РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 445 730** (13) **C2**

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

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010106685/08, 24.02.2010**

(24) Дата начала отсчета срока действия патента:
24.02.2010

Приоритет(ы):
(22) Дата подачи заявки: **24.02.2010**

(43) Дата публикации заявки: **27.08.2011** Бюл. № 24

(45) Опубликовано: **20.03.2012** Бюл. № **8**

(56) Список документов, цитированных в отчете о поиске: **RU 2007033 C1, 30.01.1994. RU 2029435 C1, 20.02.1995. RU 2324972 C2, 20.05.2008. RU 2007037 C1, 30.01.1994. SU 1633495 A1, 07.03.1991. EP 0308963 A2, 29.03.1989. JP 11-282349 A, 15.10.1999.**

Адрес для переписки:
355009, Ставропольский край, г.Ставрополь, ул. Пушкина, 1, ГОУ ВПО "Ставропольский государственный университет", Научно-исследовательская часть

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

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

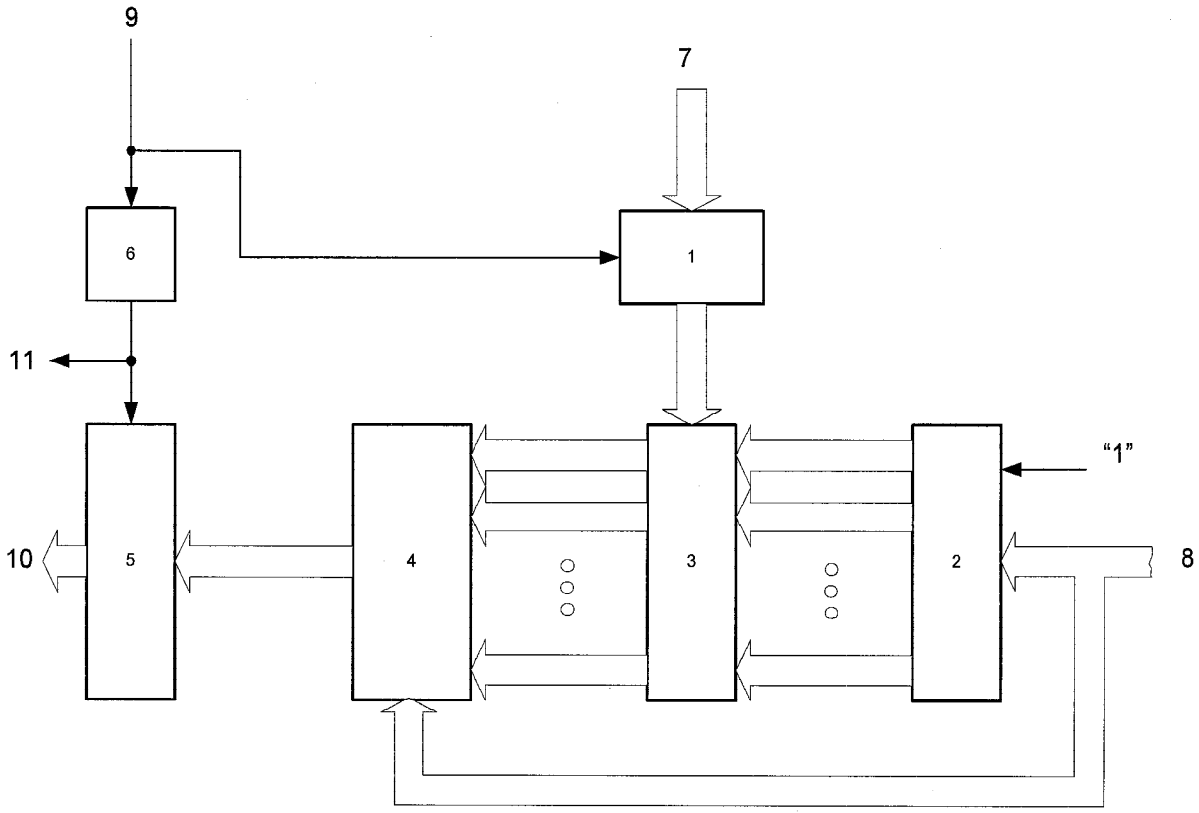
(54) УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ ОТ ЧИСЛА

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в сокращении объема оборудования. Он достигается тем, что устройство для формирования остатка по произвольному модулю от числа содержит первый и второй регистры, группу блоков элементов «И», блок сумматоров по модулю и элемент задержки, при этом в него введены (К-1) сумматоров по модулю, на вторые информационные входы которых подается код модуля, на первый информационный вход первого сумматора по модулю и на второй информационный вход группы блоков элементов «И» подается код числа «1», выход i-го сумматора по модулю соединен со вторым информационным входом группы блоков элементов «И» и со сдвигом на один разряд в сторону старших с первым информационным входом i+1 сумматора по модулю, где i=1, …, K-2, выход К-1 сумматора по модулю соединен со вторым информационным входом группы блоков элементов «И». 2 ил.

