(19) **RU** (11) **2 024 924** (13) **C1**

(51) МПК[5] **G 06 F 11/08**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: **4917275/24, 22.01.1991**

(46) Дата публикации: **15.12.1994**

(56) Ссылки: **1. Авторское свидетельство СССР N 1105895, кл. G 06F 11/08, 1983.2. Авторское свидетельство СССР N 1238077, кл. G 06F 11/08, 1984.**

(71) Заявитель:
Ставропольское высшее военное инженерное училище связи

(72) Изобретатель: **Петренко В.И., Чипига А.Ф.**

(73) Патентообладатель:
Петренко Вячеслав Иванович, Чипига Александр Федорович

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

(57) Реферат:

Изобретение относится к вычислительной технике и предназначено для использования в цифровых вычислительных устройствах для формирования конечных полей. Цель изобретения - повышение быстродействия формирования остатка, что достигается введением первой схемы сравнения 7, второй схемы сравнения 8, блока 9 умножения по произвольному модулю, сумматора 10 по произвольному модулю, регистра 11 и триггера 12. Сущность изобретения заключается в том, что для ускорения реализации выражения $g_i(\nu)=j\nu+C_o \pmod M$, где

$$\nu,\ C_o=\overline{0,M-1};\ j=\overline{1,M-1},$$

предлагается применять процедуры ускоренного получения результатов умножения и суммирования по модулю. 1 ил.

RU 2024924 C1

RU 2024924 C1

(19) **RU** (11) **2 024 924** (13) **C1**

(51) Int. Cl.[5] **G 06 F 11/08**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 4917275/24, 22.01.1991

(46) Date of publication: 15.12.1994

(71) Applicant:
Stavropol'skoe vysshee voennoe inzhenernoe uchilishche svjazi

(72) Inventor: Petrenko V.I.,
Chipiga A.F.

(73) Proprietor:
Petrenko Vjacheslav Ivanovich,
Chipiga Aleksandr Fedorovich

(54) DEVICE FOR FORMING ARBITRARY MODULO RESIDUE

(57) Abstract:

FIELD: computer engineering. SUBSTANCE: device has auxiliary comparison circuit , comparison circuit , arbitrary modulo multiplying unit , arbitrary adder , register and flip-flop . The device is characterized in that realization of expression $g_i(\nu)=j\nu+C_o(\mathrm{mod}\ M),,$ where $\nu,\ C_o=\overline{0,M-1};\ j=\overline{1,M-1}$ is sped up due to the use of modulo multiplying and adding procedures sped up. EFFECT: enhanced speed. 1 dwg

RU 2024924 C1

RU 2024924 C1

Изобретение относится к вычислительной технике и может быть использовано в цифровых вычислительных устройствах для формирования элементов конечных полей, а также в качестве генератора управляющих последовательностей при формировании дискретных частотных сигналов.

Известно устройство для формирования остатка по произвольному модулю от числа [1], содержащее первый и второй счетчики, первый и второй формирователи импульсов, генератор тактовых импульсов, элементы И, ИЛИ, ИЛИ-НЕ и группу сумматоров по модулю два.

Недостатком этого 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 и второй счетчики, элемент И, первый элемент ИЛИ, элемент ИЛИ-НЕ, группу сумматоров по модулю два, первый и второй формирователи импульсов и генератор тактовых импульсов [2].

Недостатком этого устройства является низкое быстродействие формирования остатка, так как процедура формирования остатка в нем сводится к последовательному вычитанию из числа значения модуля.

Целью изобретения является повышение быстродействия формирования остатка.

Сущность изобретения заключается в том, что для ускоренной реализации выражения $a_j(\nu) = j\nu + C_o(\mathrm{mod}M)$, где ν , ν, $C_o = \overline{0,M-1}$; $j = \overline{1,M-1}$ предлагается применять процедуры ускоренного получения результатов умножения по модулю и суммирования по модулю.

На чертеже представлена функциональная схема устройства для формирования остатка по произвольному модулю от числа.

Устройство содержит первый 1 и второй 2 счетчики, первый 3, второй 4 и третий 5 элементы ИЛИ, первую 6 и вторую 7 схемы сравнения, блок 8 умножения по произвольному модулю, сумматор 9 по произвольному модулю, а также регистр 10, триггер 11, третий счетчик 12, генератор тактовых импульсов 13 и формирователь импульсов 14. Частота генератора 13 и коэффициент пересчета счетчика 12 выбраны из такого расчета, что переполнение счетчика 12 произойдет в момент окончания процедуры формирования остатка.

