РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 368 942** (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: **2007124282/09, 27.06.2007**

(24) Дата начала отсчета срока действия патента:
27.06.2007

(43) Дата публикации заявки: **10.01.2009**

(45) Опубликовано: **27.09.2009** Бюл. № **27**

(56) Список документов, цитированных в отчете о поиске: **RU 2029435 C1, 20.02.1995. RU 2025897 C1, 30.12.1994. RU 2015537 C1, 30.06.1994. SU 1633495 A1, 07.03.1991. JP 11282349 A, 15.10.1999. EP 0308963 A2, 29.03.1989.**

Адрес для переписки:
355017, Ставропольский край, г.Ставрополь, ул. Артема, 2, Ставропольский военный институт связи РВ, научно-исследовательский отдел

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

(73) Патентообладатель(и):
Государственное образовательное учреждение высшего профессионального образования "Ставропольский военный институт связи РВ" (RU)

(54) УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА 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 и в криптографических приложениях. Техническим результатом является повышение быстродействия. Устройство содержит блок формирователей частичных остатков по модулю, блок умножителей по модулю и блок сумматоров по модулю. 3 н.п. ф-лы, 3 ил.

RU 2368942 C2

RU 2368942 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 368 942** (13) **C2**

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

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2007124282/09, 27.06.2007**

(24) Effective date for property rights:
27.06.2007

(43) Application published: **10.01.2009**

(45) Date of publication: **27.09.2009 Bull. 27**

Mail address:
355017, Stavropol'skij kraj, g.Stavropol', ul. Artema, 2, Stavropol'skij voennyj institut svjazi RV, nauchno-issledovatel'skij otdel

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

(73) Proprietor(s):
Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Stavropol'skij voennyj institut svjazi RV" (RU)

(54) DEVICE FOR GENERATING REMAINDER WITH ARBITRARY MODULUS

(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to computer engineering and can be used in digital computing devices, as well as in devices for generating finite field elements and in cryptographic applications. The device has a unit for generating partial remainders in absolute magnitude, unit of modulus multipliers and unit of modulus adders.

EFFECT: faster operation.

4 cl, 3 dwg

RU 2368942 C2

RU 2368942 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 регистры, элементы ИЛИ, вычислитель, схемы сравнения, мультиплексор, элемент задержки, сумматор, группу блоков элементов И и блок постоянной памяти со связями (см. авт. св. 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 является низкое быстродействие.

Целью изобретения является повышение быстродействия.

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

Пусть требуется сформировать остаток r от числа A по модулю p.

Число A может быть представлено в позиционной системе счисления в виде

$$A = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + a_{n-3}2^{n-3} + \ldots + a_2 2^2 + a_1 2^1 + a_0 2^0, \qquad (1)$$

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:

$$A = 2^{2t}\left(a_{2t+1}2 + a_{2t}\right) + 2^{2(t-1)}\left(a_{2(t-1)+1}2 + a_{2(t-1)}\right) + \ldots + 2^4\left(a_5 2 + a_4\right) + 2^2\left(a_3 2 + a_2\right) + \left(a_1 2 + a_0\right) \qquad (2)$$

где $t = \frac{n}{2}$, если n четное, и $t = \left[\frac{n}{2}\right] + 1$, если n нечетное, [] - целая часть от деления.

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.

Для вычисления остатка от числа A по модулю p достаточно в выражении (2) просуммировать частичные остатки по модулю p от чисел $2^{2i}(a_{2i+1}2+a_{2i})$, где $i = \overline{1, \left[\frac{n}{2}\right]}$ - при n четном и $i = \overline{1, \left[\frac{n}{2}\right] + 1}$ при n нечетном. Частичные остатки получаются в результате умножения частичного остатка от 2^{2i} по модулю p на число $(a_{2i+1}2+a_{2i})$. Способ вычисления частичных остатков от 2^{2i} по модулю p состоит в следующем. Вычисление частичного остатка от 2^{2i} заключается в умножении на четыре частичного остатка от $2^{2(i-1)}$ и приведение результата по модулю p. Операция умножения на четыре может быть реализована сдвигом всех разрядов числа на два разряда влево. Операция приведения по модулю реализуется следующим образом. Если число не превышает величину p, то оно остается без изменения. Если оно лежит в интервале от p до 2p-1, то из него вычитается модуль p. Если число лежит в интервале

от 2p до 3p-1, то из него вычитается удвоенный модуль p. Если число лежит в интервале от 3p до 4p-1, то из него вычитается утроенный модуль p. Способ умножения частичного остатка от 2^{2i} по модулю p на число ($a_{2i+1}2+a_{2i}$) состоит в следующем. Частичный остаток от 2^{2i} по модулю p, умноженный на $a_{2i+1}2$, складывается с частичным остатком от 2^{2i} по модулю p, умноженный на a_{2i}. Если полученный результат не превышает величину p, то оно остается без изменения. Если оно лежит в интервале от p до 2p-1, то из него вычитается модуль p. Если число лежит в интервале от 2p до 3p-1, то из него вычитается удвоенный модуль p. Суммирование по модулю p частичных остатков происходит последовательно.

