УДК 681.3

А.К. ТУМАНЯН, А.А. АМАЗАСПЯН, А.А. КОСТАНЯН

ВЫПОЛНЕНИЕ ОПЕРАЦИЙ УМНОЖЕНИЯ И ДЕЛЕНИЯ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Предлагаются структура и алгоритм выполнения модулярного умножения, основанного на коррекции суммы частичных произведений и множимого в каждом такте умножения. Разработаны алгоритм перехода от представления числа в системе остаточных классов в позиционную систему и схема реализации операции деления с остатком.

Ключевые слова: модулярное умножение, модулярное деление, система остаточных классов, Китайская теорема об остатках.

В последнее время вновь повысился интерес к представлению числовой информации в системе остаточных классов (СОК).

Для любой системы взаимно простых чисел $p_1, \ldots, p_n$ любое число X из диапазона [0:M-1], где $M = p_1*p_2*\ldots*p_n$, взаимно однозначно представимо в виде вектора $(x_1, x_2, \ldots, x_n)$, где $x_i = X \bmod p_i$, $x_1, x_2, \ldots, x_n$ – остатки (вычеты) числа по заданной системе модулей.

Выполнение операции умножения. В статье предлагается умножение по модулю, в основе которого лежит алгоритм двоичного умножения со сдвигом множителя вправо и множимого влево на один разряд в каждом такте умножения.

Вычисление произведения производится в соответствии с формулой

$$A\cdot B= (\ldots(((0+A\cdot b_0)+2A\bmod p\cdot b_1)\bmod p+2^2\cdot A\bmod p\cdot b_2)\bmod p+\ldots+ +2^{n-1}\cdot A\bmod p\cdot b_{n-1})\bmod p.$$

На вход схемы умножения, структура которой приведена на рис.1, подаются числа Amodp и Bmodp.

Компаратор Cmp1 производит сравнение acc (суммы частичных произведений) с модулем p (rp), компаратор Cmp2 сравнивает ra с p.

В предлагаемом алгоритме после каждого такта умножения анализируется выход компаратора CMP2. Если содержимое ra превышает rp, то производится коррекция сдвигаемого влево множимого (ra=ra-rp). Коррекция суммы частичных произведений необходима только тогда, когда значение анализируемого разряда множителя равно единице. При этом анализируется выход компаратора CMP1. Если сумма частичных произведений (acc) превышает rp, то из аккумулятора вычитается rp.

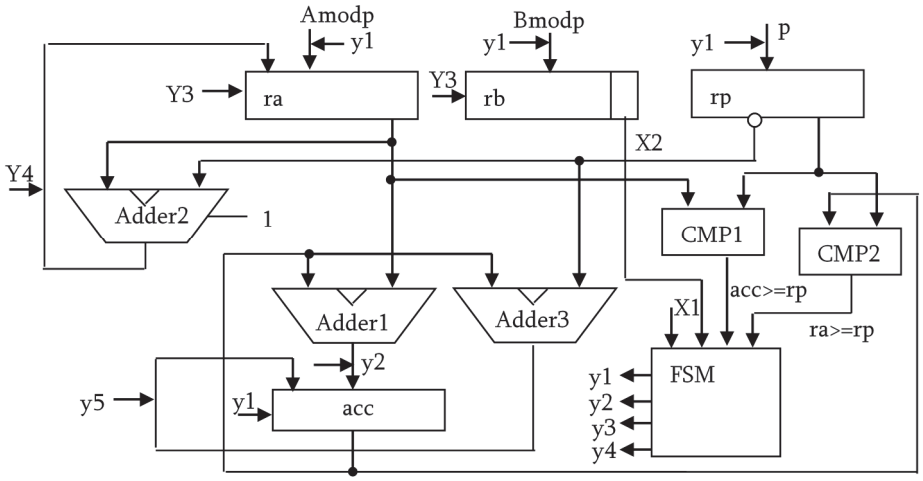

Рис. 1. Структура блока модулярного умножения

Одним из достоинств использования СОК является возможность параллельного выполнения операции над различными модулями. Модули умножения, в свою очередь, будут быстродействующими из-за небольшого количества разрядов устройств, так как в качестве модулей обычно выбираются взаимно простые числа небольшой величины.

