РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 299 462** (13) **C1**

(51) МПК
G06F 7/72 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005130896/09, 05.10.2005**

(24) Дата начала отсчета срока действия патента:
05.10.2005

(45) Опубликовано: **20.05.2007 Бюл. № 14**

(56) Список документов, цитированных в отчете о поиске: **RU 2029435 C1, 20.02.1995. RU 2132081 C1, 20.06.1999. SU 1238077 A1, 15.06.1986. SU 750484 A1, 23.07.1980. JP 10260818, 29.09.1998. JP 11282349, 15.10.1999.**

Адрес для переписки:
355017, г.Ставрополь, ул. Артема, 2, Ставропольский военный институт связи, РВ,НИО

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

(73) Патентообладатель(и):
Петренко Вячеслав Иванович (RU),
Кузьминов Юрий Владимирович (RU)

(54) УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА ПО ДВОЙНОМУ МОДУЛЮ

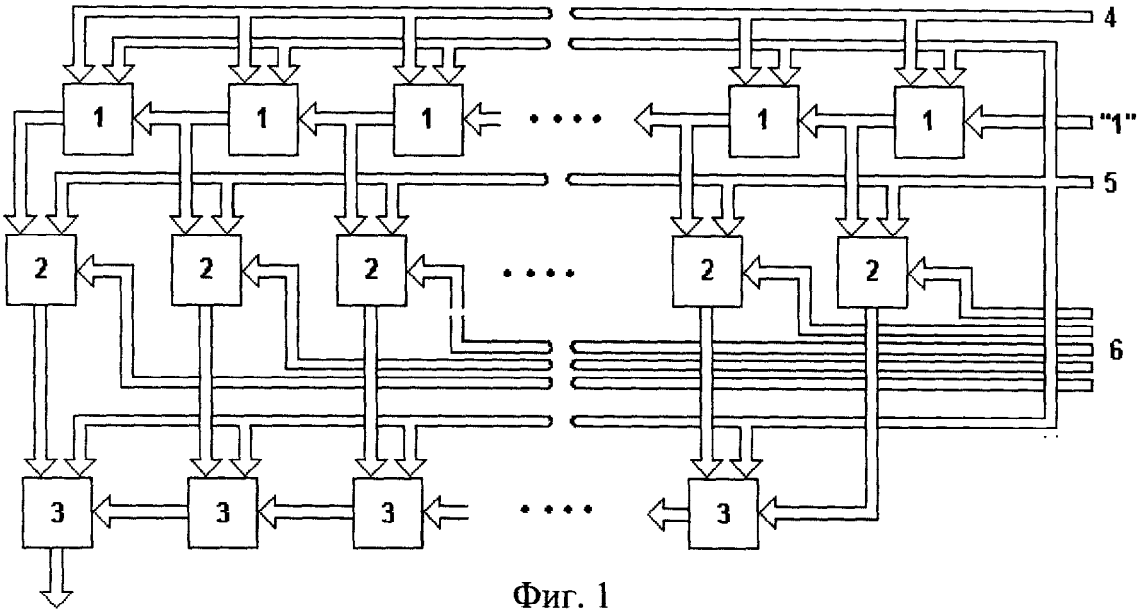
(57) Реферат:

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах для формирования кодовых последовательностей, построение которых основано на теории конечных полей. Техническим результатом является расширение функциональных возможностей за счет формирования остатков по двойному модулю, путем вычисления частичных остатков от степеней полинома с последующим их суммированием в соответствии с коэффициентами при степенях полинома. Устройство содержит блоки формирования частичных остатков, умножители по модулю, сумматоры по модулю. 2 з.п. ф-лы, 3 ил.

RU 2299462 C1

RU 2299462 C1

Устройство для формирования остатка по двойному модулю



Фиг. 1

RU 2299462 C1

RU 2299462 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 299 462** (13) **C1**

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

(12) ABSTRACT OF INVENTION

Based on Article 13, par. 3 of the Patent law of the Russian Federation of September 23, 1992, #3517-I the patent owner undertakes to transfer the exclusive right to the invention (assign the patent), on generally practiced conditions, to the first person - citizen of the Russian Federation or a Russian legal person who expresses such a wish and conveys it to the patent owner and the Federal executive body for Intellectual Property.

