УДК 621.396(075.8)

© Кузнецов В.И., Кукушкин С.С., Попов М.Н.
Kuznetsov V., Kukushkin S., Popov M.

О ПРИМЕНИМОСТИ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ НАД ЧИСЛАМИ С ДРОБНОЙ ЧАСТЬЮ

THE APPLICABILITY ARITHMETIC IN SYSTEM RESIDUAL CLASSES ON NUMBERS WITH A FRACTIONAL PART

Аннотация. *Рассмотрены теоретико-прикладные аспекты обоснования возможностей выполнения арифметических операций сложения, вычитания, умножения и деления в системе остаточных классов над числами с дробной частью. Обосновано, что для выполнения указанных операций требуется определение значений неполных частных от деления исходных значений чисел по модулям сравнения, что приводит к необходимости использования дополнительных данных, кроме остатков от деления. Сделан вывод о том, что, использование дополнительных данных приводит к появлению ненулевой вероятности правильного определения исходных значений чисел, представимых в СОК, по неполным данным.*

Annotation. *Theoretical-applied aspects of justification of opportunities performance of arithmetic operations of addition, subtraction, multiplication and division in system of residual classes over numbers with fractional part are considered. It is proved that performance of the specified operations requires determination of values incomplete private from division of reference values of numbers on comparison modules that results in need of use of additional data, except remainders of division. The conclusion that, use of additional data leads to emergence of nonzero probability of the correct definition of reference values of numbers, representable in system of residual classes, according to incomplete data is drawn.*

Ключевые слова. *Данные, классы, модули, остатки, операции, целые, числа.*

Key words. *Data, classes, modules, remains, operations, whole, numbers.*

На сегодняшний день уже оформилось самостоятельное научно-прикладное направление, открывающее широкие возможности представления различных измерительных данных в системе остаточных классов (СОК) [1-5]. И хотя вопросам представления данных в СОК и обратного восстановления исходных значений уделено достаточно внимания [6], сформулирована и на практике апробирована конструктивная теорема об остатках (КТО) [6, 7], многократно превосходящая по простоте реализации известную китайскую теорему об остатках [6], исследования в рассматриваемом научно-прикладном направлении ещё далеко не завершены.

Актуальным является исследование особенностей и области применения теории остаточных классов для чисел, содержащих дробную часть, что существенно расширяет область прикладных исследований и практических применений СОК.

В настоящей статье рассматриваются вопросы применения основных арифметических операций в СОК, сложение, вычитание, умножение и деление к числам, которые, кроме целой части, содержат и дробную составляющую. В общем случае для целых чисел справедливо [2, 6, 7]:

• представление исходного значения в виде двух и более остатков, например, целое число y можно представить в виде остатков от деления на целые числа m_1, m_2, определённые в качестве модулей сравнения

$$y_1 = y\left(\mathrm{mod}\, m_1\right) = \left[m_1 \cdot l_1\right] + b_1;$$

$$y_2 = y\left(\mathrm{mod}\, m_2\right) = \left[m_2 \cdot l_2\right] + b_2,$$

Кузнецов Валерий Иванович – доктор технических наук, старший научный сотрудник, ведущий научный сотрудник, ОАО «Военно-инженерная корпорация», тел. 8 (495) 399-98-19;
Кукушкин Сергей Сергеевич – доктор технических наук, профессор, ведущий научный сотрудник, 4 ЦНИИ Минобороны России;
Попов Михаил Николаевич – начальник отделения, ФГУП «СНПО «ЭЛЕРОН».

Kuznetsov Valery – the doctor of engineering, the senior research associate, the leading researcher, JSC «Military and Engineering Corporation», tel. 8 (495) 399-98-19;
Kukushkin Sergey – doctor of technical sciences, professor; leading researcher, 4 CRI Russian Defense Ministry;
Popov Mikhail – the chief of office, FSUE «SNPO ELERON».

где l_1, l_2 – характеризуют целое количество модулей m_1 и m_2 в значении числа y;

b_1, b_2 – соответствующие остатки от деления числа y, все числа – целые.