Схема устройства в системе остаточных классов p1, p2, p3 представлена на рис. 2.

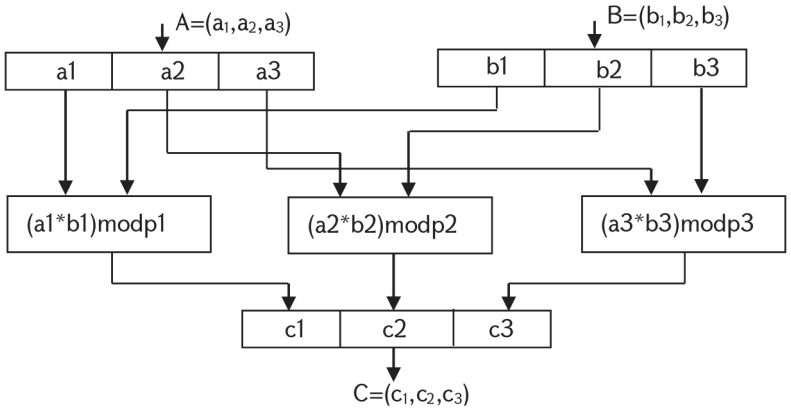

Рис. 2. Структура устройства умножения в СОК с модулями p1, p2, p3

Устройство состоит из трех блоков умножения по modp.

На вход устройства поступают числа A = (a_1,a_2,a_3) и B=(b_1,b_2,b_3). Результат умножения C = A*B = (c_1,c_2,c_3), где a1= Amodp1, a2= Amodp2, a3= Amodp3; b1= Bmodp1, b2= Bmodp2, b3= Bmodp3; c1= Cmodp1,c2= Cmodp2, c3= Cmodp3.

На вход i-го блока умножения поступают операнды ai и bi. Множительные блоки по modp работают параллельно.

Блок-схема алгоритма умножения в СОК с модулями p1, p2, p3 представлена на рис. 3.

