УДК 515.171; 681.3.053

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

Расширение задачи разделения секрета для случая использования двойных чисел

Рассмотрена возможность использования двойных чисел для решения задачи разделения секрета.

Ключевые слова: *двойные числа, задача разделения секрета, изоморфизм, сравнение чисел, непозиционная система счисления.*

Задача разделения секрета существует давно. Одним из первых примитивных решений этой задачи можно назвать способ разделения на части какой-либо известной информации (лист документа, игральной карты). Последующее восстановление полной информации может быть достигнуто сложением частей полного объекта. Отсутствие любой части не дает полного сохранения секрета. Также известна задача разделения секрета, представленного в области действительных чисел, которая состоит в том, чтобы некий секрет C разделить так, чтобы можно было полностью восстановить исходное число. Просто разделение секрета на слагаемые не может дать хороших результатов. Поэтому одним из вариантов является представление секрета в виде совокупности остатков по модулям. Восстановление секрета по имеющимся остаточным представлениям осуществляется однозначно решением системы линейных сравнений, что известно как «китайская теорема» [1].

Мы предлагаем расширить постановку задачи разделения секрета, в частности, на случаи использования числовых систем второго порядка.

Рассмотрим множество чисел вида $a+bE$, где a, b — действительные числа, E — новый элемент. Введем на этом множестве две операции:

1) сложение

$$(a+bE)+(a_1+b_1E)=(a+a_1)+(b+b_1)E;$$

2) умножение

$$(a+bE)\cdot(a_1+b_1E)=(aa_1+pbb_1)+(ab_1+ba_1+qbb_1)E,$$

где $E^2 = p + qE,\ p, q$ — некоторые вещественные числа.

Это множество чисел с определенными выше операциями является двумерной алгеброй над полем действительных чисел. Каждой паре вещественных чисел (p, q) соответствует определенная алгебра $a_{p,q}$. Имеется только три различные алгебры второй степени над полем действительных чисел:

1) комплексные числа $a + bi,\ i^2 = -1\ (p = -1, q = 0)$;

2) дуальные числа $a + be,\ e^2 = 0\ (p = 0, q = 0)$;

3) двойные числа $a + be,\ e^2 = 1\ (p = 1, q = 0)$.

Ранее нами была представлена постановка задачи разделения секрета в комплексных числах [2]. Для комплексных чисел справедлива теория сравнения, можно построить систему остатков. Постановка задачи в таком виде усиливает сложность задачи, но и вычисления становятся более трудными. Однако, благодаря фундаментальной теореме Гаусса об изоморфизме, можно перейти из системы комплексных остатков к вещественным остаткам.

Эту процедуру можно усложнить, рассматривая не комплексные, а двойные числа.

Рассмотрим свойства двойных чисел [3]. Обозначим алгебру двойных чисел D, элемент e этой алгебры назовем двойной единицей.

В алгебре двойных чисел вводим операцию сопряжения, сопоставляя каждому элементу $A = a + be$ сопряженный элемент $\overline{A} = a - be$, для которого выполняются следующие основные свойства:

$$\overline{A + B} = \overline{A} + \overline{B};$$
$$\overline{A \cdot B} = \overline{A} \cdot \overline{B};$$
$$\overline{\overline{A}} = A.$$

Абсолютную величину квадратичной формы $\left|A \cdot \overline{A}\right| = \left|\overline{A} \cdot A\right| = \left|a^2 - b^2\right|$ назовем нормой двойного числа A и обозначим как

$$N(A) = \left|A \cdot \overline{A}\right| = \left|\overline{A} \cdot A\right| = \left|a^2 - b^2\right|.$$

Очевидно, что $N(A) \geq 0$ и $N(A + B) \leq N(A) - N(B)$. Доказано, что $N(A \cdot B) \leq$ $\leq N(A) \cdot N(B)$.

Если $A \neq 0$ и $N(A) \neq 0$, то существует обратный элемент

$$A^{-1} = \frac{\overline{A}}{a^2 - b^2},$$

причем $A \cdot A^{-1} = A^{-1} \cdot A = 1$.

Элементы $A \neq 0$, для которых $N(A) = 0$, не имеют обратных элементов и являются делителями нуля. Таким образом, $A = a + ae$ есть делитель нуля тогда и

только тогда, когда $|a| = |b|$, т.е. все делители нуля имеют вид $A = a + ae$ или $A = a - ae$.

