# МЕТОД ОБРОБКИ ІНФОРМАЦІЇ В МОДУЛЯРНІЙ АРИФМЕТИЦІ

Лукашев В.О.
Науковий керівник – канд. техн. наук, доц. Загуменна К. В.
Харківській національний технічній університет сільського господарства ім. П. Василенка. (Харків, Різдвяна, 19, каф. АКІТ,
тел. (057)712-35-37), E-mail: yayaska@khntusg.info)

Існує чотири методи обробки інформації в МА: суматорний; табличний; прямий логічний метод реалізації арифметичних операцій; метод кільцевого зсуву (КРЗ). У даній доповіді розглянимо метод реалізації арифметичних операцій, котрий заснований на використанні КРЗ. Особливість даного методу полягає в том, що результат арифметичної операції $(a_i \pm b_i) mod\, m_i$ по довільному модулю МА, заданої $\{m_i\},\ j = \overline{1,n}$ основ, визначається тільки за рахунок послідовних циклічних зсувів заданої цифрової структури.

Відома теорема Келі встановлює ізоморфізм між елементами скінченої абелівої групи і елементами груп переміщень. Що дає нам змогу представити матрицю складання (віднімання) для довільного модулю в МА у вигляді таблиці. А висновок одного із наслідків, дозволяє нам визначити результат арифметичних операцій в МА за допомогою використання метода кільцевого зсуву. Так як операнд А в модулярній арифметиці представляється набором залишків від ділення його на набір n простих чисел $\{m_i\},\ i = \overline{1,n}$, то цій набір залишків можливо ототожнювати безпосередньо с сумою полей Галуа. Для вивчення метода реалізації арифметичних операцій в МА достатньо розглянути варіант для конкретної наведеної системи відрахувань по модулю.

Суть методу полягає в тому, що вихідна цифрова структура для кожного з модулів (основ) МА представляється у вигляді вмісту першого рядка (стовбця) таблиці модульного складання (віднімання) $(a_i \pm b_i) mod\, m_i$.

При технічній реалізації даного методу перший операнд $a_i$ вказує на номер розряду КРЗ, визначаючого результат модульної операції по модулю $m_i$, а другий операнд $b_i$ визначає кількість зсувів розрядів КРЗ, на які необхідно провести зсув вихідного вмісту КРЗ. При реалізації операції складання вихідна цифрова структура буде зсуватися у позитивному напрямі (проти годинникової стрілки), а при відніманні –у від'ємному напрямку (за годинниковою стрілкою).

Даний метод має ряд переваг в порівнянням з іншими методами, котрі реалізуються в модулярній арифметиці. Наприклад: відсутність міжразрядних переносів, що дає нам змогу суттєво збільшити достовірність реалізації модульних операцій. Проте час виконання модульних операцій порівняно велике, що знижує загальну ефективність застосування даного методу реалізації арифметичних операцій в модулярній арифметиці.