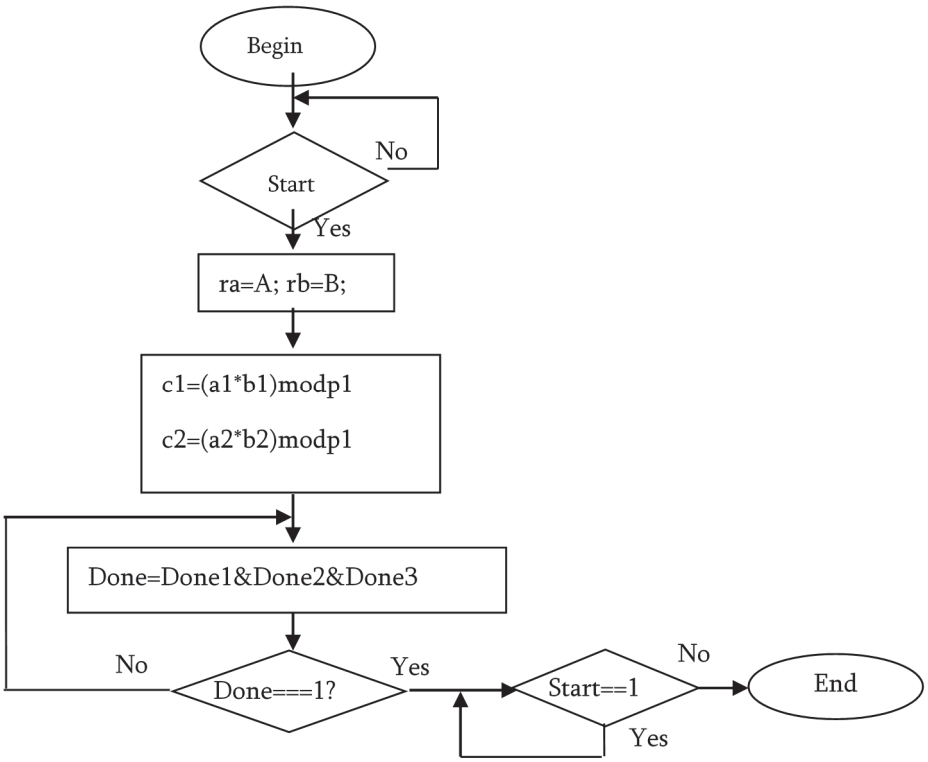

Рис. 3. Блок-схема алгоритма умножения в СОК

Пусть p1= 11, p2= 13, p3=17. Максимальное число, представимое в данной системе, будет равно 2431-1. Диапазон чисел будет [0 : 2430].

Преимущество предлагаемого блока модулярного умножения перед индексным умножением состоит в том, что данный метод не требует предварительного вычисления значений индексов и не использует специальных таблиц для их хранения.

Процесс умножения по данному алгоритму заканчивается, когда в регистре множителя окажется 0. Выход из процедуры умножения происходит после завершения операции во всех модулярных блоках.

Для ускорения операции умножения можно использовать следующий прием: произвести сравнение операндов, и если множитель существенно отличается от множимого, поменять их местами.

Выполнение операции деления с нулевым остатком. Деление может быть выполнено аналогично умножению, но только если делитель делит делимое нацело, без остатка.

Условия, необходимые для выполнения операции: делимое представляет собой число, кратное делителю, делитель и модуль р являются взаимно простыми.

Обозначим A/B=C. Заменяем операцию деления умножением: A× (1/B)= = C. (A× (1/B)mod p1 = Amodp1×(1/B)mod p1.

Пусть задана система модулей (7,11,17). Произведем операцию деления в заданной СОК - разделим число A=1377 на B=9 (остаток равен 0). A=(5, 2, 0); B=(2, 9, 9); C= (c_1,c_2,c_3). $c_i=(a_i\times(1/b_i))$ mod p_i..

$1/b_i$ – элемент, обратный b_i в поле по mod p_i (обозначим b_i^{-1}).

$(b_i\times b_i^{-1})$modp_i =1. Применив формулу (bi^{pi-1}) mod p_i=1 (малая теорема Ферма), получаем (bi^{pi-1})mod p_i= $(b_i\times b_i^{-1})$mod p_i. Следовательно, (b_i^{pi-2})mod pi=b_i^{-1}.

b_1^{-1} =(2^{7-2})mod 7=4; b_2^{-1} =(9^{11-2})mod 11=5; b_3^{-1}= (9^{17-2}) mod17=2. Отсюда $c_1=(a_1\times b_1^{-1})$modp1=(5×4)mod7=6, $c_2=(a_2\times b_2^{-1})$mod p2=(2×5)mod11=10, $c_1=(a_3\times b_3^{-1})$mod p3=(0×2)mod7=0. Результатом деления для заданного примера будет C=(6,10,0).

Для получения результата в позиционной системе счисления (обратное преобразование) применим Китайскую теорему об остатках, на которой базируется модулярная арифметика. Задано число X=(x_1, x_2, …, x_n), где x_1, x_2, …, x_n – остатки (вычеты) числа по заданной системе модулей.

Способ, основанный на Китайской теореме об остатках, базируется на следующем представлении X = (x_1, x_2, … x_n) = (x_1, 0, …, 0) + (0, x_2, …, 0) + … + (0, 0, …., x_n) = x_1*(1, 0, …, 0) + x_2*(0, 1, …, 0) + … + x_n*(0, 0, …, 1).

Для обратного преобразования требуется найти систему ортогональных базисов B1=(1, 0, …, 0), B2=(0, 1, …, 0), …, BN=(0, 0, …, 1).

Для определения базиса B_i требуется решить уравнение вида

(M_i*d_i)modp_i = 1, где M_i = M/p_i, а d_i – искомое число. В этом случае

$B_i = M_i*d_i$ и X = (x_1*(M_1*d_1) + x_2*(M_2*d_2) + … + x_n*(M_n*d_n)) modM.

Переведем полученный выше результат деления C= (6,10,0) из СОК в двоичную систему.

