РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 348 965** (13) **C1**

(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: **2007119488/09, 25.05.2007**

(24) Дата начала отсчета срока действия патента:
25.05.2007

(45) Опубликовано: **10.03.2009 Бюл. № 7**

(56) Список документов, цитированных в отчете о поиске: **RU 2029435 C1, 20.02.1995. RU 2025897 C1, 30.12.1994. SU 1633495 A1, 07.03.1991. SU 1737442 A1, 30.05.1992. JP 11282349 A, 15.10.1999. EP 0308963 A2, 29.03.1989.**

Адрес для переписки:
355009, Ставропольский край, г. Ставрополь, ул. Пушкина, 1, научно-исследовательская часть

(72) Автор(ы):
Петренко Вячеслав Иванович (RU),
Сидорчук Алеся Вячеславна (RU)

(73) Патентообладатель(и):
Государственное образовательное учреждение высшего профессионального образования "Ставропольский государственный университет" (RU)

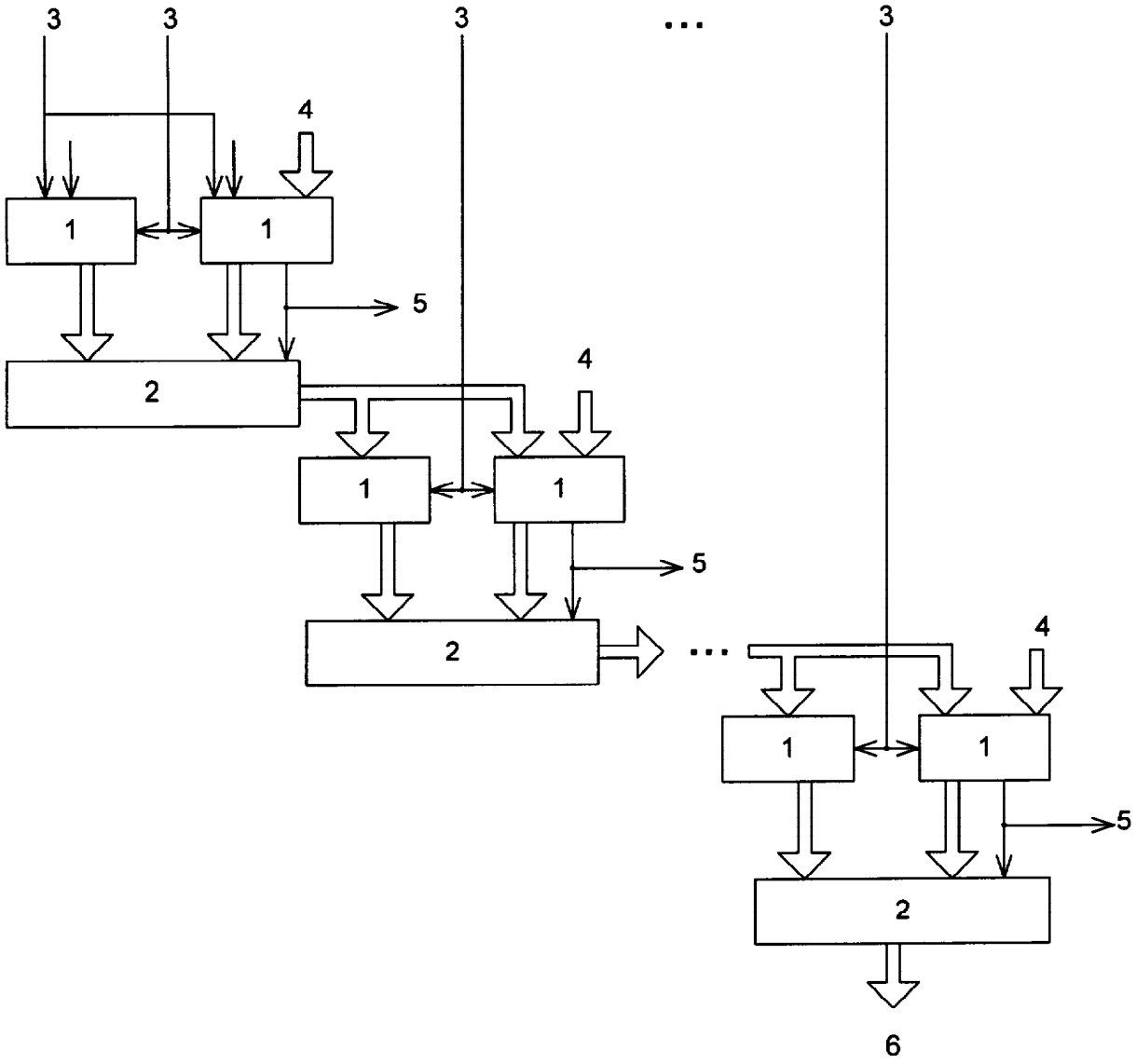
(54) ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО

(57) Реферат:

Вычислительное устройство относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах цифровой обработки сигнала и в криптографических приложениях. Техническим результатом является расширение функциональных возможностей устройства за счет обеспечения формирования неполного частного. Устройство содержит 2n-2 сумматоров и n-1 мультиплексоров. 1 ил.

RU 2348965 C1

RU 2348965 C1



RU 2348965 C1

RU 2348965 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 348 965** (13) **C1**

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

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2007119488/09, 25.05.2007**

(24) Effective date for property rights: **25.05.2007**

(45) Date of publication: **10.03.2009 Bull. 7**

Mail address:
**355009, Stavropol'skij kraj, g. Stavropol',
ul. Pushkina, 1, nauchno-issledovatel'skaja chast'**

(72) Inventor(s):
**Petrenko Vjacheslav Ivanovich (RU),
Sidorchuk Alesja Vjacheslavna (RU)**

(73) Proprietor(s):
Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Stavropol'skij gosudarstvennyj universitet" (RU)

(54) COMPUTING MECHANISM

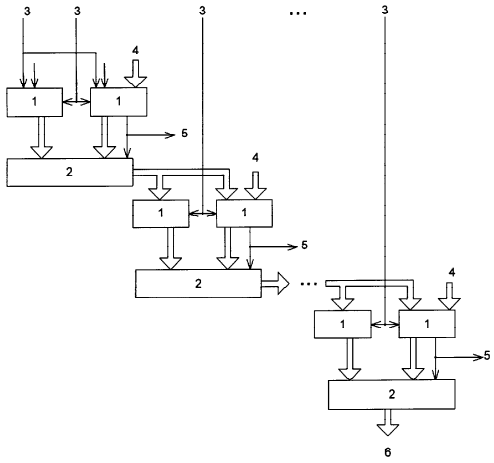
(57) Abstract:

FIELD: physics, computer facilities.

SUBSTANCE: computing mechanism concerns computer equipment and can be used in digital computing mechanisms, and also in devices of digital processing of a signal and in cryptographic applications. The device contains 2n-2 adders and n-1 multiplexers.

EFFECT: expansion of functionality of the device at the expense of provision of incomplete quotient formation.

1 dwg



RU 2348965 C1

RU 2348965 C1

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах цифровой обработки сигналов и в криптографических приложениях.

Известно устройство для формирования остатка по произвольному модулю от числа, содержащее регистры, элементы ИЛИ, вычислитель, схемы сравнения, мультиплексор, элемент задержки, сумматор, группу блоков элементов И и блок постоянной памяти со связями (см. АС СССР №1633495, кл. H03M 7/18, 1991).

Недостатком известного устройства является низкая надежность, так как для его реализации требуется большой объем оборудования.

Наиболее близким по технической сущности к заявляемому изобретению является комбинационный рекуррентный формирователь остатков, содержащий комбинационный формирователь частичных остатков, блок ключей и блок сумматоров по модулю (см. патент РФ №2029435, кл. 6 H03M 7/18, 20.02.1995, бюл. №5).

Недостатком данного устройства являются его ограниченные функциональные возможности, а именно отсутствие возможности формирования неполного частного.

Цель изобретения - расширение функциональных возможностей устройства за счет обеспечения формирования неполного частного.