RU 2445730 C2

RU 2445730 C2



Фиг.1

RU 2445730 C2

RU 2445730 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 445 730** (13) **C2**

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

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010106685/08, 24.02.2010**

(24) Effective date for property rights:
24.02.2010

Priority:
(22) Date of filing: **24.02.2010**

(43) Application published: **27.08.2011** Bull. 24

(45) Date of publication: **20.03.2012 Bull. 8**

Mail address:
355009, Stavropol'skij kraj, g.Stavropol', ul. Pushkina, 1, GOU VPO "Stavropol'skij gosudarstvennyj universitet", Nauchno-issledovatel'skaja chast'

(72) Inventor(s):
Kopytov Vladimir Vjacheslavovich (RU),
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) DEVICE FOR GENERATING REMAINDER FROM ARBITRARY MODULUS OF NUMBER

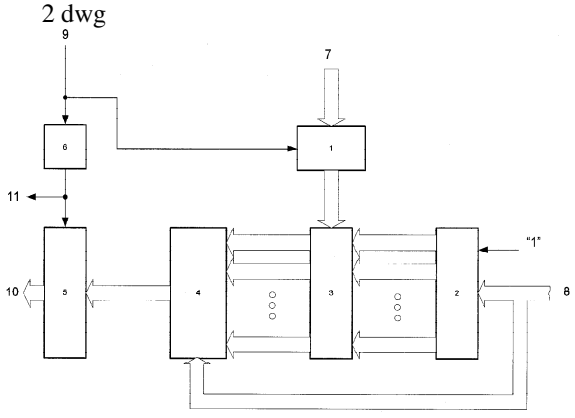
(57) Abstract:

FIELD: information technology.

SUBSTANCE: device for generating remainder on arbitrary modulus of a number has first and second registers, a group of AND elements, a unit of half-adders and a delay element, where the device also includes (K-1) half-adders, to whose second data inputs a modulus code is transmitted, and a number code "1" is transmitted to the first data input of the first half-adder and the second data input of the group of AND elements, the output of the i-th half-adder is connected to the second data input of the group of AND elements and with shift of one bit towards the most significant bits to the first data input of the i+1 half-adder, where i=1,…,K-2, the K-1 output of the half-adder is connected to the second data input of the group of AND elements.

EFFECT: cutting the size of equipment.

2 dwg



Фиг.1

RU 2445730 C2

RU 2445730 C2

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах, в криптографических приложениях, а также в устройствах для формирования кодовых последовательностей, построение которых основывается на теории конечных полей.

Известно устройство для формирования остатка по произвольному модулю от числа, содержащее первый и второй регистр, первый и второй элементы ИЛИ, вычислитель, первую схему сравнения и мультиплексор (Авторское свидетельство СССР N 1633495, кл. H03M 7/18, 1989).

Недостатком данного устройства является низкое быстродействие процесса формирования остатка.

Наиболее близким к предлагаемому по технической сущности и достигаемому результату является устройство для формирования остатка по произвольному модулю от числа, содержащее первый регистр, информационные входы которого являются входами кода числа, последовательно соединенные блок постоянной памяти, группу блоков элементов И, блок сумматоров по произвольному модулю и второй регистр, а также элемент задержки и блок инверторов (см. патент РФ №2007033, кл. H03M 7/18, 1994.01.30).

Недостатком данного устройства является большой объем оборудования.

Цель изобретения - сокращение объема оборудования.

Для достижения поставленной цели в устройство для формирования остатка по произвольному модулю от числа, содержащее первый и второй регистры, группу блоков элементов И, блок сумматоров по модулю и элемент задержки, причем вход числа соединен с информационными входами первого регистра, выходы которого соединены соответственно с первыми входами группы блоков элементов группы И, выходы которой соединены с первыми входами блока сумматоров по модулю, вход элемента задержки является входом начала вычислений и соединен со входом записи первого регистра, выход второго регистра является выходом устройства, вход модуля соединен со вторыми входами блока сумматоров по модулю, выход блока задержки соединен с выходом окончания работы устройства и входом записи второго регистра, информационные входы которого соединены с выходами блока сумматоров по модулю, введен блок формирования частичных остатков, на первый информационный вход которого подается код модуля, на второй информационный вход подается код числа «1», а информационные выходы соединены со вторыми входами группы блоков элементов И, при этом блок формирования частичных остатков содержит (К-1) сумматоров по модулю, причем первые информационные входы всех сумматоров по модулю соединены с первым информационным входом блока формирования частичных остатков, второй информационный вход блока формирования частичных остатков является его первым информационным выходом и со сдвигом на один разряд в сторону старших соединен со вторым информационным входом первого сумматора по модулю, выход i-го сумматора по модулю является i+1 информационным выходом блока формирования частичных остатков и со сдвигом на один разряд в сторону старших соединен со вторым информационным входом i+1 сумматора по модулю, где i=1, …, К-2, выход К-1 сумматора по модулю является К-ым информационным выходом блока формирования частичных остатков.

