РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **B** (11) **35918**
(51) ***G06F 7/49*** (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ИЗОБРЕТЕНИЯ
К ПАТЕНТУ

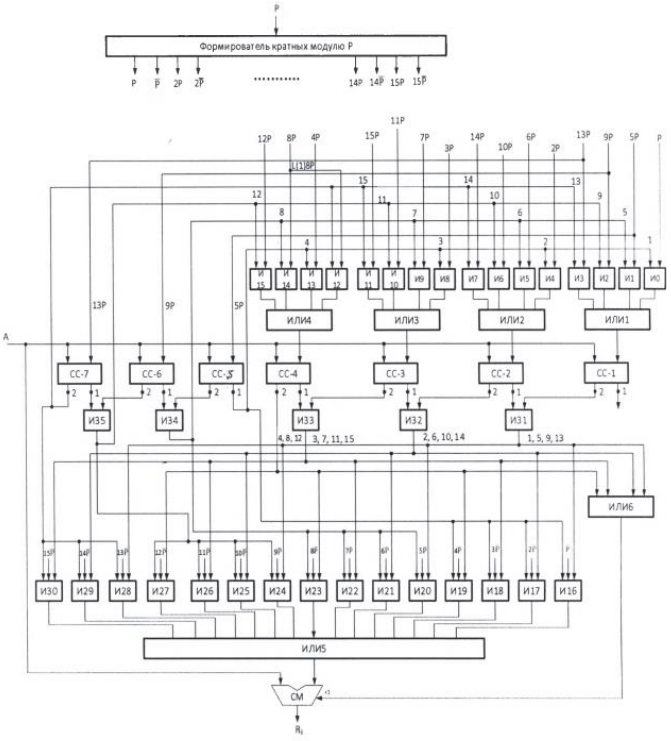
(21) 2022/0378.1
(22) 15.06.2022
(45) 21.10.2022, бюл. №42
(72) Тынымбаев Сахыбай; Мукашева Асель Коптлеувна; Досжанова Алия Амантаевна; Бердибаев Рат Шындалиевич; Бердываева Гульмира Куанышбаевна
(73) Тынымбаев Сахыбай
(56) KZ 35492 B, 04.02.2022;
KZ 35658 B, 13.05.2022;
RU 2299461 C1, 20.05.2007;
RU 2445681 C2, 20.03.2012.

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

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

Расширение функциональных возможностей достигаются путем ввода в ее состав формирователя кратких модуль P(15P÷P и 15$\overline{P}$÷$\overline{P}$), схем сравнения СС-1÷СС-7, блоков логических схем И,ИЛИ,НЕ, где число X со сдвигом на четыре разряда в сторону старшего разряда (16X) подается на левые входы схем сравнении СС-1÷СС-7 и на левые входы сумматора СМ. Сравнение кода 15P÷P с кодом 16X на схемах СС-1÷СС-7 позволяет выбрать одного из значений кратких 15$\overline{P}$÷$\overline{P}$ с выходов формирователя кратких и подавать на правые входа сумматора, где выполняется одна из операций R_i=A+15$\overline{P}$+1÷A+$\overline{P}$+1.

Технический результат заключается в расширения функциональный возможности и в сокращении вычислении выполнений операций по модулю.



Фигура 1

(19) KZ (13) B (11) 35918

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 с коммутированными на информационные выходы и значение 2X со входов сумматора через мультиплексор поступает на информационные выходы умножителя.

Недостатком устройства является ограниченная функциональная возможность - заключающаяся в ограниченном диапазоне умножения по модулю на два.

Технической задачей изобретения является выбор одного из кратных модулю к $\overline{P}$, из набора значений $15\overline{P}$,$14\overline{P}$,...$2\overline{P}$, $\overline{P}$.

Технический результат заключается в расширении функциональной возможности и в сокращении времени умножения чисел по модулю.

Технический результат достигается путем включения в состав умножителя схем сравнения, формирователя кратных модулю P, блоков схем И, ИЛИ и сумматора.

На фигуре 1 приведена функциональный схема умножителя чисел на шестнадцать по модулю P, которая состоит из блока формирования кратных модулей P (P, $\overline{P}$ и 2P, $2\overline{P}$…..14P, $14\overline{P}$ и 15P, $15\overline{P}$), двоичного сумматора СМ, семи схем сравнения (СС-1÷ СС-7), блоков схем И0÷И30, схем И31÷И35, блоков схем ИЛИ1÷ИЛИ5, схем ИЛИ6.

Значение числа X сдвинутое на четыре разряда в сторону старшего определяет число A=16X.

