УДК 511.147; 681.3

М. В. Синьков, Ю. Є. Боярінова, Я. О. Каліновський,
Т. Г. Постнікова, Т. В. Синькова
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Модульні операції над гіперкомплексними числами в системі комп'ютерної математики MAPLE

Розглянуто процедури виконання модульних операцій в гіперкомплексних числових системах. Визначено місце цих програм в структурі системи комп'ютерної математики Maple. Розглянуто застосування розробленого інструментарію на прикладі задачі розподілу секрету.

Ключові слова: *гіперкомплексна числова система, модульні операції, комп'ютерна математика, математичний пакет Maple, залишкові класи, представимість гіперкомплексних чисел.*

У статті розглядаються питання розробки програм для виконання модульних операцій над гіперкомплексними числами. Вони являються складовою частиною пакету процедур, що був створений для виконання символьних та чисельних операцій в гіперкомплексних числових системах в рамках системи комп'ютерної математики Maple [1–3].

У зв'язку з інтенсивним розвитком інформаційних технологій: при збереженні й обробці інформації, при вирішенні проблем передачі даних, при захисті інформації різного призначення криптографічними засобами [4] і т.д., виникає широкий спектр обчислювальних задач, що потребують виконання операцій над багаторозрядними числами чи проведення обчислень з величинами, що змінюються у великих діапазонах значень. Тому виникає питання представимости таких числових даних в заданому діапазоні значень, прискорення арифметичних операцій над ними, можливості проведення паралельної обробки даних. Одним із засобів вирішення цієї проблеми являється впровадження непозиційної системи числення — системи залишкових класів [5].

Не викликає сумніву питання застосування гіперкомплексних чисел в системах залишкових класів при розв'язку практичних задач обробки інформації.

Особливістю розробленого нами інструментарію є можливість виконувати модульні обчислення над гіперкомплексними числами *n*–го порядку. Надалі будемо вважати, що гіперкомплексні числа задаються у вигляді :

$$A = a_1 E_1 + a_2 E_2 + ... + a_n E_n, \qquad (1)$$

де E_i — елементи базису заданої гіперкомплексної числової системи; a_i — дійсні цілі коефіцієнти при базисних елементах; n — розмірність гіперкомплексної числової системи.

У рамках пакету виконання символьних та чисельних операцій у гіперкомплексних числових системах розроблено декілька процедур модульних обчислень.

1. Процедура побудови системи залишкових класів по гіперкомплексному модулю.

Нехай заданий ряд гіперкомплексних чисел з цілими дійсними коефіцієнтами, який будемо називати подалі модулями системи

$$M_1, M_2, ..., M_k \quad , \qquad (2)$$

де k — довжина ряду.

Визначимо поняття залишку по модулю для гіперкомплексного числа. Гіперкомплексне число A буде кратно гіперкомплексному числу M (або M буде дільником числа A), якщо частка A/M являється гіперкомплексним числом. Якщо S є таким, що $A - S$ ділиться на M, тоді можна записати

$$A \equiv S \pmod{M}. \qquad (3)$$

Гіперкомплексне число S являється залишком A по модулю M.

Під системою залишкових класів (СЗК) будемо розуміти таку систему, в якій гіперкомплексне число представляється у вигляді набору залишків по обраним модулям (2) [3].

В СЗК існує діапазон $0 - M$, який пов'язаний з модулями M_i співвідношенням:

$$M = \prod_{i=1}^{k} M_i. \qquad (4)$$

У відповідності до теореми про ділення з залишком довільне гіперкомплексне число A з вибраного діапазону $0 - M$ може бути єдиним чином представлено у вигляді

$$A = T \cdot M + \alpha, \quad 0 \le \alpha \le M. \qquad (5)$$

Довільне гіперкомплексне число A, можна представити як сукупність залишків $\{\alpha_i\}, i = 1...k$ по сукупності взаємно простих модулів $\{M_i\}, i = 1...k$ у вигляді системи рівнянь

$$\begin{aligned} A &\equiv \alpha_1 (\mathrm{mod}\, M_1) \\ A &\equiv \alpha_2 (\mathrm{mod}\, M_2) \\ A &\equiv \alpha_3 (\mathrm{mod}\, M_3) \\ &\vdots \\ A &\equiv \alpha_k (\mathrm{mod}\, M_k) \end{aligned} \qquad (6)$$

Однозначність представлення довільного числа сукупністю залишків зумовлюється взаємною простотою модулів $\{M_i\}, i = 1..k$ системи залишкових класів.

Побудова системи залишкових класів в області гіперкомплексних систем дозволяє підтримувати високошвидкісну арифметику при обробці даних представлених у гіперкомплексній формі та є одним з основних шляхів підвищення продуктивності обчислювальних процесів.

Алгоритм процедури побудови системи залишкових класів по гіперкомплексному модулю, розроблений в системі комп'ютерної математики MAPLE розглянемо на прикладі гіперкомплексної системи 2-го порядку.