Двойное число $A = a + be$ назовем целым, если a, b — целые вещественные числа.

Множество всех целых двойных чисел образует кольцо D_0. Целые двойные числа с нормой, равной единице, называются единицами кольца D_0. Будем говорить, что двойное число $A \in D_0$ делит двойное число $B \in D_0$, если существует целое двойное число $F \in D_0$, такое что $B = A \cdot F$. Это записывается как A / B.

Отношение делимости в кольце D_0 обладает такими свойствами:

1) $A/0,1/A, A/A$ для любого $A \in D_0$;

2) $0/A$ для любого $A \neq 0$;

3) из $A/B, B/F$ следует A/F;

4) из $A/B, A'/B'$ следует AA'/BB';

5) из AF/BF, $N(F) \neq 0$ и F не является делителем нуля, следует A/B;

6) из $A/B_i (i = 1...n)$ следует $A/\sum_{i=1}^{n} B_i F_i$ для любых целых двойных чисел $F_1 ... F_n$.

В кольце двойных чисел D_0 имеет место аналог алгоритма Евклида, поэтому справедливо, что для любых целых двойных чисел A и B ($B \neq 0$ и не является делителем нуля) существуют целые числа P и F такие, что $A = BP + F$, причем $N(F) < N(B)$.

Целые двойные числа, отличающиеся друг от друга множителем, равным делителю единицы, называются ассоциированными. Так, числами, ассоциированными с числом $A = a + be$, являются числа $ae + b$, $-ae - b$, $-a - be$. Делители единицы и все числа, ассоциированные с целым двойным числом A, называются тривиальными делителями A.

Целое двойное число A назовем составным, если существуют нетривиальные делители этого числа. Целое двойное число A называется простым, если не существует у него делителей, отличных от тривиальных.

Таким образом, целое двойное число A является простым тогда и только тогда, когда $N(A)$ — целое простое число.

Два целых двойных числа A и B называются взаимно простыми, если их нормы взаимно простые целые числа $(N(A), N(B)) = 1$, и существуют целые двойные числа u, v такие, что $Au + Bv = 1$.

Два целых двойных числа $A, B \in D_0$ назовем сравнимыми по модулю целого двойного числа M, если $M/(A - B)$, т.е. существует целое двойное число L такое, что $A - B = ML$.

Сравнение целых двойных чисел имеет следующие основные свойства:

1) если $A \equiv B (\mathrm{mod}\, M)$, то $B \equiv A (\mathrm{mod}\, M)$;

2) $A \equiv A (\mathrm{mod}\, M)$;

3) если $A \equiv B (\mathrm{mod}\, M)$, $B \equiv F (\mathrm{mod}\, M)$, то $A \equiv F (\mathrm{mod}\, M)$;

4) если $A \equiv B (\mathrm{mod}\, M)$, $F \in D_0$, то $AF \equiv BF (\mathrm{mod}\, M)$;

5) если $A \equiv B(\mathrm{mod}\, M)$, $P \equiv L(\mathrm{mod}\, M)$, то $A \pm P \equiv B \pm L(\mathrm{mod}\, M)$;

6) если $A \equiv B(\mathrm{mod}\, M)$, $P \equiv L(\mathrm{mod}\, M)$, то $A \cdot P \equiv B \cdot L(\mathrm{mod}\, M)$;

7) если $A_i \equiv B_i(\mathrm{mod}\, M)$ $(i = 1 \ldots n)$, то $A_1 A_2 \ldots A_n \equiv B_1 B_2 \ldots B_n(\mathrm{mod}\, M)$;

8) если $AX \equiv BX(\mathrm{mod}\, M)$ и $(M, X) = 1$, то $A \equiv B(\mathrm{mod}\, M)$.

Рассмотрим построение системы остаточных классов для двойных чисел.

Пусть $A = a + be$ — произвольное целое двойное число, $M = p + qe$ — модуль, причем $M \neq 0$ и не является делителем нуля, т.е. $p^2 - q^2 \neq 0$. Тогда

$$\frac{a+be}{p+qe} = \frac{(a+be)(p+qe)}{p^2-q^2} = \frac{ap-bq}{p^2-q^2} + \frac{bp-aq}{p^2-q^2}e.$$

Зададим некоторую полную систему вычетов по вещественному модулю $N(M)$.