• восстановление исходного значения целого числа y из остатков на основе КТО, например, для остатков b_1 и b_2 по двум модулям m_1 и m_2

$$y=\begin{cases} m_1\cdot\frac{\Delta}{n}+b_1=m_2\cdot\frac{\Delta}{n}+b_2, \\ \quad при\ \Delta\geq 0\ \ и\ \ \Delta=k\cdot n; \\ m_1\cdot\left(m_2+\frac{\Delta}{n}\right)+b_1=m_2\cdot\left(m_1+\frac{\Delta}{n}\right)+b_2, \\ \quad при\ \Delta<0\ \ и\ \ \Delta=k\cdot n; \\ m_1\cdot\left(\frac{m_2+\Delta}{n}\right)+b_1=m_2\cdot\left(\frac{m_1+\Delta}{n}\right)+b_2, \\ \quad при\ \Delta\neq k\cdot n\ \ и\ \ \left(m_2+\Delta\right)=k\cdot n, \end{cases} \qquad (1)$$

где $n=|m_1-m_2|$ и $\Delta=b_1-b_2$, k – целое.

В отношении дробных чисел, представляемых в СОК, можно записать

$$y_1=y\left(\mathrm{mod}\,m_1\right)=\left[m_1\cdot l_1\right]+\left[b_1\right]+\left\{b_1\right\};$$

$$y_2=y\left(\mathrm{mod}\,m_2\right)=\left[m_2\cdot l_2\right]+\left[b_2\right]+\left\{b_2\right\}, \text{ и т.д.,}$$

где $\{b_1\}$ и $\{b_2\}$ – дробные части остатков от деления числа y.

Правила КТО для восстановления исходных значений чисел из остатков, содержащих дробную часть, имеют следующий вид:

$$y=\begin{cases} m_1\cdot\frac{\Delta}{n}+\left[b_1\right]+\left\{b_1\right\}=m_2\cdot\frac{\Delta}{n}+\left[b_2\right]+\left\{b_2\right\}, \\ \quad при\ \Delta\geq 0\ \ и\ \ \Delta=k\cdot n; \\ m_1\cdot\left(m_2+\frac{\Delta}{n}\right)+\left[b_1\right]+\left\{b_1\right\}=m_2\cdot\left(m_1+\frac{\Delta}{n}\right)+\left[b_2\right]+\left\{b_2\right\}, \\ \quad при\ \Delta<0\ \ и\ \ \Delta=k\cdot n; \\ m_1\cdot\left(\frac{m_2+\Delta}{n}\right)+\left[b_1\right]+\left\{b_1\right\}=m_2\cdot\left(\frac{m_1+\Delta}{n}\right)+\left[b_2\right]+\left\{b_2\right\}, \\ \quad при\ \Delta\neq k\cdot n\ \ и\ \ \left(m_2+\Delta\right)=k\cdot n, \end{cases} \qquad (2)$$

где $n=|m_1-m_2|$ и $\Delta=\left[b_1\right]-\left[b_2\right]$, k – целое.

Принимая во внимание тот факт, что

$\left[b_1\right]+\left\{b_1\right\}=b_1$ и $\left[b_2\right]+\left\{b_2\right\}=b_2$,

правила (2) в точности соответствуют правилам (1) за исключением того, что для чисел, содержащих дробную часть, разность Δ должна вычисляться только с учётом целых частей чисел, т.е.

$$\Delta=\left[b_1\right]-\left[b_2\right].$$

Последнее, в частности, не противоречит правилам (1), поскольку у целых чисел дробная часть отсутствует, т.е. может рассматриваться в качестве нулевых значений. В связи с этим правила (2) восстановления исходных значений чисел из остатков, содержащих дробную часть, является расширением правил (1) для целых чисел.

Изложенных предпосылок достаточно для того, чтобы приступить к рассмотрению основных арифметических операций в СОК для чисел, содержащих дробные части в остатках.