На фиг.1 представлена схема устройства для формирования остатка по произвольному модулю от числа; на фиг.2 - формирователя частичных остатков; на фиг.3 - умножителя по модулю.

Устройство формирования остатка по произвольному модулю от числа (фиг.1) содержит блок 1 формирователей частичных остатков, блок 2 умножителей по модулю и блок 3 сумматоров по модулю. Входы 4 служат для подачи двоичного кода числа A. Выход 5 является выходом остатка устройства формирования остатка по произвольному модулю от числа.

Блок 1 формирователей частичных остатков (фиг.1) содержит n/2 формирователей частичных остатков 6, соединенных последовательно, причем на вход первого формирователя частичных остатков 6 подан код единицы, разряд которого сдвинут на два разряда влево. Выходы разрядов предыдущего формирователя частичных остатков 6 подаются на входы последующего формирователя частичных остатков 6 со сдвигом на два в сторону старших. Выходы каждого формирователя частичных остатков 6 являются информационными выходами формирователя. Блок 2 умножителей по модулю (фиг.1) содержит n/2 умножителей по модулю 7, на информационные входы которых подаются коды с выходов формирователей частичных остатков 6. Блок 3 сумматоров по модулю (фиг.1) содержит n/2 сумматоров по модулю 8, на информационные входы которых подаются коды с выходов умножителей по модулю 7 и с выходов предыдущего сумматора по модулю 8, причем на первый сумматор по модулю 8 подаются два младших разряда кода числа A.

Каждый формирователь частичных остатков (фиг.2) содержит три сумматора 12 и мультиплексор 13. На входы переносов трех сумматоров 12 подается код единицы. На первые информационные входы трех сумматоров 12 подается код с выхода формирователя частичных остатков 6. Вход 9 служит для подачи инверсного кода модуля, вход 10 - для подачи инверсного кода удвоенного кода модуля, вход 11 - для подачи инверсного кода утроенного кода модуля.

Каждый умножитель 7 по модулю (фиг.3) содержит два ключа 16, которые управляются разрядами кода числа A, три сумматора 17 и мультиплексор 18. Вход 14 служит для подачи инверсного кода модуля, вход 15 - для подачи инверсного кода удвоенного кода модуля.

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

На вход первого формирователя частичных остатков 6 подается код единицы, сдвинутый на два разряда в сторону старших, выходы разрядов предыдущего формирователя частичных остатков 6 подключены к входам последующего формирователя частичных остатков 6 со сдвигом на два разряда в сторону старших. Таким образом на выходах блока формирования частичных остатков 1 формируются

частичные остатки по модулю p от числа 2^{2i}, где $i = \overline{1, \left[\frac{n}{2}\right]}$ при n четном и $i = \overline{1, \left[\frac{n}{2}\right] + 1}$ при n нечетном.

Код числа A через входы 4 поступает на управляющие входы умножителя 7 по модулю. Умножитель 7 по модулю умножает частичный остаток по модулю p от числа 2^{2i} на число $(a_{2i+1}2+a_{2i})$, где a_i коэффициенты двоичного кода числа A, и вычисляет частичный остаток по модулю p от полученного результата. Блок сумматоров 3 по модулю суммирует по модулю p частичные остатки и число $(a_1 2+a_0)$. Результат суммирования выдается на информационные выходы 5 устройства для формирования остатка по произвольному модулю от числа.