(21), (22) Application: **2005130896/09, 05.10.2005**

(24) Effective date for property rights: **05.10.2005**

(45) Date of publication: **20.05.2007 Bull. 14**

Mail address:
**355017, g.Stavropol', ul. Artema, 2,
Stavropol'skij voennyj institut svjazi, RV,NIO**

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

(73) Proprietor(s):
**Petrenko Vjacheslav Ivanovich (RU),
Kuz'minov Jurij Vladimirovich (RU)**

(54) DEVICE FOR FORMING REMAINDER BY DOUBLE MODULUS

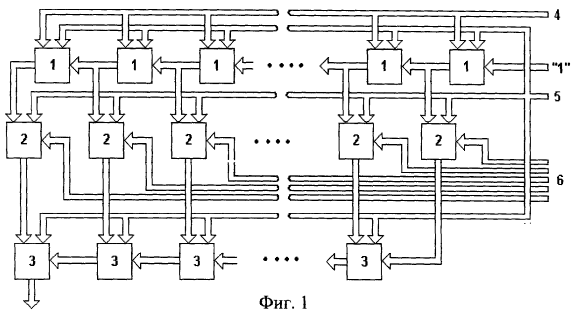
(57) Abstract:

FIELD: computer engineering, possible use in digital computing devices for forming code series, creation of which is based on finite fields theory.

SUBSTANCE: device contains block for forming partial remainders, modulus multiplexers, modulus adders.

EFFECT: expanded functional capabilities due to creation of remainders by double modulus, by calculating partial remainders from polynomial powers with their following addition in acc to coefficients of polynomial powers.

3 dwg



Фиг. 1

RU 2299462 C1

RU 2299462 C1

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

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, а также отсутствие возможности формирования остатков по двойному модулю.

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 являются его ограниченные функциональные возможности, а именно отсутствие возможности формирования остатков по двойному модулю.

Цель изобретения - расширение функциональных возможностей устройства формирования остатков за счет обеспечения формирования остатков по двойному модулю.

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

Известно, что элементами расширенного поля Галуа $GF(p^n)$ являются полиномы вида

$$A(x) = \sum_{i=0}^{n-1} a_i x^i,$$

причем a_i принадлежит полю $GF(p)$.

Процедуру вычисления остатка от полинома A(x) по двойному модулю (F(x), p), где A(x) и F(x) - полиномы над полем $GF(p^n)$, причем F(x) является неприводимым полиномом над полем $GF(p^n)$, можно представить в виде вычисления частичных остатков от каждой степени полинома A(x) с последующим их суммированием в соответствии со значением коэффициента при данной степени.

Алгоритм формирования остатка по двойному модулю имеет следующий вид.

Вычисляется частичный остаток от младшей степени полинома A(x), после чего частичный остаток умножается на коэффициент при соответствующей степени полинома A(x) и поступает в сумматор. Степень частичного остатка увеличивается на один разряд путем сдвига всех разрядов частичного остатка на один влево, после чего от полученного выражения вновь вычисляется частичный остаток.

Если полиномы A(x) и F(x) представить в виде $A(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ и $F(x)=b_kx^k+b_{k-1}x^{k-1}+...+b_1x+b_0$, причем k меньше n, то частичный остаток от A(x) по двойному модулю (F(x), p) имеет вид $R(x)=c_{k-1}x^{k-1}+c_{k-2}x^{k-2}+...+c_1x+c_0$. Коэффициенты при степенях R(x) формируются на основании коэффициентов, полученных при вычислении частичного остатка от предыдущей степени полинома A(x), и коэффициентов полинома F(x) на основании выражения:

$$R^*(x)=(c_{k-2}-c_{k-1}b_{k-1})x^{k-1}+(c_{k-3}-c_{k-1}b_{k-2})x^{k-2}+...+(c_0-c_{k-1}b_1)x+(-c_{k-1}b_0).$$

Каждый сформированный частичный остаток поступает на вход сумматора, где складывается по модулю p с результатом предыдущих вычислений. С выхода каждого сумматора результат поступает на вход последующего сумматора, а на выходе последнего сумматора по завершении всех операций будет сформирован остаток от полинома A(x) по двойному модулю (F(x), p).

На фиг.1 представлена схема устройства формирования остатка по двойному модулю, на фиг.2 - схема блока формирования частичных остатков, на фиг.3 - схема блока формирования коэффициентов.

Устройство формирования остатка по двойному модулю состоит из (n+1) последовательно соединенных блоков 1 формирования частичных остатков, (n+1)

умножителей 2 по модулю и n сумматоров 3 по модулю.

Первый вход первого блока 1 формирования частичных остатков служит для записи кода «1», являющегося кодом начала операции, на первый вход каждого из последующих блоков 1 формирования частичных остатков подаются выходы разрядов предыдущего блока 1 формирования частичных остатков со сдвигом на один разряд в сторону старшего. Второй вход каждого блока 1 формирования частичных остатков служит для записи кода модуля p, поступающего со входа 5 устройства. На третий вход каждого блока 1 формирования частичных остатков подаются коэффициенты полинома модуля.

Выход i-го блока 1 формирования частичных остатков также подается на вход i-го умножителя 2 по модулю, причем i=1, ..., n+1, для перемножения со значением коэффициента при (i-1)-й степени полинома A(x), поступающим на второй вход умножителя 2 по модулю со входа 6 устройства. На третий вход каждого умножителя 2 по модулю подается код модуля p со входа 5 устройства.

