**РЕСПУБЛИКА КАЗАХСТАН**

(19) **KZ** (13) **B** (11) **35762**
(51) ***G06F 7/52*** (2006.01)
***G06F 7/535*** (2006.01)

**МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН**

# ОПИСАНИЕ ИЗОБРЕТЕНИЯ
## К ПАТЕНТУ

(21) 2022/0135.1
(22) 03.03.2022
(45) 15.07.2022, бюл. №28
(76) Тынымбаев Сахыбай
(56) KZ 33314 B, 30.11.2018;
SU 1247863 A1, 30.07.1986;
RU 2510072 C1, 20.03.2014;
RU 2021632 C1, 15.10.1994
С.Тынымбаев, Р.Ш.Бердибаев, Т.Омар, Г.К.Бердибаева, Схемные решения приведения чисел по модулю для криптосистем с открытым ключом, Вестник Алматинского университета энергетики и связи. №4(3) (43), стр. 33, 2018.

(54) **МАТРИЧНОЕ ДЕЛИТЕЛЬНОЕ УСТРОЙСТВО НА ФОРМИРОВАТЕЛЯХ ОСТАТКОВ И ДВУХ РАЗРЯДОВ ЧАСТНОГО**

(57) Изобретение относится к вычислительной технике и может быть использовано в устройствах для деления чисел.

Матричное делительное устройство на формирователях остатков и двух разрядов частного состоит из 2N разрядных регистров делимого, блока для формирования кратных делителю B (БФКД), $^{N}/_{2}$ блоков, где формируются остаток и двух разрядов частного (ФОРЧ-2),

В ФОРЧ-2. i из ФОРЧ-2. i-1 принимается число, состоящий из суммы сдвинутого влево на два разряда предыдущего остатка $R_{i-1}$ и двух битов из регистра делимого. При этом на выходе ФОРЧ-2.i формируется остаток $R_i$ и два бит остатка.

Техническим результатом предложенного технического решения является построение однотактного делительного устройства. Длительность такта при этом определяется величиной задержки на $^{N}/_{2}$ ФОРЧ-2.

(19) KZ (13) B (11) 35762

Изобретение относится к вычислительной технике и может быть использовано в вычислительных устройствах для построения быстродействующих делительных устройств.

Прототипом делительного устройства является устройства быстрого деления [Патент KZ N:33314, бюл. N 48, от 30.11.2018, МПК GO6F 7/535], который содержит регистр делителя, регистры остатка и частного, формирователь частного остатка и двух разрядов частного (ФОРЧ-2), блок синхронизации и схемы И и ИЛИ.

Недостатком делительного устройства является его низкое быстродействие. Для формирования результата потребуется $^{N}/_{2}$ тактовых сигналов (где N – разрядность делителя).

Технической задачей изобретения является разработка однотактного делительного устройства на матрице ФОРЧ-2.

Технический результат достигается путем ввода в состав делителя $^{N}/_{2}$ формирователей остатков и разрядов частного (ФОРЧ-2).

На фигуре 1 приведена структурная схема однотактного делительного устройства на основе ФОРЧ-2, где в каждом из них формируются остатки и два разряда частного.

Делительное устройство состоит из 2N разрядного регистра делимого РгА, блока для формирования кратных делителю В (БФКД), где формируются кратные делителю В и $\overline{B}$, 2В и $2\overline{B}$, 3В и $3\overline{B}$, формирователей остатков и разрядов частного ФОРЧ-2.1 ÷ ФОРЧ-2. $^{N}/_{2}$

Рассмотрим работу устройства:

По сигналу "Пуск" операнды А и В принимаются соответственно в регистре РгА и (БФКД). С выходов БФКД значения В, $\overline{B}$…3В, $3\overline{B}$ подаются на входы ФОРЧ-2.1 ÷ ФОРЧ-2.$^{N}/_{2}$ На входы ФОРЧ-2.1 также подается число $A_1$=L(2) $R_0$+$a_{N-1}a_{N-2}$, где $R_0$ число, определяемое N старшими разрядами РгА, L(2)$R_0$=4$R_0$ – сдвинутое на два разряда влево числа $R_0$, $a_{N-1}$, $a_{N-2}$ – биты числа А следующие за младшими разрядами числа $R_0$. При этом на выходах ФОРЧ-2.1 формируется остаток $R_1$ и старшие разряды частного – $q_{N-1}q_{N-2}$ которые записываются в разряды $q_{N-1}$, $q_{N-2}$, $q_{N-3}$ регистра РгА. Не выходе также формируется остаток – $R_1$.