Счетчик 1 конструктивно выполнен таким образом, что поступление на его первый вход (вход записи) сигнала происходит запись в его ячейки когда единицы.

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

В исходном состоянии счетчики 1, 2 и 12 обнулены, триггер 11 находится в нулевом состоянии, при котором сигналом с его выхода запрещается прохождение тактовых импульсов с выхода генератора тактовых импульсов 13 на вход счетчика 12.

Перед началом работы по шине задания кода числа задается код C_o, который в течение времени формирования воздействует на вторые входы сумматора 9 по произвольному модулю. Также задается код модуля М на шине задания кода модуля, который воздействует на первые входы первой 6 и второй 7 схем сравнения, блока 8 умножения по произвольному модулю и сумматора 9 по произвольному модулю.

Импульс с шины "Пуск" запускает устройство в работу. Этот импульс проходит через элемент ИЛИ 3 на вход записи счетчика 1, в результате чего в счетчик 1 запишется код единицы, проходя через второй элемент ИЛИ 4 на вход обнуления второго счетчика 2, подтвердит его нулевое состояние, поступая через третий элемент ИЛИ 5 на вход триггера 11, переведет его в единичное состояние. Код единицы с выхода счетчика 1 поступит на вторые входы схемы сравнения 6 и блока 8 умножения по произвольному модулю. Результат умножения кодов, записанных в счетчике 1 (единица) и втором счетчике 2 (ноль), с выхода блока 8 поступит на вход сумматора 9 по произвольному модулю, в котором происходит сложение результата умножения по модулю с кодом числа C_o.

Перевод триггера 11 в единичное состояние разрешит прохождение тактовых импульсов с выхода генератора 13 на вход счетчика 12.

Как только результат суммирования по модулю появится на выходе сумматора 9, произойдет переполнение счетчика 12, поэтому сигнал с его выхода поступит на вход формирователя 14 импульсов и возвратит в нулевое состояние триггер 11, чем запретит прохождение импульсов с генератора 13 на вход счетчика 12. Импульс с выхода формирователя 14 поступит на вход записи регистра 10, что обеспечит запись в него первого сигнала и появление этого сигнала на информационных выходах устройства. Одновременно этот импульс поступит на суммирующий вход счетчика 2, записывая в него единицу, а также через второй вход элемента ИЛИ 5 поступит на первый вход триггера 11, переводя его в единичное состояние. Теперь на информационные входы блока 8 умножения по произвольному модулю с выходов счетчиков 1 и 2 подаются коды единиц. Как только результат умножения и суммирования по модулю появится на выходе сумматора 9, с выхода формирователя 14 поступит импульс, который обеспечит запись второго сформированного сигнала в регистр 10 и поступление его на выход устройства, прибавит единицу к содержимому счетчика 2 и, поступая через элемент ИЛИ 5, переведет триггер 11 в единичное состояние.

Работа устройства в таком режиме будет продолжаться до тех пор, пока в счетчик 2 не будет записан код числа М-1. С приходом очередного импульса с выхода формирователя 14 импульсов в счетчик 2 будет записан код модуля М, за счет чего вторая схема сравнения 7 выдаст импульс совпадения, который через элемент ИЛИ 4 обнулит счетчик 2 и, поступая на суммирующий вход счетчика 1, прибавит к его содержимому единицу. Поэтому в счетчике 1 будет записан код числа два, а счетчик 2 будет обнулен. Начинается новый цикл формирования остатков, при котором в счетчике 1 будет записан код числа два, а в счетчике 2 последовательно будут меняться коды от 0 до М-1. После формирования

RU 2024924 C1

RU 2024924 C1

последнего сигнала вторая схема 7 сравнения снова выдаст импульс совпадения, за счет чего счетчик 2 будет обнулен, а в счетчик 1 будет записан код числа три.

Работа устройства в таком режиме будет продолжаться до тех пор, пока в счетчик 1 не будет записан код числа М-1. Как только такой же код будет записан в счетчике 2, то с приходом импульса с формирователя 14 в счетчике 1 будет записан код числа М, поэтому произойдет совпадение также в схеме 6 сравнения, за счет чего на ее выходе появится импульс, который, поступая на управляющий выход устройства, явится сигналом конца формирования. Кроме того, этот импульс, проходя через элемент 4 на вход записи счетчика 2, запишет в нем код единицы.

