(19) Евразийское патентное ведомство

(11) 040463 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.06.06

(21) Номер заявки
202190998

(22) Дата подачи заявки
2021.05.11

(51) Int. Cl. ***G06F 7/72*** (2006.01)

(54) УСТРОЙСТВО ДЕЛЕНИЯ ЧИСЕЛ, ПРЕДСТАВЛЕННЫХ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

(43) **2022.06.03**
(96) **2021000048 (RU) 2021.05.11**

(71)(73) Заявитель и патентовладелец:
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ" (RU)

(72) Изобретатель:
Бабенко Михаил Григорьевич, Кучуков Виктор Андреевич (RU)

(74) Представитель:
Лиховид А.А. (RU)

(56) US-B2-9395952
KR-B1-101731921
US-B2-8452831
US-A1-20140195581

(57) Изобретение относится к вычислительным модулярным системам и предназначено для выполнения деления чисел, представленных в системе остаточных классов (СОК). Техническим результатом данного изобретения является повышение точности вычислений деления чисел, представленных в системе остаточных классов. Технический результат достигается применением в устройстве вычислений на основе функции ядра $C(X) = |\sum_{i=1}^{n} C(B_i) \cdot x_i|_{c_P}$, которая подбирается из условия монотонности и отсутствия критических ядер, что позволяет точно производить сравнение чисел в СОК и определение знака числа.

040463 B1

040463 B1

Изобретение относится к вычислительным модулярным системам и предназначено для выполнения деления чисел, представленных в системе остаточных классов (СОК).

В СОК обычное целое число представляется в виде остатков от деления на набор модулей. Арифметические операции над числами заменяются операциями над остатками. Выполнение операций происходит параллельно и без межразрядных переносов, что позволяет очень быстро реализовать сложение, вычитание и умножение. Однако операция деления является немодульной и требует разработки новых позиционных методов вычисления.

Известна нейронная сеть основного деления модулярных чисел (патент на изобретение RU № 2400813, опубликован 27.09.2010). Недостатком устройства является большой объем оборудования и невозможность работы с отрицательными числами. Известная нейронная сеть предназначена для деления модулярных чисел в случае, когда в качестве делителя используется целое положительное число, попарно простое с модулями СОК p_1, p_2, ..., p_n, либо целое положительное число, представляющее собой произведение чисел, попарно простых с p_i. Для выполнения этого условия возникает необходимость нахождения приблизительного делителя путем использования обобщенной позиционной системы счисления (ОПСС). Для нахождения приблизительного делителя необходимо дополнительное оборудование и время.

Известно устройство для основного деления модулярных чисел в формате системы остаточных классов (патент на изобретение RU № 2559772, опубликован 10.08.2015). Недостатком данного устройства является большой объем оборудования и необходимость перевода чисел из основной СОК во вспомогательную СОК.

Известно устройство для основного деления модулярных чисел (патент на изобретение RU № 2559771, опубликован 10.08.2015), содержащее входные шины делимого и делителя, которые подают делимое непосредственно, а делитель через схему умножения либо через мультиплексор на вход схемы сравнения модулярных чисел, выходы которой реализуют вычислительную модель a<b, a>b или a=b, где a - делимое, b - делитель;

управляющие выходы схемы сравнения a<b, a>b соединены со схемой управления, выходы которой соединены с адресными входами мультиплексора, входами управления счетчика, регистров сдвига и хранения, сумматоров частного, делителя и вычитателя, а также с одним из входов ключей, вторые входы которых соединены с выходом памяти, входы которой соединены с регистром сдвига, а выход a=b схемы сравнения соединен со входом сумматора частного, помещая в него "единицу", а информационные выходы соединены со схемами сумматоров делимого и делителя, выходы которого соединены регистром сдвига влево, выход которого соединен со счетчиком определения высшей степени аппроксимационного ряда частного;