Операции сложения и вычитания. Пусть даны два числа y_1 и y_2, для которых вводится операция сложения (вычитания).

Представим слагаемые в виде, например, остатков по модулям m_1 и m_2

$$y_1=\left[m_1\cdot l_{11}\right]+\left[b_{11}\right]+\left\{b_{11}\right\}=\left[m_2\cdot l_{12}\right]+\left[b_{12}\right]+\left\{b_{12}\right\} \qquad (3)$$

и

$$y_2=\left[m_1\cdot l_{21}\right]+\left[b_{21}\right]+\left\{b_{21}\right\}=\left[m_2\cdot l_{22}\right]+\left[b_{22}\right]+\left\{b_{22}\right\}, \qquad (4)$$

где $[\cdot]$ – есть целая часть числа;

$\{\cdot\}$ – обозначает дробную часть числа, а остатки представлены в виде целых и дробных частей

$$b_{11}=\left[b_{11}\right]+\left\{b_{11}\right\},\ b_{12}=\left[b_{12}\right]+\left\{b_{12}\right\}$$

и

$$b_{21}=\left[b_{21}\right]+\left\{b_{21}\right\};\ b_{22}=\left[b_{22}\right]+\left\{b_{22}\right\}. \qquad (5)$$

После сложения (вычитания) будет получен следующий результат:

$$\begin{gathered} y_1=\left[m_1\cdot l_{11}\right]+\left[b_{11}\right]+\left\{b_{11}\right\} \\ \pm \\ y_2=\left[m_1\cdot l_{21}\right]+\left[b_{21}\right]+\left\{b_{21}\right\} \\ \hline \left(\left[m_1\cdot\left(l_{11}\pm l_{21}\right)\right]+\left[b_{11}\pm b_{21}\right]+\left\{b_{11}\pm b_{21}\right\}\right)\left(\mathrm{mod}\,m_1\right)= \\ =\left(\left[b_{11}\pm b_{21}\right]+\left\{b_{11}\pm b_{21}\right\}\right)\left(\mathrm{mod}\,m_1\right)=\left(b_{11}\pm b_{21}\right)\left(\mathrm{mod}\,m_1\right) \end{gathered} \qquad (6)$$

и

$$\begin{gathered} y_1=\left[m_2\cdot l_{12}\right]+\left[b_{12}\right]+\left\{b_{12}\right\} \\ \pm \\ y_2=\left[m_2\cdot l_{22}\right]+\left[b_{22}\right]+\left\{b_{22}\right\} \\ \hline \left(\left[m_2\cdot\left(l_{12}\pm l_{22}\right)\right]+\left[b_{12}\pm b_{22}\right]+\left\{b_{12}\pm b_{22}\right\}\right)\left(\mathrm{mod}\,m_2\right)= \\ =\left(\left[b_{12}\pm b_{22}\right]+\left\{b_{12}\pm b_{22}\right\}\right)\left(\mathrm{mod}\,m_2\right)=\left(b_{12}\pm b_{22}\right)\left(\mathrm{mod}\,m_2\right). \end{gathered} \qquad (7)$$

Таким образом, операция сложения (вычитания) в СОК для чисел, содержащих дробные части остатков, может быть выполнена без каких-либо ограничений.

Операция умножения. Пусть даны два числа y_1 и y_2, для которых вводится операция умножения.

Представим сомножители в виде остатков по модулям m_1 и m_2

$$y_1=\left[m_1\cdot l_{11}\right]+\left[b_{11}\right]+\left\{b_{11}\right\}=\left[m_2\cdot l_{12}\right]+\left[b_{12}\right]+\left\{b_{12}\right\}$$

и

$$y_2=\left[m_1\cdot l_{21}\right]+\left[b_{21}\right]+\left\{b_{21}\right\}=\left[m_2\cdot l_{22}\right]+\left[b_{22}\right]+\left\{b_{22}\right\},$$

где [·] – есть целая часть числа;