Нехай ми маємо два гіперкомплексних числа $A = a_1 E_1 + a_2 E_2$ і $B = b_1 E_1 + b_2 E_2$ та число $N = b_1^2 - \rho \cdot b_2^2$, де $\rho = \{-1,0,1\}$. Якщо виконуються рівняння

$$a_1 b_1 - \rho a_2 b_2 \equiv x b_1 - \rho y b_2 (\mathrm{mod}\, N) \qquad (7)$$

та

$$a_2 b_1 - a_1 b_2 \equiv y b_1 - x b_2 (\mathrm{mod}\, N), \qquad (8)$$

тоді

$$A = x E_1 + y E_2 \ (\mathrm{mod}\, N). \qquad (9)$$

З іншого боку можна визначити залишки по таблиці множення T заданої гіперкомплексної системи. Виберемо таблицю T, що відповідає закону множення комплексних чисел

$$T = \begin{vmatrix} E_1 & E_2 \\ E_2 & -E_1 \end{vmatrix}. \qquad (10)$$

Позначимо через $R = r_1 E_1 + r_2 E_2$ результат множення гіперкомплексного числа $A = a_1 E_1 + a_2 E_2$ на число $\overline{B}$, що є спряженим вихідному гіперкомплексному числу B. При цьому маємо

$$R = (a_1 b_1 - a_2 b_2 (\mathrm{mod}\, N)) \cdot E_1 + (a_2 b_1 - a_1 b_2 (\mathrm{mod}\, N)) \cdot E_2 . \qquad (11)$$

Модифікована таблиця множення запишеться у вигляді:

$$\tilde{T} = \begin{vmatrix} & b_1 & b_2 \\ r_1 & x & y \\ r_2 & y & -x \end{vmatrix} . \qquad (12)$$

Звідси маємо

$$\begin{aligned} x &= r_1 \cdot b_1 - r_2 \cdot b_2 , \\ y &= r_1 \cdot b_2 + r_2 \cdot b_1 . \end{aligned} \qquad (13)$$

Такий самий алгоритм існує і для знаходження залишків для гиперкомплексных систем більше високих порядків.

2. Процедура визначення представимости гіперкомплексного числа.

Поняття представимости гіперкомплексного числа (1) полягає в можливості представлення даного числа в деякій n – мірній області.

Гіперкомплексне число A представимо в деякій системі модулів M (5), якщо воно являється найменшим лишком по модулю M. В протилежному випадку A не представимо в даній системі. Якщо гіперкомплексне число A представимо в системі з взаємопростими модулями $\{M_1, M_2, ..., M_k\}$ то таке представлення єдине, і може бути зображене сукупністю своїх найменших залишків по модулям системи $(\alpha_1, ..., \alpha_k)$.

Якщо для дійсних чисел областю представимости являється відрізок на прямій, то для гіперкомплексних систем розмірності два — це ромб, сторони якого задаються нерівностями

$$\begin{aligned} -\frac{1}{2} \le \frac{a_1 b_1 - \rho a_2 b_2}{N(B)} \le \frac{1}{2}, \\ -\frac{1}{2} \le \frac{a_2 b_1 - \rho a_1 b_2}{N(B)} \le \frac{1}{2}, \end{aligned} \qquad (14)$$

де $\rho = \{-1, 0, 1\}$, $N(B)$ — норма гіперкомплексного числа $B = b_1 E_1 + b_2 E_2$, в чисельнику вираз для лишку.

Для гіперкомплексних числових систем розмірності n область представимости представляє собою n-мірну область, межі якої задаються системою з n нерівностей виду:

$$-\frac{1}{2} \le \frac{V_i(A(\mathrm{mod}\, B))}{N(B)} \le \frac{1}{2}, \quad i = 1...n, \tag{15}$$

де $V_i(A(\mathrm{mod}\, B))$ — є лишок i-ї компоненти гіперкомплексного числа $A = a_1E_1 + a_2E_2$ по модулю числа $B = b_1E_1 + b_2E_2$.

За допомогою розробленої процедури можна визначити, чи знаходиться залишок α_i усередині заданої n-мірної області.

3. Процедура, що реалізує алгоритм Евкліда для гіперкомплексних числових систем [6].

Алгоритм Евкліда полягає в наступному [7]. Знаходимо ряд рівнянь:

$$\begin{cases} R_0 = R_1 \cdot Q_1 + R_2,\ 0 < R_2 < R_1, \\ R_1 = R_2 \cdot Q_2 + R_3,\ 0 < R_3 < R_{2,} \\ \cdots \\ R_{n-2} = R_{n-1} \cdot Q_{n-1} + R_n,\ 0 < R_n < R_{n-1}, \\ R_{n-1} = R_n \cdot Q_n, \end{cases} \tag{16}$$

де початкові значення $R_0 = A, R_1 = B$, A та B — гіперкомплексні числа (1). Ряд закінчується тоді, коли одержуємо деяке значення $R_{n+1} = 0$. Отже, найбільший загальний дільник дорівнює R_n.

На величини $Q_t = q_{t1}E_1 + ... + q_{tn}E_n$ накладаються такі умови:

$$\sum_{j=1}^{n} (V_j - q_j)^2 \le \frac{1}{2}, \tag{17}$$

де $V = V_1E_1 + ... + V_nE_n = A \cdot \overline{B}$.