выход счетчика соединен с адресными входами памяти, выходы которой через схему ключей и запрет подают на вход сумматора частного степень члена ряда, входящего в уточненный член ряда частного, и на вход схемы умножения высшей степени ряда на делитель, выход которой через мультиплексор соединен со схемой сравнения, выходы которой соединены с сумматорами делимого и делителя;

выход сумматора делителя соединен со входом регистра сдвига вправо, выход которого соединен со схемой вычитателя, на второй вход которого подключен выход сумматора делимого;

выход вычитателя соединен с регистром хранения остатка при вычитании из делимого членов ряда частного, выход которого соединен через сумматор делимого с вычитателем, выход которого соединен со схемой запрета, выходы которой соединены с регистром хранения остатка при вычитании из делимого членов ряда частного и схемой сумматора частного.

Недостатками данного изобретения являются ограниченные функциональные возможности, связанные с невозможностью работы с отрицательными числами.

Известно устройство деления модулярных чисел (патент РФ № 2628179, опубл. 15.08.2017 г.), которое содержит вход тактового импульса, вход глобального сброса, вход делимого, вход делителя, элемент ИЛИ, блок вычисления позиционных характеристик, блок уточнения аппроксимационного ряда, блок вывода частного и выход вывода частного. При этом блок вычисления позиционных характеристик содержит регистр делимого, n инверторов делимого, n регистров хранения модуля p_i, где i=1, ..., n, n регистров хранения коэффициента k_i, n сумматоров делимого, n умножителей отрицательного делимого, n умножителей положительного делимого, сумматор значения F(A), сумматор значения F(-A), регистр хранения значения F(-A), регистр хранения значения F(A), регистр делителя, n инверторов делителя, n регистров хранения модуля p_i, n регистров хранения коэффициента k_i, n сумматоров делителя, n умножителей отрицательного делителя, n умножителей положительного делителя, сумматор значения F(B), сумматор значения F(-B), регистр хранения значения F(-B), регистр хранения значения F(B), элемент XOR, мультиплексор делимого, мультиплексор делителя, блок сравнения. Блок уточнения аппроксимационного ряда содержит регистр сдвига, счетчик, регистр хранения F(|A|), регистр хранения уменьшаемого, мультиплексор выбора уменьшаемого, инвертор, память хранения степеней "2" в СОК, сумматор, мультиплексор выбора следующего уменьшаемого, элемент НЕ, элемент И. Блок вывода частного состоит из элемента ИЛИ, элемента задержки, удерживающего регистра, n регистров хранения остатка по модулю

p_i, n сумматоров по модулю p_i, n демультиплексоров по модулю p_i, n регистров хранения суммы по модулю p_i, n инверторов, n регистров хранения модуля p_i, n сумматоров, n регистров хранения обратного значения суммы по модулю n мультиплексоров выбора суммы, удерживающего регистра знака, регистра хранения суммы в СОК, регистра хранения значения "1", регистра хранения значения "-1", мультиплексора равенства абсолютных величин делимого и делителя, мультиплексора вывода частного, регистра хранения частного.

Недостатком данного изобретения является недостаточная точность, связанная с округлением приближенных значений, что в ряде случаев приводит к ошибкам.

Техническим результатом данного изобретения является повышение точности вычислений деления чисел, представленных в системе остаточных классов.

Технический результат достигается тем, что устройство деления чисел, представленных в системе остаточных классов, содержащее входы делимого и делителя, блок вычисления позиционных характеристик, блок уточнения аппроксимационного ряда, блок вывода частного и выход частного,

при этом вход делимого и вход делителя соединены с первым и вторым входами блока вычисления позиционных характеристик;

первый, второй и третий выходы блока вычисления позиционных характеристик соединены с первым, вторым и третьим входами блока вывода частного;

четвертый и шестой выходы блока вычисления позиционных характеристик соединены с первым и третьим входами блока уточнения аппроксимационного ряда, первый и второй выходы которого соединены с четвертым и пятым входами блока вывода частного, выход которого является выходом частного; и

блок вычисления позиционных характеристик содержит два инвертора, четыре блока умножения на константы, четыре блока сложения, два мультиплексора, элемент XOR и блок сравнения,

