УДК 681. 01

# АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ ОБРАТНОЙ МУЛЬТИПЛИКАТИВНОЙ ВЕЛИЧИНЫ ЧИСЛА В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

д.т.н., проф. В.А. Краснобаев

*Предлагаются алгоритмы реализации обратной мультипликативной величины числа в системе остаточных классов. С помощью рассмотренных алгоритмов можно реализовать непозиционные операции в классе вычетов. Рассмотрены конкретные примеры реализации разработанных алгоритмов.*

В данной статье рассматриваются два алгоритма реализации процесса нахождения обратной мультипликативной величины числа. Данные алгоритмы целесообразно использовать при определении непозиционных характеристик операндов в системе остаточных классов (СОК).

При обработке информации в системе остаточных классов возникает необходимость получить обратную мультипликативную величину $\mathbf{A^{-1}}$ числа $\mathbf{A}$ $\left(\text{т.е. } \mathbf{A \cdot A^{-1} = 1\ (mod\ M)}, \text{ где } \mathbf{M = \prod_{i=1}^{n} m_i}\right)$. Так, в частности, при реализации операции деления двух операндов $\mathbf{A_1}$ и $\mathbf{A_2}$ в СОК необходимо производить операцию модульного деления над остатками операндов, т.е. операцию вида

$$\mathbf{(a_{1i} / a_{2i})\ mod\ m_i},$$

где $\mathbf{A_1 = (a_{11}, a_{12}, \ldots, a_{1i}, \ldots, a_{1n})}$; $\mathbf{A_2 = (a_{21}, a_{22}, \ldots, a_{2i}, \ldots, a_{2n})}$; и $\mathbf{a_{1i} \equiv A_1 (mod\ m_i)}$; $\mathbf{a_{2i} \equiv A_2 (mod\ m_i)}$.

Один из методов определения частного $\mathbf{(A_1/A_2)\ mod\ M}$ заключается в замене операции деления на операцию умножения, где делитель $\mathbf{A_2}$ заменяется на сомножитель $\mathbf{A_2^{-1}}$; $\mathbf{C = A_1 / A_2 = A_1 \cdot (1 / A_2) = A_1\ A_2^{-1}}$, т.е. производится **n** операций типа из СОК в позиционную систему счисления и обратно. Действительно, определения $\mathbf{a_{1i} / a_{2i} = a_{1i} \cdot a_{2i}^{-1} (mod\ m_i)}$. Эта задача стоит и при реализации операции перевода чисел ортогональных базисов $\mathbf{\beta_i = (M/m_i)\overline{m}_i}$ в СОК и приводит к необходимости решения сравнения вида $\mathbf{\beta_i \equiv 1\ (mod\ m_i)}$ по весу $\mathbf{\overline{m}_i}$ ортогонального базиса, т.е. определения величины $\mathbf{(M/m_i)}$. Очевидно, что во всех вышеприведенных случаях возникает необходимость определения обратной мультипликативной величины числа [1].

Рассмотрим первый алгоритм определения величины $\mathbf{a_{2i}^{-1}}$. В соответствии с теоремой Ферма [2] имеем

$$a_{2i}^{m_i-1} \equiv 1(\mathrm{mod}\, m_i),$$

или

$$a_{2i}^{-1} \equiv a_{2i}^{m_i-2}(\mathrm{mod}\, m_i). \quad (1)$$

Выражение (1) есть формула для нахождения обратной мультипликативной величины числа при простом $m_i$. Пусть $m_i = 5$. Рассмотрим примеры определения частного, т.е. $(a_{1i}/a_{2i}) \bmod m_i$.

**Пример 1**. Пусть $a_{1i} = 3$, $a_{2i} = 4$. Необходимо определить значение 3/4.

В соответствии с выражением (1) определим значение $a_{2i}^{-1} = 4^3 = 4(\mathrm{mod}\, 5)$. Действительно: $a_{2i} \cdot a_{2i}^{-1} = 4 \cdot 4 = 1(\mathrm{mod}\, 5)$. Далее $a_{1i} / a_{2i} = a_{1i} \cdot a_{2i}^{-1} = 3 \cdot 4 = 2(\mathrm{mod}\, 5)$.

**Пример 2**. Пусть $a_{1i} = 4$, $a_{2i} = 3$. Необходимо определить значение 4/3.

Определим $a_{2i}^{-1} = 3^3 = 2(\mathrm{mod}\, 5)$. Найдем результат операции $a_{1i} / a_{2i} = a_{1i} \cdot a_{2i}^{-1} = 4 \cdot 2 = 3(\mathrm{mod}\, 5)$.

Проверим правильность полученных в примерах 1 и 2 результатов. Для этого перемножим полученные значения: **2 · 3 = 1 (mod 5)** или $\frac{3}{4} \cdot \frac{4}{3} \equiv 1(\mathrm{mod}\, 5)$.

