РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 356 086** (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: **2007117648/09, 11.05.2007**

(24) Дата начала отсчета срока действия патента:
11.05.2007

(43) Дата публикации заявки: **20.11.2008**

(45) Опубликовано: **20.05.2009** Бюл. № **14**

(56) Список документов, цитированных в отчете о поиске: **RU 2007037 C1, 30.01.1994. 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, ГОУ ВПО "Ставропольский государственный университет", 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)

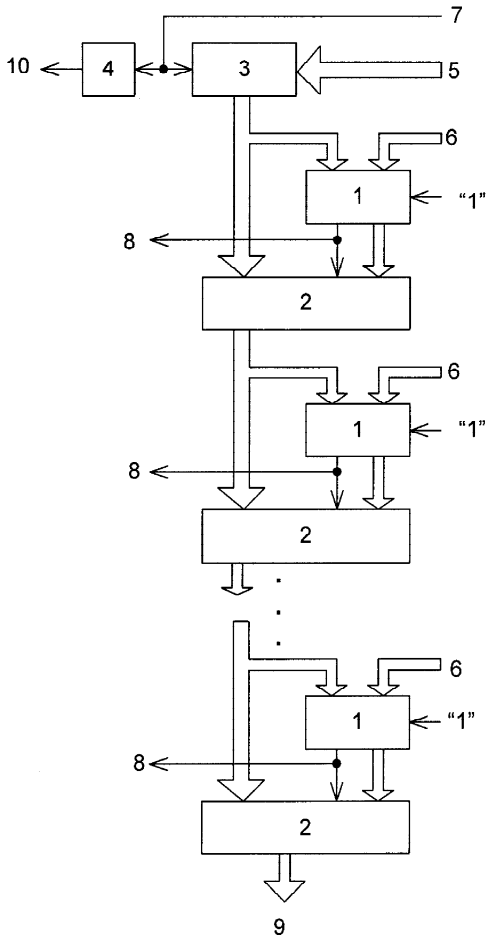
(54) ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО

(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах для формирования элементов конечных полей и в криптографических приложениях. Техническим результатом является расширение функциональных возможностей устройства за счет обеспечения формирования неполного частного. Устройство содержит (n-k+1) сумматоров, (n-k+1) мультиплексоров, регистр и элемент задержки. 1 ил.

RU 2356086 C2

RU 2356086 C2



RU 2356086 C2

RU 2356086 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 356 086** (13) **C2**

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

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2007117648/09, 11.05.2007**

(24) Effective date for property rights:
11.05.2007

(43) Application published: **20.11.2008**

(45) Date of publication: **20.05.2009 Bull. 14**

Mail address:
355009, Stavropol'skij kraj, g.Stavropol', ul. Pushkina, 1, GOU VPO "Stavropol'skij gosudarstvennyj universitet", 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 DEVICE

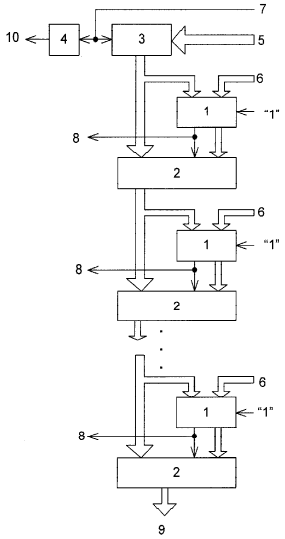
(57) Abstract:

FIELD: physics, computer engineering.

SUBSTANCE: invention is related to computer engineering and may be used in digital computing devices, and also in devices for formation of finite fields formation in cryptographic applications. Device comprises (n-k+1) summators, (n-k+1) multiplexers, register and delay element.

EFFECT: expansion of functional resources of device due to provision of formation of incomplete quotient.

1 dwg



RU 2356086 C2

RU 2356086 C2

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

Известно устройство для формирования остатка по произвольному модулю от числа, содержащее регистр, блок ключей, блок сумматоров и элемент задержки, соединенные между собой функционально (см. АС СССР №1633495, кл. H03M 7/18, 1989).

Недостатком данного устройства является низкая надежность его функционирования и небольшая область функциональных возможностей.

Наиболее близким по технической сущности к заявляемому изобретению является рекуррентный формирователь остатков по произвольному модулю, содержащий блок сумматоров, блок формирования частичных остатков, инвертор, элемент задержки и регистр, соединенные между собой функционально (см. патент РФ №2007037, кл. H03M 7/18, 30.01.1994, бюл. №2).

