(19) **RU** (11) **2 029 434** (13) **C1**

(51) МПК[6] **H 03 M 7/18**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: **4888770/24, 05.12.1990**

(46) Дата публикации: **20.02.1995**

(56) Ссылки: **Авторское свидетельство СССР N 1105895, кл. G 06F 11/08, 1983.Авторское свидетельство СССР N 1658388, кл. H 03M 7/18, 1991.**

(71) Заявитель:
Петренко Вячеслав Иванович,
Чипига Александр Федорович

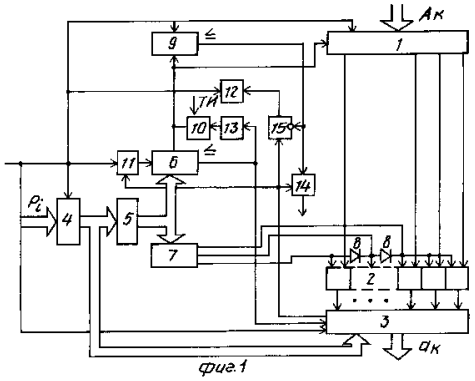
(72) Изобретатель: **Петренко Вячеслав Иванович,**
Чипига Александр Федорович

(73) Патентообладатель:
Петренко Вячеслав Иванович,
Чипига Александр Федорович

(54) УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ ОТ ЧИСЛА

(57) Реферат:

Изобретение относится к вычислительной технике и предназначено для использования в цифровых вычислительных устройствах, а также в устройствах для формирования конечных полей. Цель изобретения - повышение быстродействия формирования остатка - достигается введением элементов И2, группы, накапливающего сумматора 3 по модулю, дешифраторов 5, 7, счетчика 6, ключевых элементов 8, триггера 13 и элемента 15 запрета. Сущность изобретения заключается в том, что число A (начиная с младшего разряда) в зависимости от величины модуля P_i разбивается на числа, длина которых равна периоду повторения остатков от чисел 2^i, $i = \overline{0,n}$, и последовательному суммированию по модулю p_i этих чисел. 1 з.п.ф-лы, 2 ил.



фиг.1

RU 2029434 C1

RU 2029434 C1

(19) **RU** (11) **2 029 434** (13) **C1**

(51) Int. Cl.[6] **H 03 M 7/18**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 4888770/24, 05.12.1990

(46) Date of publication: 20.02.1995

(71) Applicant:
Petrenko Vjacheslav Ivanovich,
Chipiga Aleksandr Fedorovich

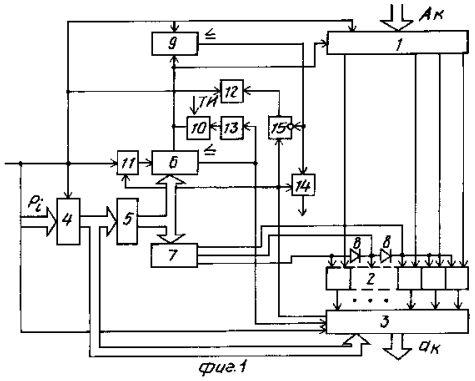
(72) Inventor: Petrenko Vjacheslav Ivanovich,
Chipiga Aleksandr Fedorovich

(73) Proprietor:
Petrenko Vjacheslav Ivanovich,
Chipiga Aleksandr Fedorovich

(54) DEVICE FOR FORMATION OF REMAINDER BY ARBITRARY MODULUS OF NUMBER

(57) Abstract:

FIELD: computer engineering. SUBSTANCE: increased speed of action of formation of remainder is achieved by insertion of group of AND 2 gates, accumulator 3 by modulus, decoders 5, 7, counter 6, key elements 8, flip-flip 13 and inhibition gate 15. Essence of invention lies in that number A (starting from less significant position) is divided depending on value modulus P_i into numbers which length is equal to period of repetition of remainders of numbers z^i, $i = \overline{0,n}$, and successive summing of these numbers by modulus p_i. EFFECT: increased speed of action of device. 2 cl, 2 dwg



фиг.1

RU 2029434 C1

RU 2029434 C1

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах для формирования элементов конечных полей.

Цель изобретения - повышение быстродействия формирования остатка.

Сущность изобретения состоит в реализации следующего алгоритма приведения чисел по произвольному модулю.

