РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **B** (11) **35492**
(51) ***G06F 7/49*** (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ИЗОБРЕТЕНИЯ
К ПАТЕНТУ

(21) 2021/0712.1
(22) 24.11.2021
(45) 04.02.2022, бюл. №5
(72) Тынымбаев Сахыбай; Бердибаев Рат Шындалиевич; Мукашева Асель Коптлеувна; Әділбекқызы Сайран; Бекетова Гульжанат Сакитжанова
(73) Тынымбаев Сахыбай
(56) RU 2015537 C1, 30.06.1994
RU 2299461 C1, 20.05.2007
RU 2316042 C1, 27.01.2008
RU 24445681 C2, 20.03.2012

(54) **УМНОЖИТЕЛЬ ЧИСЕЛ НА ЧЕТЫРЕ ПО МОДУЛЮ**

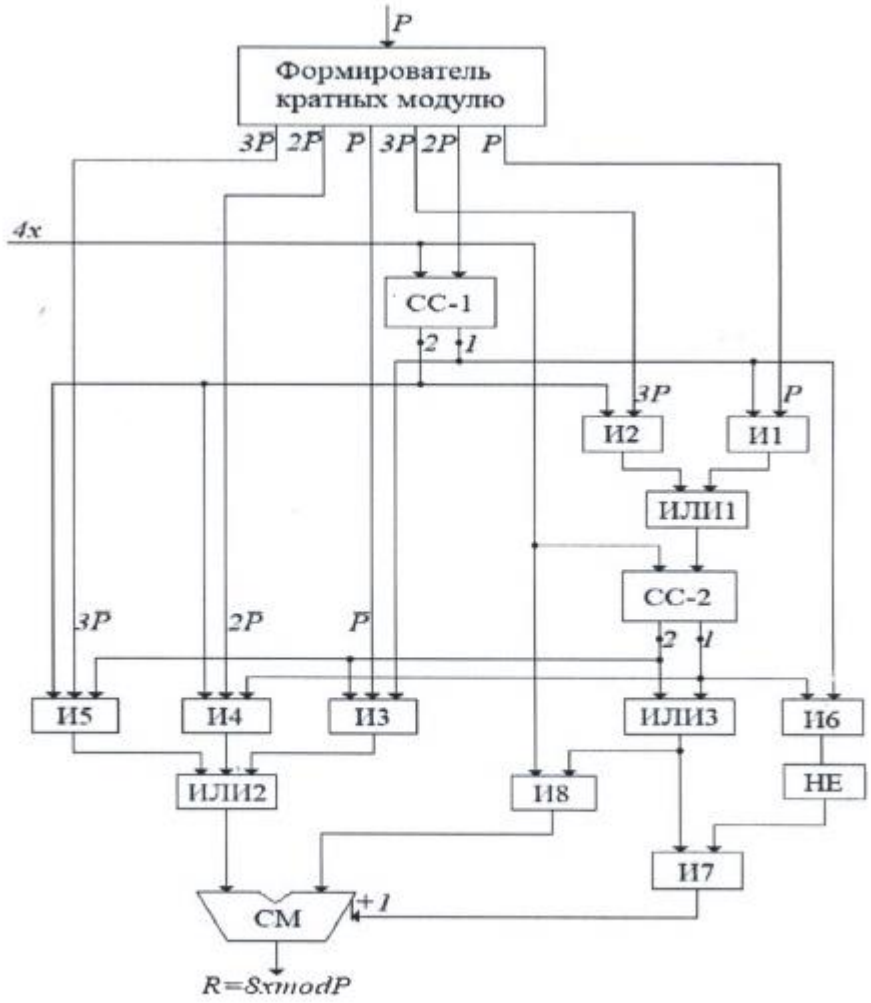
(57) Изобретение относится к вычислительной технике и может быть использовано в устройствах для формирования элементов конечных полей и в криптографических приложениях.

