РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 316 042** (13) **C1**

(51) МПК
G06F 7/523 (2006.01)
G06F 7/72 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2006128654/09, 07.08.2006**

(24) Дата начала отсчета срока действия патента:
07.08.2006

(45) Опубликовано: **27.01.2008 Бюл. № 3**

(56) Список документов, цитированных в отчете о поиске: **RU 2015537 C1, 30.06.1994. RU 2143723 C1, 27.12.1999. SU 1187161 A, 23.10.1985. SU 1691834 A1, 15.11.1991. WO 00/05645 A1, 03.02.2000. US 6321247 A, 20.11.2001. JP 2002251137, 06.09.2002.**

Адрес для переписки:
355009, Ставропольский край, г.Ставрополь, ул. Пушкина, 1, НИЧ, ГОУ ВПО СГУ

(72) Автор(ы):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (RU)

(73) Патентообладатель(и):
ГОУ ВПО Ставропольский государственный университет (RU)

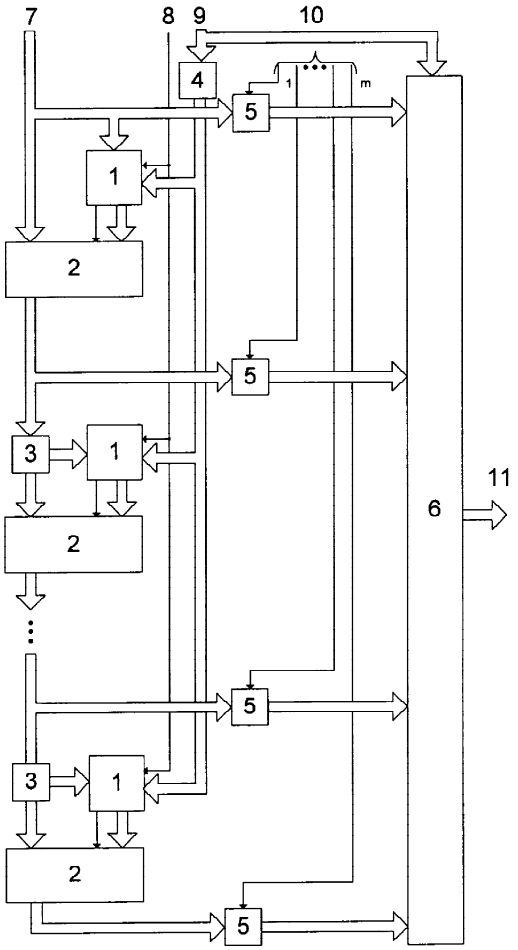
(54) УСТРОЙСТВО ДЛЯ УМНОЖЕНИЯ ЧИСЕЛ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ

(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, а также в устройствах для формирования элементов конечных полей. Техническим результатом является расширение функциональных возможностей устройства. Устройство содержит (m-1) сумматоров, (m-1) мультиплексоров, m ключей, (m-2) блоков сдвига, инвертор и сумматор по модулю. 1 ил.

RU 2316042 C1

RU 2316042 C1



RU 2316042 C1

RU 2316042 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 316 042** (13) **C1**

(51) Int. Cl.
G06F 7/523 (2006.01)
G06F 7/72 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2006128654/09, 07.08.2006**

(24) Effective date for property rights: **07.08.2006**

(45) Date of publication: **27.01.2008 Bull. 3**

Mail address:
355009, Stavropol'skij kraj, g.Stavropol', ul. Pushkina, 1, NICh, GOU VPO SGU

(72) Inventor(s):
Petrenko Vjacheslav Ivanovich (RU),
Kuz'minov Jurij Vladimirovich (RU)

(73) Proprietor(s):
GOU VPO Stavropol'skij gosudarstvennyj universitet (RU)

(54) DEVICE FOR MULTIPLYING NUMBERS WITH ARBITRARY MODULUS

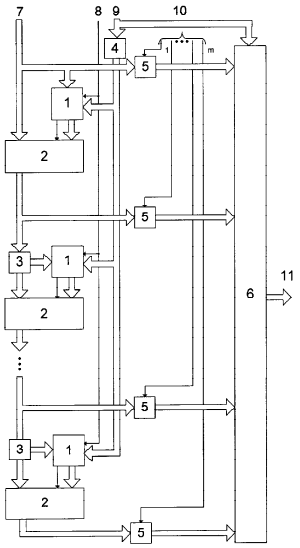
(57) Abstract:

FIELD: computer engineering, possible use in digital computing devices, and also in devices for forming elements of finite fields.

SUBSTANCE: device contains (m-1) adders, (m-1) multiplexers, m keys, (m-2) shift blocks, inverter and modulus adder.

EFFECT: expanded functional capabilities of the device.

1 dwg



RU 2316042 C1

RU 2316042 C1

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

Известно устройство для умножения чисел по модулю, содержащее два входных регистра, два дешифратора, три группы элементов ИЛИ, четыре группы элементов И, табличный вычислитель значений вида $\alpha'\beta'(\mathrm{mod}\ p/2)+p/2$, пять элементов ИЛИ, два элемента И и шифратор (см. АС СССР №1187161, кл. G06F 7/49, 23.10.1985).