Если любое целое число A представить в двоичном виде:

$A = a_n 2^n + \ldots + a_1 2^1 + a_0 2^0$, где $a_i (i = \overline{0,n})$ - символы двоичных разрядов числа A;

$2^i (i = \overline{0,n})$ - веса разрядов числа A, то последовательность чисел $r_i (i = \overline{0,n})$ являющихся остатками по любому модулю P от соответствующих весов 2^i, $i = \overline{0,n}$, разрядов числа A, всегда имеют некоторый период $r_j (j = \overline{0,k})$, где $k < P$.

Из теории чисел известно что основание весов разрядов числа A - число 2 является элементом любого простого поля GF(P).

Как следует из общеизвестной теории Ферма, для любого элемента b поля GF(P) всегда существует такой наименьший положительный показатель степени q, что $b^q \equiv 1 (\mathrm{mod}\ P)$, при этом $q_{макс} = P-1$. Следовательно, степени $b^0, b^1, \ldots, b^{q-1}$ различны. Отсюда $2^q \equiv 1 (\mathrm{mod}\ P)$ и веса разрядов числа A: $2^i (\mathrm{mod} P)$, $i = \overline{1,q-1}$, различны, т.е. остатки r_j, $j = \overline{0,k}$, по модулю P различны. Таким образом, последовательность числа r_i, $i = \overline{0,n}$, имеет период повторения $r_0, r_1, \ldots, r_k$.

Очевидно, что если количество разрядов двоичного представления числа A (начиная с младшего разряда) разбить на числа с длительностью периода повторения r_j, $j = \overline{0,k}$, для заданного модуля P, дополнив нулями в старших разрядах до целого k+1, а затем просуммировать образовавшиеся кодовые комбинации по заданному модулю P, то для другого модуля P_1 изменится период r_j, $j = \overline{0,m}$ Следовательно, для каждого модуля P_i, с которым предполагается работа устройства, необходимо знать период повторения остатков от чисел r^i, $i = \overline{0,k}$, который не превышает величины модуля. Этот период может быть предварительно вычислен и зашит в ПЗУ или в дешифраторе. При этом процесс формирования остатка сводится к суммированию определенного числа разрядов входного числа A, а количество этих разрядов зависит от величины модуля P.

На фиг. 1 представлена функциональная схема устройства для формирования остатка по произвольному модулю от числа; на фиг. 2 - функциональная схема накапливающего сумматора по модулю.

Устройство (фиг. 1) содержит первый регистр 1, n элементов И 2 группы, накапливающий сумматор 3 по модулю, второй регистр 4, первый дешифратор 5, счетчик 6, второй дешифратор 7, n-1 ключевых элементов 8, счетчик 9, элемент И 10, элементы ИЛИ 11, 12, триггер 13, элемент И 14, элемент 15 запрета.

Накапливающий сумматор 3 по модулю (фиг.2) содержит комбинационный сумматор 16, мультиплексор 17, регистр 18 и элемент 19 сравнения, вычислитель 20, элементы ИЛИ 21, 22, элементы 23, 24 задержки.

Накапливающий сумматор 3 по модулю обеспечивает сложение по модулю частей числа A, величина которых, начиная с младших разрядов, равна периоду совпадения значений остатков от чисел 2^k при представлении числа A в позиционной системе счисления, где k - разрядность представляемого числа.

Счетчик 6 обеспечивает подсчет тактовых сдвигающих импульсов, подаваемых на вход первого регистра.

Дешифратор 5 обеспечивает преобразование кода модуля в код числа разрядов, равного периоду совпадения значений остатков от чисел 2^k при представлении числа A в позиционной системе счисления. Дешифратор 7 обеспечивает преобразование кода числа разрядов в десятичный код.

Элементы И 2 группы обеспечивают подключение информационных выходов первого регистра к информационным входам накапливающего сумматора по модулю.

Ключевые элементы 8 обеспечивают подключение числа информационных выходов первого регистра, равного периоду совпадения значений остатков от чисел 2^k при представлении числа A в позиционной системе счисления.

Триггер 13 обеспечивает режим подачи и отключения тактовых импульсов, необходимый для нормального функционирования устройства.

Запись информации в счетчик 6 производится обратным фронтом управляющего импульса.

Устройство для формирования остатка по произвольному модулю от числа работает следующим образом.