Формирователь частичных остатков работает следующим образом. На первые информационные входы трех сумматоров 12 и на первый информационных вход мультиплексора 13 подается частичный остаток t_{i-1} по модулю p от числа $2^{2(i-1)}$, сдвинутый на два разряда в сторону старших. На входы переносов трех сумматоров 12 подается код единицы. На второй вход первого сумматора 12 подается инверсный код модуля p. На второй вход второго сумматора 12 подается инверсный код удвоенного модуля p. На второй вход третьего сумматора 12 подается инверсный код утроенного модуля p. Первый сумматор 12 выполняет операцию $\left(t_{i-1} + \overline{p} + 1\right)$. Сигнал со старшего (k+1)-го разряда полученного значения, где k - количество разрядов инверсного двоичного кода модуля p, поступает на выход переноса первого сумматора 12. Остальные разряды представляют собой разность $(t_{i-1}-p)$. Второй сумматор выполняет операцию $\left(t_{i-1} + \overline{2p} + 1\right)$. Сигнал со старшего (k+1)-го разряда полученного значения, где k - количество разрядов инверсного двоичного кода удвоенного модуля p, поступает на выход переноса второго сумматора 12. Остальные разряды представляют собой разность $(t_{i-1}-2p)$. Третий сумматор выполняет операцию $\left(t_{i-1} + \overline{3p} + 1\right)$. Сигнал со старшего (k+1)-го разряда полученного значения, где k - количество разрядов инверсного двоичного кода утроенного модуля p, поступает на выход переноса третьего сумматора 12. Остальные разряды представляют собой разность $(t_{i-1}-3p)$. Если на выходе переноса третьего сумматора 12 сигнал равен "1", то на выходе формирователя частичных остатков будет разность $(t_{i-1}-3p)$. Если на выходе переноса третьего сумматора 12 сигнал равен "0", а на выходе переноса втоого сумматора 12 сигнал равен "1", то на выходе формирователя частичных остатков будет разность $(t_{i-1}-2p)$. Если на выходе переноса третьего сумматора 12 сигнал равен "0" и на выходе переноса второго сумматора 12 сигнал равен "0", а на выходе переноса первого сумматора 12 сигнал равен "1", то на выходе формирователя частичных остатков будет разность $(t_{i-1}-p)$. Если на выходе переноса третьего сумматора 12 сигнал равен "0", на выходе переноса второго сумматора 12 сигнал равен "0" и на выходе переноса первого сумматора 12 сигнал равен "0", то на выходе формирователя частичных остатков будет число t_{i-1}.

Умножитель по модулю работает следующим образом. Коэффициенты a_{i+1} и a_i, через входы 4 поступают на управляющие входы двух ключей 16. На информационные входы двух ключей подается частичный остаток t_i по модулю p от числа 2^{2t}. В зависимости от того, на управляющий вход какого из ключей 16 поступает

логическая "1", тот из ключей 16 оказывается открытым и коммутирует на свои выходы значения с информационных входов, которые поступают на входы первого сумматора 17. Причем на первый вход первого сумматора 17 поступает значение, сдвинутое на один разряд влево. На выходе первого сумматора оказывается результат умножения частичного остатка t_1, по модулю p от числа 2^{2i} на число ($a_{2i+1}2+a_{2i}$,). Результат вычисления поступает на первые входы второго и третьего сумматоров 17. На входы переносов второго и третьего сумматоров 17 подается код единицы. На второй вход второго сумматора 17 подается инверсный код модуля p. На второй вход третьего сумматора 17 подается инверсный код удвоенного модуля p. Второй сумматор 17 выполняет операцию $\left(t_i + \overline{p} + 1\right)$. Сигнал со старшего (k+1)-го разряда полученного значения, где k - количество разрядов инверсного двоичного кода модуля p, поступает на выход переноса второго сумматора 17. Остальные разряды представляют собой разность (t_i-p). Третий сумматор выполняет операцию $\left(t_i + \overline{2p} + 1\right)$. Сигнал со старшего (k+1)-го разряда полученного значения, где k - количество разрядов инверсного двоичного кода удвоенного модуля p, поступает на выход переноса третьего сумматора 17. Остальные разряды представляют собой разность (t_i-2p). Если на выходе переноса третьего сумматора 17 сигнал равен "1", то на выходе умножителя по модулю будет разность (t_i-2p). Если на выходе переноса третьего сумматора 17 сигнал равен "0", а на выходе переноса второго сумматора 17 сигнал равен "1", то на выходе умножителя по модулю будет разность (t_i-p). Если на выходе переноса третьего сумматора 17 сигнал равен "0" и на выходе переноса второго сумматора 17 сигнал равен "0", то на выходе умножителя по модулю будет число t_i.

Рассмотрим работу устройства формирования остатка по произвольному модулю от числа на примере.

