УДК 515.171; 681.3

Ю. Е. Бояринова, Я. В. Одарич, П. В. Трубников
Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина

Разработка алгоритмов восстановления информации в задаче разделения секрета

Рассмотрены примеры восстановления секрета, используя изоморфный переход к системе действительных чисел, что исключает необходимость вычисления функции Эйлера в гиперкомплексных числовых системах второго порядка.

Ключевые слова: *алгоритм Евклида, задача разделения секрета, комплексные числа, двойные числа, дуальные числа.*

Двухмерное расширение поля действительных чисел приводит первоначально к множеству чисел вида $a+bE$, где a,b — действительные числа, E — некоторый элемент. Это множество чисел с операциями сложения и умножения является двухмерной алгеброй над полем действительных чисел. Имеется только три различные алгебры второго порядка над полем действительных чисел: комплексные числа $a+bi, i^2=-1$; дуальные числа $a+b\varepsilon, \varepsilon^2=0$; двойные числа $a+be, e^2=1$.

Общая формула нормы для этих гиперкомплексных чисел:

$$N(A)=a^2-\rho b^2, \tag{1}$$

где $\rho=-1$ для комплексных чисел; $\rho=0$ для дуальных чисел; $\rho=1$ для двойных чисел.

В этих алгебрах построена теория сравнений, даны понятия простых и составных чисел. В дальнейшем вместо слова алгебра будем применять термин гиперкомплексная числовая система.

Для этих гиперкомплексных чисел может быть построена непозиционная система счисления, в которой выбираются взаимнопростые комплексные модули $m_1,...,m_i,...,m_n$ и определяются полные системы наименьших комплексных вычетов. Важным здесь является вопрос представимости некоторого комплексного числа в диапазоне множества комплексных чисел $0-M=\prod_{i=1}^{n} m_i$. Если в процессе вычислений и работе с остаточными представлениями в действительных числах

может быть применена функция Эйлера, то при вычислениях в гиперкомплексных числах такая возможность отсутствует, и требуется в вычислительный процесс «включать» алгоритм Евклида.

Построение вычетов для этих гиперкомплексных систем происходит следующим образом.

Теорема. Пусть $A = a + bi, m = p + qi$, и выполняются сравнения:

$$ap - \rho bq \equiv xp - \rho yq (\mathrm{mod}\, N), \tag{2}$$

$$bp - aq \equiv yp - xq (\mathrm{mod}\, N), \tag{3}$$

где $\rho = \{-1,0,1\}$.

Тогда $A = a + bi \ (\mathrm{mod}\, m)$.

Если найдены наименьшие вычеты выражений (2) и (3)

$$ap - \rho bq = r,$$

$$bp - aq = r',$$

то наименьший вычет числа A по модулю m равен:

$$x + yi = \frac{ra + \rho r'b}{a^2 - \rho b^2} + \frac{r'a + rb}{a^2 - \rho b^2}.$$

При этом задача разделения секрета может быть сформулирована в различных гиперкомплексных системах.

Существует два варианта решения задачи, первый из которых базируется на том, что используется изоморфный переход к системе действительных чисел, а второй базируется на использовании алгоритма Евклида. При этом исключается необходимость вычисления функции Эйлера в гиперкомплексных числах.

Алгоритм восстановления

Даны взаимно простые модули и соответствующие им вычеты

m_1	m_2	m_3
α_1	α_2	α_3

причем $m_1 > m_2 > m_3$.