В исходном состоянии все регистры и счетчики обнулены. Триггер 13 находится в нулевом состоянии. Модуль P_i, по которому осуществляется формирование остатков чисел, задается параллельным двоичным кодом, подаваемым на входы регистра 4. На входы регистра 1 поступает число A_k в параллельном двоичном коде. После подачи кодов числа и модуля на входы устройства на вход начала вычисления подают импульс, который, поступая на входы записи регистров 1 и 4, осуществляет запись кодов числа A_k и модуля P_i. Одновременно этот импульс поступает на вход записи счетчика 9, чем обеспечивается запись в него в двоичном коде числа, равного количеству разрядов регистра 1. Импульс начала вычисления поступает также через элемент ИЛИ 11 на вход записи счетчика 6, через элемент ИЛИ 12 на вход триггера 13 и на второй управляющий вход накапливающего сумматора 3 по модулю.

Как только код модуля P_i записан в регистр 4, информация с его выхода поступает на вход дешифратора 5, который преобразует код модуля в код числа

RU 2029434 C1

RU 2029434 C1

разрядов, равный периоду совпадения значений остатков от чисел 2^k при представлении числа А в позиционной системе счисления. Код числа разрядов поступает на входы счетчика 6 и обратным фронтом импульса с выхода элемента ИЛИ 11 записывается в ячейки памяти счетчика 6. В двоично-десятичном дешифраторе 7 код числа разрядов преобразуется в десятичную форму, в результате чего на одном из его выходов появляется единичный потенциал, который, поступая через ключевые элементы 8 на объединенные входы элементов И 2 группы, обеспечивает подключение младших разрядов регистра 1 к информационным входам второй группы накапливающего сумматора 3 по модулю, причем число подключаемых разрядов равно периоду совпадения значений остатков от чисел 2^k при представлении числа А в позиционной системе счисления.

В накапливающем сумматоре 3 по модулю (фиг.2) код младших разрядов через комбинационный сумматор 16 и мультиплексор 17 поступает на входы регистра 18. Одновременно с выхода элемента 24 задержки (величина задержки которого равна времени записи информации в регистр 1 и времени переходных процессов в элементах И 2 группы, сумматоре 16 и мультиплексоре 17) через элемент ИЛИ 22 на вход записи регистра 18 поступает импульс записи, чем обеспечивается запись в него кода младших разрядов числа A_k.

Таким образом, приход импульса начала вычисления обеспечивает запись кода числа A_k в регистр 1, кода модуля P_i в регистр 4, кода числа разрядов регистра 1 в счетчик 9, кода периода совпадения значений остатков в счетчик 6 и младших разрядов A_i, равных периоду совпадения значений остатков, в регистр 18 накапливающего сумматора 3 по модулю.

Обратным фронтом импульса с выхода элемента ИЛИ 12 триггер 13 переводится в единичное состояние. При этом на его выходе появляется единичный потенциал, который поступает на первый вход элемента И 10. Этим обеспечивается прохождение тактовых импульсов с выхода элемента И 10 на вычитающие входы счетчиков 6 и 9 и сдвигающий вход регистра 1. При этом в регистре 1 с приходом каждого тактового импульса осуществляется сдвиг информации вправо на один разряд, а в счетчиках 6 и 9 - уменьшение их содержимого на единицу. В таком режиме устройство работает до тех пор, пока счетчик 6 не обнулится. При этом на его выходе обнуления появляется единичный импульс, который поступает на вход триггера 13 и первый управляющий вход накапливающего сумматора 3 по модулю. Под воздействием этого импульса триггер 13 переводится в нулевое состояние и прохождение тактовых импульсов через элемент И 10 прекращается.

Так как в регистре 1 происходит сдвиг информации вправо на величину периода совпадения значения остатков чисел 2^k при представлении числа А в позиционной системе счисления, то на первые входы комбинационного сумматора 16 поступает следующая информационная часть числа A_k, которая записана теперь в младших разрядах регистра 1, а на вторые его входы с выхода регистра 18 поступает информационная часть младших разрядов числа A_k. Результат суммирования в параллельном коде через мультиплексор 17 поступает на информационные входы регистра 18. Поступление единичного потенциала с первого управляющего входа накапливающего сумматора по модулю через второй вход элемента ИЛИ 22 на вход разрешения записи регистра 18 обеспечивает запись результата суммирования в последний. Код результата суммирования поступает на первые входы элемента 19 сравнения и входы уменьшаемого вычитателя 20. Так как на входы вычитаемого вычитателя поступает код модуля P_i с выхода регистра 4, то с выходов вычитателя 20 на вторые входы мультиплексора 17 поступает код разности результатов суммирования и модуля.

Через время задержки, равное времени записи информации в регистр 18, с выхода элемента 23 задержки на вход разрешения элемента 19 сравнения поступает единичный потенциал, который разрешает сравнение кода результата суммирования и кода модуля P_i. При этом возможно три варианта. Если код результата суммирования, записанный в регистре 18, меньше кода модуля P_i, то на выходе "Меньше" элемента 19 сравнения появляется единичный потенциал, который через элемент ИЛИ 21 поступит на управляющий выход накапливающего сумматора 3 по модулю.