Далее, остаток $R_1$ со сдвигом на два разряда влево с присоединением битов $a_{N-3}$ и $a_{N-4}$ числа А подается на вход ФОРЧ-2.2. На выходе которого формируется остаток $R_2$ и разряды частного $q_{N-3}$ $q_{N-4}$.

Аналогично формируются другие остатки $R_3$ $R_4$ … и частичные остатки $q_{N-5}$ $q_{N-6}$…

После поступления числа L(2) $R_{N/2-1}$+$a_1a_0$ на вход ФОРЧ-2. $^{N}/_{2}$ на выходе которого формируется результат $R_{N/2}$=R и разряды остатка $q_1q_0$. Задержанным сигналом ПУСК на выходе Л3.1 результат операции $R_{N-2}$ передаётся на вход старших разрядов регистра $P_rA$. Задержанным сигналом ПУСК с выхода Л3.2 регистра $P_rA$ результаты операции Q и R выдаются на выходы устройства.

На фигуре 2 приведена функциональная схема ФОРЧ-2, которая состоит из двоичного сумматора СМ, двух схем сравнения СС-1, СС-2, блоков схем И1÷И5, И8, схем И6, И7, И9, И10, И11, ИЛИ3, ИЛИ4, ИЛИ5, блоков схем ИЛИ1, ИЛИ2 и схемы НЕ. Из блока 2 формирования кратных делителя значение удвоенного делителя 2В поступает на правые входы схемы СС-1. На правые входы схемы СС-2 поступает из блока 2 значение делителя В через И1 и ИЛИ1, или значение 3В через И2 и ИЛИ1.

Значение $A_i$ подается на правые входы сумматора СМ через блок схем И8 и на левые входы СС-2 и СС-2.

Схемой СС-1 сравнивается код $A_i$ с кодом 2В. При сравнении кода $A_i$ с кодом 2В, если имеет место неравенство $A_i$<2В, на выходе 1 схемы СС-1 формируется сигнал 1, разрешая прохождение частного В через блок схем И1 на правые входы схемы СС-2. При этом на выходе 2 схемы СС-1 – сигнал 0, который блокирует прохождение 3В через блок схем И2 на входы схемы СС-2.

Если при этом $A_i$≥2В, то на выходе 2 схемы СС-1 формируется единичный сигнал 1, который подается на управляющий вход схемы И2, разрешая прохождению разрядов кратных делителя 3В на правые входы схемы СС-2. При этом на выходе 1 схемы СС-1 формируется сигнал 0, который блокирует прохождение разрядов делителя В через блок схем И1 на входы схемы СС-2 и через схемы И6, НЕ приводит к формированию 1 на правом входе схемы И7.

При выполнении условий $A_i$≥2В схемой СС-2 осуществляется сравнение кода Ai с кодом 3В. Если при этом $A_i$<3В, 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 делителя $2\overline{B}$, поданного на информационные входы И4, на вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение $A_i$ через блок схем И8 на сумматор СМ, и прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. Сумматором СМ выполняется операция $R_i$= $A_i$+2$\overline{B}$+1. При этом очередные два разряда частного $q_iq_{i-1}$ должны быть $10_2$=$2_{10}$. Их формирование осуществляется с помощью схем И9, И10 и И11. На вход схемы И10 подается сигнал 1 с выхода 1 схемы сравнения СС-2 и сигнал 1 с выхода 2 схемы сравнения СС-1. На выходе схемы И10 формируется сигнал 1, который через схему ИЛИ4 формирует $q_i$=1. На вход схемы И11 подается сигнал 0 с выхода 2 схемы сравнения СС-2 и сигнал 0 с выхода 1 схемы сравнения СС-1. На выходе схемы И11 формируется сигнал 0, который через схему ИЛИ5 формирует $q_{i-1}$=0, так как на выходе схемы И9 также нулевой сигнал. Двоичный код двух разрядов частного: $10_2$.