Пусть $A=49_{10}=110001_2$, $p=9_{10}=001001_2$. Первый формирователь частичных остатков формирует значение частичного остатка от 2^2 по модулю p, который равен 000100_2. Второй формирователь частичных остатков формирует частичный остаток от 2^4 по модулю p, который равен 000111_2. Первый умножитель по модулю производит умножение частичного остатка, полученного на первом формирователе частичных остатков, и коэффициентов $a_2=0$ и $a_3=0$. В результате получается значение, равное 0. Первый сумматор по модулю выполняет операцию сложения полученного значения и коэффициентов $a_0=1$ и $2a_1=00$ и находит остаток по модулю p. В результате получается значение, равное 1. Второй умножитель по модулю производит умножение частичного остатка, полученного на втором формирователе частичных остатков, и коэффициентов $a_4=1$ и $a_5=1$. В результате получается значение, равное 000011. Второй сумматор по модулю выполняет операцию сложения полученного значения и результата с первого сумматора по модулю и находит остаток по модулю p. В результате получается значение, равное $100_2=4_{10}$.

$49=9\cdot3+4$

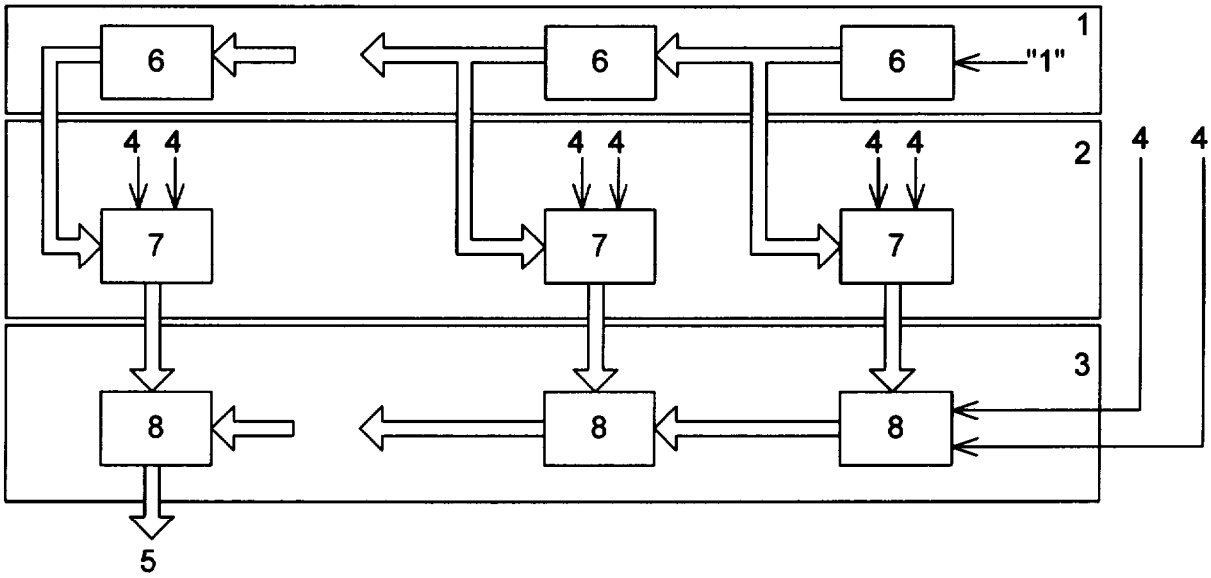
Формула изобретения

1. Устройство для формирования остатка по произвольному модулю, содержащее блок формирователей частичных остатков и блок сумматоров по модулю, причем на

