УДК 681.04

В.И. Барсов

Украинская инженерно-педагогическая академия, Харьков

МЕТОД ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБОК В МОДУЛЯРНОЙ АРИФМЕТИКЕ

Рассмотрены метод обнаружения и исправления ошибок в модулярной арифметике. Особенность данного метода состоит в повышении быстродействия коррекции ошибок. Метод рекомендован к использованию для систем цифровой обработки информации реального времени.

Ключевые слова: *модулярная арифметика, цифровая обработка информации.*

Введение

Известно [1 – 3], что использования непозиционной системы счисления в модулярной арифметике (МА) позволяет улучшить такие характеристики систем цифровой обработки информации (СЦОИ), как пользовательская производительность, надежность и отказоустойчивость при решении определенного класса задач (для определенного типа операций). Как правило в известных работах [4 – 6] рассматриваются коды в МА со взаимно-попарно-простыми основаниями (модулями). Однако если ставится задача минимизации времени коррекции ошибок, то в этом случае целесообразно рассмотреть коды в МА со взаимно-непростыми основаниями.

Цель данной статьи. В предлагаемой статье рассматривается метод и алгоритмы коррекции ошибок в СЦОИ посредством применения кодов в МА со взаимно-непростыми модулями.

Изложение основного материала

В МА произвольный операнд А представляется в виде набора остатков $\{a_i\}$ от последовательного деления его на совокупность $\{m_i\}$ натуральных чисел, т.е. число А представится как

$$A = [A(\mathrm{mod}\ m_1), A(\mathrm{mod}\ m_2), \ldots, A(\mathrm{mod}\ m_n)]$$
$$\text{или } A = (a_1, a_2, \ldots, a_n),$$

где $i \equiv A(\mathrm{mod}\ m_i)$.

Диапазон представимых чисел представится в виде (0, М], где $M = [\, m_1, m_2, \ldots m_n \,]$ – НОК оснований МА.

Для последующего доказательства предлагаемого научного положения 1, на основании которых базируется метод коррекции ошибок, предположим, что любого целого числа А, заданного в МА с основаниями $\{m_i\}$, $i = \overline{1,n}$ и для любой пары оснований m_i, m_j ($i,j = \overline{1,n}$; $i \neq j$) должно выполнятся следующее условие $(a_i - a_j) \bmod d_{ij} = 0$, где $d_{ij} = (m_i, m_j)$ – НОД оснований m_i и m_j.

Используя результаты леммы сформулируем и докажем следующее научное положение, которая определяет необходимые условия обнаружения ошибок в МА.

Научное положение 1. Для обнаружения ошибки в остатке по произвольному основанию m_i числа А, заданного в МА совокупностью оснований $\{m_i\}$, $i = \overline{1,n}$, необходимо, чтобы произвольное основание m_i имело хотя бы один, отличный от единицы, общий делитель с каждым из остальных оснований m_j ($j = \overline{1,n}$; $j \neq i$).

Это можно объяснить следующим образом. Обозначим НОД оснований m_i и m_j как $d_{ij} = (m_i, m_j)$ для $i,j = \overline{1,n}$ и $j \neq i$. Пусть ошибка произошла по модулю m_i, т.е. $\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i$.

Вначале покажем, что выражение

$$(\tilde{a}_i - \Delta a_i) \bmod d_{ij} \tag{1}$$

эквивалентно выражению $\Delta a_j \ (\mathrm{mod}\ d_{ij})$. Действительно, в соответствии с результатами вышеприведенной леммы имеем $(a_i + a_j) \bmod d_{ij} \equiv 0$. Запишем выражение $\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i$ в следующем виде:

$$a_i + \Delta a_i = m \cdot m_i + \tilde{a}_i, \tag{2}$$

где m – целое число. Из выражения (2) определим значение искаженного остатка $\tilde{a}_i = a_i + \Delta a_i - m \cdot m_i$ и подставив его в выражение (1), получим:

$$\begin{aligned}(\tilde{a}_i - a_j) \bmod d_{ij} &= [(a_i + Дa_i - m \cdot m_i) - a_j] \bmod d_{ij} = \\ &= [(a_i - a_j) + (-m \cdot m_i + Дa_i)] \bmod d_{ij} = \\ &= [(a_i - a_j) + (-m \cdot k \cdot d_{ij} + Дa_i)] \bmod d_{ij},\end{aligned} \tag{3}$$

где: $m_i = k \cdot d_{ij}$ (по условию; k – натуральное число.