Тогда первое приближение исходного числа можно выразить так:

$$M_1 = m_1 n_1 + \alpha_1. \tag{1}$$

Модуль m_1 можно выразить через модуль m_1:

$$m_1 = m_2 + \xi_1 . \qquad (2)$$

Подставляя (2) в (1), получим:

$$M_1 = m_2 n_1 + \xi_1 n_1 + \alpha_1 \equiv \alpha_2 \ (\mathrm{mod}\, m_2) .$$

Используя свойства сравнений, получаем:

$$\xi_1 n_1 + \alpha_1 \equiv \alpha_2 \ (\mathrm{mod}\, m_2) ,$$

откуда:

$$\xi_1 n_1 \equiv \alpha_2 - \alpha_1 \ (\mathrm{mod}\, m_2) ,$$

$$n_1 \equiv (\alpha_2 - \alpha_1)\xi_1^{\varphi(m_2)-1} \ (\mathrm{mod}\, m_2) . \qquad (3)$$

С другой стороны, исходное число можно выразить так:

$$M_2 = m_1 m_2 n_2 + M_1 \equiv \alpha_3 \ (\mathrm{mod}\, m_3) . \qquad (4)$$

Иначе модуль $m_1 m_2$ можно выразить через модуль m_3:

$$m_1 m_2 = m_3 + \xi_2 . \qquad (5)$$

Подставляя (5) в (4), получим:

$$m_3 n_2 + \xi_2 n_2 + M_1 \equiv \alpha_3 \ (\mathrm{mod}\, m_3) ,$$

$$\xi_2 n_2 \equiv (\alpha_3 - M_1)(\mathrm{mod}\, m_3) , \qquad (6)$$

$$n_2 \equiv (\alpha_3 - M_1)\xi_2^{\varphi(m_3)-1}(\mathrm{mod}\, m_3) .$$

Подставляя (6) в (4), получаем исходное число:

$$M_2 = m_1 m_2 (\alpha_3 - M_1)\xi_2^{\varphi(m_3)-1}(\mathrm{mod}\, m_3) + m_1(\alpha_2 - \alpha_1)\xi_1^{\varphi(m_2)-1}(\mathrm{mod}\, m_2) + \alpha_1 .$$

Пример 1.

Восстановить исходную величину, если:

$m_1 = 25$	$m_2 = 17$	$m_3 = 13$
$\alpha_1 = 11$	$\alpha_2 = 9$	$\alpha_3 = 5$

$$\xi_1 = 25 - 17 = 8,$$

$$n_1 \equiv (9-11)\cdot 8^{\varphi(17)-1} (\mathrm{mod}17) \equiv 4(\mathrm{mod}17),$$

$$M_1 = 25\cdot 4 + 11 = 111,$$

$$n_2 \equiv (5-111)\cdot 9^{\varphi(13)-1} (\mathrm{mod}13) \equiv 7(\mathrm{mod}13).$$

Тогда исходное число:

$$M_2 = 25\cdot 17\cdot 7 + 111 = 3086.$$

Пример 2.

Восстановить исходную величину, если модули и вычеты заданы комплексными величинами:

$m_1 = 3 + 4i$	$m_2 = 1 + 4i$	$m_3 = 2 + 3i$
$\alpha_1 = 2i$	$\alpha_2 = -2i$	$\alpha_3 = -i$

$$\xi_1 = (3+4i) - (1+4i) = 2,$$

$$n_1 \equiv (-2i - 2i)\cdot 2^{\varphi(1+4i)-1} (\mathrm{mod}1+4i).$$

Для вычислений изоморфным переходом получаем действительные числа:

$$\tilde{n}_1 = 1\cdot 2^{15} = 1\cdot 9 = 9.$$

Тогда: $$n_1 = -2i,$$

$$M_1 = (3+4i)(-2i) + 2i = 8 - 4i,$$

$$\xi_2 = (3+4i)(1+4i) - (2+3i) = -18 + 13i,$$

$$n_2 \equiv (-i - (8-4i))(-18+13i)^{\varphi(2+3i)-1} (\mathrm{mod}\, 2+3i) \equiv 2i\cdot(-2)^{\varphi(2+3i)-1} (\mathrm{mod}\, 2+3i).$$

Переходя к действительным числам, получаем:

$$\tilde{n}_2 \equiv 3\cdot 11^{11} \equiv 3\cdot 6 \equiv 18 \equiv 5(\mathrm{mod}13),$$

$$n_2 = -i.$$

Тогда:

$$M_2 = (3+4i)(1+4i)(-i) + (8-4i) = 24+9i\,.$$

Пример 3.

