РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 324 972** (13) **C2**

(51) МПК
G06F 7/72 (2006.01)
H03M 7/18 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2006102753/09, 31.01.2006**

(24) Дата начала отсчета срока действия патента:
31.01.2006

(43) Дата публикации заявки: **20.08.2007**

(45) Опубликовано: **20.05.2008 Бюл. № 14**

(56) Список документов, цитированных в отчете о поиске: **RU 2029435 C1, 20.02.1995. RU 2020759 C1, 30.09.1994. SU 1238077 A1, 15.06.1986. SU 1765896 A1, 30.09.1992. JP 11282349 A, 15.10.1999. EP 0308963 A2, 29.03.1989.**

Адрес для переписки:
355017, Ставропольский край, г.Ставрополь, ул.Артема, 2, СВИС РВ, НИО

(72) Автор(ы):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (RU),
Карагулян Дмитрий Левонович (RU),
Мосин Олег Викторович (RU)

(73) Патентообладатель(и):
Ставропольский военный институт связи ракетных войск (RU)

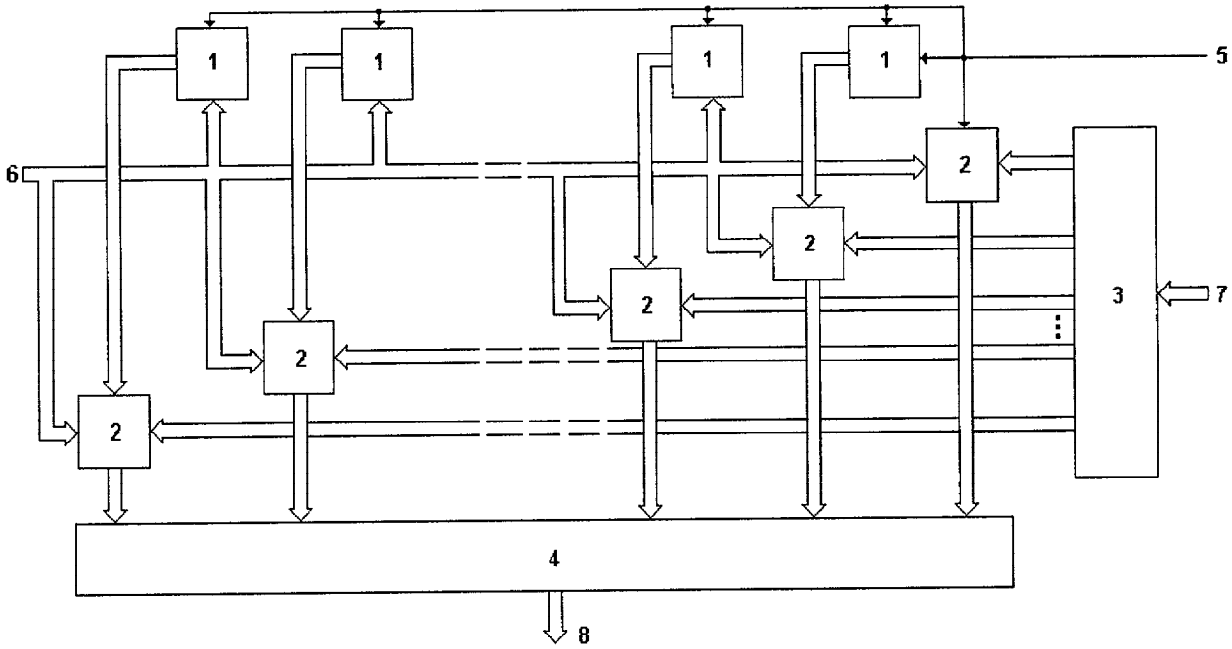
(54) УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ ОТ ЧИСЛА

(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах для формирования кодовых последовательностей. Техническим результатом является повышение быстродействия путем сокращения количества выполняемых операций за счет увеличения основания преобразования числа. Устройство содержит блоки формирования частичных остатков, умножители по модулю, блок распределения коэффициентов, сумматор по модулю. 2 н.п. ф-лы, 2 ил.