Значение A подается на левые входы сумматора и на левые входы схем СС-1÷СС-7, где выполняются сравнение с кратными модулями P. Работа схем сравнения СС-1÷СС-4 зависит от результата сравнения A с кодами 5P, 9P, 13P на схемах СС-5, СС-6, СС-7 соответственно. В зависимости от этого результата схемой СС-1 значение A сравнивается с кодами P или 5P, или 9P, 13P; схемой СС-2 A сравнивается с кодами 2P или 6P, или 10P, или 14P; схемой СС-3 A сравнивается с кодами 3P или 7P, или 11P, или 15P; схемой СС-4 A сравнивается с кодами 4P или 8P, или 12P, или 14P.

Если в результате сравнения 5P с A на схеме СС-5 имеет место соотношение A<5P, то на выходе 1СС-5 вырабатывается сигнал «1», который коммутирует значения кодов P, 2P, 3P,4P блоками схем И0, И4, И8 и И13 на правые входы соответствующих схем сравнения СС-1, СС-2, СС-3 и СС-4, где они сравниваются со значением A. Единичный сигнал с выхода 1 СС-5 также подается на управления входы блоков схем И16, И17, И18, И19 для разрешения прохождения в дальнейшем на сумматор СМ кодов $\overline{P}$ или $2\overline{P}$, или $3\overline{P}$ или $4\overline{P}$, которые подаются на информационные входы схем И16÷И19, соответственно.

Если в результате сравнения 9P с A на схеме СС-6 и сравнения 5P с A на схеме сравнения СС-5 имеет место соотношение 9P>A>5P, то на выходе 2 схема СС-5 и на выходе 1 схемы СС-6 вырабатываются сигналы «1», которые подаются на входы схемы И34. В результате на выходе схемы И34 вырабатывается сигнал «1», который коммутирует значения кодов 5P,6P,7P и 8P блоками схем И1,И5, И9, И14 на правые входы соответствующих схем сравнения СС-1, СС-2, СС-3, СС-4, где они сравниваются с A. Единичный сигнал с выхода схемы И34 также подается на управляющие входы блоков схем И20, И21, И22, И23 для разрешения прохождения в дальнейшем на сумматор СМ кодов $5\overline{P}$ или $6\overline{P}$, или $7\overline{P}$, или $8\overline{P}$, которые подаются на информационные входы схем И20÷И23, соответственно.

Если в результате сравнения 9P с A на схеме СС-6 и 13P с A на схеме сравнения СС-7 имеет место соотношение 13P>A>9P, то на выходе 2 СС-6 и на выходе 1 схемы СС-7 вырабатываются сигналы «1», которые подаются на входы И35. В результате на выходе схемы И35 вырабатывается сигнал «1», который коммутирует значения кодов 9P, 10P, 11P и 12P блоками схем И2, И6, И10 и И15 на правые входы соответствующих схем сравнения СС-1, СС-2, СС-3 и СС-4, где они сравниваются с A. Единичный сигнал с выхода схемы И35 также подается на управляющие входы блоков схем И24, И25, И26, И27 для разрешения прохождения в дальнейшем на сумматор СМ кодов $9\overline{P}$ или $10\overline{P}$, или $11\overline{P}$ или $12\overline{P}$, которые подаются на информационные входы схем И24÷И27, соответственно.

При сравнении Ас 13P на схеме СС-7, если имеет место соотношении A≥13P, то на ее выходе 2 вырабатывается сигнал «1», который коммутирует значения кодов 13P, 14P, 15P, 16P (образуется сдвигом влево на один разряд значения 8P) блоками И3, И7, И11, И12 через соответствующие блоки схем ИЛИ1, ИЛИ2, ИЛТ3, ИЛИ4 на правые и входы соответствующих схем сравнения СС-1, СС-2, СС-3, и СС-4 где они сравнивается с A. Единственный сигнал с выхода 2 СС-1 также подается на управляющие входы блоков схем И28÷И30,

При сравнений А с Р на схеме СС-1, если А<Р ни одна из схем И16-И35 не сработает. Значение А поданное на левы вход сумматора формируется R=A.

При сравнений Р с А на схеме СС-1 и кода 2Р с А; на схеме СС-2, значение кода 2Р>А>Р, то на выходе схемы И31, формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блока схем И17, что приводит к выполнению на сумматоре СМ операция $R=F+2\overline{P}+1$.

При сравнений кода 3Р с А на схеме СС-3, и кода 4Р с А на схеме СС-4 если выполняются условия 4Р>А>3Р, то на выходе схемы И33 формируется сигнал «1», который подается на входе схем ИЛИ и на трети вход блок схем И18, что приводит к на сумм формирует сигнал «1», операции $R_i=A+3\overline{P}+1$.