Недостатком данного устройства является низкое быстродействие.

Наиболее близким по технической сущности к заявляемому изобретению является умножитель на два по модулю, содержащий сумматор и мультиплексор (см. патент РФ №2015537, кл. G06F 7/49, 30.06.1994).

Недостатком данного устройства являются его ограниченные функциональные возможности, а именно отсутствие возможности умножения на число, отличное от двух.

Цель изобретения - расширение функциональных возможностей умножителя на два по модулю за счет обеспечения возможности производить вычисление произведения по модулю чисел, отличных от двух.

Цель достигается путем применения следующего способа формирования остатков.

Пусть a, b, p (где a и b - множители, от произведения которых требуется сформировать остаток по произвольному модулю, p - модуль) - простые целые числа, представленные в двоичном виде, причем a<p и b<p.

Двоичная форма множителей имеет следующий вид:

$$a = a_n 2^n + a_{n-1} 2^{n-1} + \ldots + a_1 2^1 + a_0, \quad (1)$$

$$b = b_m 2^m + b_{m-1} 2^{m-1} + \ldots + b_1 2^1 + b_0. \quad (2)$$

Для формирования остатка от произведения $(a \times b) \bmod p$ необходимо сформировать частичный остаток по модулю p от числа a, умножить на два полученный результат и от полученного значения вновь вычислить частичный остаток. Данная операция повторяется m раз (где m - количество разрядов в двоичном коде числа b). Так как a<p, то частичным остатком на первом шаге вычислений будет являться само число a. То есть правило формирования частичных остатков от числа a имеет вид:

$$\begin{cases} r_1 = a; \\ r_j = (r_{j-1} \times 2) \bmod p, (j = 2 \ldots m+1). \end{cases} \quad (3)$$

Операция же умножения на два для двоичной системы счисления заключается в сдвиге кодовой комбинации на один разряд в сторону увеличения с записью нуля в младший разряд. Полученный на i-м шаге вычислений (i=1....m+1) остаток r_i суммируется по модулю p с остатками, сформированными на других шагах вычислений, в соответствии с коэффициентом при (i-1)-й степени двоичной формы числа b. Если $b_i=1$, остаток на i-м шаге вычислений суммируется с остальными, если $b_i=0$ - не суммируется. Результатом суммирования по модулю p полученных частичных остатков является остаток от произведения $(a \times b) \bmod p$.

Пример.

Пусть $a=10_{10}=1010_2$, $b=11_{10}=1011_2$, $p=13_{10}=1101_2$, тогда $(a \times b) \bmod p=(110_{10}) \bmod 13_{10}=6_{10}$.

Согласно вышеизложенному алгоритму, для вычисления искомого остатка от произведения $(a \times b) \bmod p$ необходимо m раз (m - количество разрядов в двоичной форме числа b, в данном случае m=3) вычислить частичные остатки от числа a, которые затем необходимо просуммировать в соответствии с коэффициентами при соответствующих степенях числа b.

На первом шаге вычислений частичным остатком r_1 будет являться само число a: $r_1=a=1010_2=10_{10}$.

Остальные частичные остатки формируются следующим образом:

$r_2=(r_1 \times 2) \bmod p=(10100_2) \bmod 1101_2=0111_2=7_{10}$;

$r_3=(r_2 \times 2) \bmod p=(01110_2) \bmod 1101_2=0001_2=1_{10}$;

$r_4=(r_3\times 2) \bmod p=(00010_2) \bmod 1101_2=0010_2=2_{10}$.

Так как число $b=11_{10}=1011_2$, необходимо просуммировать по модулю p частичные остатки с индексами, соответствующими номерам позиций ненулевых коэффициентов в двоичном коде числа b начиная с младшего разряда (в данном случае, первый, второй и четвертый частичные остатки). То есть

$r=(r_1+r_2+r_4) \bmod p=(10_{10}+7_{10}+2_{10}) \bmod 13_{10}=6_{10}$.

На чертеже представлена схема устройства для умножения чисел по произвольному модулю.

Устройство для умножения чисел по произвольному модулю содержит (m-1) сумматоров 1, (m-1) мультиплексоров 2, (m-2) блоков 3 сдвига, инвертор 4, m ключей 5 и сумматор 6 по модулю.

Входы 7 и 10 служат для подачи двоичных кодов умножаемых чисел a и b соответственно. Вход 8 служит для записи символа «1», служащего кодом начала операции. Вход 9 служит для записи кода модуля p. Выход 11 является выходом устройства.

Устройство для умножения чисел по произвольному модулю работает следующим образом.

Код числа a поступает на первый вход первого сумматора 1, первый информационный вход первого мультиплексора 2, а также на первый ключ 5, код модуля p поступает на вход инвертора 4, с выхода которого инверсный код модуля p подается на второй вход каждого сумматора 1. На третий вход каждого сумматора 1 подается символ «1», служащий для перевода инверсного кода модуля в дополнительный.