Восстановить исходную величину, если модули и вычеты заданы двойными величинами:

$m_1 = 7+6i$	$m_2 = 6+5i$	$m_3 = 5+4i$
$\alpha_1 = 1+1i$	$\alpha_2 = 8+8i$	$\alpha_3 = 6+6i$

$$\xi_1 = (7+6i) - (6+5i) = 1+i\,,$$

$$n_1 \equiv ((8+8i-(1+1i)) \cdot (1+i)^{\varphi(6+5i)-1} (\mathrm{mod}\, 6+5i)\,.$$

Для вычислений изоморфным переходом получаем действительные числа

$$\tilde{n}_1 \equiv 3 \cdot 2^9 \equiv 7(\mathrm{mod}\, 11)\,.$$

Тогда: $$n_1 = 9+9i\,,$$

$$M_1 = (7+6i)(9+9i) + (1+i) = 118+118i\,,$$

$$\xi_2 = (7+6i)(6+5i) - (5+4i) = 67+67i\,,$$

$$n_2 \equiv (-112-112i)(67+67i)^{\varphi(5+4i)-1} (\mathrm{mod}\, 5+4i) \equiv (5+5i) \cdot (4+4i)^{\varphi(5+4i)-1} (\mathrm{mod}\, 5+4i)\,.$$

Переходя к действительным числам, получим:

$$\tilde{n}_2 \equiv 1 \cdot 8^5 \equiv 8(\mathrm{mod}\, 9)\,,$$

$$n_2 = 4+4i\,.$$

Тогда:

$$M_2 = (7+6i)(6+5i)(4+4i) + (118+118i) = 690+690i\,.$$

Пример 4.

Восстановить исходную величину, если модули и вычеты заданы дуальными величинами:

$m_1 = 5+i$	$m_2 = 3+2i$	$m_3 = 2+i$
$\alpha_1 = -1-2i$	$\alpha_2 = i$	$\alpha_3 = -1-i$

$$\xi_1 = (5+i)-(3+2i) = 2-i\,,$$

$$n_1 \equiv (i-(-1-2i))\cdot(2-i)^{\varphi(3+2i)-1} (\mathrm{mod}\, 3+2i)\,.$$

Для вычислений изоморфным переходом получаем действительные числа

$$\tilde{n}_1 \equiv 1\cdot(-1)^5 \equiv 8(\mathrm{mod}\, 9)\,.$$

Тогда: $$n_1 = -1\,,$$

$$M_1 = (5+i)(-i)+(-1-2i) = -6-3i\,,$$

$$\xi_2 = (5+i)(3+2i)-(2+i) = 13+12i\,,$$

$$n_2 \equiv (5+2i)\cdot(13+12i)^{\varphi(2+3i)-1} (\mathrm{mod}\, 2+i)\,.$$

Переходя к действительным числам, получим:

$$\tilde{n}_2 \equiv 1\cdot(-1)^3 \equiv -1 \equiv 3(\mathrm{mod}\, 4)\,,$$

$$n_2 = -1\,.$$

Тогда:

$$M_2 = (5+i)(3+2i)(-1)+(-6-3i) = -21-16i\,.$$

Материалы данной статьи подготовлены и написаны при участии научного руководителя докт. техн. наук, профессора М.В. Синькова.

1. *Синьков М.В., Губарени Н.М.* Непозиционные представления в многомерных числовых системах. — К.: Наук. думка, 1979. — 138 с.

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

3. *Бояринова Ю.Е., Трубников П.В.* Расширение задачи разделения секрета для случая использования двойных чисел // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 1. — С. 47–52.

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

5. *Виноградов И.М.* Основы теории чисел. — М: Наука, 1972. — 168 с.

Поступила в редакцию 08.12.2004