Задана система модулей (7, 11, 17), найдем значения M_i и d_i ($0 < i <= 3$);

$$M=7\times11\times17;\ M_3=11\times7;\ M_2=17\times7;\ M_1=17\times11.$$

Определим коэффициенты d_1, d_2, d_3.

$$(77\times d_3)\text{mod}17=1;\Rightarrow d_3=2;\ (17\times7\times d_2)\text{mod}11=1;\Rightarrow d_2=5;$$

$$(17\times11\times d_1)\text{mod}7=1;\ \Rightarrow d_1=3;$$

$$C=(c_1(M_1\times d_1)+c_2(M_2\times d_2)+c_3(M_3\times d_3))\text{mod}M=(6\times187\times3+10\times119\times5)\text{mod}1309=153.$$

Операция деления без остатка имеет ограниченную область использования, поскольку должно быть заранее известно, удовлетворены ли условия, необходимые для осуществления операции [Л1].

Деление для случая, когда остаток не равен нулю. В общем случае операции целочисленного деления соответствует следующее выражение: A=B×C +R, где A и B - делимое и делитель соответственно, а R – остаток.

Для реализации немодульных операций, к числу которых относится операция деления, используются блоки немодульной арифметики [Л2].

Для этого требуется разработать блок, осуществляющий переход из СОК в позиционную систему и обратный переход.

Предлагаемая в данной работе структурная схема устройства приведена на рис. 4.

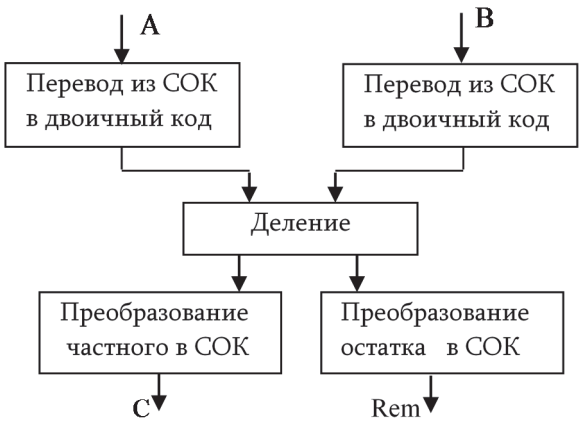

Рис. 4. Структура устройства деления

На рис. 5 приведена блок-схема алгоритма перевода из СОК в позиционную систему с числом модулей n. Вычисление коэффициентов производится на основании формулы $(M_i\times d_i)\text{mod}p_i=1$.

