M_3/m_2 = 10$, $M_{3,3} = M_3/m_3 = M_2 = 6$;

$M_{1,2} = M_2/m_1 = 3$, $M_{2,2} = M_2/m_2 = M_1 = m_1 = 2$;

$|M_{1,4}^{-1}|_{m_1} = |105^{-1}|_2 = 1$, $|M_{2,4}^{-1}|_{m_2} = |70^{-1}|_3 = 1$, $|M_{3,4}^{-1}|_{m_3} = |42^{-1}|_5 = 3$, $|M_{4,4}^{-1}|_{m_4} = |M_3^{-1}|_{m_4} = |30^{-1}|_7 = 4$;

$|M_{1,3}^{-1}|_{m_1} = |15^{-1}|_2 = 1$, $|M_{2,3}^{-1}|_{m_2} = |10^{-1}|_3 = 1$, $|M_{3,3}^{-1}|_{m_3} = |M_2^{-1}|_{m_3} = |6^{-1}|_5 = 1$;

$|M_{1,2}^{-1}|_{m_1} = |3^{-1}|_2 = 1$, $|M_{2,2}^{-1}|_{m_2} = |M_1^{-1}|_{m_2} = |2^{-1}|_3 = 2$;

$$\left|-m_1^{-1}\right|_{m_4}=\left|-\frac{1}{2}\right|_7=3,\ \left|-m_2^{-1}\right|_{m_4}=\left|-\frac{1}{3}\right|_7=2,\ \left|-m_3^{-1}\right|_{m_4}=\left|-\frac{1}{5}\right|_7=4;$$

$$\left|-m_1^{-1}\right|_{m_3}=\left|-\frac{1}{2}\right|_5=2,\ \left|-m_2^{-1}\right|_{m_3}=\left|-\frac{1}{3}\right|_5=3;$$

$$\left|-m_1^{-1}\right|_{m_2}=\left|-\frac{1}{2}\right|_3=1,\ \left|m_1^{-1}\right|_{m_2}=\left|\frac{1}{2}\right|_3=2.$$

Пример 1. Сформируем интегрально-характеристические таблицы, которые необходимы для вычисления ранга, ИИ и цифр полиадического кода числа.

Используя полученные константы из (14), находим

TIC1_4=$\{R_{1,4}(\chi_1) \mid \chi_1\in \mathbf{Z}_{m_1}\}=\{\left|-m_1^{-1}\left|M_{1,3}^{-1}\chi_1\right|_{m_1}\right|_{m_4} \mid \chi_1\in\mathbf{Z}_{m_1}\}=\{\left|3\left|\chi_1\right|_2\right|_7 \mid \chi_1\in\{0,1\}\}=\{0,3\}$;

TIC2_4=$\{\left|2\left|\chi_2\right|_3\right|_7 \mid \chi_2\in\mathbf{Z}_3\}=\{0,2,4\}$; TIC3_4=$\{\left|4\left|\chi_3\right|_5\right|_7 \mid \chi_3\in\mathbf{Z}_5\}=\{0,4,1,5,2\}$;

TIC4_4=$\{\left|M_3^{-1}\chi_4\right|_{m_4} \mid \chi_4\in\mathbf{Z}_{m_4}\}=\{\left|4\chi_4\right|_7 \mid \chi_4\in\mathbf{Z}_7\}=\{0,4,1,5,2,6,3\}$;

TIC1_3=$\{\left|2\left|\chi_1\right|_2\right|_5 \mid \chi_1\in\{0,1\}\}=\{0,2\}$; TIC2_3=$\{\left|3\left|2\chi_2\right|_3\right|_5 \mid \chi_2\in\mathbf{Z}_3\}=\{0,1,3\}$;

TIC3_3=$\{\left|M_2^{-1}\chi_3\right|_{m_3} \mid \chi_3\in\mathbf{Z}_{m_3}\}=\{\left|1\cdot\chi_3\right|_5 \mid \chi_3\in\mathbf{Z}_5\}=\{0,1,2,3,4\}$;

TIC1_2=$\{\left|1\left|\chi_1\right|_2\right|_3 \mid \chi_1\in\{0,1\}\}=\{0,1\}$; TIC2_2=$\{\left|2\chi_2\right|_3 \mid \chi_2\in\mathbf{Z}_3\}=\{0,2,1\}$.