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 вычислительное устройство, содержащее элемент задержки и регистр, причем вход начала вычисления устройства соединен со входом записи регистра и со входом элемента задержки, выход которого является выходом окончания процесса вычисления, вход числа устройства соединен с информационными входами регистра, введены (n-k+1) сумматоров и (n-k+1) мультиплексоров, причем на входы переноса всех сумматоров подается логическая единица, выход переноса i-го сумматора соединен с управляющим входом i-го мультиплексора и является выходом (n-k-i+1)-го разряда неполного частного устройства, где i=1,…,(n-k+1) номер ступени преобразования, на первый информационный вход i-го сумматора подается инверсный код модуля, сдвинутый на (n-k-i+1) разрядов в сторону старших, причем выход (i-1)-го, где i=2,…,(n-k+1), мультиплексора соединен с первым входом i-го мультиплексора и со вторым информационным входом i-го сумматора, выход (i-1)-го сумматора соединен со вторым информационным входом (i-1)-го мультиплексора, причем выход регистра соединен с первым информационным входом первого мультиплексора и со вторым информационным входом первого сумматора, выход (n-k+1)-го сумматора 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 $a=qp+r$.

При проведении вычислений по модулю p значение числа a сравнивается со значением числа $z=p\times 2^{n-k}$, где n количество разрядов числа a, а k количество разрядов модуля p. Если значение $a\geq z$, то из числа a вычитается значение числа z, то есть $a_1=a-z$, при этом формируется ненулевой старший (n-k+1)-й разряд неполного частного q. Если $a<z$, то число a остается без изменений $a_1=a$, а значение старшего (n-k+1)-го разряда неполного частного q принимается равным нулю. Полученное в результате значение a_1 сравнивается со значением $z_1=p\times 2^{n-k-1}$. Если значение $a_1\geq z_1$, то из a_1 вычитается значение модуля z_1, то есть $a_2=a_1-z_1$, при этом формируется ненулевой

(n-k)-й разряд неполного частного q. Если $a_1<z_1$, то число a_1 остается без изменений $a_2=a_1$, а значение (n-k)-го разряда неполного частного q принимается равным нулю. Полученное в результате значение a_2 сравнивается со значением $z_2=p\times 2^{n-k-2}$ и т.д. На последнем (n-k+1)-м шаге число a_{n-k} сравнивается с модулем p. Если значение $a_{n-k}\geq p$, то из a_{n-k} вычитается значение числа p, то есть $a_{n-k+1}=a_{n-k}$ - P, при этом формируется ненулевой младший разряд неполного частного q. Если $a_{n-k}<p$, то число a_{n-k} остается без изменений $a_{n-k+1}=a_{n-k}$, а значение младшего разряда неполного частного q принимается равным нулю. Полученное в результате значение $r=a_{n-k}+1$ является остатком от деления числа a на число p.

Предлагаемое вычислительное устройство осуществляет данный метод путем последовательного выполнения (n-k+1) операций, в ходе i-й операции значение a_i сравнивается со значением $p\times 2^{n-k-i}$ путем вычисления разности $a_i-p\times 2^{n-k-i}$, где i=1,…,(n-k), и формируется (n-k-i)-й разряд неполного частного q. При выполнении (n-k+1)-й операции результатом вычисления числа a по модулю p будет являться значение разности, полученное на последнем (n-k+1)-м шаге.

На чертеже представлена схема вычислительного устройства.

Вычислительное устройство содержит (n-k+1) сумматоров 1, (n-k+1) мультиплексоров 2, регистр 3 и элемент 4 задержки. Вход 5 служит для подачи двоичного кода числа a, вход 6 - для подачи двоичного кода модуля p. Вход 7 начала вычисления соединен со входом записи регистра 3 и входом элемента 4 задержки. На вход 6 подается двоичный инверсный код числа $p\times 2^{n-k-i}$, где i=1, …, (n-k) порядковый номер ступени преобразования, а (n-k) количество ступеней преобразования, n равно количеству разрядов двоичного представления числа a, k равно количеству разрядов двоичного представления модуля p. Инверсный код числа $p\times 2^{n-k-i}$ может быть получен путем сдвига двоичного кода числа p на i разрядов в сторону старшего с последующей его инверсией. Выход 9 является выходом двоичного кода остатка r, а выход 8 является выходом двоичного кода неполного частного q. Выход 10 элемента 4 задержки - выходом окончания процесса вычисления.

Вычислительное устройство работает следующим образом.