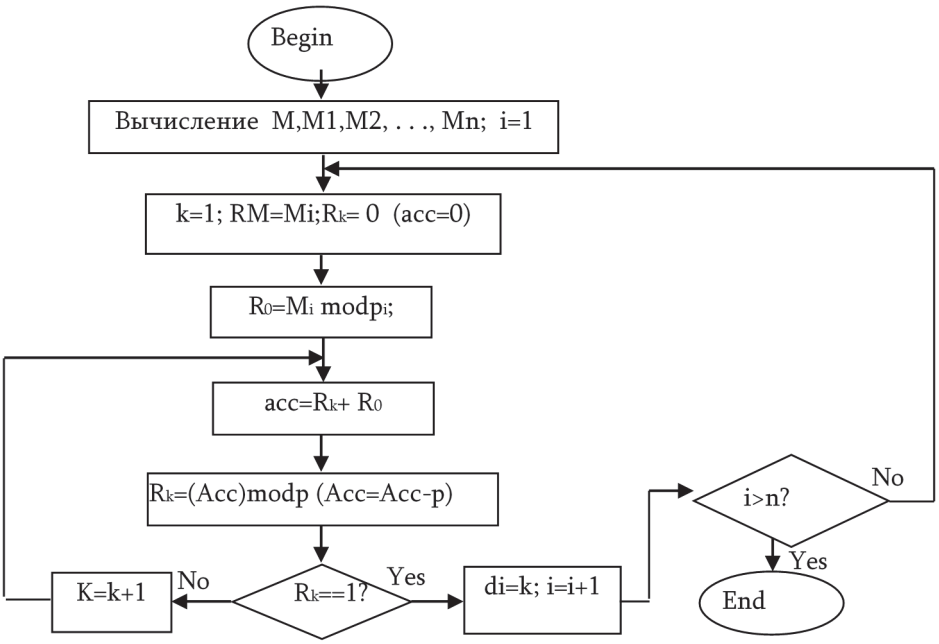

Рис. 5. Блок-схема алгоритма определения коэффициентов d

Предлагается итерационный алгоритм формирования коэффициентов d. На каждом шаге (итерации) к содержимому аккумулятора добавляется R_0. Определяется R_k=(acc)modp_i. Формирование R_k заканчивается на итерации, которой соответствует R_k, равное 1. Следовательно, коэффициент d_i=k. Внешний цикл по переменной i может отсутствовать, если коэффициенты $d_1, d_2, \ldots, d_n$ формируются параллельно n блоками.

На рис. 6 приведена схема блока формирования коэффициента d.

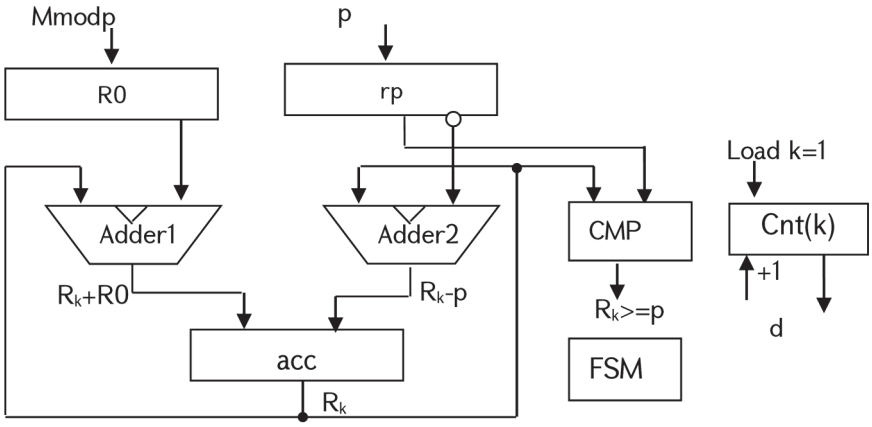

Рис. 6. Структура блока формирования коэффициентов d

Выводы

К достоинствам предложенных реализаций можно отнести следующее:

- малая сложность схем умножения, так как модули p1, p2, … имеют небольшую величину (по сравнению с индексным методом и методом квадратов);
- высокое быстродействие (параллельные вычисления остатков);
- раннее завершение операций (как следствие, повышение быстродействия и уменьшение потребления энергии).

К числу недостатков следует отнести следующее:

- необходимость преобразования в позиционную систему и обратное преобразование при выполнении операции деления;
- наличие блоков немодульных операций (например, деление).

Следует отметить, что в настоящее время модулярная арифметика применяется в следующих областях: цифровая обработка сигналов, криптография, аудио- и видеообработка. Во всех этих применениях широко используются операции сложения и умножения векторов, скалярное произведение векторов (как пример, умножение матриц, скалярное произведение векторов, преобразование Фурье). Операция деления применяется редко.

СПИСОК ЛИТЕРАТУРЫ

1. Метод деления на двоичную экспоненту для преобразования минимально избыточного модулярного кода в позиционный код /**А.А. Коляда, П.В. Кучинский, Н.И. Червяков** и др. // Инфокоммуникационные технологии.-2014.- Том 12, № 3.
2. **Амербаев В.М., Тельпухов Д.В., Балака Е.С., Константинов А.В.** Реализация обратного преобразователя модулярной арифметики, совмещенного с операцией округления для задач ЦОС". МЭС-2012, ИППМ РАН, Nofrost@inbox.ru.