{·} – обозначает дробную часть числа, а остатки представлены в виде целых и дробных частей

$$b_{11}=\left[b_{11}\right]+\left\{b_{11}\right\};\ b_{12}=\left[b_{12}\right]+\left\{b_{12}\right\};$$

$$b_{21}=\left[b_{21}\right]+\left\{b_{21}\right\};\ b_{22}=\left[b_{22}\right]+\left\{b_{22}\right\}.$$

После перемножения будет получен следующий результат:

$$\begin{array}{l} y_1=\left[m_1\cdot l_{11}\right]+\left[b_{11}\right]+\left\{b_{11}\right\} \\ \times \\ y_2=\left[m_1\cdot l_{21}\right]+\left[b_{21}\right]+\left\{b_{21}\right\} \\ \hline \left(\left[m_1\cdot l_{11}\right]\cdot\left[m_1\cdot l_{21}\right]+\left[m_1\cdot l_{11}\right]\cdot\left[b_{21}\right]+\left[m_1\cdot l_{11}\right]\cdot\left\{b_{21}\right\}+\right. \\ +\left[b_{11}\right]\cdot\left[m_1\cdot l_{21}\right]+\left[b_{11}\right]\cdot\left[b_{21}\right]+\left[b_{11}\right]\cdot\left\{b_{21}\right\}+ \\ \left.+\left\{b_{11}\right\}\cdot\left[m_1\cdot l_{21}\right]+\left\{b_{11}\right\}\cdot\left[b_{21}\right]+\left\{b_{11}\right\}\cdot\left\{b_{21}\right\}\right)\left(\mathrm{mod}\,m_1\right)= \end{array} \quad (8)$$

$$=\left(\left[m_1\cdot l_{11}\right]\cdot\left\{b_{21}\right\}+\left[b_{11}\right]\cdot\left[b_{21}\right]+\left[b_{11}\right]\cdot\left\{b_{21}\right\}+\right.$$
$$\left.+\left\{b_{11}\right\}\cdot\left[m_1\cdot l_{21}\right]+\left\{b_{11}\right\}\cdot\left[b_{21}\right]+\left\{b_{11}\right\}\cdot\left\{b_{21}\right\}\right)\left(\mathrm{mod}\,m_1\right)=$$
$$=\left(\left[m_1\cdot l_{11}\right]\cdot\left\{b_{21}\right\}+\left\{b_{11}\right\}\cdot\left[m_1\cdot l_{21}\right]+b_{11}\cdot b_{21}\right)\left(\mathrm{mod}\,m_1\right);$$

и

$$\begin{array}{l} y_1=\left[m_2\cdot l_{12}\right]+\left[b_{12}\right]+\left\{b_{12}\right\} \\ \times \\ y_2=\left[m_2\cdot l_{22}\right]+\left[b_{22}\right]+\left\{b_{22}\right\} \\ \hline \left(\left[m_2\cdot l_{12}\right]\cdot\left[m_2\cdot l_{22}\right]+\left[m_2\cdot l_{12}\right]\cdot\left[b_{22}\right]+\left[m_2\cdot l_{12}\right]\cdot\left\{b_{22}\right\}+\right. \\ +\left[b_{12}\right]\cdot\left[m_2\cdot l_{22}\right]+\left[b_{12}\right]\cdot\left[b_{22}\right]+\left[b_{12}\right]\cdot\left\{b_{22}\right\}+ \\ \left.+\left\{b_{12}\right\}\cdot\left[m_2\cdot l_{22}\right]+\left\{b_{12}\right\}\cdot\left[b_{22}\right]+\left\{b_{12}\right\}\cdot\left\{b_{22}\right\}\right)\left(\mathrm{mod}\,m_2\right)= \end{array} \quad (9)$$

$$=\left(\left[m_2\cdot l_{21}\right]\cdot\left\{b_{22}\right\}+\left[b_{21}\right]\cdot\left[b_{22}\right]+\left[b_{21}\right]\cdot\left\{b_{22}\right\}+\right.$$
$$\left.+\left\{b_{21}\right\}\cdot\left[m_2\cdot l_{22}\right]+\left\{b_{21}\right\}\cdot\left[b_{22}\right]+\left\{b_{21}\right\}\cdot\left\{b_{22}\right\}\right)\left(\mathrm{mod}\,m_2\right)=$$
$$=\left(\left[m_2\cdot l_{21}\right]\cdot\left\{b_{22}\right\}+\left\{b_{21}\right\}\cdot\left[m_2\cdot l_{22}\right]+b_{21}\cdot b_{22}\right)\left(\mathrm{mod}\,m_2\right).$$