при этом значение делимого, представленное в СОК, с первого входа поступает на вход первого блока умножения на константы и на вход первого инвертора, выход которого подключен ко входу второго блока умножения на константы;

выходы первого и второго блоков умножения на константы подключены ко входам первого и второго блоков сложения, выходы которых соединены с первым и третьим входами первого мультиплексора;

значение делителя, представленное в СОК, со второго входа блока вычисления позиционных характеристик поступает на вход третьего блока умножения на константы и на вход второго инвертора, выход которого подключен ко входу четвертого блока умножения на константы;

выходы третьего и четвертого блоков умножения на константы подключены ко входам третьего и четвертого блоков сложения, выходы которых соединены с первым и третьим входами второго мультиплексора;

первые выходы первого и второго мультиплексоров подключены ко второму и третьему входам блока сравнения, первый и второй выходы которого являются вторым и третьим выходами блока вычисления позиционных характеристик;

первый выход первого мультиплексора дополнительно соединен с пятым выходом блока вычисления позиционных характеристик;

выход элемента XOR является первым выходом блока вычисления позиционных характеристик,

блок уточнения аппроксимационного ряда содержит регистр хранения уменьшаемого, блок вычитания по модулю, мультиплексор, регистр хранения степеней "2", блок отсчета степеней и элемент И,

при этом выход блока вычитания по модулю соединен со вторым входом мультиплексора, выход которого соединен со вторым входом регистра хранения уменьшаемого;

третий выход блока отсчета степеней является первым выходом блока уточнения аппроксимационного ряда;

выход элемента И является вторым выходом блока уточнения аппроксимационного ряда;

блок вывода частного содержит блок сложения по модулю, демультиплексор, инвертор, регистр хранения "1" в СОК, регистр хранения "-1" в СОК, мультиплексор частного, мультиплексор единицы и мультиплексор выбора частного,

при этом первый вход блока сложения по модулю является пятым входом блока вывода частного;

второй вход блока сложения по модулю подключен к первому выходу демультиплексора, а выход соединен со входом демультиплексора, управляющий вход которого подключен к четвертому входу блока вывода частного, а второй выход - ко второму входу и через инвертор к первому входу мультиплексора частного, выход которого соединен с первым входом мультиплексора выбора частного, второй вход которого соединен с выходом мультиплексора единицы, первый и второй входы которого соединены с регистрами хранения "1" и "-1" в СОК соответственно;

управляющие входы мультиплексора частного и мультиплексора единицы соединены с первым входом блока вывода частного;

управляющий вход мультиплексора выбора частного подключен к третьему входу блока вывода частного,

отличается тем, что дополнительно пятый выход блока вычисления позиционных характеристик со-

единен со вторым входом блока уточнения аппроксимационного ряда;

в блок вычисления позиционных характеристик введены первый и второй блоки определения знака;

в блоках умножения на константы производится умножение на ортогональные базисы СОК

$$C(B_i) = \frac{B_i \cdot C_P}{P} - \frac{w_i}{p_i},$$

где $B_i = P_i \cdot \left|P_i^{-1}\right|_{p_i}$, $P_i = P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ - мультипликативная инверсия,

$P = \prod_{i=1}^{n} p_i$ - рабочий диапазон СОК с модулями p_1, p_2, ..., p_n,

в блоках суммирования происходит следующее вычисление функции ядра:

$$C(X) = \left|\sum_{i=1}^{n} C(B_i) \cdot x_i\right|_{C_P},$$

которая подбирается из условия монотонности и отсутствия критических ядер,

где $C_P=2^N$ - максимальный диапазон функции ядра, а

веса w_i характеризует конкретную функцию ядра,

при этом на выход блоков сложения подаются N младших бит суммы;

выходы первого и третьего блоков сложения дополнительно соединены со вторыми входами первого и второго блоков определения знака, первые входы которых соединены с первым и вторым входами блока вычисления позиционных характеристик, а выходы соединены с управляющими входами первого и второго мультиплексоров соответственно и с первым и вторым входами элемента XOR;