Для достижения поставленной цели в вычислительном устройство, содержащее 2n-2 сумматоров и n-1 мультиплексоров, где n - разрядность входного числа, (n-2-i)-й разряд двоичного кода входного числа подается на входы переносов первого и второго сумматоров i-й ступени преобразования, где i=1, ..., n-1, а старший (n-1)-й разряд двоичного кода входного числа, сдвинутый на один разряд в сторону старшего, подается на первые входы первого и второго сумматоров первой ступени преобразования, на второй вход второго сумматора каждой ступени преобразования подается дополнительный двоичный код модуля, причем информационные входы i-го мультиплексора, где i=1, ..., n-1 номер ступени преобразования, соединены с выходами первого и второго сумматоров i-й ступени преобразования, выход переноса второго сумматора i-й ступени преобразования соединен с управляющим входом i-го мультиплексора и является выходом (n-i-1)-го разряда неполного частного устройства, выход i-го мультиплексора, где i=1, ..., n-2 номер ступени преобразования, соединен с первыми входами первого и второго сумматоров (i+1)-й ступени преобразования, причем j-й разряд мультиплексора, где j=1, ..., n, соединен с (j+1)-м разрядом первого и второго сумматоров, выход (n-1)-го мультиплексора является выходом вычислительного устройства.

Сущность изобретения заключается в реализации следующего способа формирования остатка по произвольному модулю.

Пусть требуется сформировать остаток r от числа A по модулю p и вычислить частное q, то есть решить уравнение A=qp+r.

Число A может быть представлено в позиционной системе счисления в виде $A=a_{n-1}2^{n-1}+a_{n-2}2^{n-2}+a_{n-3}2^{n-3}+...+a_2 2^2+a_1 2^1+a_0 2^0$, где a_i, $i=\overline{0,n-1}$ - коэффициенты, принимающие значения 0 или 1, n - количество разрядов в представлении числа A. Это выражение может быть представлено в следующем виде:

$$A=\underbrace{2(2(...(2(2}_{n-1}a_{n-1}+a_{n-2})+a_{n-3})...)+a_1)+a_0$$

$$A\,\mathrm{mod}\,p=(\underbrace{2(2(...(2(2}_{n-1}a_{n-1}+a_{n-2})+a_{n-3})...)+a_1)+a_0)\,\mathrm{mod}\,p=$$

$$=(\underbrace{2(2(...(2(2}_{n-1}a_{n-1}+a_{n-2})\,\mathrm{mod}\,p+a_{n-3})\,\mathrm{mod}\,p...)\,\mathrm{mod}\,p+a_1)\,\mathrm{mod}\,p+a_0)\,\mathrm{mod}\,p=$$

$$=r\,\mathrm{mod}\,p\,.$$

Из теории чисел известно, что операция приведения по модулю инвариантна к сложению и умножению, т.е. величина остатка не зависит от того, вычислен он от суммы (произведения) или от каждого слагаемого (сомножителя), а затем соответствующие частичные остатки просуммированы (перемножены) и от результата вычислен остаток по

модулю.

В таком виде значительно облегчается задача нахождения остатка r от числа A.