Тогда имеем однозначное разложение

$$ap - bq = r + m_1 N;$$

$$bp - aq = r' + m_2 N,$$

где $r = [ap - bq](\mathrm{mod}\, N)$; $r = [bp - aq](\mathrm{mod}\, N)$.

В результате получаем

$$\frac{a+be}{p+qe} = [(m_1 + m_2 e)N + (r + r'e)]\frac{1}{p^2-q^2}$$

или

$$a + be = (r + r'e)\frac{p+q}{p^2-q^2} + (\tilde{m}_1 + \tilde{m}_2 e)(p + qe),$$

где $\tilde{m}_i = m_i (i = 1, 2)$, если $p^2 - q^2 > 0$, $\tilde{m}_i = -m_i (i = 1, 2)$, если $p^2 - q^2 < 0$, и это разложение определено однозначно.

Таким образом, если обозначить t как остаток от деления числа $A = a + be$ на $M = p + qe$, то справедлива формула

$$t = (r + r'e)\frac{M}{p^2-q^2},$$

из которой следует, что способ задания полной системы вычетов по двойному модулю $M = p + qe$ зависит от способа задания полной системы вычетов по вещественному модулю $N(M)$.

Если двойное число $A = a + be$ принадлежит полной системе вычетов по модулю двойного числа $M = p + qe$, то имеем тождество

$$a + be = (r + r'e)\frac{M}{p^2 - q^2},$$

так как в этом случае $t = a + be$.

Полную систему вычетов по модулю двойного числа A, определяемую формулой

$$t^+ = (r^+ + r'^+ e)\frac{M}{p^2 - q^2},$$

будем называть полной системой наименьших вычетов по модулю двойного числа M.

Полную систему вычетов по модулю двойного числа $M = p + qe$, определяемую формулой

$$t^- = (r^- + r'^- e)\frac{M}{p^2 - q^2},$$

будем называть полной системой абсолютно наименьших вычетов по модулю двойного числа.

Для двойных чисел справедливо развитие теоремы Гаусса об изоморфизме.

Теорема.

Пусть $M = p + qe$ — целое двойное число, причем $(p,q) = 1$ и $N(M) \neq 0$. Тогда существует взаимно однозначное соответствие между остатками любого двойного числа $A = a + be$ по модулю $M = p + qe$ и вычетами по модулю $N(M)$.

При этом изоморфное соответствие между полной системой вычетов по модулю $M = p + qe$ и полной системой вычетов по модулю $N = p^2 - q^2$ задается формулой

$$a + be \sim a + b\rho,$$

где $\rho = -(px - qy)$. Число ρ назовем коэффициентом изоморфизма.

Назовем двойное число $A = a + be$ представимым в системе S, если A является наименьшим вычетом по модулю *M*, в противном случае A не представимо в данной системе.

В системе с взаимно простыми основаниями $M_1, M_2 \ldots M_n$, где $m_i = p_i + q_i e$, $(p_i, q_i) = 1$ $(i = 1 \ldots n)$, любое представимое число $A = a + be$ единственным способом изображается набором чисел $(A_1, A_2 \ldots A_n)$, где A_i — наименьший вычет по модулю $M_i (i = 1 \ldots n)$.

Любое представимое двойное число $A = a + be$ в системе наименьших вычетов по основаниям взаимно простых чисел $M_1, M_2 \ldots M_n$ единственным образом представляется в виде совокупности целых чисел $\{K_1, K_2 \ldots K_n\}$, где K_i — наименьший вычет числа A по модулю $M_i (i = 1 \ldots n)$.

Таким образом, для числовой системы двойных чисел могут быть построены теоретико-числовые сравнения, правила выполнения алгебраических операций. Для двойных чисел сформулирован аналог фундаментальной теоремы Гаусса об изоморфизме в классах остаточных представлений в действительных и двойных числах. Это указывает на то, что для повышения производительности обработки информации можно осуществлять изоморфные переходы из двойных чисел в действительные и обратно.

Представление информации — секрета в двойных числах — может дать определенные преимущества при решении задачи разделения секрета в целом.

Статья была подготовлена под научным руководством доктора технических наук, профессора М.В.Синькова.

1. *Берник В., Матвеев С., Харин Ю.* Математические и компьютерные основы криптологии. — М.: Новое знание, 2003.

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. 90–97.

3. *Синьков М.В., Губарени Н.М.* Непозиционное представление в многомерных числовых системах. — К.: Наук. думка, 1979.

Поступила в редакцию 12.03.2004