первый и второй входы блока вычисления позиционных характеристик дополнительно соединены со вторыми входами первого и второго мультиплексора, четвертые входы которых соединены с выходами первого и второго инверторов;

вторые выходы первого и второго мультиплексоров соединены с первым и четвертым входами блока сравнения и четвертым и шестым выходами блока вычисления позиционных характеристик; и

в блок уточнения аппроксимационного ряда введен регистр хранения делителя, блок умножения по модулю, демультиплексор, два блока умножения на константу, два блока сложения и блок определения знака,

при этом блок отсчета степеней во время прямого отсчета вычисляет максимальную степень частного, а во время обратного отсчета последовательно передает адреса степеней "2" в порядке убывания на первый вход регистра хранения степеней "2", выход которого подключен ко второму входу блока умножения по модулю и второму входу демультиплексора, на управляющий вход которого поступает сигнал со второго выхода блока отсчета степеней, а на первый вход - сигнал с выхода блока умножения по модулю, первый вход которого соединен с выходом регистра хранения делителя, вход которого является третьим входом блока уточнения аппроксимационного ряда, первый вход которого подключен к первому входу регистра хранения уменьшаемого, а второй вход подключен к первому входу блока отсчета степеней;

третий выход демультиплексора подключен ко входу первого блока умножения на константы, выход которого подключен ко входу первого блока сложения, выход которого подключен ко второму входу блока отсчета степеней;

выход регистра хранения уменьшаемого подключен к первому входу мультиплексора и первому входу блока вычитания по модулю, выход которого подключен ко входу второго блока умножения на константы и второму входу блока определения знака;

выход второго блока умножения на константы подключен ко входу второго блока сложения, выход которого подключен к первому входу блока определения знака, выход которого подключен к управляющему входу мультиплексора и через инвертор к первому входу элемента И, второй вход которого соединен со вторым выходом демультиплексора, первый выход которого подключен ко второму входу блока вычитания по модулю;

в блок вывода частного дополнительно введен элемент И, первый вход которого соединен с выходом мультиплексора выбора частного, а второй вход - через инвертор со вторым входом блока вывода частного; и

выход элемента И является выходом частного.

Сущность изобретения основана на следующем математическом аппарате. Пусть даны делимое X, делитель Y, частное Q и остаток R. Тогда R=X-Y·Q, при этом R<Y. Рассмотрим алгоритм деления, основанный на последовательном приближении частного Q степенями основания системы счисления, т.е. для двоичной системы процесс заключается в нахождении таких $q_i=\{0,1\}$, чтобы выполнялось равенство

$$Q = q_n \cdot 2^n + q_{n-1} \cdot 2^{n-1} + \cdots + q_1 \cdot 2^1 + q_0 \cdot 2^0 \qquad (1)$$

Подставляя (1) в формулу деления, получим

$$R = X - Y \cdot q_n \cdot 2^n - Y \cdot q_{n-1} \cdot 2^{n-1} - \cdots - Y \cdot q_1 \cdot 2^1 - Y \cdot q_0 \cdot 2^0 \qquad (2)$$

Таким образом процесс деления можно свести к последовательности вычитаний. Пусть 2^n входит в представление частного Q, т.е. $q_n=1$, тогда обозначим $\Delta_1=X-2^n \cdot Y$, причем $\Delta_1 \geq 0$. Подставим Δ_1 в (2).

$$R = \Delta_1 - Y \cdot q_{n-1} \cdot 2^{n-1} - \cdots - Y \cdot q_1 \cdot 2^1 - Y \cdot q_0 \cdot 2^0$$

Продолжим данный процесс. Обозначим $\Delta_2=\Delta_1-2^{n-1} \cdot Y$. Поскольку Δ_i является суммой остатка от деления и оставшихся членов последовательности степеней системы счисления, умноженных на делитель,

то всегда выполняется $\Delta_i \geq 0$.