Если, при выполнении условия $A_i$≥2В, при сравнении кода $A_i$ с кодом 3В на схеме СС-2 оказывается, что $A_i$≥3В, то на выходе 2 схемы СС-2

установится сигнал 1, который подается на вход схемы ИЛИ3 и на управляющие входы блока схем И5 разрешая прохождение обратного кода $3\overline{B}$, поданного на информационные входы И5, на левый вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение $A_i$ через блок схем И8 на правый вход сумматора СМ, и прохождение которого через схему И7 на вход +1 сумматора СМ разрешается единичным сигналом с выхода схемы НЕ. Сумматором СМ выполняется операция $R_i=A_i+3\overline{B}+1$. При этом очередные два разряда частного $q_iq_{i-1}$ должны быть $11_2=3_{10}$. Их формирование осуществляется с помощью схемы И9, на входы который подается сигнал 1 с выхода 2 схемы сравнения СС-1 и сигнал 1 с выхода 2 схемы сравнения СС-2. Двоичный код двух разрядов частного ($11_2$) формируется с помощью схем ИЛИ4 и ИЛИ5, на входы которых подается единичный сигнал с выхода схемы И9.

При выполнении условия $A_i<2B$ схемой СС-2 осуществляется сравнение кода $A_i$ с кодом делителя В. Если при этом $A_i\geq B$, 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 $\overline{B}$, поданного на информационные входы И3, на левый вход сумматора СМ через блок схем ИЛИ2. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение $A_i$ через блок схем И8 на правый вход сумматора СМ, и прохождение которого через схему И7 на вход +1 сумматора См разрешается единичным сигналом с выхода схемы НЕ. Сумматором СМ выполняется операция $R_i=A_i+\overline{B}+1$. При этом очередные два разряды частного $q_iq_{i-1}$ должны быть $01_2=1_{10}$. Их формирование осуществляется с помощью схем И9, И10 и И11. На вход схемы И10 подается сигнал 0 с выхода 1 схемы сравнения СС-2 и сигнал 0 с выхода 2 схемы сравнения СС-1. На выходе схемы И10 формируется сигнал 0, который через схему ИЛИ4 формирует $q_i=0$, так как на выходе схемы И9 также нулевой сигнал. На вход схемы И11 подается сигнал 1 с выхода 2 схемы сравнения СС-2 и сигнал 1 с выхода 1 схемы сравнения СС-1. На выходе схемы И11 формируется сигнал 1, который через схему ИЛИ5 формирует $q_{i-1}=1$. Двоичный код двух разрядов частного: $01_2$.

Если, при выполнении условия $A_i<2B$, при сравнении кода $A_i$ с кодом В на схеме СС-2 оказывается, что $A_i<B$, то на выходе 1 схемы СС-2 установится сигнал 1, который подается на вход схемы ИЛИ3 и И6. На выходе схемы ИЛИ3 формируется сигнал 1, разрешающий прохождение $A_i$ через блок схем И8 на сумматор СМ, и прохождение которого через схему И7 на вход +1 сумматора СМ запрещается нулевым сигналом с выхода схемы НЕ. При этом сумматором СМ выполняется операция $R_i=A_i+0$, так как на второй вход сумматора СМ не подаются кратные делителя $\overline{B}, 2\overline{B}, 3\overline{B}$, заблокированные нулевыми управляющими сигналами на блоках схем И3, И4, И5. При этом очередные два разряда частного $q_iq_{i-1}$ должны быть $00_2=0_{10}$. Их формирование осуществляется с помощью схем И9, И10 и И11. На вход схемы И10 подается сигнал 0 с выхода 2 схемы сравнения СС-1. На выходе схемы И10 формируется сигнал 0, который через схему ИЛИ4 формирует $q_i=0$, так как на выходе схемы И9 также нулевой сигнал. На вход И11 подается сигнал 0 с выхода 2 схемы сравнения СС-2. На выходе схемы И11 формируется сигнал 0, который через схему ИЛИ5 формирует $q_{i-1}=0$, так как на выходе схемы И9 также нулевой сигнал. Двоичный код двух разрядов частного: $00_2$.