В общем виде i-й сумматор 2 (i=1...m-1) осуществляет операцию, описываемую выражением: $c = a + \bar{p} + 1$, где c - результат суммирования, a - число, поступающее на вход сумматора, $\bar{p}$ - инверсный код модуля. При сложении чисел, состоящих из l разрядов (где l - количество разрядов в двоичном представлении модуля p), (l+1)-й разряд сформированного значения c поступает на выход переноса сумматора 1, который подключен к управляющему входу i-го мультиплексора 2. Остальные разряды поступают на информационный выход сумматора 1, который подключен ко второму информационному входу i-го мультиплексора 2. Для вышеописанного примера, где $a=10_{10}=1010_2$, $p=13_{10}=1101_2$, $\bar{p} = 0010_2$, то есть для случая a<p, на выходе сумматора 1 сформируется результат вычисления $c = a + \bar{p} + 1 = 1010_2 + 0010_2 + 0001_2 = 01101_2$. На выход переноса сумматора 1 поступит символ «0». Если же a≥p, например $a=14_{10}=1110_2$, $p=13_{10}=1101_2$, $\bar{p} = 0010_2$, то на выходе сумматора 1 сформируется результат вычисления $c = a + \bar{p} + 1 = 1110_2 + 0010_2 + 0001_2 = 10001_2$. На выход переноса сумматора поступит символ «1». Остальные же разряды представляют разность (a-p).

Мультиплексор 2 при поступлении на управляющий вход символа «0» подключает на выход свой первый информационный вход, при поступлении символа «1» - второй информационный вход.

Таким образом, формирование значения на выходе связки «сумматор - мультиплексор» можно описать следующими выражениями:

$$r_1 = \begin{cases} a, a \prec p; \\ (a-p), a \geq p. \end{cases} \quad (4)$$

$$r_i = \begin{cases} r_{i-1} \times 2, (r_{i-1} \times 2) \prec p; \\ (r_{i-1} \times 2) - p, (r_{i-1} \times 2) \geq p. \end{cases} \quad (5)$$

В данных формулах i=2, ..., m.

С выхода j-го мультиплексора 2 (j=1, ..., m-2) сформированный частичный остаток поступает на вход j-го блока 3 сдвига (который, путем переноса всех разрядов входного числа на один разряд в сторону увеличения, осуществляет операцию умножения входного

числа на два), а также на вход (j+1)-го ключа 5. Сдвинутый на один разряд код числа с выхода j-го блока 3 сдвига подается на первый информационный вход (j+1)-го мультиплексора и на первый вход (j+1)-го сумматора 1. С выхода последнего мультиплексора 2 выходное значение поступает только на вход последнего ключа 5. То есть на входе первого ключа сформируется частичный остаток $r_1=a$, на входе i-го ключа (i=2, ..., m) сформируется частичный остаток r_i. Управление ключами осуществляется коэффициентами при соответствующих степенях двоичного представления числа b, поступающими со входа 7 устройства. На k-й ключ 5 поступает k-й коэффициент (k=1, ..., m) двоичного представления числа b. Для вышеописанного примера, где $b=11_{10}=1011_2$, на первый ключ 5 поступит символ «1», на второй - «1», на третий - «0», на четвертый - «1». Ключ пропускает информацию на выход в случае наличия на управляющем входе символа «1».

С выходов ключей значения частичных остатков поступают на вход сумматора 6 по модулю. Результатом суммирования по модулю p частичных остатков, формируемым на выходе сумматора 6 по модулю, будет являться искомое значение $(a\times b) \bmod p$.

Формула изобретения

Устройство для умножения чисел по произвольному модулю, содержащее (m-1) сумматоров, (m-1) мультиплексоров, отличающееся тем, что в него введены (m-2) блоков сдвига, m ключей и сумматор по модулю, причем вход записи двоичного кода первого из умножаемых чисел подключен к первому входу первого сумматора, первому информационному входу первого мультиплексора, а также к первому ключу, вход записи двоичного кода второго умножаемого числа поразрядно подключен к управляющему входу каждого ключа, вход записи символа «1» подключен к третьему входу каждого сумматора, вход записи двоичного кода модуля подключен ко входу инвертора, выход которого подключен ко второму входу каждого сумматора, причем выход переноса i-го сумматора подключен к управляющему входу i-го мультиплексора (i=1...m-1), информационный выход 1-го сумматора подключен ко второму информационному входу i-го мультиплексора, выход j-го мультиплексора (j=1...m-2) подключен ко входу j-го блока сдвига и ко входу (j+1)-го ключа, выход j-го блока сдвига подключен к первому информационному входу (j+1)-го мультиплексора и первому входу (j+1)-го сумматора, выход последнего мультиплексора подключен ко входу последнего ключа, выходы ключей подключены ко входам сумматора по модулю, выход которого является выходом устройства.