Если же 2^k не входит в представление частного Q, т.е. $q_k=0$, тогда $\Delta_{n-k-1}=\Delta_{n-k-2}-2^k \cdot Y<0$. И тогда необходимо проверить вхождение 2^{k-1}, для чего находится $\Delta_{n-k}=\Delta_{n-k-2}-2^{k-1} \cdot Y$.

В системе остаточных классов любое число X<P однозначно представляется набором остатков x_i от деления числа X на взаимно простые модули СОК p_i, где $x_i \equiv X \bmod p_i$, $P=\prod_{i=1}^{n} p_i$ - рабочий диапазон СОК, $i=\overline{1,n}$. Восстановление числа X из СОК в позиционную систему счисления может быть произведено как в прототипе с использованием приближенной Китайской теоремы об остатках

$$F(X)=\frac{X}{P}=\left|\sum_{i=1}^{n}\frac{\left|P_i^{-1}\right|_{p_i}}{p_i}\cdot x_i\right|_P=\left|\sum_{i=1}^{n}k_i\cdot x_i\right|_1,$$

где $k_i=\frac{\left|P_i^{-1}\right|_{p_i}}{p_i}$, $P_i=P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ - мультипликативная инверсия.

Однако коэффициенты k_i редко оказываются конечной дробью и округление приводит к накоплению ошибок.

Знак в системе остаточных классов чаще всего вводится разбиением диапазона на две части, тогда с учетом динамического диапазона P в СОК можно представить числа

$$-\frac{P-1}{2}\leq X\leq\frac{P-1}{2},\text{ если P нечетное,}$$

$$-\frac{P}{2}\leq X\leq\frac{P}{2}-1,\text{ если P четное.}$$

Тогда

X - положительное, если $0\leq X\leq\frac{P}{2}-1$, если P - четное, $0\leq X\leq\frac{P-1}{2}$, если X - нечетное,

X - отрицательное, если $\frac{P}{2}\leq X<P$, если P - четное, $\frac{P+1}{2}\leq X<P$, если X - нечетное.

Для выполнения деления по формуле необходимо выполнение операций сравнения чисел, представленных в СОК, и определения знака.

Поскольку СОК является непозиционной системой счисления, то для сравнения чисел и определения знака, т.е. нахождения положения числа на числовой прямой, вычисляют позиционную характеристику. Примером позиционной характеристики может служить Китайская теорема об остатках с дробями, использованная в прототипе. Другой позиционной характеристикой может быть введенная И.Я. Акушским функция ядра

$$C(X)=\sum_{i=1}^{n}w_i\left\lfloor\frac{X}{p_i}\right\rfloor$$

Числа w_i, называемые весами, в данной формуле могут быть в определенном смысле произвольными. Именно они определяют каждую конкретную функцию ядра и могут меняться в зависимости от задачи. Базовым свойством функции ядра является то, что ее максимальный диапазон может меняться и может быть значительно меньше числа P в зависимости от выбора весов. Например, мы можем в качестве C(P) использовать некоторое произвольное значение C_P, обладающее необходимыми для решения конкретной задачи свойствами. Значения функции ядра C(X), заданной весами w_1, w_2, ..., w_n, при условии $0\leq C(X)<C_P$, $X\in[0,P]$, можно вычислить с использованием формулы

$$C(X)=\left|\sum_{i=1}^{n}C(B_i)\cdot x_i\right|_{C_P}$$

где $B_i=P_i\cdot\left|P_i^{-1}\right|_{p_i}$ - ортогональные базисы СОК.

Однако в общем случае функция ядра не обладает монотонностью, необходимой для сравнения чисел.

Для построения функции ядра с заданными свойствами воспользуемся алгоритмом 1.

Алгоритм 1. Подбор параметров функции ядра специального вида для заданного набора модулей.

Входные данные: набор модулей СОК p_1, p_2, ... , p_n. Требуется построить функцию ядра с модулем специального вида с $C_P=R(N)$ и неотрицательными коэффициентами.