Как следует из соотношений (8),(9), результат умножения не столь безобиден, как для сложения. Теперь для вычисления произведения требуется иметь значения величин l_{11}, l_{12}, l_{21} и l_{22}, что, однако, не является непреодолимым препятствием, поскольку в соответствии с выводами КТО значения этих величин легко можно определить на основе правил (2), т.е.

$$l_{11}=\begin{cases}\frac{\Delta_1}{n},\ \ при\ \Delta_1\geq 0\ \ и\ \ \Delta_1=k\cdot n;\\ m_2+\frac{\Delta_1}{n},\ \ при\ \Delta_1<0\ \ и\ \ \Delta_1=k\cdot n;\\ \frac{m_2+\Delta_1}{n},\ \ при\ \Delta_1\neq k\cdot n\ \ и\ \ \left(m_2+\Delta_1\right)=k\cdot n;\end{cases} \quad (10)$$

$$l_{21}=\begin{cases}\frac{\Delta_2}{n},\ \ при\ \Delta_2\geq 0\ \ и\ \ \Delta_2=k\cdot n;\\ m_2+\frac{\Delta_2}{n},\ \ при\ \Delta_2<0\ \ и\ \ \Delta_2=k\cdot n;\\ \frac{m_2+\Delta_2}{n},\ \ при\ \Delta_2\neq k\cdot n\ \ и\ \ \left(m_2+\Delta_2\right)=k\cdot n;\end{cases} \quad (11)$$

и

$$l_{12}=\begin{cases}\frac{\Delta_1}{n},\ \ при\ \Delta_1\geq 0\ \ и\ \ \Delta_1=k\cdot n;\\ m_1+\frac{\Delta_1}{n},\ \ при\ \Delta_1<0\ \ и\ \ \Delta_1=k\cdot n;\\ \frac{m_1+\Delta_1}{n},\ \ при\ \Delta_1\neq k\cdot n\ \ и\ \ \left(m_1+\Delta_1\right)=k\cdot n;\end{cases} \quad (12)$$

$$l_{22}=\begin{cases}\frac{\Delta_2}{n},\ \ при\ \Delta_2\geq 0\ \ и\ \ \Delta_2=k\cdot n;\\ m_1+\frac{\Delta_2}{n},\ \ при\ \Delta_2<0\ \ и\ \ \Delta_2=k\cdot n;\\ \frac{m_1+\Delta_2}{n},\ \ при\ \Delta_2\neq k\cdot n\ \ и\ \ \left(m_1+\Delta_2\right)=k\cdot n,\end{cases} \quad (13)$$

где $n=\left|m_1-m_2\right|$ и $\Delta_1=\left[b_{11}\right]-\left[b_{21}\right]$, $\Delta_2=\left[b_{12}\right]-\left[b_{22}\right]$, k – целое.

Для полученных соотношений (8), (9) следует сделать ряд выводов:

- если перемножаются целые числа, то $y_1\cdot y_2=\left(\left[b_1\cdot b_2\right]\right)\left(\mathrm{mod}\,m\right)=b_1\cdot b_2\left(\mathrm{mod}\,m\right)$;
- если хотя бы один сомножитель содержит дробную часть, то для выполнения операции умножения необходимо дополнительно проводить вычисления в соответствии с соотношениями (10)–(13). Важным является то, что операция умножения в СОК чисел, содержащих дробную часть, не выполнима только на остатках.

Операция деления. Пусть даны два числа y_1 и y_2, для которых вводится операция деления y_1 на y_2, при этом предполагается, что $y_2\neq 0$.

