СОЮЗ СОВЕТСКИХ СОЦИАЛИСТИЧЕСКИХ РЕСПУБЛИК

(19) SU (11) 1697079 A1

(51)5 G 06 F 7/72

ГОСУДАРСТВЕННЫЙ КОМИТЕТ ПО ИЗОБРЕТЕНИЯМ И ОТКРЫТИЯМ ПРИ ГКНТ СССР

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

(21) 4622474/24
(22) 20.12.88
(46) 07.12.91. Бюл. № 45
(72) В.И.Глушков, В.П.Ирхин, В.А.Краснобаев, И.В.Кононова и А.И.Сахно
(53) 681.325(088.8)
(56) Авторское свидетельство СССР
№ 1617439, кл. G 06 F 7/72, 1988.
Авторское свидетельство СССР
№ 1259255, кл. G 06 F 7/72, 1985.

(54) УСТРОЙСТВО ДЛЯ УМНОЖЕНИЯ ЧИСЕЛ ПО МОДУЛЮ

(57) Изобретение относится к автоматике и вычислительной технике и может быть использовано в вычислительных машинах и устройствах, функционирующих в системе остаточных классов. Целью изобретения является упрощение устройства. Устройство для умножения чисел по модулю содержит группу блоков 3 элементов И, группу блоков 4 умножения на константу по модулю, кольцевые регистры 5 и 16 сдвига, блок 8 элементов ИЛИ, счетчик 9, элемент ИЛИ 10, элементы И 11, 13 и 14, элемент НЕ 12, блок 15 элементов И и шифратор 17 с соответствующими связями, 1 ил.

Изобретение относится к автоматике и вычислительной технике и может быть использовано в вычислительных машинах и устройствах, функционирующих в системе остаточных классов.

Цель изобретения – упрощение устройства.

На чертеже представлена схема устройства для умножения чисел по модулю.

Устройство содержит вход 1 первого сомножителя, вход 2 второго сомножителя, группу блоков 3 элементов И, группу блоков 4 умножения на константу по модулю, первый кольцевой регистр 5 сдвига, выход 6 устройства, тактовый вход 7 устройства, блок элементов ИЛИ 8, счетчик 9, элемент ИЛИ 10, первый элемент И 11, элемент НЕ 12, второй и третий элементы И 13 и 14, блок элементов И 15, второй кольцевой регистр 16 сдвига, шифратор 17.

Блоки 4 умножения на константу по модулю группы реализованы как в аналоге.

Сущность изобретения состоит в следующем: пусть A – первый операнд, B – второй и необходимо провести операцию модульного умножения $A \cdot B \pmod m$, где m – модуль. Представим число B в виде $B = S_{n-1} \cdot 2^{n-1} + S_{n-2} \cdot 2^{n-2} + \ldots + S_0 \cdot 2^0$ ($n = \log_2 (m-1) + 1$). Тогда $A \cdot B = \sum_{i=0}^{n-1} A \cdot 2^i \cdot S_i$ (S_i равно "0" либо "1", т.е. соответствует значению соответствующего разряда в двоичном представлении числа B). Произведение вида $A \cdot 2^i \pmod m$ можно получить при помощи блока умножения на константу. Следовательно, для получения результата операции $A \cdot B \pmod m$ необходимо произвести последовательное сложение чисел вида $A \cdot 2^i \pmod m$ для тех разрядов двоичного представления, числа B, S_i которых равны единице.