RU 2324972 C2

RU 2324972 C2



Фиг.1

RU 2324972 C2

RU 2324972 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 324 972** (13) **C2**

(51) Int. Cl.
G06F 7/72 (2006.01)
H03M 7/18 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2006102753/09, 31.01.2006**

(24) Effective date for property rights: **31.01.2006**

(43) Application published: **20.08.2007**

(45) Date of publication: **20.05.2008 Bull. 14**

Mail address:
355017, Stavropol'skij kraj, g.Stavropol', ul.Artema, 2, SVIS RV, NIO

(72) Inventor(s):
Petrenko Vjacheslav Ivanovich (RU),
Kuz'minov Jurij Vladimirovich (RU),
Karaguljan Dmitrij Levonovich (RU),
Mosin Oleg Viktorovich (RU)

(73) Proprietor(s):
Stavropol'skij voennyj institut svjazi raketnykh vojsk (RU)

(54) CREATOR OF RANDOM MODULE REMINDER OF NUMBER

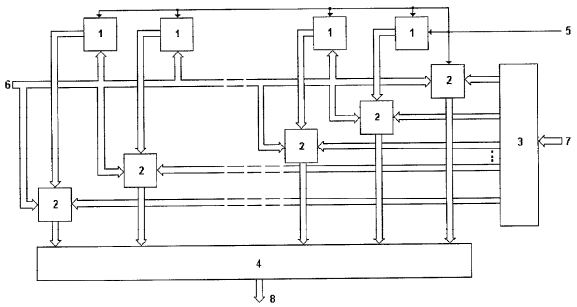
(57) Abstract:

FIELD: computer engineering.

SUBSTANCE: creator comprises units of partial reminder formation, multipliers by module, coefficients allocator, and adder by module. The result is achieved by increase of transformation base.

EFFECT: performance improvement by means of decrease of executable operations.

2 cl, 2 dwg



Фиг.1

RU 2324972 C2

RU 2324972 C2

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах для формирования кодовых последовательностей.

Известно устройство для формирования остатка по произвольному модулю от числа, содержащее элементы ИЛИ, формирователи импульсов, счетчики, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ, блоки умножения, элемент И, группу сумматоров по модулю два (см. АС СССР №1238077, кл. G06F 11/08, 15.06.1986).

Недостатком данного устройства является низкое быстродействие.

Наиболее близким по технической сущности к заявляемому изобретению является комбинационный рекуррентный формирователь остатков, содержащий узлы формирования частичных остатков, ключи и сумматоры по произвольному модулю (см. патент РФ №2029435, кл. H03M 7/18, 20.02.1995).

Недостатком данного устройства является его низкое быстродействие.

Цель изобретения - повышение быстродействия за счет увеличения основания преобразования числа.

Сущность изобретения заключается в реализации следующего способа формирования остатков по модулю.

Известно, что любое целое положительное число A может быть представлено в виде степеней числа 2, просуммированных в соответствии с коэффициентами при каждой степени, то есть

$$A = a_n 2^n + a_{n-1} 2^{n-1} + \ldots + a_1 2 + a_0 \qquad (1)$$

Существующие устройства формирования остатков в основном используют процедуру вычисления частичных остатков от каждой из степеней числа, представленного в двоичном виде с последующим умножением их по модулю на коэффициенты при соответствующих степенях и суммированием по модулю.

В таких устройствах число 2 в выражении (1) одновременно является и основанием системы счисления, и основанием преобразования при вычислении остатка

Предлагаемое устройство реализует процедуру приведения числа A по произвольному модулю p, используя основание преобразования $M=2^N$, где N - целое положительное число, большее 1. В этом случае число

$A=a_n2^n+a_{n-1}2^{n-1}+...+a_12+a_0$

для выполнения вычислений может быть приведено к виду

$$A = b_r M^r + b_{r-1} M^{r-1} + \ldots + b_1 M + b_0, \qquad (2)$$

где $M=2^N$ - основание преобразования; b_i (i=1, ..., r) - соответствующий коэффициент при основании преобразования. Если количество разрядов k=n+1 при представлении числа A в виде (1) кратно N, то

$$r = \left(\frac{k}{N}\right) - 1,$$

в противном случае

$$r = \left(\frac{k^*}{N}\right) - 1,$$

где k^* - ближайшее к k целое число, большее k и кратное N. Для достижения k значений k^*количество разрядов увеличивают путем добавления нулевых коэффициентов перед старшим разрядом числа A. Тогда

$b_r=\{a_n, a_{n-1}, ..., a_{n-N+1}\}$, $b_{r-1}=\{a_{n-N}, a_{n-N-1}, ..., a_{n-2N}\}$

и т.д.

Система счисления при изменении основания преобразования остается двоичной, то есть коэффициенты b_i есть числа, которые в двоичном виде представляют собой последовательность, состоящую из коэффициентов a_j, количество которых зависит от выбранного значения N.