Если код результата суммирования, записанный в регистре 18, равен коду модуля P_i, то на выходе "Равно" элемента 19 сравнения появляется единичный потенциал, который, поступая на вход обнуления регистра 18, обнуляет его и через третий вход элемента ИЛИ 21 поступает на управляющий вход накапливающего сумматора 3 по модулю.

Если код результата суммирования, записанный в регистре 18, больше кода модуля P_i, то на выходе "Больше" элемента 19 сравнения появляется единичный потенциал, который, поступая на управляющий вход мультиплексора 17, осуществляет подключение выходов вычитателя 20 к входам регистра 18, а поступая через первый вход элемента ИЛИ 22 на вход разрешения записи регистра 18, осуществляя в последний запись кода разности результата суммирования и кода модуля P_i. Одновременно единичный потенциал через первый вход элемента ИЛИ 21 поступает на управляющий выход накапливающего сумматора 3 по модулю.

Единичный потенциал с управляющего выхода накапливающего сумматора по модулю поступает на второй вход элемента ИЛИ 11, информационный вход элемента запрета и второй вход элемента И 14.

Единичный сигнал, поступая с выхода элемента ИЛИ 11 на вход записи счетчика 6, обеспечивает запись в него кода числа разрядов, поступающего с выхода дешифратора 5.

Единичный потенциал с выхода элемента 15 запрета через элемент ИЛИ 12 поступает на вход триггера 13, чем обеспечивает перевод последнего в единичное состояние.

RU 2029434 C1

RU 2029434 C1

Единичный потенциал, поступая на второй вход элемента И 14, на его выход не поступает, так как на первом его входе присутствует нулевой потенциал, поступающий с выхода обнуления счетчика 9.

Начнется новый цикл поступления тактовых импульсов через второй вход элемента И 10 на вычитающие входы счетчиков 6 и 9 и сдвигающий вход регистра 1.

Работа устройства в таком режиме происходит до тех пор, пока счетчик 9 не обнулится. В этом случае на его выходе появляется единичный потенциал, который поступает на первый вход элемента И 14 и на вход элемента 15 запрета, закрывая прохождение информации. Поэтому очередной сигнал, поступивший с управляющего выхода накапливающего сумматора 3 по модулю, через элемент 15 запрета не проходит, а поступает на выход элемента И 14, сигнализируя об окончании процесса формирования остатка.

В таком состоянии устройство находится до тех пор, пока на его входы не поступят коды новых чисел A_i и P_i, а на вход начала вычисления - импульс записи. В этом случае устройство работает аналогично описанному выше.

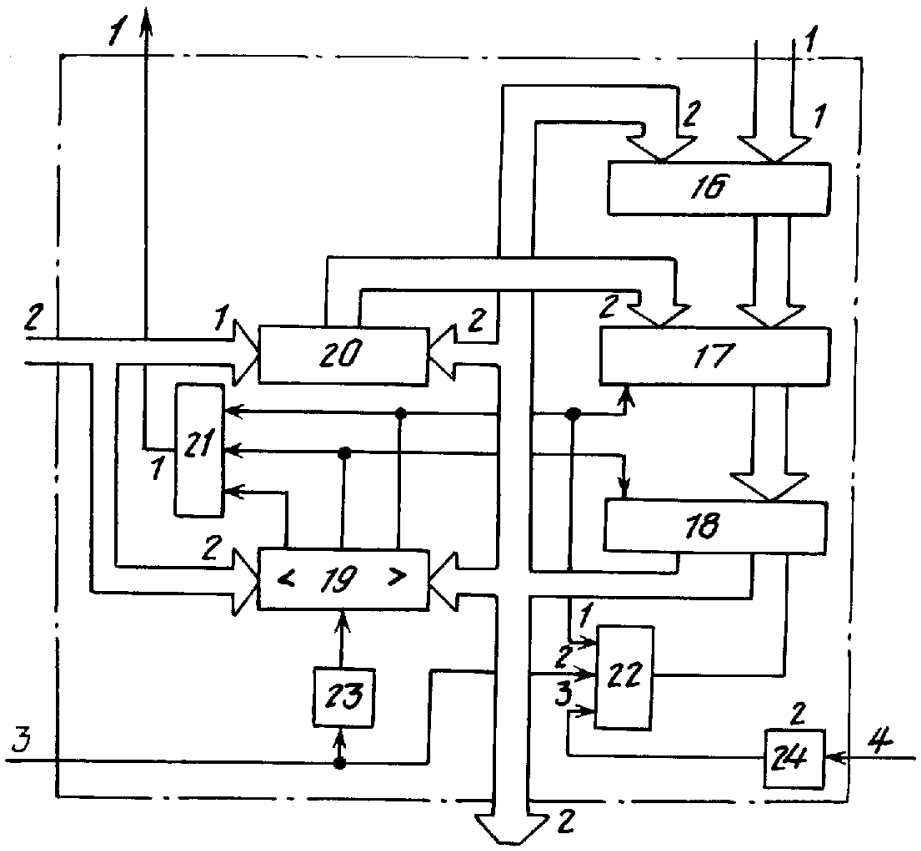
Формула изобретения:

1. УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ ОТ ЧИСЛА, содержащее два регистра, два элемента И, два элемента ИЛИ и первый счетчик, причем информационные входы кодов числа и модуля устройства соединены соответственно с информационными входами первого и второго регистров, входы записи которых соединены с входом записи первого счетчика, первыми входами первого и второго элементов ИЛИ и входом начала вычисления устройства, выход обнуления счетчика соединен с первым входом первого элемента И, отличающееся тем, что, с целью повышения быстродействия, в него введены накапливающий сумматор по модулю, второй счетчик, элемент запрета, два дешифратора, группа из n элементов И (где n - разрядность входного кода числа), n - 1 ключевых элементов и триггер, причем выходы второго регистра соединены с информационными входами первой группы накапливающего сумматора по модулю, а через первый дешифратор - с информационными входами второго дешифратора и второго счетчика, выход обнуления которого соединен с первым управляющим входом накапливающего сумматора по модулю и информационным входом триггера, вход сброса которого соединен с выходом первого элемента ИЛИ, а выход через второй элемент И - с вычитающими входами первого и второго счетчиков и входом сдвига первого регистра, разрядные выходы которого соединены с первыми входами соответствующих элементов И группы, выходы которых соединены с информационными входами второй группы накапливающего сумматора по модулю, второй управляющий вход которого соединен с входом начала вычислений устройства, выход результата которого соединен с информационными выходами накапливающего сумматора по модулю, управляющий выход которого соединен с вторыми входами первого элемента И и второго элемента ИЛИ и прямым входом элемента запрета, инверсный вход которого соединен с выходом обнуления первого счетчика, а выход - с вторым входом первого элемента ИЛИ, выход первого элемента И соединен с выходом окончания формирования остатка устройства, тактовый вход которого соединен с вторым входом второго элемента И, выход i-го разряда второго дешифратора соединен с входом i-го элемента И группы (i = 1, ..., n), между выходами (j - 1)-го и j-го (j=2, ..., n) разрядов второго дешифратора подключены ключевые элементы.

2. Устройство по п.1, отличающееся тем, что накапливающий сумматор по модулю содержит вычитатель, два элемента задержки, два элемента ИЛИ, комбинационный сумматор, мультиплексор, регистр и элемент сравнения, причем информационные входы второй группы накапливающего сумматора соединены с первыми входами комбинационного сумматора, выходы которого соединены с первыми информационными входами мультиплексора, выходы которого соединены с информационными входами регистра, выходы которого соединены с вторыми входами комбинационного сумматора, с входами уменьшаемого вычитателя, первыми информационными входами элемента сравнения и информационными выходами накапливающего сумматора, информационные входы второй группы которого соединены с вторыми информационными входами элемента сравнения и входами вычитаемого вычитателя, выходы которого соединены с вторыми информационными входами мультиплексора, управляющий вход которого соединен с первыми входами первого и второго элементов ИЛИ и выходом "Больше" элемента сравнения, выход "Равно" которого соединен с входом сброса регистра и вторым входом второго элемента ИЛИ, третий вход которого соединен с выходом "Меньше" элемента сравнения, управляющий вход которого соединен с выходом первого элемента задержки, вход которого соединен с первым управляющим входом накапливающего сумматора и вторым входом первого элемента ИЛИ, выход которого соединен с входом записи регистра, а третий вход - с выходом второго элемента задержки, вход которого соединен с вторым управляющим входом накапливающего сумматора, управляющий выход которого соединен с выходом второго элемента ИЛИ.

RU 2029434 C1

RU 2029434 C1



фиг.2

RU 2029434 C1

RU 2029434 C1