Представим делимое и делитель в виде остатков по модулям m_1 и m_2

$$y_1=\left[m_1\cdot l_{11}\right]+\left[b_{11}\right]+\left\{b_{11}\right\}=\left[m_2\cdot l_{12}\right]+\left[b_{12}\right]+\left\{b_{12}\right\} \quad (14)$$

и

$$y_2=\left[m_1\cdot l_{21}\right]+\left[b_{21}\right]+\left\{b_{21}\right\}=\left[m_2\cdot l_{22}\right]+\left[b_{22}\right]+\left\{b_{22}\right\}, \quad (15)$$

где [·] – есть целая часть числа;

{·} – обозначает дробную часть числа, а остатки представлены в виде целых и дробных частей

$$b_{11}=\left[b_{11}\right]+\left\{b_{11}\right\};\ b_{12}=\left[b_{12}\right]+\left\{b_{12}\right\};$$

$$b_{21}=\left[b_{21}\right]+\left\{b_{21}\right\};\ b_{22}=\left[b_{22}\right]+\left\{b_{22}\right\}.$$

В этом случае для каждого из модулей можно записать

$$\frac{y_1}{y_2}=\frac{\left[m_1\cdot l_{11}\right]+\left[b_{11}\right]+\left\{b_{11}\right\}}{\left[m_1\cdot l_{21}\right]+\left[b_{21}\right]+\left\{b_{21}\right\}} \quad (16)$$

и

$$\frac{y_1}{y_2}=\frac{\left[m_2\cdot l_{12}\right]+\left[b_{12}\right]+\left\{b_{12}\right\}}{\left[m_2\cdot l_{22}\right]+\left[b_{22}\right]+\left\{b_{22}\right\}}. \quad (17)$$

Выражения (16) и (17) не удаётся привести к эквивалентной форме, когда в знаменателях отсутствуют слагаемые $\left[m_1\cdot l_{21}\right]$ и $\left[m_2\cdot l_{22}\right]$. В связи с этим также, как и для операций умножения, необходимо вычислять значения величин l_{11}, l_{12}, l_{21} и l_{22} по правилам (10)–(13), представленных выше.

В целом представленные в настоящей статье результаты позволяют сделать вывод о том, что выполнение арифметических операций сложения, вычитания, умножения и деления в СОК над числами, содержащими дробную часть, принципиально выполнимо. При этом остаётся открытым вопрос о возможности параллельного выполнения рассмотренных арифметических операций в отдельности по каждому модулю. В связи с этим необходимо рассмотреть состав данных, необходимых для выполнения этих операций по каждому отдельному модулю, что, по сути, сводится к определению значений пар неполных частных от деления $\langle l_{11}, l_{21}\rangle$ и $\langle l_{12}, l_{22}\rangle$ для модулей сравнения m_1 и m_2.

Так, для определения значений пары $\langle l_{11}, l_{21}\rangle$ по правилам (10), (11) необходимо знать:

- значения остатков b_{11}и b_{21};
- разность модулей сравнения $n=\left|m_1-m_2\right|$;
- значение модуля m_1,

а для пары $\langle l_{12}, l_{22}\rangle$, соответственно по правилам (13), (14):

- значения остатков b_{12} и b_{22};
- разность модулей сравнения $n=\left|m_1-m_2\right|$;
- значение модуля m_2.

В этих случаях для восстановления исходных значений всякий раз необходимо устранять неоднозначность в определении значения недостающего модуля. Так, при известном $n=\left|m_1-m_2\right|$ и значении модуля m_1 для модуля m_2 можно записать

$$m_2=\begin{cases}m_1-n;\\ m_1+n,\end{cases} \quad (18)$$

а при известном $n=\left|m_1-m_2\right|$ и значении модуля m_2 для модуля m_1 пролучим

$$m_1=\begin{cases}m_2-n;\\ m_2+n.\end{cases} \quad (19)$$

В обоих случаях (18), (19) возможно использование имеющейся информации об остатках, например, для варианта (18) и $b_{21}\ge m_1$ ($b_{22}\ge m_1$) следует $m_2=m_1+n$ или для варианта (19) и $b_{11}\ge m_2$ ($b_{21}\ge m_2$) следует $m_1=m_2+n$. В остальных случаях восстановление исходного значения не является безошибочным.