Расширение функциональных возможностей и повышения быстродействия достигаются путем ввода в ее состав формирователя кратных модулю $3\overline{P}$, $2\overline{P}$, $\overline{P}$, 3P, 2P и P , схем сравнения СС-1 и СС-2, блоков логических схем И, ИЛИ, НЕ, где число X со сдвигом на два разряда в сторону старшего разряда (4X) подается на левые входы схем СС-1 и СС-2 и на правые входы сумматора; на правые входы СС-1 подается из формирователя кратных код 2P, на правые входы схемы СС-2 через логические схемы подается из формирователя кратных либо 3P, либо 2P в зависимости от результата сравнения на СС-1 кода 4X с кодом 2P; по результатам сравнения схем СС-1 и СС-2 сумматором СМ выполняются следующие операции: $R=4X+2\overline{P}+1$, если $2P\leq 4X<3P$; $R=4X+3\overline{P}+1$, если $2P\leq 4X>3P$; $R=4X+\overline{P}+1$, если $2P>4X\geq 3P$.

При $4X<P$ поступление кратных $\overline{P}$, $2\overline{P}$, $3\overline{P}$ на вход сумматора блокируется, при этом $R=4X+0=4X$.

Технический результат заключается в расширениях функциональной возможности и в сокращении времени выполнений операций чисел по модулю.

(19) KZ (13) B (11) 35492


P
Формирователь кратных модулю
3P 2P P 3P 2P P
4x
СС-1
2 1
3P
P
И2
И1
ИЛИ1
СС-2
3P
2P
P
2 1
И5
И4
И3
ИЛИ3
И6
ИЛИ2
И8
НЕ
И7
СМ
+1
R=8xmodP

Фигура 1

Изобретение относится к области вычислительной техники и может быть использовано в цифровых вычислительных устройствах, а также в устройствах для выполнения арифметических операций в конечных полях.

Известно устройство для умножения чисел на два по модулю [Патент RU №2015537, опубликован 30.06.94, МПК G06F/49]. Умножитель содержит сумматор и мультиплексор.

На первые входы сумматора и мультиплексора подается число X со сдвигом на один разряд в сторону старших разрядов, т.е. 2X, на вторые входы сумматора подаются разряды модуля в инверсном коде и на младший разряд сумматора подается +1.

Если 2X>P, то в сумматоре за счет перевода инверсного кода в дополнительный происходит вычитание из кода 2X под модуль. При этом на выходе переноса сумматора появляется управляющий сигнал, переключающий вторые информационные входы мультиплексора на его выход и значение остатка с выхода сумматора через вторые входы мультиплексора, поступают на информационные выходы умножителя. Если значение 2X не превышает значения модуля, то с выхода переноса сумматора управляющий сигнал на вход мультиплексора не подается, первые его информационные входы остаются скоммутированными на информационные выходы и значение 2X со входов сумматора через мультиплексор поступает на информационные выходы умножителя.

Недостатком устройства является ограниченная функциональная возможность.

Технической задачей изобретения является расширение функциональной возможности умножителя.

Технический результат заключается в расширениях функциональной возможности и в сокращении времени выполнений операций чисел по модулю.

Технический результат достигается путем включения состав умножителя сумматора, формирователя кратных модулю, двух схем сравнения, блоков логических схем И1÷И5, И8; схем И6, И7, ИЛИ3; блоков схем ИЛИ1, ИЛИ2, ИЛИ3 и НЕ.

На фигуре 1 приведена функциональная схема умножителя чисел на четыре по модулю, которая состоит из двоичного сумматора СМ; формирователя кратных модулю, двух схем сравнения СС-1 и СС-2; блоков логических схем И1÷И5, И8; схем И6, И7, ИЛИ3; блоков схем ИЛИ1, ИЛИ2, ИЛИ3 и НЕ.

Из формирователя кратных модулю разряды модуля 2P поступают на входы схемы СС-1. На правые входы схемы СС-2 поступает значение модуля P через блок схем И1 и ИЛИ1 или значение 3P через блок схем И2 и ИЛИ1. Значение X сдвинутое влево на два разряда в сторону старших разрядов определяет значение 4X.

Значение 4X подается на правые входы сумматора СМ через блок схем И8 и на левые входы схем СС-1 и СС-2. Схемой СС-1 сравнивается код 4x с кодом 2P. Если при этом 4X≥2P, то на выходе 2 схемы СС-1 формируется единичный сигнал 1, который подается на управляющий вход блока схем И2, разрешая прохождение разрядов кратных модуля 3P на правые входы схемы СС-2. При этом на выходе 1 схемы СС-1 – сигнал 0, который блокирует прохождение разрядов модуля P через блок схемы И1 на входы схемы СС-2 и через схемы И6, НЕ приводит к формированию 1 на правом входе схемы И7.