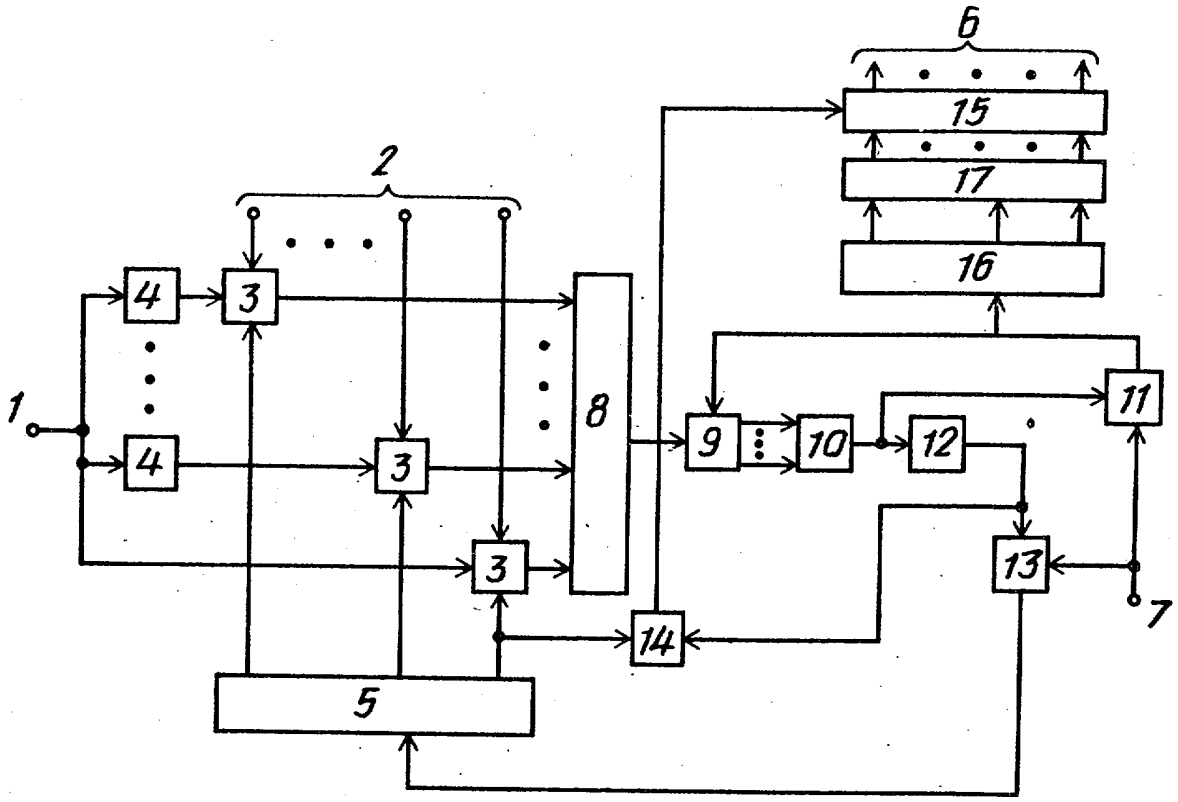
Рассмотрим работу устройства. Первый кольцевой регистр 5 сдвига состоит из n двоичных разрядов (с 0-го по n-1-й). Второй