Пример:

Пусть $A=189=1\cdot2^7+0\cdot2^6+1\cdot2^5+1\cdot2^4+1\cdot2^3+1\cdot2^2+0\cdot2+1\cdot1=10111101$.

Очевидно, что для формирования остатка необходимо сформировать значение

частичного остатка от каждой степени числа «2» от 1 до n (т.к. увеличение степени числа 2 осуществляется сдвигом старшей степени на одну позицию в сторону возрастания, то требуется провести (n-1) операций сдвига), умножить каждое из них на коэффициент при соответствующей степени (n операций) и просуммировать, то есть выполнить 2n операций.

Пусть N=A, тогда $M=2^N=16$. В этом случае число A можно представить в следующем виде:

$A=b_r16^r+b_{r-1}16^{r-1}+...+b_116+b_0$.

Наивысшая степень r в данном представлении числа A определяется отношением

$$r = (\frac{k}{N}) - 1,$$

так как количество разрядов при представлении числа A в двоичном виде кратно выбранному значению N. В данном случае k=n+1=8, N=4. Следовательно, r=1. Тогда

$A=b_116^1+b_016^0=b_1\cdot16+b_0$.

Коэффициент b_1 определяется первыми N коэффициентами a_n, a_{n-1}, ..., a_{n-N} при представлении числа A в двоичном виде, b_0 - следующими N коэффициентами, то есть, если A=10111101, то b_1=1011, b_0=1101.

Тогда рассматриваемое число A с измененным основанием преобразования может быть записано как

$A=(1011)\cdot16+1101=11\cdot16+13=176+13=189$

Очевидно, что для нахождения остатка от числа A с измененным основанием преобразования необходимо найти частичный остаток только от одной степени числа 16, после чего умножить его по модулю на соответствующий коэффициент и просуммировать по модулю полученные результаты.

При формировании частичных остатков от степеней числа A с измененным основанием преобразования используется следующая процедура. Известно, что любая степень числа 2, представленная в двоичной форме, может быть сформирована путем сдвига символа «1» на определенное количество разрядов в сторону возрастания. Таким образом, число 2^N может быть получено при сдвиге символа «1» на N разрядов вверх. Для приведения полученного значения z степени числа A с измененным основанием преобразования по модулю данное значение сравнивается со значением модуля p. Если полученное значение $z\geq p$, то из z вычитается значение модуля p, а полученное в результате значение $z_1=z-p$ вновь сравнивается со значением p. Если и в этом случае значение $z_1\geq p$, то из z_1 вновь вычитается значение p, а полученное в результате значение $z_2=z_1-p$ сравнивается со значением p. Данные операции проводятся до тех пор, пока значение z_n, полученное на n-м шаге вычислений, не станет меньше значения модуля p. В этом случае значение z_n является частичным остатком от степени числа A с измененным основанием преобразования по модулю p. Если уже на первом шаге входное значение $z<p$, значение z остается без изменений и является частичным остатком от степени числа A с измененным основанием преобразования по модулю p.

Следует отметить, что в случае представления числа A двоичной последовательностью, количество элементов которой не является кратным N, данная последовательность дополняется нулями перед старшим разрядом до достижения размеров последовательности, кратной N.

Таким образом, увеличение основания преобразования при формировании остатков с M=2 до $M=2^N$ позволяет уменьшить количество последовательных ступеней преобразования, тем самым увеличив быстродействие выполнения операции формирования остатков.

На фиг.1 представлена схема устройства для формирования остатка по произвольному модулю от числа, на фиг.2 - схема блока формирования частичных остатков.

Устройство для формирования остатка по произвольному модулю состоит из $l=((k^*/N)-1)$ блоков 1 формирования частичных остатков (где k^* - количество разрядов в двоичном

представлении числа, от которого формируется остаток, с учетом добавленных для достижения кратности N разрядов), (l+1) блоков 2 умножения по модулю, блока 3 распределения коэффициентов и сумматора 4 по модулю.

Блок 1 формирования частичных остатков состоит из блока 10 сдвига, t сумматоров 11 (где t равно отношению $(2^{k'-N}) / p$, округленному в сторону большего целого числа), t инверторов 12, (t-1) умножителей 13 на константу и мультиплексора 14.