Выход j-го умножителя 2 по модулю подается на первый вход (j-1)-го сумматора 3 по модулю, причем j=2, ...n+1, выход первого умножителя 2 по модулю подается на второй вход первого сумматора 3 по модулю. На второй вход j-го сумматора 3 по модулю подается выход (j-1)-го сумматора 3 по модулю. На третий вход каждого сумматора 3 по модулю подается код модуля p со входа 5 устройства. Выход n-го сумматора является выходом устройства.

Блок 1 формирования частичных остатков (фиг.2) содержит k блоков 7 формирования коэффициентов, на первые входы которых подается коэффициент при (k-1)-й степени частичного остатка, полученного на предыдущем шаге. На второй вход m-го блока 7 формирования коэффициентов подается коэффициент при (m-2)-й степени частичного остатка, полученного на предыдущем шаге, причем m=2, ..., k, второй вход первого блока 7 формирования коэффициентов отключен. На третий вход r-го блока 7 формирования коэффициентов подается коэффициент при (r-1)-й степени полинома модуля, поступающий со входа 4 устройства, причем r=1, ..., k. Выход r-го блока 7 формирования коэффициентов представляет коэффициент при (r-1)-й степени частичного остатка.

Блок 7 формирования коэффициентов (фиг.3) содержит последовательно соединенные умножитель 8 по модулю, вычитатель 9 по модулю и сумматор 10 по модулю, причем на первый вход умножителя 8 по модулю подключен первый вход блока 7 формирования коэффициентов, на второй вход умножителя 8 по модулю подключен третий вход блока 7 формирования коэффициентов. Второй вход блока 7 формирования коэффициентов подключен ко второму входу сумматора 10 по модулю. Выход умножителя 8 по модулю подключен к первому входу вычитателя 9 по модулю, выход которого подключен к первому входу сумматора 10 по модулю. К третьему входу умножителя 8 по модулю, второму входу вычитателя 9 по модулю и третьему входу сумматора 10 по модулю подается код модуля p со входа 5 устройства.

Устройство работает следующим образом. В исходном состоянии на вход 4 поданы коэффициенты полинома модуля F(x), на вход 5 устройства подан код модуля p. Входы 4 и 5 определяют двойной модуль (F(x),p), по которому формируется остаток от полинома A(x). Коэффициенты данного полинома со входа 6 устройства поданы на вторые входы соответствующих умножителей 2 по модулю и определяют значение частичного остатка от соответствующей степени полинома A(x), которое поступит в сумматор 3 по модулю.

Процесс формирования остатка начинается с подачи на первый вход первого блока 1 кода числа «1». В блоке 1 формирования частичных остатков данный код поступает на второй вход второго блока 7 формирования коэффициентов. В блоке 7 формирования коэффициентов данный код складывается в сумматоре 10 по модулю с результатом, полученным в блоке вычитателя 9 при вычитании значения, поступившего с выхода умножителя 8 по модулю, из значения модуля p. Умножитель 8 по модулю формирует произведение значений, поступающих на его вход со входов 1 и 3 блока 7 формирования коэффициентов.

Полученное значение коэффициента с выхода сумматора 10 по модулю поступает на выход блока 7 формирования коэффициентов, после чего вместе со значениями коэффициентов, сформированными в остальных блоках 7 формирования коэффициентов, поступает на выход блока 1 формирования частичных остатков. С выхода блока 1 формирования частичных остатков значения коэффициентов поступают на вход последующего блока 1 формирования частичных остатков со сдвигом на один разряд в сторону старшего, где с ними осуществляются все вышеуказанные операции, а также на вход умножителя 2 по модулю. В умножителе 2 по модулю значения коэффициентов частичного остатка умножаются на значение коэффициента при степени полинома A(x), от которой вычисляется остаток (на вход i-го умножителя 2 по модулю подается значение коэффициента при (i-1)-й степени полинома A(x), где i=1, ..., n) в соответствии с модулем p, поступающим со входа 5 устройства. С выхода умножителя 2 по модулю полученные значения поступают на вход сумматора 3 по модулю, где суммируются со значениями, полученными на предыдущем шаге, в соответствии с модулем p, поступающим со входа 5 устройства. Значения коэффициентов, полученные на выходе n-го сумматора 3 по модулю, являются коэффициентами остатка от полинома A(x) по двойному модулю (F(x), p).