Рассматривая каждое из слагаемых выражений (3), получим: $(a_i - a_j) \bmod d_{ij} \equiv 0$ (согласно лемме) и также $(m \cdot k \cdot d_{ij}) \bmod d_{ij} \equiv 0$. В этом случае

$$\Delta a \equiv (\tilde{a}_i - a_j) \bmod d_{ij}. \tag{4}$$

Анализируя формулу (4) очевидно, что при отсутствии для модулей m_i и m_j общих делителей больше единицы выполняется условие $\Delta a_i \ (\mathrm{mod}\ d_{ij}) \equiv 0$. Таким образом, необходимым условием обнаружения ошибки по одному из оснований является выполнение условия

$$d_{ij} = (m_i, m_j) \neq 1. \tag{5}$$

Необходимое условие (5) теоремы 1 является и достаточным, если величина $\Delta a_i \equiv (\tilde{a}_i - a) \bmod d_{ij}$ не кратна одновременно двум делителям $d_{i-1,i}$ и $d_{i,i+1}$, т.е.

$$НОД\ d_{Дa_i}^{(i-1)}=(d_{i-1,i},Дa_i)=1$$

$$и\ НОД\ d_{Дa_i}^{(i+1)}=(d_{i,i+1},Дa_i)=1. \qquad (6)$$

Для исправления ошибок в МА воспользуемся доказательством следующей теоремы [1].

Научное положение 2. Для исправления ошибки в остатке по произвольному основанию m_i ($i=\overline{1,n}$) числа А, заданного в МА основаниями $\{m_i\}$, необходимо выполнение следующего условия:

$$(d_{ik}-1)\cdot(d_{ij}-1)\ge д(Дa_i),$$

где $д(Дa_i)=m_i-1-(K_{d_{ik}}+K_{d_{ij}}-K_{[d_{ik},d_{ij}]})$.

При этом: $K_{d_{ik}}$ – число возможных делителей значения ошибки Δa_i по основанию m_i, кратных значению d_{ik}; $K_{d_{ij}}$ – число возможных делителей значения ошибки Δa_i по основанию m_i, кратных значению d_{ij}; $K_{[d_{ik},d_{ij}]}$ – число возможных делителей ошибки Δa_i по основанию m_i, кратных значению НОК чисел d_{ik}, d_{ij}. Условие (7) является и достаточным, если различным возможным значениям $\delta(\Delta a_i)$ ошибок соответствуют различные пары величин a_{ik}, a_{ij}.

На основании вышеприведенных теорем построим алгоритмы обнаружения и исправления однократных (по одному из оснований МА) ошибок.

Рассмотрим алгоритмы обнаружения ошибок.

Алгоритм 1. Пусть необходимо проверить факт наличия либо отсутствия ошибок в операнде $A=(a_1, a_2,\dots, a_n)$.

1. Определим такую совокупность значений

$$\begin{cases} a_{12}=(a_1-a_2)\bmod d_{12}; \\ a_{13}=(a_1-a_3)\bmod d_{13}; \\ \quad . \quad . \quad . \\ a_{1n}=(a_1-a_n)\bmod d_{1n}. \end{cases}$$

Если вся совокупность (8) значений $a_{1i}=0$ ($i=\overline{1,n}$; $i\ne 1$) равно нулю, то далее вычисляется и проверяется совокупность значений $a_{2i}=(a_2-a_1)\bmod d_{2i}\,(i\ne 2)$ и т.д.

2. При получении всех возможных значений a_{ij} ($j\ne j$) составляем матрицу G вида

$$G=\begin{vmatrix} a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{23} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

При составлении матрицы G нет необходимости указывать истинное числовое значение элементов a_{ij}, а достаточно представить элементы матрицы в виде единицы или нуля, т.е.

$$a_{ij}=\begin{cases} 0,\ при\, a_{ij}=0; \\ 1,при\, a_{ij}\ne 0. \end{cases}$$

3. Если определитель $|G|=0$, то А считается неискаженным, а если $|G|\ne 0$ - число А искажено.

Если воспользоваться соотношением

$$a_i-a_j\equiv[d_{ij}-(a_j-a_i)]\bmod d_{ij}, \qquad (7)$$

то для определения правильности или неправильности операнда А достаточно определить лишь следующую совокупность чисел

$$a_{12}, a_{23}, a_{34},\dots, a_{n-1n}, a_{n1}.$$

Исходя из вышеизложенного очевидно, что посредством предлагаемого метода кодирования информации в МА исключительно просто реализуется процесс обнаружения ошибок. При этом время обнаружения ошибок, сравнительно с обнаружением ошибок в позиционной двоичной системе счисления, достаточно мало и постоянно для любого числа оснований МА [4].

Алгоритм 2. Приведем некоторые соображения, позволяющие упростить вышеприведенный алгоритм обнаружения ошибок.

Покажем, что

$$[(a_1+\overline{a_j})+(\overline{a_1}+a_j)]\equiv 0 \pmod{d_{1j}},$$

где: $\overline{a_j}=m_j-a_j$; $\quad \overline{a_1}=m_1-a_1$.