**Пример 3**. Определим частное **C** от деления числа $A_{21}$ **= (1, 0, 1)** на число $B_7$ **= (1, 1, 2)** в СОК, заданной основаниями $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, т.е. найдем значение $C = A_{21}/B_7 (\mathrm{mod}\, M)$ для $A_{21} = 21$ и $B_7 = 7$ в ПСС. В соответствии с изложенным $C = A_{21} / B_7 = A_{21} \cdot B_7^{-1}$. Для операнда $B_7$ определим значение $B_7^{-1}$. На основании теоремы Ферма определим для числа $B_7^{-1}$ соответствующие остатки:

$$b_1^{-1} \equiv 1^0 \equiv 1(\mathrm{mod}\, 2); \quad b_2^{-1} \equiv 1 \equiv 1(\mathrm{mod}\, 3); \quad b_3^{-1} \equiv 2^3 \equiv 3(\mathrm{mod}\, 5),$$

т.е. $B_7^{-1} = (1, 1, 3)$. Значит, $C = A_{21}/B_7 = A_{21} \cdot B_7^{-1} = (1,0,1) \cdot (1,1,3) = (1,0,3)$.

**Проверка**. **21 : 7 = 3**, а значение **C = 3** определится в СОК в виде $C_3$ **= (1, 0, 3)**.

Второй алгоритм определения $a_{2i}^{-1}$ состоит в использовании теоремы Вильсона [3]:

$$(m_i - 1)! + 1 \equiv 0(\mathrm{mod}\, m_i). \quad (2)$$

Из выражения (2) получим:

$$(m_i - 1)! \equiv -1(\mathrm{mod}\, m_i); \quad (m_i - 1)! \equiv (m_i - 1) \bmod m_i; \quad (m_i - 2)! \equiv 1(\mathrm{mod}\, m_i);$$

$$a_{2i}^{-1} \equiv [1 \cdot 2 \ldots (a_{2i} - 1)(a_{2i} + 1) \ldots (m_i - 2)] \bmod m_i \ . \quad (3)$$

Используя выражение (3), для значений $2 \le a_{2i} \le m_i - 2$, можно по-

лучить формулу для определения величины

$$a_{2i}^{-1} \equiv \Big[ \underset{a_{2i}}{V}(m_i - 2)! \Big] \bmod m_i , \qquad (4)$$

где выражение $\underset{z}{V} k!$ будет обозначать произведение натуральных чисел от 1 до **k**, исключая число **z**. Определим конкретное значение $(m_i - 1)^{-1}$ . Пользуясь выражением (2) получим:

$$(m_i - 2)! = \left(-1/(m_i - 1)\right) \bmod m_i \quad . \qquad (5)$$

Выражение (5) можно также представить в виде

$$(m_i - 1)^{-1} = m_i - \Big[ \underset{m_i - 1}{V}(m_i - 1) \Big] !(\bmod m_i). \qquad (6)$$

**Пример 4**. Пусть $m_i = 5$, $a_{2i} = 4$. Необходимо определить $a_{2i}^{-1}$ . В соответствии с выражением (6)

$$a_{2i}^{-1} \equiv 5 - [3!] \bmod 5 \equiv 4 (\bmod 5)$$ (см. пример 1).

**Пример 5**. Пусть $m_i = 5$, $a_{2i} = 3$. Тогда, используя (4), получим:

$$a_{2i}^{-1} \equiv 1 \cdot 2 \equiv 2 (\bmod 5)$$ (см. пример 2).

Таким образом, предложенные алгоритмы определения обратной мультипликативной величины числа позволяют значительно упростить выполнение наиболее трудоемких (непозиционных) операций в СОК.

С точки зрения простоты технической реализации рекомендован первый алгоритм определения обратной мультипликативной величины числа, так как существует класс патентоспособных устройств (например, [4 - 6]), позволяющих эффективно решить задачу нахождения значений величин вида $a^{m_i - 2} (\bmod m_i)$.

## ЛИТЕРАТУРА


1. *Краснобаев В.А., Ирхин В.П., Квасов М.В. Вариант определения обратной мультипликативной величины числа в системе остаточных классов. – Х.: ХВВКИУ. – Тематический НТС № 427, 1992. – С. 94 - 96.*
2. *Виноградов М. Основы теории чисел. – М.: Наука, 1981. – 176 с.*
3. *Долгов В.І., Лисицька І.В. Конспект лекцій з дисципліни "Спеціальні розділи математики". Теорія чисел. – Х.: ХТУРЕ, 2000. – 124 с.*
4. *А.с. № 1160397 СССР. Устройство для возведения чисел в степень по модулю / В.А. Краснобаев, А.Ю. Семенов. Опубл. в БИ. 1985. № 21.*
5. *А.с. № 1509903 СССР. Устройство для свертки по произвольному модулю / В.А. Краснобаев, Г.М. Чигасов, В.Д. Экста и др. Опубл. в БИ. 1989. № 35*
6. *А.с. № 1594541 СССР. Устройство для свертки чисел по модулю / В.А. Краснобаев, Л.С. Сорока, С.А. Чепига . Опубл. в БИ. 1990. №35.*


*Поступила 8.07.2002*

***КРАСНОБАЕВ Виктор Анатольевич**, доктор техн. наук, профессор, профессор кафедры автоматизации и компьютерных технологий Харьковского ГТУСХ. В 1973 году окончил ХВВКИУ. Область научных интересов – АСУ, компьютерные технологии.*