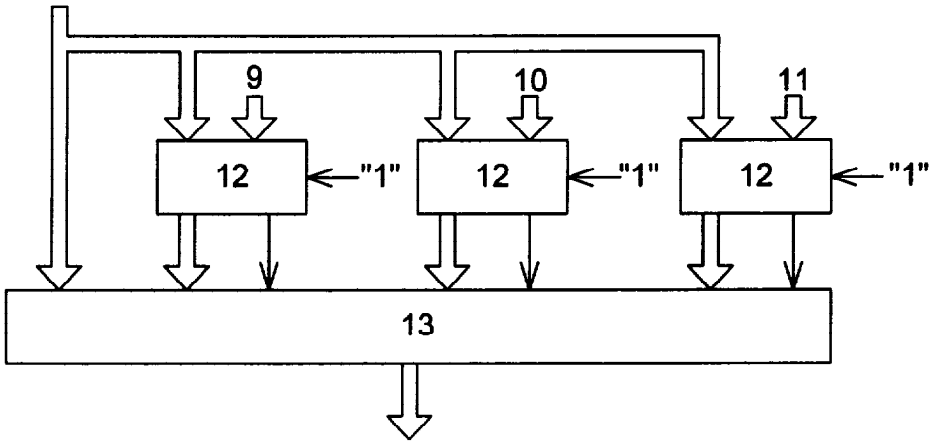
первый формирователь частичных остатков блока формирователей частичных остатков подается код единицы, выход каждого формирователя частичных остатков соединен с входом последующего формирователя частичных остатков и является соответствующим информационным выходом блока формирователей частичных остатков, второй вход каждого сумматора по модулю блока сумматоров по модулю соединен с выходом предыдущего сумматора по модулю, выход последнего сумматора по модулю является выходом устройства для формирования остатков по произвольному модулю, отличающееся тем, что в него введен блок умножителей по модулю, содержащий t умножителей по модулю, где $t = \frac{n}{2}$, если n четное, и $t = \left[\frac{n}{2}\right] + 1$, если n нечетное, n - разрядность входного числа, управляющие входы которых соединены с входами двоичного кода числа, причем два младших разряда числа подаются на второй вход первого сумматора по модулю, блок формирователей частичных остатков содержит t формирователей частичных остатков, блок сумматоров по модулю содержит t сумматоров по модулю, t выходов блока формирователей частичных остатков соединены соответственно с информационными входами умножителей по модулю блока умножителей по модулю, t выходов которого соединены соответственно с информационнми входами блока сумматоров по модулю, являющихся первыми входами сумматоров по модулю.

2. Формирователь частичных остатков, содержащий три сумматора и мультиплексор, причем первые входы сумматоров и мультиплексора соединены с входом формирователя частичных остатков, второй вход первого сумматора соединен с входом инверсного кода модуля, второй вход второго сумматора соединен с входом инверсного кода удвоенного модуля, второй вход третьего сумматора соединен с входом инверсного кода утроенного модуля, на входы переносов всех сумматоров подается код единицы, входы мультиплексора соединены с информационными выходами и выходами переноса всех сумматоров, выход мультиплексора соединен с выходом формирователя частичных остатков.

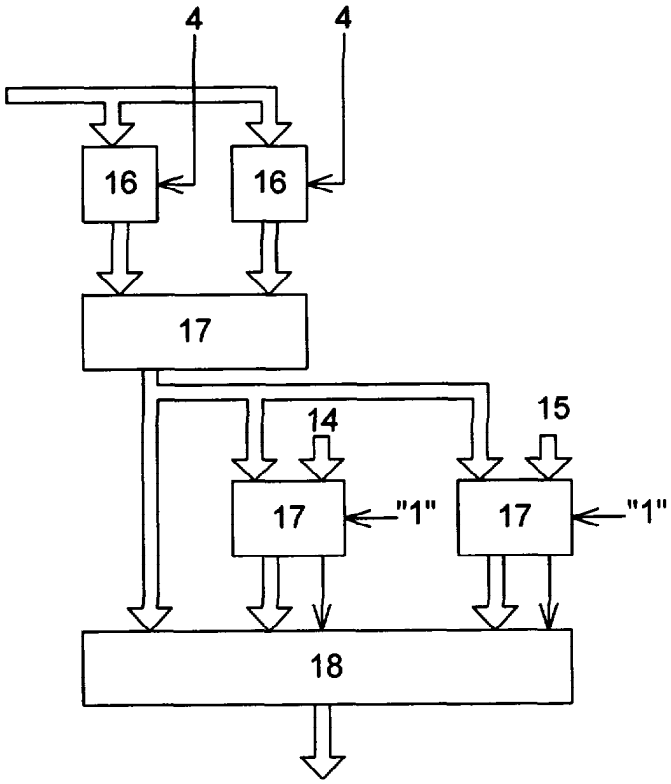
3. Умножитель по модулю, содержащий мультиплексор, три сумматора, два ключа, информационные входы которых соединены с входом умножителя по модулю, на управляющие входы ключей подаются разряды кода числа, а выходы соединены с входами первого сумматора, выход которого соединен с первыми входами второго и третьего сумматоров, второй вход второго сумматора соединен с входом инверсного кода модуля, второй вход третьего сумматора соединен с входом инверсного кода двойного модуля, на входы переносов второго и третьего сумматоров подается код единицы, информационные выходы всех сумматоров и выходы переноса второго и третьего сумматоров соединены с входами мультиплексора, выход которого соединен с выходом умножителя по модулю.



Фиг.1



Фиг. 2



Фиг.3