При сравнений кода 4Р с А на схеме СС-4, если выполняются условие А>Р, то на его 2 выходе вырабатывается единичный сигнал, которые подается на вход схемы ИЛИ6 и на третий вход блока схемы И19, что приводит к выполнению на сумматоре СМ операции $F+R=4\overline{P}+1$.

При сравнении кода 5Р с А на схеме СС-1 и кода 6Р с А на схеме СС-2 если выполняется условия 6Р>А>5Р, то на выходе схемы И 31 формируется сигнал «1», который », который подается на входе схем ИЛИ6 и на трети вход блок схем И20, что приводит к выполнению на сумматоре СМ операция $R=A+5\overline{P}+1$.

При сравнений кода 6Р с А на схеме СС-2, и кода 7Р с А на схеме СС-3, если выполняются условия 7Р>А>6Р, то на выходе схемы И32 формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блок схем И21, что приводит к выполнению на сумматоре СМ операции $R=A+6\overline{P}+1$.

При сравнений кода 7Р с А на схеме СС-4, и кода 8Р с А на схеме СС-4, если выполняются условия 8Р>А>7Р, то на выходе схемы И33 формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блок схем И22, что приводит к выполнению на сумматоре СМ операции $R=A+7\overline{P}+1$.

При сравнений кода 8Р с А на схеме СС-4, если А>8Р, то на выходе 2 СС-4, формируется единичный сигнал, который подается на входе схем ИЛИ6 и на третий вход блока схем И23, что приводит к выполнению на сумматоре СМ операция $R=A+8\overline{P}+1$.

При сравнений кода 9Р с А на схеме СС-2, и кода 10Р с А на схеме СС-3, если выполняются условия 10Р>А>9Р, то на выходе схемы И31 формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блок схем И24, что приводит к выполнению на сумматоре СМ операции $R=A+9\overline{P}+1$.

При сравнений кода 10Р с А на схеме СС-2, и кода 11Р с А на схеме СС-3, если выполняются условия 12Р>А>11Р, то на выходе схемы И32 формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блок схем И25, что приводит к выполнению на сумматоре СМ операции $R=A+10\overline{P}+1$.

При сравнений кода 11Р с А на схеме СС-3, и кода 12Р с А на схеме СС-4, если выполняются условия 12Р>А>11Р, то на выходе схемы И33 формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блок схем И26, что приводит к выполнению на сумматоре СМ операции $R=A+11\overline{P}+1$.

При сравнений кода 12Р с А на схеме СС-4, если А>12Р, то на выходе 2 СС-4, формируется единичный сигнал, который подается на входе схем ИЛИ6 и на третий вход блока схем И27, что приводит к выполнению на сумматоре СМ операция $R=A+12\overline{P}+1$.

При сравнений кода 14Р с А на схеме СС-3, и кода 15Р с А на схеме СС-3, если выполняются условия 15Р>А>14Р, то на выходе схемы И32 формируется сигнал «1», который подается на входе схем ИЛИ6 и на третий вход блок схем И29, что приводит к выполнению на сумматоре СМ операции $R=A+14\overline{P}+1$.

При сравнений кода 15Р с А на схеме СС-3, и кода 16Р с А на схеме СС-4, если выполняются условия 16Р>А>15Р, то на выходе схемы И33 формируется единичный сигнал, который подается на входе схем ИЛИ6 и на третий вход блок схем И30, что приводит к выполнению на сумматоре СМ операции $R=A+15\overline{P}+1$.

Рассмотрим пример, пусть $X=136_{10}$ и $P=187_{10}$; $2P=374_{10}$, $3P=561_{10}$; $4P=748_{10}$, $5P=935_{10}$, $6P=1122_{10}$, $7P=1309_{10}$, $8P=1496_{10}$, $9P=1683_{10}$, $10P=1870_{10}$. $11P=2057_{10}$, $12p=2244_{10}$, $13P=2431_{10}$, $14P=2618_{10}$ $15P=2805_{10}$.