Сигнал конца формирования свидетельствует о том, что закончился процесс формирования сигналов по выбранному модулю М и коду числа C_o и может быть использован для смены исходных параметров и выбора новых значений М1 и С1.

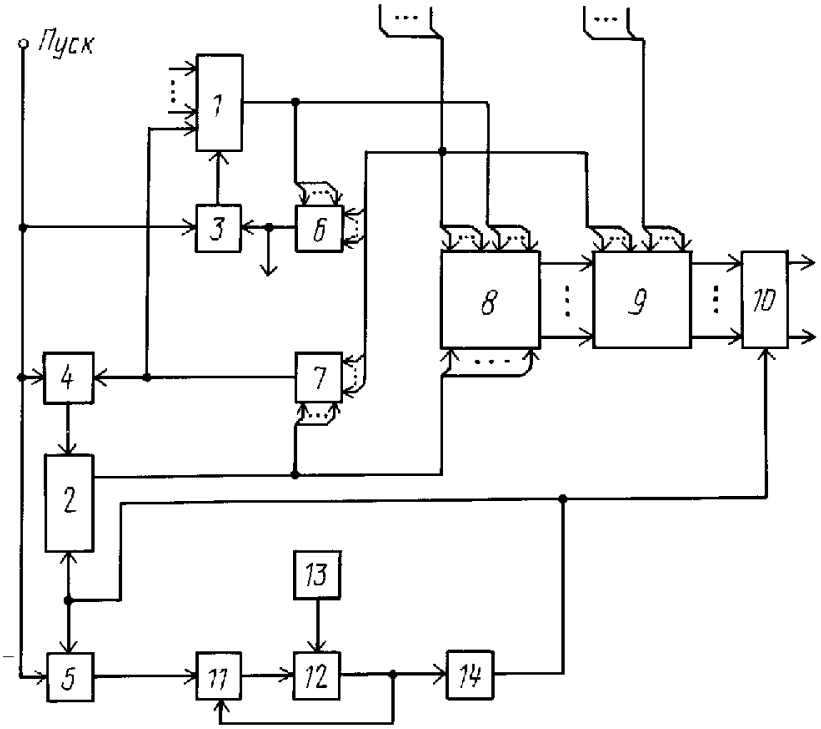
Техническое преимущество предложенного устройства состоит в том, что по сравнению с устройством-прототипом достигнуто повышение быстродействия формирования остатка по произвольному модулю.

Формула изобретения:

УСТРОЙСТВО ДЛЯ ФОРМИРОВАНИЯ ОСТАТКА ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ ОТ ЧИСЛА, содержащее первый, второй, третий счетчики, три элемента ИЛИ, генератор тактовых импульсов, формирователь импульсов, причем вход пуска устройства соединен с первыми входами первого, второго и третьего элементов ИЛИ, выход первого элемента ИЛИ соединен с входом записи первого счетчика, выход второго элемента ИЛИ соединен с входом сброса второго счетчика, выход переполнения третьего счетчика соединен с входом формирователя импульсов, отличающееся тем, что, с целью повышения быстродействия устройства, в него введены триггер, две схемы сравнения, блок умножения по произвольному модулю, сумматор по произвольному модулю и триггер, причем вход задания кода модуля устройства соединен с первыми входами первой и второй схем сравнения, блока умножения по произвольному модулю и сумматора по произвольному модулю, вход задания кода числа устройства соединен с вторым входом сумматора по произвольному модулю, выход первого счетчика соединен с вторым входом блока умножения по произвольному модулю и первой схемы сравнения, выход которой соединен с вторым входом первого элемента ИЛИ и является выходом конца работы устройства, выход второго счетчика соединен с третьим входом блока умножения по произвольному модулю и вторым входом второй схемы сравнения, выход которой соединен с вторым входом второго элемента ИЛИ и счетным входом первого счетчика, выход третьего элемента ИЛИ соединен с единичным входом триггера, выход которого соединен с входом сброса третьего счетчика, выход переполнения которого соединен с входом сброса триггера, выход формирователя импульсов соединен с входом записи регистра, вторым входом третьего элемента ИЛИ и счетным входом второго счетчика, выход генератора тактовых импульсов соединен со счетным входом третьего счетчика, выход блока умножения по произвольному модулю соединен с третьим входом сумматора по произвольному модулю, выход которого соединен с информационным входом регистра, выход которого является выходом результата устройства.

RU 2024924 C1

RU 2024924 C1



RU 2024924 C1

RU 2024924 C1