Сущность изобретения состоит в реализации следующей идеи приведения чисел по произвольному модулю. Известно, что позиционные системы счисления строятся по следующему принципу. Выбирается некоторое число m - основание системы счисления. Целое число А в m-ичной системе счисления представляется в виде конечной линейной

комбинации степеней числа m:

$$A = \sum_{i=0}^{k-1} a_i m^i, \qquad (1)$$

где k - разрядность представляемого числа, a_i - это целые числа, удовлетворяющие неравенству $0 \le a_i \le m-1$. Для двоичной системы счисления выражение (1) принимает вид:

$$A = \sum_{i=0}^{k-1} a_i 2^i, \qquad (2)$$

где a_i принимает значение 0 или 1.

Известно также, что сравнения можно почленно складывать, т.е.:

$A_1 \equiv B_1 (\mathrm{mod} P)$, $A_2 \equiv B_2 (\mathrm{mod} P) \ldots (A_k \equiv B_k (\mathrm{mod} P)$.

Тогда справедливо следующее выражение:

$$A_1 + A_2 + \ldots + A_k \equiv (B_1 + B_2 + \ldots + B_k)(\mathrm{mod}\ P) \qquad (3)$$

Учитывая выражения (2) и (3), можно записать:

$$\left(\sum_{i=0}^{k-1} a_i 2^i\right)(\mathrm{mod}\ P) \equiv \left(\sum_{i=0}^{k-1} \left(a_i 2^i\right)(\mathrm{mod}\ P)\right)(\mathrm{mod}\ P)$$

Так как для двоичной системы счисления коэффициенты a_i, i=0, …k-1, где k - разрядность представляемого числа A, принимают только два значения 0 и 1, то суммируя заранее вычисленные остатки по модулю P от чисел 2^i, i=0, … k-1, для тех i, для которых коэффициенты a_i=1, получают остаток по модулю P от числа A.

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

Устройство для формирования остатка по произвольному модулю от числа содержит (фиг.1) первый регистр 1, блок 2 формирования частичных остатков, группу 3 блоков элементов И, блок 4 сумматоров по модулю, второй регистр 5, элемент 6 задержки. Вход 7 служит для подачи кода числа A, вход 8 служит для подачи кода модуля P. Вход 9 - вход начала вычисления. Выход 11 - выход конца вычисления. Выход 10 является информационным выходом устройства.

Блок 2 формирования частичных остатков содержит (фиг.2) К-1 сумматоров 14 по модулю. Вход 12 служит для подачи кода модуля P, выходы 13.1-13.К являются выходами частичных остатков модуля P. На второй информационный вход блока 2 формирования частичных остатков подается код числа «1».

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

В исходном состоянии регистры 1 и 5 обнулены. На вход 7 подается код числа A. На управляющий вход 9 подается сигнал начала вычислений. Под воздействием сигнала начала вычислений в регистр 1 записывается код числа A. На вход 8 подается код модуля P и блок 2 формирования частичных остатков формирует частичные остатки от чисел 2^i по модулю P, которые подаются на вторые информационные входы группы блоков 3 элементов «И». Поразрядно в блоке 3 элементов И умножаются частичные остатки модуля P и разряды числа A, поступающие на первые входы блока. В блоке 4 сумматоров по модулю результаты умножения складываются и снова вычисляются по модулю P. Результат поступает на вход регистра 5, выход которого является информационным выходом устройства для формирования остатка по произвольному модулю от числа. Под воздействием импульса, поступающего с выхода элемента задержки 6, рассчитанного на задержку, равную времени формирования остатка, в регистр 5 происходит запись результата, который в

результате этого появляется на выходе устройства. Импульс с выхода элемента задержки 6 поступает также на выход 11 устройства, свидетельствуя об окончании процесса формирования остатка.

Блок 2 формирования частичных остатков работает следующим образом (см. фиг.2). На первый вход первого сумматора 14 по модулю и на выход 13.0 поступает логическая единица. На вторые входы всех сумматоров 14 по модулю подается код модуля. Результат вычислений с выхода сумматора 14 по модулю поступает на соответствующий выход блока 13.i, где i=1…K-1, а также со сдвигом на один разряд в сторону старшего поступает на первый вход следующего по схеме сумматора 14 по модулю. Каждый сумматор 14 по модулю сравнивает модуль и поступающее число. Если модуль больше числа, то на выход сумматора 14 по модулю подается число, иначе - разность модуля и числа.