Для вариантов (18) и (19) можно дать вероятностную оценку. Пусть для определённости $m_1>m_2$ и значения случайного числа в шкале представления имеет равномерное распределение. Тогда вероятность того, что $b_{21}\ge m_1$ ($b_{22}\ge m_1$), будет определяться величиной

$$P\left(b_2\ge m_1\right)=\frac{m_1-m_2+1}{m_2}. \quad (20)$$

Например, при m_1=17 и m_2=15

$$P\left(b_2\ge m_1\right)=\frac{17-15+1}{17}=\frac{3}{17}\approx 0{,}18,$$

а при m_1=33 и m_2=31

$$P\left(b_2\ge m_1\right)=\frac{33-31+1}{33}=\frac{3}{33}\approx 0{,}09.$$

Таким образом, существует ненулевая вероятность того, что исходное значение числа может быть определено правильно. Ниже приведен пример, поясняющий полученный вывод.

Пример 1. Пусть для чисел x_1 и x_2 заданы остатки от деления на модули m_1 и m_2:

b_{11}= 7; b_{12}= 17;

b_{21}= 20; b_{22}= 17.

В отношении модулей сравнения известно, что их значения равны 31 и 33, но не известно, какое значение принадлежит какому модулю.

Для имеющихся остатков от деления исходных чисел на модули сравнения не удаётся сделать вывод о порядке следования модулей, поскольку остатки меньше указанных значений модулей. В связи с этим возможны следующие ситуации:

- m_1=31, m_2=33 и тогда в соответствии с правилами (10)–(12) следует, что

m_1: x_1=[28·31]+7=875 и x_2=[18· 31]+20=578;

m_2: x_1=[26·33]+17=875 и x_2=[17· 33]+17=578;

- m_1=33, m_2=31 и тогда в соответствии с правилами (10)–(12) следует, что

m_1: x_1=[26·33]+7=865 и x_2=[17·33]+20=581,

m_2: x_1=[28·31]+17=885 и x_2=[18·31]+17=614.

Можно отметить, что в первом случае восстановленные по разным модулям значения исходных чисел совпадают, а во-втором, напротив, не совпадают. Это может рассматриваться в качестве показателя того, что значения модулей сравнения определены верно.

Пример 2. Пусть для чисел x_1 и x_2 заданы остатки

от деления на модули m_1 и m_2:

b_{11}= 21; b_{12}= 31;

b_{21}= 27; b_{22}= 32.

В отношении модулей сравнения известно, что их значения равны 31 и 33, при этом, исходя из величин остатков определение порядка следования модулей не вызывает сомнений, поскольку вторые остатки чисел не меньше значений первого модуля.

В связи с этим для имеющихся остатков от деления исходных чисел на модули сравнения возможна только одна ситуация:

• m_1=31, m_2=33 и тогда в соответствии с правилами (10)–(12) следует, что

m_1: x_1=[28·31]+21=889 и x_2=[14· 31]+27=461;

m_2: x_1=[26·33]+31=889 и x_2=[13· 33]+32=461.

Для приведенного примера вероятность возникновения описанной ситуации соответствует соотношению (20) в отношении каждого из модулей сравнения. С учётом возможности совместного появлении события, связанного с равенством или превышением значений остатков над одним из модулей, зависимость (20) принимает вид

$$P\left(b_2 \ge m_1, b_1 \ge m_2\right) = \frac{|m_1 - m_2|+1}{m_2} + \frac{|m_1 - m_2|+1}{m_1} - \frac{|m_1 - m_2|+1}{m_2}\cdot\frac{|m_1 - m_2|+1}{m_1} = \quad (21)$$
$$= P\left(b_2 \ge m_1\right) + P\left(b_1 \ge m_2\right) - P\left(b_2 \ge m_1\right)\cdot P\left(b_1 \ge m_2\right).$$