При проведении вычислений по модулю p значение выражения $(2a_{n-1}+a_{n-2})$ сравнивается с модулем p, где n количество разрядов числа A. Если значение $(2a_{n-1}+a_{n-2})\geq p$, то из числа $(2a_{n-1}+a_{n-2})$ вычитается значение модуля p, то есть $t_1=(2a_{n-1}+a_{n-2})-p$. При этом формируется ненулевой старший (n-1)-й разряд неполного частного q. Если $(2a_{n-1}+a_{n-2})<p$, то число $(2a_{n-1}+a_{n-2})$ остается без изменений $t_1=2a_{n-1}+a_{n-2}$, а значение старшего (n-1)-го разряда неполного частного q принимается равным нулю. Полученное в результате значение t_1 умножается на 2, складывается с a_{n-3} и сравнивается со значением p. Если значение $(2t_1+a_{n-3})\geq p$, то из $(2t_1+a_{n-3})$ вычитается значение модуля p, то есть $t_2=(2t_1+a_{n-3})-p$, при этом формируется ненулевой (n-2)-й разряд неполного частного q. Если $(2t_1+a_{n-3})<p$, то число $(2t_1+a_{n-3})$ остается без изменений $t_2=(2t_1+a_{n-3})$, а значение (n-2)-го разряда неполного частного q принимается равным нулю. Полученное в результате значение t_2 умножается на 2, складывается с a_{n-4} и сравнивается со значением p и т.д. На последнем (n-1)-м шаге число $(2t_{n-2}+a_0)$ сравнивается с модулем p. Если значение $(2t_{n-2}+a_0)\geq p$, то из $(2t_{n-2}+a_0)$ вычитается значение числа p, то есть $t_{n-1}=(2t_{n-2}+a_0)-p$, при этом формируется ненулевой младший разряд неполного частного q. Если $(2t_{n-2}+a_0)<p$, то число $(2t_{n-2}+a_0)$ остается без изменений $t_{n-1}=2t_{n-2}+a_0$, а значение младшего разряда неполного частного q принимается равным нулю. Полученное в результате значение $r=t_{n-1}$ является остатком от деления числа A на число p. Операция умножения на два во всех случаях осуществляется сдвигом всех разрядов множимого на один в сторону старших. Суммирование осуществляется обычным способом с применением комбинационных двоичных сумматоров.

На чертеже представлена схема вычислительного устройства.

Вычислительное устройство содержит 2n-2 сумматоров 1 и n-1 мультиплексоров 2, где n-разрядность входного числа, (n-2-i)-й разряд двоичного кода входного числа подается на входы 3 переносов первого и второго сумматоров 1 i-й ступени преобразования, где i= 1, ..., n-1, а старший (n-1)-й разряд двоичного кода входного числа, сдвинутый на один разряд в сторону старшего, подается на первые входы 3 первого и второго сумматоров 1 первой ступени преобразования, на второй вход 4 второго сумматора 1 каждой ступени преобразования подается дополнительный двоичный код модуля, причем информационные входы i-го мультиплексора 2, где i=1, ..., n-1 номер ступени преобразования, соединены с выходами первого и второго сумматоров 1 i-й ступени преобразования, выход переноса второго сумматора 1 i-й ступени преобразования соединен с управляющим входом i-го мультиплексора и является выходом 5 (n-i-1)-го разряда неполного частного устройства, выход i-го мультиплексора, где i=1, ..., n-2 номер ступени преобразования, соединен с первыми входами первого и второго сумматоров 1 (i+1)-й ступени преобразования, причем j-й разряд мультиплексора 2, где j=1, ..., n, соединен с (j+1)-м разрядом первого и второго сумматоров 1, выход 6 (n-1)-ого мультиплексора является выходом вычислительного устройства.

Вычислительное устройство работает следующим образом.

На первые входы первых двух сумматоров 1 со входа 3 подается сигнал со старшего (n-1)-го разряда двоичного кода числа A, умноженный на 2, где n равно количеству разрядов двоичного представления числа A. На второй вход второго сумматора 1 со входа 4 подается дополнительный двоичный код $P_Д$ модуля p. На входы переноса первых двух сумматоров подается сигнал с (n-2)-го разряда двоичного кода числа A. Первый сумматор 1 выполняет операцию $(2a_{n-1}+a_{n-2})$, второй сумматор 1 выполняет операцию $(2a_{n-1}+a_{n-2}+p_д)$. Сигнал со старшего (k+1)-го разряда полученного значения, где k количество разрядов дополнительного двоичного кода модуля p, поступает на выход переноса второго сумматора 1. Остальные разряды представляют собой разность $((2a_{n-1}+a_{n-2})-p)$. На первый вход первого мультиплексора 2 поступает информационный сигнал с первого сумматора 1, а на второй вход - информационный сигнал со второго сумматора 1. Если сигнал на выходе переноса второго сумматора 1 равен "1", то на