Ниже рассматривается пример деления 2N-разрядного делимого А на N-разрядный делитель В.

Пусть $A=\begin{cases} a_{11}\ a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0 \\ 0\quad 1\quad 0\quad 1\quad 1\quad 0\quad 0\quad 1\quad 1\quad 1\quad 1\quad 1_2 \end{cases}$

2N=12, N=6, N/2=3. Первоначальное значение СчТИ равно $3_{10}=11_{10}$, $B=35_{10}=100011_2$; $2B=70_{10}$ $3B=105_{10}$ и $3B = 105_{10}$;

Старше 6 битов двоичного кода числа А определяют значение $R_0 = 010110_2 = 22_{10}$. Присоединение к сдвинутому влево на два разряда остатку $R_0$ следующих двух битов $a_5a_4$ числа А, дает число

$$A_i = L(2)R_0 + (a_5a_4) =$$
$$4R_0 + (a_5a_4) = 88 + 1_{10} = 89_{10}$$

Для наглядности все вычисления по определению остатков и разрядов частного приведены в таблице 1 в десятичной системе счисления.

Таблица 1.

Порядок выполнения операции деления, делимого А на делитель В с формированием двух разрядов частного за шаг.

| ФОРЧ-2 | Вычисления |
|---|---|
| ФОРЧ-2.1 | $A_1 = L(2)R_0 + a_5a_4 = 22 \times 4 + 1 = 89_{10}$ |

| | |
|---|---|
| | Поскольку $70 < 89 < 105$, то имея соотношение $2B \leq A_1 < 3B$<br>Следовательно: при этом в ФОРЧ-2.1 выполняется операция:<br>$R_1 = A_1 - 2B = 89 - 70 = 19_{10}$<br>При этом сформируется $q_3 = 1, q_4 = 0$ |
| ФОРЧ-2.2 | $A_2 = L(2)R_1 + a_3 a_2 = 76_{10} + 3_{10} = 79_{10}$<br>Поскольку $70 < 79 < 105$, то имеет место соотношения $2B \leq A_2 < 3B$; при этом в ФОРЧ-2.2 выполняется операция:<br>$R_1 = A_3 - B = 39_{10} - 35_{10} = 4_{10}$<br>При этом формируется разряды $q_1 = 0$ и $q_4 = 1$ |
| ФОРЧ-2.3 | $A_3 = L(2)R_2 + a_1 a_0 = 36_{10} + 3_{10} = 39_{10}$<br>Поскольку $35 < 39 \leq 70$, то $B \leq A_3 < 2B$ в ФОРЧ-2.3 выполняется операция<br>$R_3 = A_3 - 39_{10} - 35_{10} = 4_{10}$<br>При этом формируется $q_1 = 0$ и $q_0 = 1$ |