(19) SU (11) 1697079 A1

кольцевой регистр 16 сдвига состоит из m двоичных разрядов (с 0-го по m-1-й). В исходном состоянии в нулевые разряды регистров 5 и 16 записаны единицы, а в остальные разряды – нули по входу начальной установки устройства (на чертеже не показан). Первый сомножитель А поступает на входы блоков 4 умножения на константу по модулю, а также на первый вход последнего блока 3 элементов И группы, на входах блоков 4 умножения на константу по модулю группы получаем произведения вида $(a \cdot 2^l) \bmod m$ ($l = n-1-1$), а на третьем входе последнего блока 3 элементов И имеем $(A \cdot 2^0) \bmod m = A$. Второй сомножитель В в двоичном коде поступает на соответствующие вторые входы блоков 3 элементов И группы. На первые входы блоков 3 элементов И группы поступает сигнал с выходов разрядов первого кольцевого регистра 5 сдвига. Первоначально в нулевом разряде регистра 5 записана единица. В соответствующий n-1-й разряд операнда В тоже записывается единица. Тогда через соответствующий блок элементов И 3 и через блок элементов ИЛИ 8 число $(A \cdot 2^{n-1}) \bmod m$ поступает на импульсный вход установки числа счетчика 9. Сигнал с элемента ИЛИ 10 открывает элемент И 11, и импульсы с входа 7 устройства поступают на вход разрешения сдвига разрядов регистра 16 и вычитающий вход счетчика 9. Через $(A \cdot 2^{n-1}) \bmod m$ импульсов единица из нулевого разряда регистра 16 переходит в $(A \cdot 2^{n-1}) \bmod m$-й разряд, а содержимое счетчика 9 становится равно нулю. Тогда сигнал поступает через элемент НЕ 12 на элемент И 13. С входа 7 устройства один импульс поступает на вход разрешения сдвига разрядов регистра 5, передвинув единицу из нулевого разряда в первый. Если в n-2-м двоичном разряде операнда В имеется нуль, сигнал с элемента 12 поступает на элемент И 13, и единица из первого разряда регистра 5 переходит во второй. Процесс продолжается до тех пор, пока единица в регистре 5 не перейдет в n-1-й разряд. В этом случае, если соответствующий (нулевой) разряд операнда В равен нулю, на выходе элемента НЕ 12 оказывается сигнал, который поступает с элемента И 14 на первый вход блока элементов И 15, и результат операции модульного умножения, полученный в унитарном коде на выходах разрядов регистра 16, поступает через шифратор 17, который преобразует его в двоичное представление, на выход 6 устройства. Если нулевой двоичный разряд операнда В равен единице, сигнал с элемента И 14 поступает только тогда, когда содержимое счетчика 9 становится равно нулю, т.е. после последнего сложения.

Формула изобретения

Устройство для умножения чисел по модулю, содержащее группу блоков элементов И, первый и второй кольцевые регистры сдвига, блок элементов ИЛИ, счетчик, элемент НЕ, с первого по третий элементы И и блок элементов И, причем выходы разрядов первого кольцевого регистра сдвига соединены с первыми входами соответствующих блоков элементов И группы, выходы которых соединены с соответствующими входами блока элементов ИЛИ, тактовый вход устройства соединен с первыми входами первого и второго элементов И, выход элемента НЕ соединен со вторым входом второго элемента И, выход третьего элемента И соединен с первым входом блока элементов И, *отличающееся* тем, что, с целью упрощения устройства, оно содержит группу блоков умножения на константу по модулю, элемент ИЛИ и шифратор, причем вход первого сомножителя устройства соединен со входами блоков умножения на константу по модулю группы, входы разрядов входа второго сомножителя устройства соединены со вторыми входами соответствующих блоков элементов И группы, выходы блоков умножения на константу по модулю группы соединены соответственно с третьими входами блоков элементов И, кроме последнего, группы, вход первого сомножителя устройства соединен с третьим входом последнего блока элементов И группы, выход блока элементов ИЛИ соединен с установочным входом счетчика, выходы разрядов которого соединены с соответствующими входами элемента ИЛИ, выход которого соединен со входом элемента НЕ и со вторым входом первого элемента И, выход которого соединен с вычитающим входом счетчика и со входом разрешения сдвига второго кольцевого регистра сдвига, выходы разрядов которого соединены с соответствующими входами шифратора, выход которого соединен со вторым входом блока элементов И, выход которого является выходом устройства, выход последнего разряда первого кольцевого регистра сдвига и выход элемента НЕ соединены соответственно с первым и вторым входами третьего элемента И, выход второго элемента И соединен со входом разрешения сдвига первого кольцевого регистра сдвига.



Составитель А.Клюев
Редактор Б.Федотов Техред М.Моргентал Корректор Т.Палий

Заказ 4307 Тираж Подписное
ВНИИПИ Государственного комитета по изобретениям и открытиям при ГКНТ СССР
113035, Москва, Ж-35, Раушская наб., 4/5

Производственно-издательский комбинат "Патент", г. Ужгород, ул.Гагарина, 101