При сравнении кода 4x с кодом 2P, если имеет место неравенство 4x<2P, на выходе 1 схемы СС-1 формируется сигнал 1, разрешая прохождение разрядов кратных модуля P через схемы И1 на правые входы схемы СС-2. При этом на выходе 2 схемы СС-1 – сигнал 0, который блокирует прохождение 3P через блок схем И2 на входы схемы СС-2.

При выполнении условия 4X≥2P схемой СС-2 осуществляется сравнение кода 4X с кодом 3P. Если при этом 4X<3P, то на выходе 1 схемы СС-2 установится сигнал 1, который подается на вход схемы ИЛИ3 и на управляющие входы блока схем И4, разрешая прохождение обратного кода $2\overline{P}$, поданного на информационные входы И4, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 2X через блок схемы И8 на сумматор СМ, и прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция $R=4X+2\overline{P}+1$.

Если при выполнения условия 4X≥2P при сравнении кода 4X с кодом 3P на схеме СС-2 оказывается, что 4X≥3P, то на выходе 2 схемы СС-2 установится сигнал 1, который подается на вход системы ИЛИ3 и на управляющие входы блока схем И5, разрешая прохождение обратного кода $3\overline{P}$, поданного на информационные входы И5, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 4X через блок схемы И8 на сумматор СМ, прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция $R=4X+3\overline{P}+1$.

При выполнения условия 4X<2P схемой СС-2 осуществляется сравнение кода 2X с кодом модуля P. Если при этом 4X≥P, то на выходе 2 схемы СС-2 установится сигнал 1, который подается на вход схемы ИЛИ3 и на управляющие входы блока схем И3, разрешая прохождение обратного кода $\overline{P}$, поданного на информационные входы И3, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 2X через блок схемы И8 на сумматор СМ, прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция $R=4X+\overline{P}+1$.

Если при выполнения условия 4X<2P при сравнении кода 4X с кодом P на схеме СС-2

оказывается, что 4X<P, то на выходе 1 схемы СС-2 установится сигнал 1, который подается на вход системы ИЛИ3 и И6. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение 2х через блок схемы И8 на сумматор СМ, прохождение которого через схему И7 на вход +1 сумматора СМ запрещается нулевым сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция R=4X+0=4X, т.к. на второй вход сумматора СМ не подаются кратные модуля $\overline{P}$, $2\overline{P}$,$3\overline{P}$, заблокированные нулевыми управляющими сигналами на блоках схем И3, И4, И5.

Ниже рассмотрим примеры.