В более сложных ситуациях, когда речь идёт о восстановлении вектора значений $\mathbf{x} = \{x_1, x_2, ..., x_n\}$ по остаткам $\mathbf{b}_1 = \{b_{11}, b_{21}, ..., b_{n1}\}$ и $\mathbf{b}_2 = \{b_{12}, b_{22}, ..., b_{n2}\}$ при условии, что для каждого значения $x_i \in \mathbf{x}$, $i \in [1, ..., n]$ использованы различные пары модулей $\langle m_{1i}, m_{2i}\rangle \in \mathbf{M}$, выражение для оценки вероятности восстановления вектора **x** принимает вид

$$P\left(\mathbf{b}_1 \ge \mathbf{M}\right) = \prod_{i=1}^{n} \frac{m_{1i} - m_{2i}}{m_{1i}}.$$

Например, пусть использованы следующие наборы модулей сравнения: ⟨17, 15⟩, ⟨17, 16⟩, ⟨17, 15⟩, тогда

$$P\left(\mathbf{b}_1 \ge \mathbf{M}\right) = \frac{17-15+1}{17}\cdot\frac{17-16+1}{17}\cdot\frac{16-15+1}{16} =$$
$$= 0{,}174\cdot 0{,}118\cdot 0{,}125 \approx 0{,}260\cdot 10^{-2}.$$

Более полная оценка вероятности безошибочного восстановления исходных значений чисел при использовании неполных данных, необходимых для корректного выполнения арифметических операций сложения (вычитания), умножения и деления, может быть выполнена с учётом динамики изменений значений параметров, а также проверки совпадения результирующих значений, получаемых по различным модулям сравнения.

В целом основной вывод, который следует из представленного материала, сводится к тому, что для чисел, содержащих дробную часть и представленных в СОК, возможно выполнение арифметических операций сложения, вычитания, умножения и деления. Для выполнения указанных операций требуется определение значений неполных частных от деления исходных значений чисел на модули сравнения, что приводит к необходимости использования дополнительных данных, кроме остатков от деления. В свою очередь, использование дополнительных данных приводит к появлению ненулевой вероятности правильного определения исходных значений чисел, представимых в СОК, что может рассматриваться как негативный фактор, например, в системах, предусматривающих некриптографическую защиту данных.

Литература

1. Кукушкин С.С., Шемигон Н.Н., Нестеровский И.С., Першин С.М. Методические основы повышения эффективности передачи информации за счёт одновременного использования различных технологий нетрадиционного формирования данных и сигналов// Двойные технологии.-2012.-№3(60).-с.33-38.

2. Кукушкин С.С., Нестеровский И.С. Методы нетрадиционного представления данных образами-остатками и оценка эффективности их применения//Двойные технологии.-2011.-№3(56).-с.40-48.

3. Кукушкин С.С., Супрун А.С. Методика формирования оптимальных структурно-кодовых конструкций, основанных на нетрадиционном представлении результатов телеизмерений образами-остатками//Двойные технологии.-2011.-№3(56).-с.55-63.

4. Кукушкин С.С. Методы анализа и синтеза различных проблемно-ориентированных подходов к устранению избыточности передаваемой информации//Двойные технологии.-2010.-№2(51).-с.14-21.

5. Кукушкин С.С., Войналович В.В., Половников А.Ю. Метод синтеза проблемно-ориентированного кода для повышения помехоустойчивости передачи измерительной информации//Двойные технологии.-2009.-№4(49).-с.46-49.

6. Кукушкин С.С. Теория конечных полей и информатика: т.1 Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках.-М.:МО РФ, 2003.-284 с.

7. Кукушкин С.С. Методы конструктивной теории синтеза нетрадиционных представлений данных и сигналов для повышения эффективности передачи информации//Двойные технологии.-2010.-№3(52).-с.21-28.

Материал поступил в редакцию 19. 03. 2014 г.