Ա.Կ. ԹՈՒՄԱՆՅԱՆ, Ա.Հ. ՀԱՄԱԶԱՍՊՅԱՆ, Ա.Հ. ԿՈՍՏԱՆՅԱՆ

ԲԱԶՄԱՊԱՏԿՄԱՆ ԵՎ ԲԱԺԱՆՄԱՆ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐԻ ԻՐԱԳՈՐԾՈՒՄԸ ՄՆԱՑՈՐԴԱՅԻՆ ԴԱՍԵՐԻ ՀԱՄԱԿԱՐԳՈՒՄ

Ներկայացված են մոդուլյար բազմապատկման իրագործման կառուցվածքը և ալգորիթմը, որոնք հիմնված են բազմապատկման յուրաքանչյուր փուլում մասնակի արտադրյալների գումարի և բազմապատկելիների ճշգրտման վրա: Մշակված են մնացորդային դասերի համակարգում ներկայացված թվերի դիրքային համակարգ անցման ալգորիթմը և մնացորդով բաժանման գործողության իրագործման սխեման:

Առանցքային բառեր. մոդուլյար բազմապատկում, մոդուլյար բաժանում, մնացորդային դասերի համակարգ, մնացորդների վերաբերյալ չինական թեորեմ:

A.K. TUMANYAN, A.H. HAMAZASPYAN, A.H. KOSTANYAN

IMPLEMENTATION OF MULTIPLICATION AND DIVISION OPERATIONS IN THE RESIDUE NUMBER SYSTEM

A structure and an algorithm of modular multiplication based on correction of the sum of partial products and multiplicand in each cycle of multiplication are proposed. The algorithm of transition from the representation of the number in the RNS in the positional system and the division operation with the remainder scheme are also developed.

Keywords: modular multiplication, residue number system, modular division, Chinese remainder theorem.

ՀՏԴ 004.451.3

Լ.Գ. ԿԻՐԱԿՈՍՅԱՆ

ՏՎՅԱԼՆԵՐԻ ՕԲՅԵԿՏԱՅԻՆ ՊԱՀՊԱՆՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՈՒՍՈՒՄՆԱՍԻՐՈՒԹՅՈՒՆ ԵՎ ԸՆՏՐՈՒԹՅՈՒՆ

Տվյալների կառավարումն առաջնային դեր ունի ամպի շահագործման ժամանակ: Հիշողությունը պետք է ոչ միայն լինի հուսալի և անվտանգ, այլև ունենա ընդլայնման հնարավորություն՝ չխաթարելով նախնական կառուցվածքը: Մեծածավալ տվյալների պահեստավորման, գրանցման/ընթերցման համակարգը պետք է հնարավորություն ունենա իր առջև դրված գործողություններն իրագործել արագ և առանց ընդհատումների: Վերլուծված են տվյալների պահպանման համակարգերը՝ Հայաստանի ազգային պոլիտեխնիկական համալսարանում ստեղծվող ամպային համակարգում կիրառելու տեսանկյունից:

Առանցքային բառեր. տվյալներ, տվյալների ընդլայնում, կառավարում, ceph, glusterfs, ֆայլային համակարգ:

Տվյալների օբյեկտային պահպանման համակարգեր: Տվյալների պահպանման ավանդական լուծումները չեն կարող ապահովել անհրաժեշտ հուսալիություն՝ ու անվտանգություն դրանք կիրառող համակարգերի թե՛ ծավալային, թե՛ սկզբունքային առանձնահատկություններից ելնելով: Տվյալների օբյեկտային պահպանման համակարգերն արդեն ծանոթ ֆայլային համակարգերից տարբերվում են նրանով, որ տվյալները պահպանում են որպես օբյեկտներ [1], ի տարբերություն ֆայլային համակարգերի, որտեղ այն գրանցվում է բլոկների մեջ [2]: Յուրաքանչյուր օբյեկտ պարունակում է տվյալ և նույնականացնող հատուկ համար: Տվյալների օբյեկտային պահպանման համակարգը կարող է կիրառվել մի շարք մակարդակներում, ինչպիսիք են, օրինակ՝ համակարգային կամ ինտերֆեյսային մակարդակները: Յուրաքանչյուր դեպքում համակարգի նպատակն է տրամադրել նոր միջոցներ, որոնք ֆայլային համակարգերն ընդունակ չեն տրա-