Рассмотрим работу устройства для формирования частичных остатков на примере. Зададим начальные условия. $A=29_{10}=11101_2$, модуль $P=13_{10}=1101_2$

Коэффициент 2^i	2^0	2^1	2^2	2^3	2^4
2^i (modl3)	1	2	4	8	3
Код числа А	1	0	1	1	1
Результат логической операции «И»	1	0	4	8	3
Суммирование	16				
Сумма по mod 13	3				

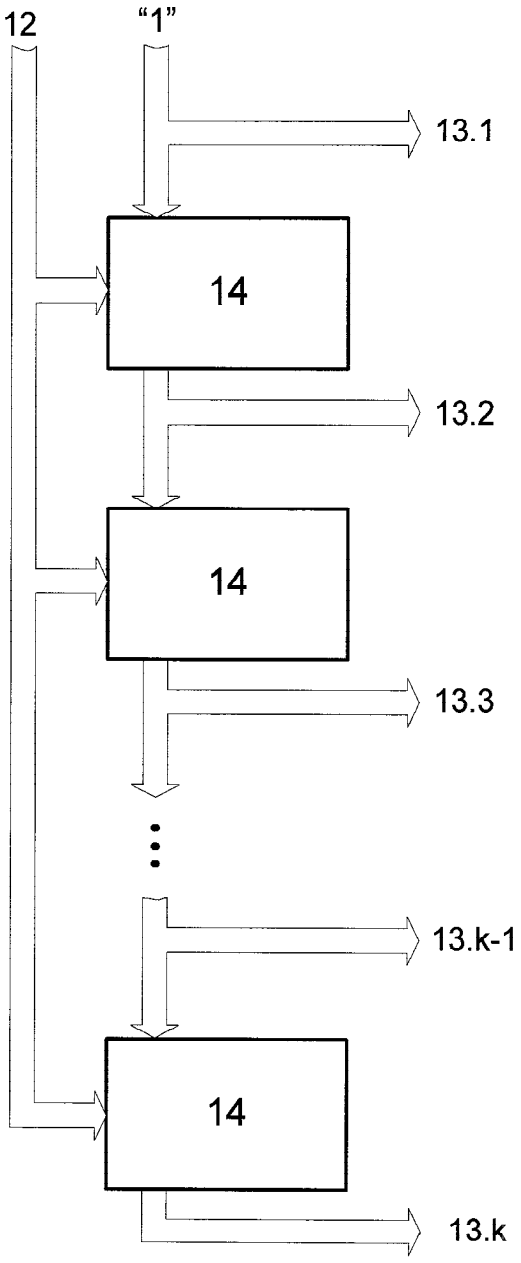
Проверим: 29≡3 mod 13.

Эффективность заявляемого устройства перед устройством-прототипом заключается в существенном уменьшении объема оборудования при формировании остатков. Расчеты показывают, что если проводить вычисления с 64-разрядными числами, то устройство-прототип должно иметь блок постоянной памяти для хранения k*l частичных остатков, где k=64 количество разрядов числа, $l=2^{64}$ количество модулей, то есть объем блока постоянной памяти составит $k*l=64*2^{64}=2^{70}$ ячеек. В заявляемом устройстве при тех же исходных данных вырабатывается k частичных остатков, т.е. объем оборудования составляет $64=2^6$ сумматоров, т.к. частичные остатки вычисляются в процессе формирования остатка для одного определенно заданного модуля.

Формула изобретения

Устройство для формирования остатка по произвольному модулю от числа, содержащее первый и второй регистры, группу блоков элементов «И», блок сумматоров по модулю и элемент задержки, причем вход числа соединен с информационными входами первого регистра, выходы которого соединены соответственно с первыми входами группы блоков элементов «И», выходы которой соединены с первыми входами блока сумматоров по модулю, вход элемента задержки является входом начала вычислений и соединен со входом записи первого регистра, выход второго регистра является выходом устройства, вход кода модуля соединен со вторыми входами блока сумматоров по модулю, выход элемента задержки соединен с выходом окончания работы устройства и входом записи второго регистра, разрядные входы которого соединены с выходами блока сумматоров по модулю, отличающееся тем, что в него введены (К-1) сумматоров по модулю, на вторые информационные входы которых подается код модуля, на первый информационный вход первого сумматора по модулю и на второй информационный вход группы блоков элементов

«И» подается код числа «1», выход i-го сумматора по модулю соединен со вторым информационным входом группы блоков элементов «И» и со сдвигом на один разряд в сторону старших с первым информационным входом i+1 сумматора по модулю, где i=1, …, K-2, выход K-1 сумматора по модулю соединен со вторым информационным входом группы блоков элементов «И».



Фиг. 2