Первый вход каждого блока 1 формирования частичных остатков служит для записи символа «1», являющегося кодом начала операции. В блоке 1 формирования частичных остатков данный символ подается на вход блока 10 сдвига, а также на третьи входы каждого сумматора 11. Ко второму входу каждого блока 1 формирования частичных остатков подключен вход 6 записи кода модуля устройства. Выход i-го блока 1 формирования частичных остатков (где i=1, ..., l-1) подключен к первому входу i+1-го блока 2 умножения по модулю. Ко второму входу каждого блока 2 умножения по модулю подключен вход 6 записи кода модуля устройства. К третьему входу j-го блока 2 умножения по модулю (где j=1, ..., l+1) подключен j-й выход блока 3 распределения коэффициентов. Выход j-го блока 2 умножения по модулю подключен к j-му входу сумматора 4 по модулю. На (j+1)-й вход сумматора 4 по модулю подан код модуля p со входа 6 устройства. Выход сумматора 4 по модулю является выходом 8 устройства.

Устройство работает следующим образом.

В исходном состоянии на вход 6 подан двоичный код модуля p, по которому будет осуществляться формирование остатков. На вход 7 подан двоичный код числа A, от которого формируется остаток. Процесс формирования остатка начинается с подачи на вход 5 устройства символа «1», который поступает на вход каждого блока 1 формирования частичных остатков. В блоке 1 формирования частичных остатков символ «1» подается на вход блока 10 сдвига, который путем сдвига символа «1» на $m \times N$ разрядов в сторону увеличения (m=1, ..., l), на своем выходе формирует двоичный код числа z, соответствующего определенной степени числа A с измененным основанием преобразования (в m-м блоке формирования частичных остатков блок 10 сдвига формирует двоичный код m-й степени числа A). Код числа z поступает на первые входы сумматоров 11 и на первый информационный вход мультиплексора 14. Со входа 2 блока 1 формирования частичных остатков двоичный код модуля p подается на входы умножителей 13 на константу и на вход первого инвертора 12. Значение модуля в k-м умножителе 13 (где k=1, ..., t-1) умножается на величину f=(k+1). С выхода k-го умножителя на константу 13 код полученного значения поступает на вход (k+1)-го инвертора 12. В h-м (где h=1, ..., t) инверторе 12 поступающий на его вход код переводится в инверсный код, который подается на второй вход h-го сумматора 11, причем на вход первого инвертора 12 поступает непосредственно код модуля p. Очевидно, что на выходе h-го сумматора формируется инверсный код значения $h \times p$, поступающий на второй вход h-го сумматора 11. На третий вход каждого сумматора 11 с первого входа блока 1 формирования частичных остатков поступает код числа «1», служащий для перевода инверсного кода модуля в дополнительный код.

В общем виде сумматор 11 осуществляет операцию, описываемую выражением: $c = z + \overline{h \times p}$, где c - результат суммирования, z - значение степени числа A с измененным основанием преобразования, h - номер сумматора, p - модуль. Старший разряд сформированного кода значения c поступает на выход переноса сумматора 11, остальные разряды представляют разность $z-h \times p$ и поступают на информационный выход сумматора 11.

До тех пор, пока значение z превышает значение $h \times p$, на выходе переноса h-го сумматора 11 будет формироваться символ «1», который будет поступать на h-й управляющий вход мультиплексора 14. При превышении значением $h \times p$ значения z на выходе переноса h-го сумматора 11 сформируется символ «0». При поступлении на h-й управляющий вход мультиплексора 14 символа «0» с выхода переноса h-го сумматора 11

мультиплексор 14 подключит на выход 3, являющийся выходом блока 1 формирования коэффициентов, тот свой информационный вход, на который подается значение с информационного выхода (h-1)-го сумматора 11. Данное значение представляет частичный остаток от степени числа A с по модулю p.

С выхода m-го блока 1 формирования частичных остатков полученное значение поступает на первый вход (m+1)-го блока 2 умножения по модулю. На первый вход первого блока 2 умножения по модулю подается символ «1» с входа 5 устройства.

На второй вход каждого блока 2 умножения подается код модуля со входа 6 устройства. На третий вход j-го блока 2 умножения по модулю поступает последовательность из N символов с j-го выхода блока 3 распределения коэффициентов. Данный блок представляет собой коммутатор с динамическими или жесткими связями, формирующий на выходах из поступающей на его вход последовательности длиной k символов (k^*/N) последовательностей длиной N символов. Данные последовательности по сути являются коэффициентами b_i при представлении числа A с помощью переменного основания преобразования. Причем на первый выход блока 3 распределения коэффициентов подаются младшие N разрядов входной последовательности, на второй выход - следующие N разрядов и т.д. В случае, если k не кратно N, последняя формируемая последовательность дополнится нулями в старших разрядах и также будет состоять из N символов.