$A=L(4)X=16*136=2176_{10}$. Поскольку $2057_{10}<2176_{10}<2057$ или 11Р<2176<12р $R=2176_{10}-2057_{10}=119_{10}$

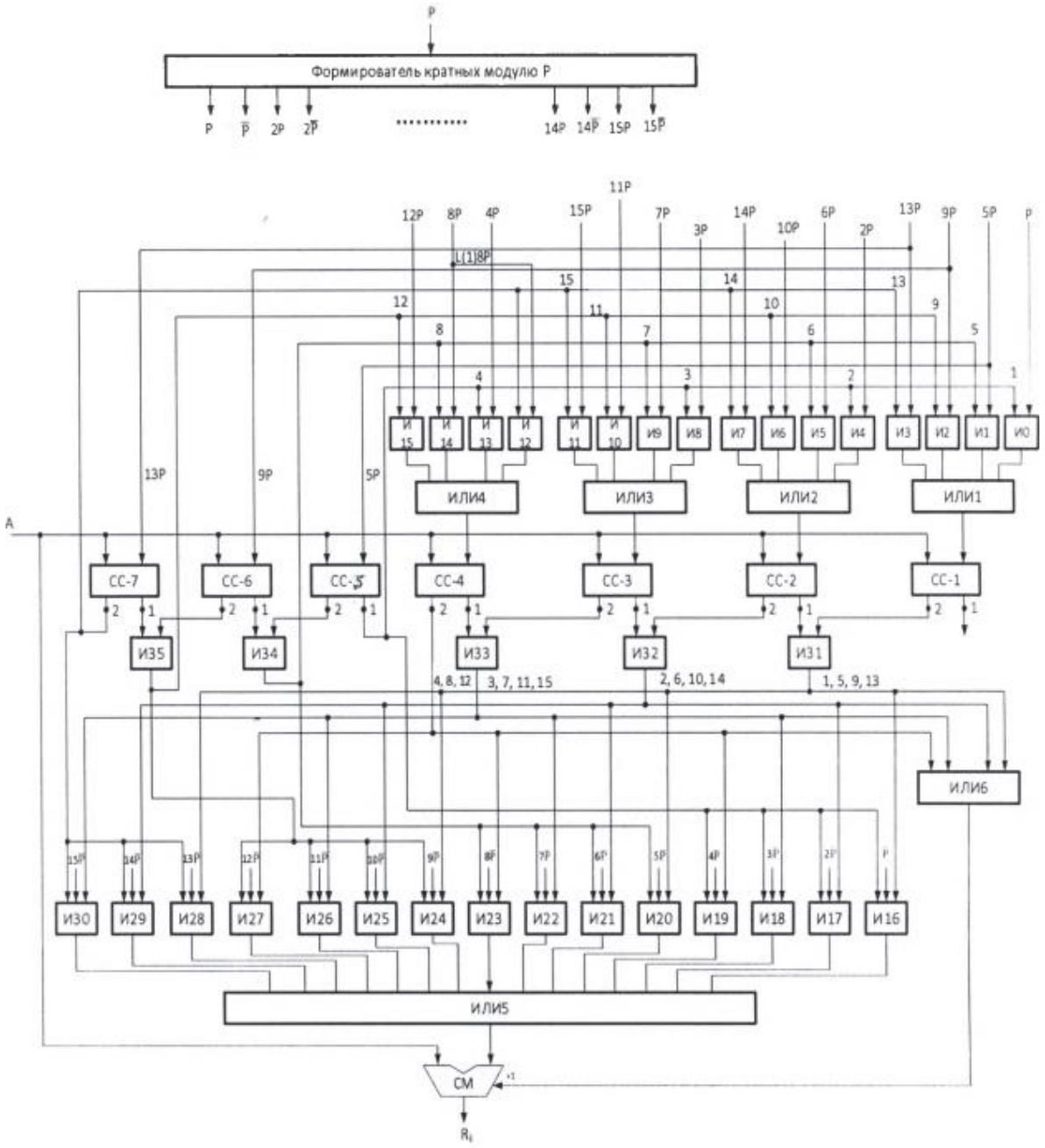
Проверка:

$$\begin{array}{r|l} 2176 & 187 \\ \underline{2057} & 11 \\ 119 & \end{array}$$

$R=2176 \bmod 187=119_{10}$.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Умножитель чисел на шестнадцать по модули, содержащий сумматор, мультиплексор, ***отличающийся*** тем, что введены формирователь кратных по модулю, где формируются значения 15Р,14Р,...,Р и $15\overline{P}$,$14\overline{P}$,...$2\overline{P}$ и $\overline{P}$, схемы сравнение СС-1 ÷ СС-7, блоки логических схем И,ИЛИ,НЕ; число Х со сдвигом на четыре разряда в сторону страшего разряда (А=16Х) подается на левые входы схем сравнение СС-7÷СС-1 и левые входы сумматора СМ; значения обратных кодов $15\overline{P}\div\overline{P}$ с выходов формирователя кратких модули Р через логических схем подаются на правые входы схем сравнение СС-1÷СС-7, где они сравниваются с А=16Х и в результате значение одного обратного кода из $15\overline{P}\div\overline{P}$ подаются на правые входы сумматора СМ.



Фигура 1

Верстка Д. Женысова
Корректор Г. Косанова