На вход 3 подается двоичный код числа a, который далее поступает на информационные входы регистра 3. Одновременно на вход 7 начала вычисления подается импульс, который поступает на вход элемента 4 задержки и на вход записи регистра 3. При этом код числа a записывается в регистр 3, появляется на его информационных выходах и поступает на второй вход сумматора 1 и первый вход мультиплексора 2 первой ступени преобразования. На первый вход сумматора 1 подается инверсный код $p\times 2^{n-1}$ со входа 4 устройства. На вход переноса всех сумматоров 1 подается логическая единица. Сумматор 1 выполняет операцию, описываемую выражением: $c = a + \overline{p \times 2^{n-1}} + 1$, где c - результат суммирования, a - входное число, p - модуль, n - количество разрядов числа a. Старший n+1 разряд полученного значения c поступает на выход переноса сумматора 1. Остальные разряды представляют собой разность $a - \overline{p \times 2^{n-1}}$. На первый вход мультиплексора 2 поступает код числа a, на второй вход мультиплексора 2 поступает разность $a - \overline{p \times 2^{n-1}}$. Если сигнал на выходе переноса сумматора 1 равен "1", то на второй вход сумматора 1 второй ступени преобразования и на первый вход

мультиплексора 2 второй ступени преобразования поступает разность $a - \overline{p \times 2^{n-1}}$, если же он равен "0", то на второй вход сумматора 1 и на первый вход мультиплексора 2 поступает само число a. На первый вход сумматора 1 второй ступени преобразования поступает инверсный код $p \times 2^{n-2}$. Далее выполняются те же действия, что и на первой ступени преобразования. После проведения n таких операций на выходе 4 окажется результат вычисления числа a по модулю p, а на выходах 6 - код неполного частного q. Одновременно с выхода элемента 4, время задержки которого равно времени работы (n-k+1) сумматоров 1 и (n-k+1) мультиплексоров 2, на выход 10 поступает импульс, сигнализирующий об окончании процесса формирования остатка и неполного частного.

Рассмотрим работу вычислительного устройства на примере.

Пусть $a=189_{10}=10111101_2$, модуль $p=19_{10}=10011_2$, $\overline{p} = 01100_2$, n=8, k=5. Первый сумматор формирует значение $c_1 = a + \overline{p \times 2^{n-k}} + 1 = 10111101_2 + 01100111_2 + 1 = 100100101_2$. Старший разряд c_1 равен 1, следовательно, мультиплексор 2 переводит на второй сумматор код числа $a_1=a-p\times 2^{n-k}=00100101_2$ и 3-й разряд неполного частного q принимает значение 1. Второй сумматор 1 формирует значение $c_2 = a_1 + \overline{p \times 2^{n-k-1}} + 1 = 00100101_2 + 0110011_2 + 1 = 01011001_2$. Старший разряд c_2 равен 0, следовательно, мультиплексор 2 переводит на третий сумматор 1 код числа a_1 и 2-й разряд неполного частного q принимает значение 0. Третий сумматор 1 формирует значение $c_3 = a_1 + \overline{p \times 2^{n-k-2}} + 1 = 00100101_2 + 011001_2 + 1 = 0111111_2$. Старший разряд c_3 равен 0, следовательно, мультиплексор 2 переводит на четвертый сумматор 1 код числа a_1 и 1-й разряд неполного частного q принимает значение 0. Четвертый сумматор 1 формирует значение $c_4 = a_1 + \overline{p \times 2^{n-k-3}} + 1 = 00100101_2 + 01100_2 + 1 = 110010_2$. Старший разряд c_4 равен 1, следовательно, мультиплексор 2 переводит на выход код числа $a_2=a_1-p\times 2^{n-k-3}=10010_2=18_{10}$ и 0-й разряд неполного частного q принимает значение 1. В результате неполное частное имеет значение $q=1001_2=9_{10}$

$189=19\times 9+18$

Формула изобретения

Вычислительное устройство, содержащее элемент задержки и регистр, причем вход начала вычисления устройства соединен со входом записи регистра и со входом элемента задержки, выход которого является выходом окончания процесса вычисления, вход числа устройства соединен с информационными входами регистра, отличающееся тем, что в него введены (n-k+1) сумматоров и (n-k+1) мультиплексоров, где n - количество разрядов двоичного представления числа a, k - количество разрядов модуля p, причем на входы переноса всех сумматоров подается логическая единица, выход переноса i-го сумматора соединен с управляющим входом i-го мультиплексора и является выходом (n-k-i+1)-го разряда неполного частного устройства, где i=1,…,(n-k+1) номер ступени преобразования, на первый информационный вход i-го сумматора подается инверсный код модуля, сдвинутый на (n-k-i+1) разрядов в сторону старших, причем выход (i-1)-го, где i=2,…,(n-k+1), мультиплексора соединен с первым входом

i-го мультиплексора и со вторым информационным входом i-го сумматора, выход (i-1)-го сумматора соединен со вторым информационным входом (i-1)-го мультиплексора, причем выход регистра соединен с первым информационным входом первого мультиплексора и со вторым информационным входом первого сумматора, выход (n-k+1)-ого сумматора является выходом вычислительного устройства.