Відміною розробленої процедури полягає в тому, що алгоритм Евкліда реалізований для гіперкомплексних числових систем. Алгебраїчні операції над гіперкомплексними числами (1) відрізняються від операцій над дійсними числами. Необхідною умовою функціонування алгоритму являється перевірка того, чи являється число B дільником нуля.

Розглянемо застосування розробленого пакету процедур виконання модульних операцій над гіперкомплексними числами в середовищі Maple на прикладі задачі розподілу секрету, що відноситься до питань криптографії з відкритим ключем [6].

Суть цієї задачі полягає в тому, як зберегти секрет, розділивши його на складові частини між декількома законними користувачами, а потім знов відновити його.

Приклад.

```
restart;
read("d:\\HNS_lib\\HNS_lib.m");
 T:=HNS_lib[Tabl_2order](1,1);
 n:=HNS_lib[Size_GNS](T);
 M1:=3*E[1]+4*E[2];
 M2:=1*E[1]+4*E[2];
 M3:=2*E[1]+3*E[2];
 al1:=0*E[1]+2*E[2];
 al2:=0*E[1]-2*E[2];
 al3:=0*E[1]-1*E[2];
 MM12:=HNS_lib[Mult](M1,M2,T);
 M:=HNS_lib[Mult](MM12,M3,T);
 MM13:=HNS_lib[Mult](M1,M3,T);
 MM23:=HNS_lib[Mult](M2,M3,T);
 MS1:=HNS_lib[eucl](T,MM23,M1);
 MS2:=HNS_lib[eucl](T,MM13,M2);
 MS3:=HNS_lib[eucl](T,MM12,M3);
 R1:=HNS_lib[Mult](al1,M23,T);
 R2:=HNS_lib[Mult](al2,M13,T);
 R3:=HNS_lib[Mult](al3,M12,T);
 RR1:=HNS_lib[Mult](R1,MS1,T);
 RR2:=HNS_lib[Mult](R2,MS2,T);
 RR3:=HNS_lib[Mult](R3,MS3,T);
 Y1:=HNS_lib[Mult](R1,RR1,T);
 Y2:=HNS_lib[Mult](R2,RR2,T);
 Y3:=HNS_lib[Mult](R3,RR3,T);
 Y4:=HNS_lib[Addition](Y1,Y2,n);
 Y5:=HNS_lib[Addition](Y3,Y4,n);
 yy:=HNS_lib[ostat](T,Y5,M);
 REZULT:=yy;
```

Як видно з приведеного тексту програми, для розв'язку задачі розподілу секрету та відновлення інформації використовуються процедури алгоритмічно-програмного інструментарію аналітичних обчислень над гіперкомплексними числами в системі комп'ютерної математики MAPLE [1]: завдання таблиці множення гіперкомплексних чисел HNS_lib[Tabl_2order]**,** обчислення розміру вибраної гіперкомплексної числової системи HNS_lib[Size_GNS], додавання двох гіперкомплексних чисел HNS_lib[Addition], множення двох гіперкомплексних чисел HNS_lib[Mult]**,** алгоритму Евкліда HNS_lib[eucl], обчислення залишків по модулю для гіперкомплексного числа HNS_lib[ostat]. Вихідними параметрами

задачі є три гіперкомплексних модулі M_1, M_2, M_3 і найменші ненегативні залишки a_1, a_2, a_2. Результатом є відновлений секрет .

Використання алгоритмічно – програмного інструментарію для виконання практичних задач дозволяє значно підвищити швидкість виконання математичних обчислень, зменшити об'єм програм.

1. *Синьков М.В., Боярінова Ю.Є., Каліновський Я.О., Постнікова Т.Г., Синькова Т.В.* Алгоритмічно - програмний інструментарій аналітичних обчислень над гіперкомплексними числами в системі комп'ютерної математики MAPLE. - Реєстрація, зберігання і обробка даних. – 2005. – Т. 7. - №2. - С.

2. *Аладьев В, Шишаков М.* Автоматизированное рабочее место. Математический пакет Maple V. М.: Лаборатория Базовых Знаний – 2000-572стр.

3. *Дьяконов В.П.* Maple 9 в математике, физике и образовании –М.: Солон · 2004. · 688 стр.

4. *Синьков М.В., Бояринова Ю.Е., Калиновский Я.А., Трубников П.В.* Развитие задачи разделения секрета. - Реєстрація, зберігання і обробка даних. – 2003. – Т. 5. - №4. - С.90-96

5. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.:Советское радио, 1968. – 438 стр.

6. *Бояринова Ю.Е., Одарич Я.В., Трубников П.В.* Реализация алгоритма Евклида для задачи разделения секрета. Реєстрація, зберігання і обробка даних. – 2004. – Т. 6 - №3. - С.58-65

7. *Виноградов И.М.* Основы теории чисел. - М: Наука - 1972-168 стр.

8. *П.Ноден, К.Китте.* Алгебраическая алгоритмика с упражнениями и решениями. М.: Мир, 1999.-720 стр.

Надійшла до редакції 01.09.2005