Пример 2. Получим в заданной МСС ранговую форму (5) для числа $X=(1, 0, 1, 6)$. Найдем сначала ранг $\rho_4(X)$ ЦЧ X. Используя полученные в примере 1 таблицы, из (13), (21), (29) имеем

$$\hat{I}_4(X)=\left|\sum_{i=1}^{4}\mathrm{TIC}i\_4[\chi_i]\right|_{m_4}=\left|3+0+4+3\right|_7=3;$$

$$\hat{\rho}_4(X)=\left\lfloor m_4^{-1}\sum_{i=1}^{4}\mathrm{TIC}i\_4[\chi_i]\right\rfloor=\left\lfloor(3+0+4+3)/7\right\rfloor=1;$$

$$\hat{\rho}_3(X)=\left\lfloor m_3^{-1}\sum_{i=1}^{3}\mathrm{TIC}i\_3[\chi_i]\right\rfloor=\left\lfloor(2+0+1)/5\right\rfloor=0.$$

Так как ЦЧ $\hat{\rho}_3(X)+\hat{I}_4(X)-m_4=0+3-7=-4$ отрицательно, то согласно теоремам 8 и 9 минимальное ИХМК $\Theta_4(X)=0$. Следовательно, по теореме 3 ранг $\rho_4(X)=\hat{\rho}_3(X)+\Theta_4(X)=1$.

Таким образом, ранговая форма (5) ЦЧ X имеет вид $X=105\left|1\cdot\chi_1\right|_2+70\left|1\cdot\chi_2\right|_3+42\left|3\chi_3\right|_5+30\left|4\chi_3\right|_7-210\rho_4(X)=105+0+126+90-210=111$.

Пример 3. Для числа $X=(1, 0, 1, 6)$ получим ИМФ (6), по теореме 5 ИИ $I_4(X)=\hat{I}_4(X)-m_4\Theta_4(X)=3-7\cdot0=3$. С учетом этого согласно (6) $X=15\left|1\cdot\chi_1\right|_2+10\left|1\cdot\chi_2\right|_3+6\left|1\cdot\chi_3\right|_5+30I_4(X)=15+0+6+90=111$.

Пример 4. Получим полиадическую форму (8) ЦЧ $X=(1, 0, 1, 6)$. Согласно теореме 7 $x_1=\chi_1=1$, $x_2=\hat{I}_2(X)=\left|\mathrm{TIC1\_2}[\chi_1]+\mathrm{TIC2\_2}[\chi_2]\right|_{m_2}=\left|1+0\right|_3=1$, $x_3=\hat{x}_3=\left|\hat{\rho}_2(X)+\hat{I}_3(X)\right|_{m_3}=\left|\left\lfloor(1+0)/3\right\rfloor+\left|2+0+1\right|_5\right|_5=3$. Так как ЦЧ $\hat{\rho}_2(X)+\hat{I}_3(X)-m_3=0+3-5=-2<0$, то $\Theta_3(X)=0$ (см. теоремы 8 и 9). Согласно примеру 2 $\hat{x}_4=\left|\hat{\rho}_3(X)+\hat{I}_4(X)\right|_{m_4}=\left|0+3\right|_7=3$. Следовательно, $x_4=\left|\hat{x}_4+\Theta_3(X)\right|_{m_4}=\left|3+0\right|_7=3$.

Таким образом, в рассматриваемом случае (8) имеет вид $X = \sum_{i=1}^{4} M_{i-1}x_i = 1 + 2\cdot 1 + 6\cdot 3 + 30\cdot 3 = 111.$

Приведенные примеры показывают, что среди рассмотренных форм ЦЧ ИМФ занимает приоритетное положение. В первую очередь это обусловлено модульностью расчетного соотношения для оценочного значения $\hat{I}_k(X)$ ИИ $I_k(X)$, что упрощает его вычисление, а следовательно, и синтезируемые на базе ИМФ немодульные процедуры. В наибольшей мере данное свойство интервально-индексных характеристик и ИМФ проявляется при оперировании в диапазонах больших чисел.

Заключение

Исследования по проблематике разработки и оптимизации технологий расчета ИХМК показали следующие результаты:

1. Все известные ИХМК: ранг, ИИ, коэффициенты полиадической формы, интервальный номер ЦЧ – имеют одинаковую вычислительную структуру. Она описывается расчетными соотношениями, в рамках которых исходные значения ИХМК представляются в виде суммы по основанию МСС приближенного (оценочного) значения характеристики и минимальной ИХМК, умноженной на целочисленную константу. Благодаря отмеченному обстоятельству все ИХМК формируются по единому алгоритму.