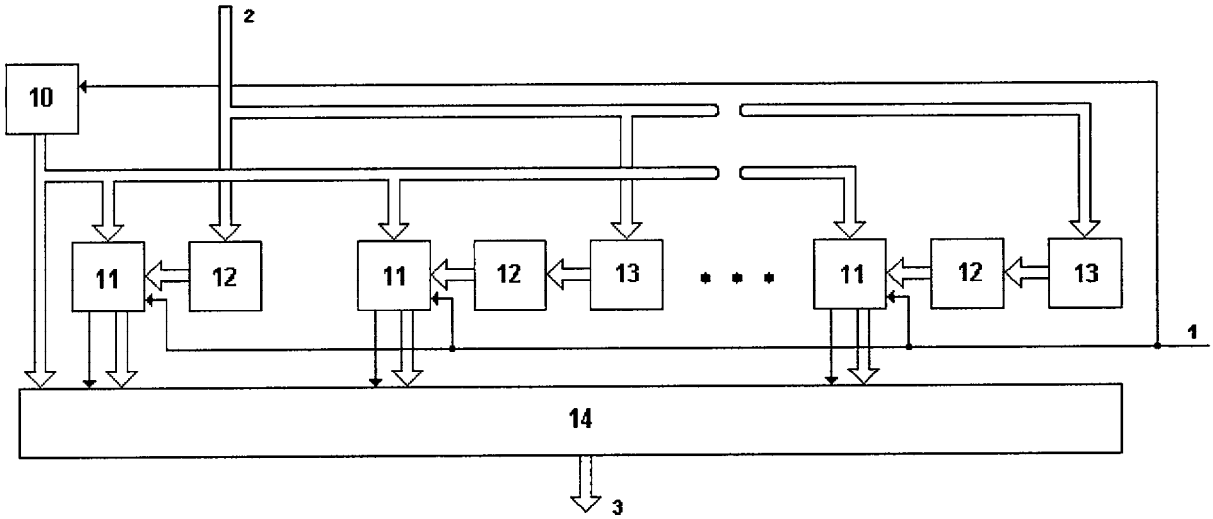
Сформированное на выходе j-го блока 2 умножения по модулю значение, представляющее собой произведение частичного остатка от степени числа A с измененным основанием на коэффициент при данной степени, подается на сумматор 4 по модулю, где суммируется в соответствии с модулем со значениями, сформированными в других блоках 2 умножения. Полученное в результате суммирования по модулю значение, являющееся остатком от числа A по произвольному модулю p, подается на выход сумматора, который является выходом 8 устройства.

Формула изобретения

1. Устройство для формирования остатка по произвольному модулю, содержащее l блоков формирования частичных остатков, (l+1) умножителей по модулю, сумматор по модулю, причем вход каждого блока формирования частичных остатков соединен с входом записи кода начала операции устройства, выход m-го блока формирования частичных остатков соединен с первым входом (m+1)-го блока умножения по модулю, где m=1, ..., l, первый вход первого блока умножения по модулю соединен со входом записи кода начала операции устройства, отличающееся тем, что в него введен блок распределения коэффициентов, формирующий коэффициенты при основании преобразования, причем вход блока распределения коэффициентов соединен со входом записи двоичного кода исследуемого числа устройства, j-й выход блока распределения коэффициентов соединен с третьим входом j-го блока умножения по модулю, где j=1, ..., l+1, причем вторые входы умножителей по модулю соединены со входом записи двоичного кода модуля устройства, выход j-го умножителя соединен с j-м входом сумматора по модулю, вход записи двоичного кода модуля устройства соединен с (j+1)-м входом сумматора по модулю и вторым входом каждого блока формирования частичных остатков, выход сумматора по модулю является выходом устройства.

2. Блок формирования частичных остатков, содержащий блок сдвига, t сумматоров, t инверторов, (t-1) умножителей на константу и мультиплексор, причем вход записи кода начала операции устройства подключен ко входу блока сдвига и к третьему входу каждого сумматора, выход блока сдвига подключен к первому информационному входу мультиплексора и первым входам сумматоров, выход переноса h-го сумматора подключен к h-му управляющему входу мультиплексора, информационный выход h-го сумматора подключен к (h+1)-му информационному входу мультиплексора, где h=1, ..., t, вход записи двоичного кода модуля подключен ко входу первого инвертора и ко входу каждого умножителя на константу, k-й умножитель на константу производит умножение значения на

своем входе на величину (k+1), где k=1, ..., t-1, выход k-го умножителя на константу подключен ко входу (k+1)-го инвертора, выход h-го инвертора подключен ко второму входу h-го сумматора, выход мультиплексора является выходом формирователя.



Фиг. 2