В результате выполнения операций получаем остаток $R = 4_{10}$ и частное

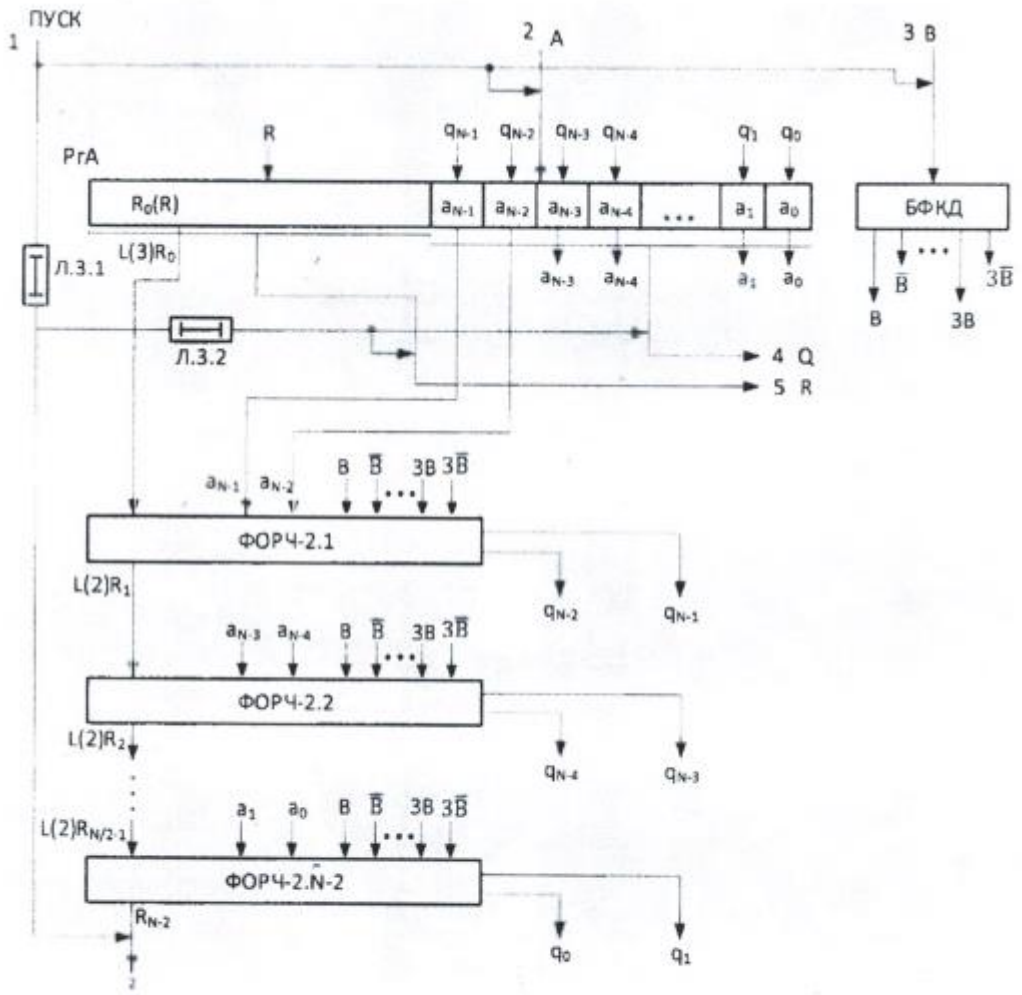
$$Q = q_5 q_4 q_3 q_2 q_1 q_0 = 101001_2 = 40_{10}$$

Проверка:

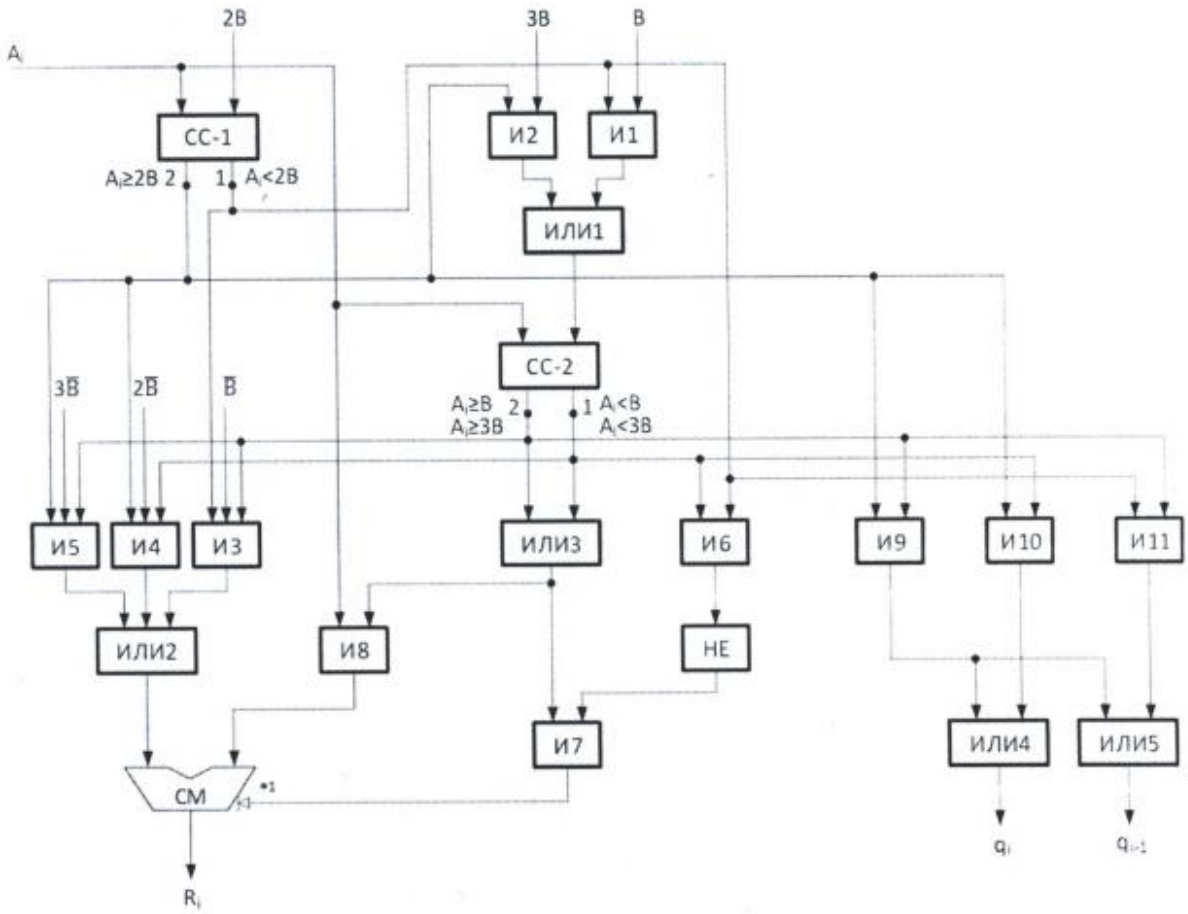
$$A = (Q \times B) + R = (41 \times 35) + 4 = 1439_{10}$$

## *ФОРМУЛА ИЗОБРЕТЕНИЯ*

Матричное делительное устройство на формирователях остатков и двух разрядов частного, содержащее регистров для хранения делимого и делителя, формирователя остатков и двух разрядов частного, блок для формирования кратных делителю (БФКД) ***отличающийся*** тем, что для функционирования делителя в однотактном режиме в его состав включены $^{N}/_{2}$ формирователей остатков и двух разрядов частного (ФОРЧ-2), на входы ФОРЧ-2.1 ÷ ФОРЧ-2. $^{N}/_{2}$ из блока БФКД подаются значения делителя Ви$\overline{B}$, 2В и 2$\overline{B}$, 3В и 3$\overline{B}$; на входы ФОРЧ-2.i подается остаток из выходов предыдущее ФОРЧ-2.i число со сдвигом на два разряда влево с присоединением двух соответствующих разрядов из регистра делимого, на выходах ФОРЧ-2.i и формируется остаток $R_i$ и два разряда частного, которые запоминаются в соответствующих разрядах регистра $P_rA$.


ПУСК
1
2 A
3 B
R
PrA
$R_0(R)$
$a_{N-1}$ $a_{N-2}$ $a_{N-3}$ $a_{N-4}$ ... $a_1$ $a_0$
$q_{N-1}$ $q_{N-2}$ $q_{N-3}$ $q_{N-4}$ $q_1$ $q_0$
БФКД
B $\overline{B}$ 3B $3\overline{B}$
Л.3.1
L(3)$R_0$
Л.3.2
4 Q
5 R
ФОРЧ-2.1
L(2)$R_1$
ФОРЧ-2.2
L(2)$R_2$
ФОРЧ-2.N-2
L(2)$R_{N/2-1}$
$R_{N-2}$

**Фигура 1**




Фигура 2

Верстка Д. Женысова
Корректор Г. Косанова