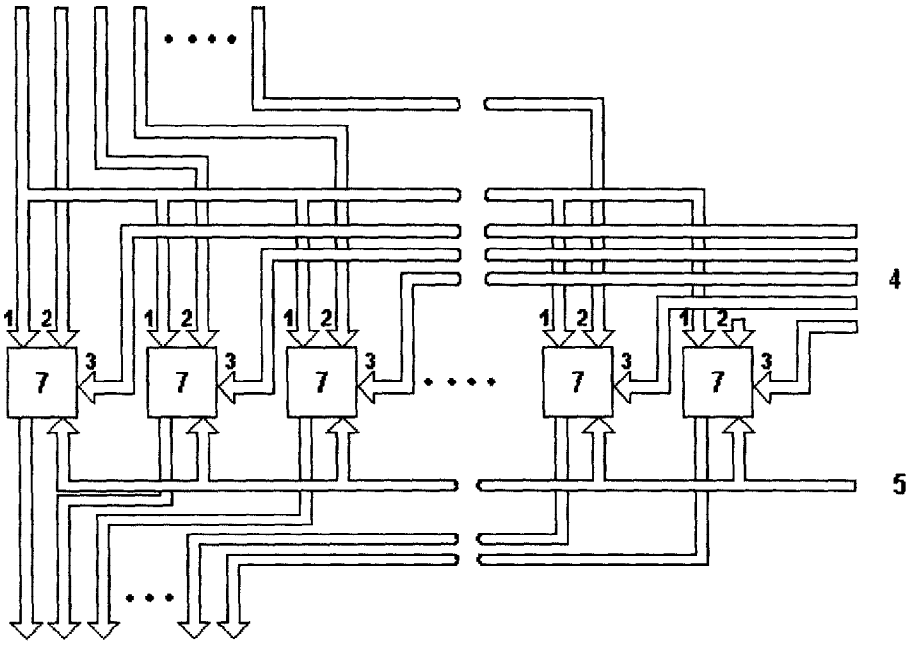
Формула изобретения

1. Устройство для формирования остатка по двойному модулю, содержащее (n+1) блоков формирования частичных остатков, n сумматоров по модулю, причем первый вход первого блока формирования частичных остатков соединен с входом записи кода начала операции, первый вход i-го блока формирования частичных остатков соединен с выходом (i-1) блока формирования частичных остатков, где i=2, ..., n+1, вторые входы блоков формирования частичных остатков соединены со входом записи значений коэффициентов полинома модуля, отличающееся тем, что в него введены (n+1) умножителей по модулю, причем первый вход j-го умножителя по модулю соединен с выходом j-го блока формирования частичных остатков, где j=1, ...,n+1, вторые входы умножителей по модулю соединены с входом записи значений коэффициентов полинома, третьи входы умножителей по модулю соединены с входом записи кода модуля, выход i-го умножителя по модулю соединен с первым входом (i-1) сумматора по модулю, выход первого умножителя по модулю соединен со вторым входом первого сумматора по модулю, выход m-го сумматора по модулю соединен со вторым входом (m+1)-го сумматора по модулю, где m=1, ...,n-1, третьи входы сумматоров по модулю соединены с входом записи кода модуля, выход n-го сумматора по модулю является выходом устройства.

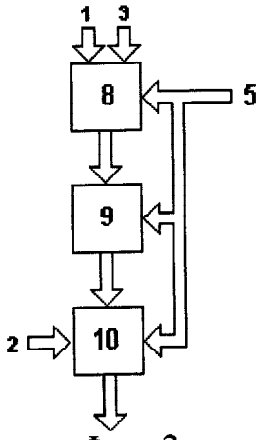
2. Устройство по п.1, отличающееся тем, что в блок формирования частичных остатков содержит k блоков формирования коэффициентов, причем первые входы блоков формирования коэффициентов подключены к входу записи коэффициента при (k-1)-й степени частичного остатка, второй вход r-го блока формирования коэффициентов подключен к входу записи коэффициента при (r-1)-й степени частичного остатка, где r= 2, ..., k, второй вход первого блока формирования коэффициентов отключен, третий вход v-го блока формирования коэффициентов, где v=1, ..., k, соединен с входом записи коэффициента при (v-1)-й степени полинома модуля, четвертый вход блоков формирования коэффициентов подключен к входу записи кода модуля, выходы блоков формирования коэффициентов являются выходом блока формирования частичных остатков.

3. Устройство по п.2, отличающееся тем, что блок формирования коэффициентов содержит умножитель по модулю, вычитатель по модулю и сумматор по модулю, причем к первым двум входом умножителя по модулю подключены соответственно первый и третий входы блока формирования коэффициентов, выход умножителя по модулю подключен к первому входу вычитателя по модулю, выход вычитателя по модулю подключен к первому входу сумматора по модулю, ко второму входу сумматора по модулю подключен второй вход блока формирования коэффициентов, к третьему входу умножителя по модулю,

второму входу вычитателя по модулю, третьему входу сумматора по модулю подключен вход записи кода модуля, выход сумматора по модулю является выходом блока формирования коэффициентов.



Фиг. 2



Фиг. 3