первый вход первого сумматора 1 второй ступени преобразования и на первый вход второго сумматора 1 второй ступени преобразования поступает разность $t_1=((2a_{n-1}+a_{n-2})-p)$, если же он равен "0", то на первый вход первого сумматора 1 и на первый вход второго сумматора 1 поступает число $t_1=(2a_{n-1}+a_{n-2})$. На входы переноса обоих сумматоров 1 второй ступени преобразования подается (n-3)-й разряд двоичного кода числа A. На второй вход второго сумматора 1 второй ступени преобразования подается дополнительный двоичный код модуля p. Первый сумматор 1 выполняет операцию $(2t_1+a_{n-3})$, второй сумматор 1 выполняет операцию $(2t_1+a_{n-3}+P_д)$. Далее выполняются те же действия, что и на первой ступени преобразования. После проведения n-1 таких операций на выходе 6 окажется результат вычисления числа A по модулю p, а на выходах 5 - код неполного частного q.

Рассмотрим работу вычислительного устройства на примере.

Пусть $A=25_{10}=11001_2$, $p=7_{10}=111_2$, $p_д=001_2$, n=5. Первый сумматор первой ступени преобразования формирует значение $2a_{n-1}+a_{n-2}=10+1=11$. Второй сумматор первой ступени преобразования формирует значение $2a_{n-1}+a_{n-2}+p_д=10+1+001=100$. Старший 4-й разряд полученного значения равен 0, следовательно, первый мультиплексор переводит на сумматоры второй ступени преобразования значение $t_1=(2a_{n-1}+a_{n-2})=11$ и 3-й разряд неполного частного q принимает значение 0. Первый сумматор второй ступени преобразования формирует значение $2t_1+a_{n-3}=110+0=110$. Второй сумматор второй ступени преобразования формирует значение $2t_1+a_{n-3}+p_д=110+0+001=111$. Старший 4-й разряд полученного значения равен 0, следовательно, второй мультиплексор переводит на сумматоры третьей ступени преобразования значение $t_2=(2t_1+a_{n-3})=110$ и 2-й разряд неполного частного q принимает значение 0. Первый сумматор третьей ступени преобразования формирует значение $2t_2+a_{n-4}=1100+0=1100$. Второй сумматор третьей ступени преобразования формирует значение $2t_2+a_{n-4}+p_д=1100+0+001=1101$. Старший 4-й разряд полученного значения равен 1, следовательно, третий мультиплексор переводит на сумматоры четвертой ступени преобразования значение $t_3=(2t_2+a_{n-4})-p=101$ и 1-й разряд неполного частного q принимает значение 1. Первый сумматор четвертой ступени преобразования формирует значение $2t_3+a_{n-5}=1010+1=1011$. Второй сумматор четвертой ступени преобразования формирует значение $2t_3+a_{n-5}+p_д=1010+1+001=1100$. Старший 4-й разряд полученного значения равен 1, следовательно, четвертый мультиплексор переводит на выход код значения $t_4=(2t_3+a_{n-5})-p=100$ и 0-й разряд неполного частного q принимает значение 1. В результате неполное частное имеет значение $q=001_2=3_{10}$.

Формула изобретения

Вычислительное устройство, содержащее 2n-2 сумматоров и n-1 мультиплексоров, где n-разрядность входного числа, отличающееся тем, что (n-2-i)-й разряд двоичного кода входного числа подается на входы переносов первого и второго сумматоров i-й ступени преобразования, где i=1, ..., n-1, а старший (n-1)-й разряд двоичного кода входного числа, сдвинутый на один разряд в сторону старшего, подается на первые входы первого и второго сумматоров первой ступени преобразования, на второй вход второго сумматора каждой ступени преобразования подается дополнительный двоичный код модуля, причем информационные входы i-го мультиплексора, где i=1, ..., n-1 номер ступени преобразования, соединены с выходами первого и второго сумматоров i-й ступени преобразования, выход переноса второго сумматора i-й ступени преобразования соединен с управляющим входом i-го мультиплексора и является выходом (n-i-1)-го разряда неполного частного устройства, выход i-го мультиплексора, где i=1, ..., n-2 номер ступени преобразования, соединен с первыми входами первого и второго сумматоров (i+1)-й ступени преобразования, причем j-й разряд мультиплексора, где j=1, ..., n, соединен с (j+1)-м разрядом первого и второго сумматоров, выход (n-1)-ого мультиплексора является выходом вычислительного устройства.