Пусть в операнде $A=(a_1, a_2,\dots, a_j,\dots, a_n)$ искажен остаток a_j по основанию m_j, т.е. $\tilde a_j=(a_j+Дa_j)\bmod m_j$. Запишем систему равенств:

$$\begin{cases} K_1=a_i-\tilde a_j=a_i+(m_j-\tilde a_j)=a_i+m_j-a_j-Дa_j; \\ K_2=\tilde a_j-a_i=a_j+Дa_j-a_i=a_j-a_i+Дa_j. \end{cases} \qquad (8)$$

Сложив эти два равенства, получим:

$$K_1+K_2=m_j\ \text{ или }\ K_1+K_2\equiv 0 \pmod{m_j}.$$

Таким образом, очевидно, что

$$a_1+\overline{a}_j=d_{1j}-(\overline{a}_1+a_j),$$

т.е. для определения факта наличия или отсутствия ошибок нет необходимости вычисления точного значения величины $(a_1+\overline{a}_j)\bmod d_{1j}$, а достаточно знать факт равенства или неравенства этого значения нулю. Это в свою очередь позволит в техническом устройстве для обнаружения ошибок в МА вместо $(n-1)$-го сумматоров по модулям m_j ($j=\overline{2,n}$), которые определяют совокупность значений $\overline{a}_j=m_j-a_j$, использовать всего один сумматор по модулю m_1, определяющий значение $\overline{a}_1=m_1-a_1$. Алгоритм обнаружения и исправления ошибок можно представить следующим образом:

1. Определим все возможные значения вида $a_{i,i+1}=(a_1-a_{i+1})\bmod d_{i,i+1}$:

$$\begin{cases} a_{12}=(a_1-a_2)\bmod d_{12}; \\ a_{23}=(a_2-a_3)\bmod d_{23}; \\ \qquad \dots \\ a_{n-1,n}=(a_{n-1}-a_n)\bmod d_{n-1,n}; \\ a_{n1}=(a_n-a_1)\bmod d_{n1}. \end{cases} \qquad (9)$$

2. Если вся совокупность (9) значений принимает нулевое значение, то ошибка отсутствует, либо

она кратна одному из делителей $d_{i-1,i}, d_{i,i+1}$, что противоречит условию ограничения класса возможных корректируемых ошибок. Таким образом, считается, что ошибка отсутствует.

3. Если одновременно выполняются условия $a_{i-1,i} \neq 0$ и $a_{i,i+1} \neq 0$, а все остальные значения в совокупности (9) принимают значения ноль, то считается, что ошибка имеется в остатке по модулю m_i, т.е.

$$\tilde{a}_i = (a_i + Дa_i) \bmod m_i (0 < Дa_i \le m_{i-1}).$$

4. В соответствии с известным алгоритмом производится коррекция ошибок по i – у основанию МА.

Выводы

Таким образом, в статье предложен метод обнаружения и исправления ошибок в МА. На основе данного метода разработаны алгоритмы реализации процесса обнаружения и исправления ошибок.

Разработанные алгоритмы обнаружения и исправления ошибок в МА рекомендуются для использования в системах и устройствах обработки цифровой информации реального времени.

Список литературы

1. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.

2. Краснобаев В.А. Техническая реализация метода коррекции ошибок в системе остаточных классов / В.А. Краснобаев // АСУ и приборы автоматики. – 1987. – Вып. 81. – С. 97-101.

3. Методы многоверсионной обработки информации в модулярной арифметике: монографія / В.И. Барсов, В.А. Краснобаев, А.А. Сиора, И.В. Авдеев. – Х.: МОН, УПА, 2008. – 459 с.

4. Барсов В.И.. Моделі і методи підвищення відмовостійкості і продуктивності управляючих обчислювальних комплексів спеціалізованих систем управління реального часу на основі застосування непозиційних кодових структур модулярної арифметики: монографія / В.И. Барсов, В.А. Краснобаєв, Хері Алі Абдула. – Х.: МОН, УПА, 2008. – 161 с.

5. Барсов В.И. Отказоустойчивые вычислительные системы на основе модулярной арифметики: концепции, методы и средства / В.И. Барсов, В.А. Краснобаев, Е.В. Яськова // Радіоелектронні і комп'ютерні системи: науково-технічний журнал. – Х.: НАКУ „ХАІ", 2007. – Вип. 8 (27). – С. 82-90.

6. Барсов В.И. Створення відмовостійких управляючих обчислювальних комплексів автоматизованих систем контролю і управління електроспоживанням на основі модулярної арифметики / В.И. Барсов // Вісник ХНТУСГ ім. П. Василенка. – Х.,2007. – Т. 2, вип. 57. – С. 77-81.

Поступила в редколлегию 27.10.2008

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

МЕТОД ВИЯВЛЕННЯ І ВИПРАВЛЕННЯ ПОМИЛОК В МОДУЛЯРНІЙ АРИФМЕТИЦІ

В.І. Барсов

Розглянуті метод виявлення і виправлення помилок в модулярній арифметиці. Особливість даного методу полягає в підвищенні швидкодії корекції помилок. Метод рекомендований до використання для систем цифрової обробки інформації реального часу.

***Ключові слова:** модулярна арифметика, цифрова обробка інформації.*

METHOD OF DISCOVERY AND CORRECTION OF ERRORS IN MODULAR ARITHMETIC

V.I. Barsov

Considered method of discovery and correction of errors in modular arithmetic. The feature of this method consists of increase of fast-acting of correction of errors. A method is recommended to the use for the systems of digital treatment of information of the real time.

***Keywords:** modular arithmetic, digital treatment of information.*