2. В построенной интегрально-характеристической базе модулярной арифметики ключевая роль принадлежит интервально-индексным характеристикам. Это обусловлено тем, что по ИИ и главному ИИ с помощью тривиальных выражений вычисляются оценочные значения всех других ИХМК. Что касается ранга и ранговой формы ЦЧ, то они используются в качестве вспомогательного средства в процессе математической формализации аппарата ИМФ, а также при выводе определяющего выражения для минимальных ИХМК.

3. Центральное место в разработанной интегрально-характеристической базе МСС занимает процедура сужения ИМФ. Именно она позволяет вычислять все ИХМК, включая минимальные, в рамках общего универсального алгоритма. С точки зрения компьютерной реализации важнейшим свойством процедуры сужения ИМФ является ее параллелизм, порождаемый независимостью друг от друга осуществляемых вычислений по разным модулям базиса МСС.

Разработка выполнена в рамках задания 1.5.06 ГПНИ «Информатика и космос» (2011−2015 гг.).

Список литературы

1. Жуков-Емельянов, О.Д. Информационные технологии на основе модулярной алгебры / О.Д. Жуков-Емельянов. – М. : КРАСАНД, 2010. – 248 с.

2. Параллельная компьютерная алгебра // Всерос. науч. конф. с элементами научной школы для молодежи : сб. науч. тр. Ставрополь, 11−15 окт., 2010 г. – Ставрополь : Издательско-информационный центр «Фабула», 2010. − 364 с.

3. Теоретические основы минимально избыточных квадратичных модулярных систем счисления / А.Ф. Чернявский [и др.] // Доклады НАН Беларуси. – 1998. – Т. 42, № 1. – С. 5–12.

4. Минимально избыточные полиномиально-скалярные модулярные системы счисления / А.А. Коляда [и др.] // Весці НАН Беларусі. Сер. фіз.-мат. навук. – 1998. – № 3. – С. 103–107.

5. Калмыков, И.А. Теоретические основы вычислений в полиномиальной системе классов вычетов, ориентированных на построение отказоустойчивых систем : автореф. дис. ... д-ра техн. наук : 05.13.17, 05.13.15 / И.А. Калмыков. – Ставрополь, 2006. – 32 с.

6. Амербаев, В.М. Теоретические основы машинной арифметики / В.М. Амербаев. – Алма-Ата : Наука, 1976. – 324 с.

7. Cox-Rower architecture for fast parallel Montgomery multiplication / S. Kawamura [et al.] // Eurocrypt 2000, LNCS. – Berlin, 2000. – Vol. 1807. – P. 523–538.

8. Нейрокомпьютеры в остаточных классах. Кн. 11 / Н.И. Червяков [и др.]. – М. : Радиотехника, 2003. – 272 с.

9. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М. : Наука, 1972. – 168 с.

10. Коляда, А.А. Модулярные структуры конвейерной обработки цифровой информации / А.А. Коляда, И.Т. Пак. – Минск : Университетское, 1992. – 256 с.

11. Червяков, Н.И. Нейронная сеть для преобразования полиадического кода в код системы остаточных классов / Н.И. Червяков, Д.В. Сивоплясов, Д.В. Горденко // Нейрокомпьютеры: разработка, применение. – 2003. – № 10–11. – С. 10–12.

12. Преобразователь из модулярного кода в обобщенную полиадическую систему счисления для отказоустойчивых систем управления / И.А. Калмыков [и др.] // Успехи современного естествознания. – 2009. – № 4. – С. 41–43.

Поступила 25.09.2012

Институт прикладных физических проблем
им. Севченко БГУ,
Минск, Курчатова, 7
e-mail: shabinskaya@rambler.ru

A.A. Kolyada, A.F. Chernyavsky

INTEGRATED CHARACTERISTIC BASE OF MODULAR NUMBER SYSTEMS

The problem of development of an integrated characteristic base of a modular number system defined on the ranges of non-negative integers is studied. A mechanism of interval-modular forms of integer numbers is applied to solve this problem. Interval index characteristics – the interval index and the main interval index - play a key role in this mechanism. Priority of these characteristics is explained by their essential advantages over known integrated characteristics of a modular code when optimizing algorithms of non-modular operations.