Пусть $X=20_{10}$; $4X=80_{10}$; $P=35_{10}$; $2P=70_{10}$; $3P=105_{10}$

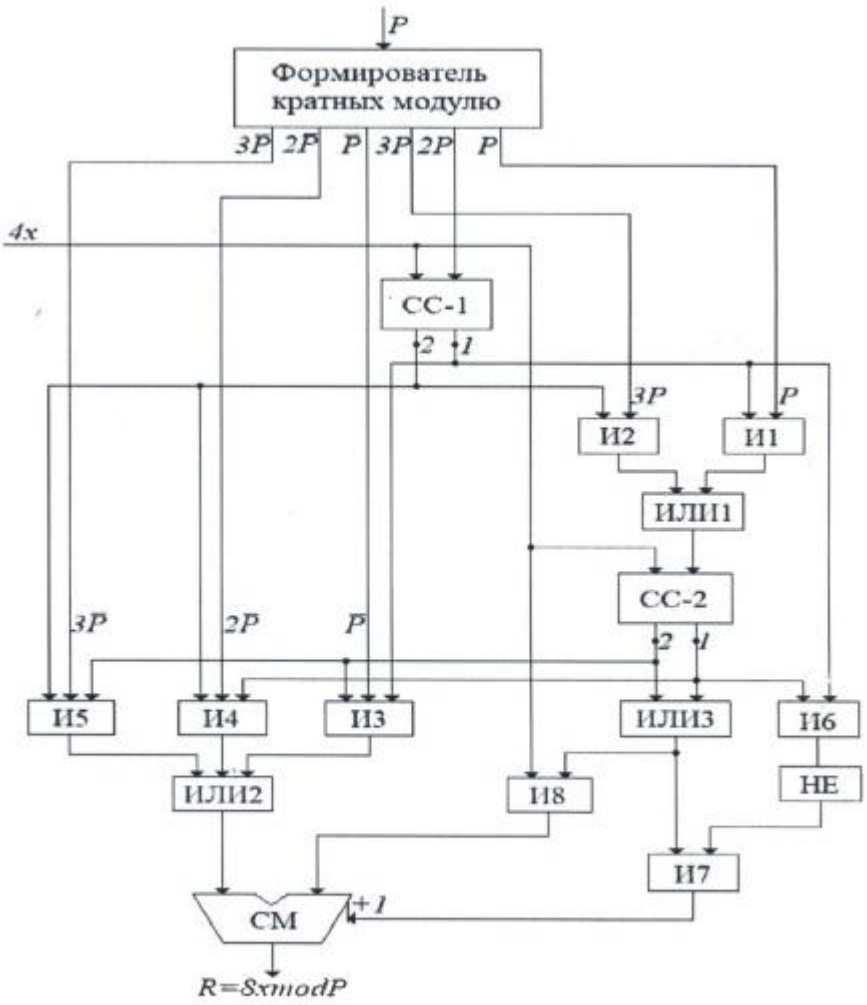
Схемой СС-1 число 80 сравнивается с числом 2P=70, при этом на выходе 1 СС-1 формируется единичный сигнал, который позволяет сравнивать число 4X=80 с числом 3P=105 на СС-2. При этом т.к. 80<105 на выходе 1 СС-2 вырабатывается сигнал 1, который подается на управляющий вход блока схем И4, на вторые входы которого подается обратный код $2\overline{P}$ и единичный сигнал с выхода схемы СС-1. Единичный сигнал с выхода СС-2 через схему ИЛИ3 подается на управляющий вход схемы И8, разрешая прохождение кода 4X на правые входя сумматора СМ. Одновременно сигнал 0 на выходе 1 схемы СС-1 инвертируется схемой НЕ и подается на вход схемы И7, на второй вход которого подана 1 с выхода схемы ИЛИ3. На выходе схемы И7 формируется сигнал +1, который подается на вход сумматора СМ. В сумматоре выполняется операция $R=4X+2\overline{P}+1=80_{10}-70_{10}=10_{10}$

По фигуре 1 нетрудно проследить, что при тех же значениях модуля P если $X=10_{10}$ и $4X=40_{10}$, то $R=4X+\overline{P}+1=40_{10}-35_{10}=5_{10}$.

Если $X=30_{10}$, и $4X=120_{10}$, тогда $R=4X+3\overline{P}+1=120_{10}-105_{10}=15_{10}$.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Умножитель чисел на четыре по модулю, содержащий сумматор, мультиплексор ***отличающийся*** тем, что для расширения функциональной возможности и сокращения времени умножения по модулю в состав умножителя введен формирователь кратных модулю P, где формируются $3\overline{P}$, $2\overline{P}$, $\overline{P}$ и 3P, 2P и P, схемы сравнения СС-1 и СС-2, блоки логических схем И, ИЛИ, НЕ; число X со сдвигом на два разряда в сторону старшего разряда (4X) подается на левые входы схемы СС-1 и СС-2 и на правые входы сумматора СМ; с выходов формирователя кратных коды 3P и P подаются на правые входы схемы СС-2, код модуля 2P подается на правые входы схемы СС-1; значения обратных кодов $3\overline{P}$, $2\overline{P}$, $\overline{P}$ с выходов формирователя кратных через логические схемы подаются на левые входы сумматора СМ; по результатом сравнения 4X с 2P на СС-1 и по результатом сравнения 4X с 3P и 4X с P на СС-2 значения обратных кодов $3\overline{P}$, $2\overline{P}$, $\overline{P}$ с выходов формирователя кратных через логические схемы подаются на левые входы сумматора СМ.



Фигура 1

Верстка Д. Женысова
Корректор Г. Косанова