Выходные данные: коэффициенты w_1, w_2, ..., w_n построенной функции ядра.

1. Положим вначале $N=[\log_2 P_n]$.

2. Для заданной величины N рассчитать $w_i^*=\left|R(N)\cdot P_i^{-1}\right|_{p_i}$, i=1, 2, ..., n и $C_P^*=P\cdot\sum_{i=1}^{n}\frac{w_i^*}{p_i}$, где $R(N)=2^N$.

3. Рассчитать Q по формуле $Q=\frac{R(N)-C_P^*}{P}$.

4. Если Q<0, то положить N=N+1 и перейти к шагу 2. Иначе, перейти к шагу 5.

5. Подобрать q_i так, чтобы $Q=q_1+q_2+...+q_n$. Рассчитать $w_i = q_i \cdot p_i + w_i^*$ для i=1, 2, ..., n.

6. Проверить условия отсутствия критических ядер снизу $C(p_k) = \sum_{i=1}^{k} w_i \left\lfloor \frac{p_k}{p_i} \right\rfloor \geq 0$ и отсутствия критических ядер сверху $\sum_{i=1}^{n} \left(\left\lfloor \frac{p_k}{p_i} \right\rfloor + 1 \right) w_i - w_k > 0,$ для всех k=1, 2, ..., n. Если не выполняется, то положить N=N+1 и перейти к шагу 2.

Конец алгоритма 1.

Тогда функция ядра с заданными свойствами будет задана выражением

$$C(X) = \left| \sum_{i=1}^{n} C(B_i) \cdot x_i \right|_{C_P} \qquad (3)$$

где $C(B_i) = \frac{B_i \cdot C_P}{P} - \frac{w_i}{p_i}$ и $B_i = P_i \cdot \left| P_i^{-1} \right|_P$.

Использование $C_P=2^N$ позволит эффективно выполнять операции деления и нахождения остатка от деления, поскольку результат равен младшим N битам суммы.

Для сравнения чисел воспользуемся алгоритмом 2.

Алгоритм 2. Сравнение чисел, представленных в СОК, с использованием функции ядра с неотрицательными коэффициентами.

Входные данные: $X=(x_1, x_2, ..., x_n)$ и $Y=(y_1, y_2, ..., y_n)$.

1. Вычислить C(X) и C(Y).

2. Сравнить:

(a) если C(X)<C(Y), то X<Y;

(b) если C(X)>C(Y), то X>Y;

(c) если C(X)=C(Y), то

1) если $x_k<y_k$, то X<Y;

2) если $x_k>y_k$, то X>Y;

3) если $x_k=y_k$, то X=Y.

Конец алгоритма 2.

В данном случае взяты неотрицательные коэффициенты $w_1, w_2, ..., w_n$ и $w_k \neq 0$ - первый не равный нулю коэффициент.

Для определения знака числа необходимо построить такую функцию ядра, чтобы

C(X)≤C(K) для положительных чисел, и

C(X)>C(K) для отрицательных,

где K=P/2, если P - четное,

K=(P-1)/2, если P - нечетное.

K - является серединой диапазона СОК. Т.е. воспользоваться алгоритмом 2 для X и K.

Рассмотрим пример деления в СОК на основе функции (3) и алгоритма 2.

Возьмем в качестве СОК {11, 13, 17, 19}. Тогда P=46189, $P_1=4199$, $P_2=3553$, $P_3=2717$, $P_4=2431$, $P_1^{-1}=7$, $P_2^{-1}=10$, $P_3^{-1}=11$, $P_4^{-1}=18$, $B_1=29393$, $B_2=35530$, $B_3=29887$, $B_4=43758$. Воспользовавшись алгоритмом 1, получим N=17, $w_1=16$, $w_2=8$, $w_3=5$, $w_4=9$.

Тогда вспомогательные значения $C(B_i)$ будут равны $C(B_1)=83408$, $C(B_2)=100824$, $C(B_3)=84811$, $C(B_4)=124173$. И функция ядра примет вид

$$C(X) = |83408 \cdot x_1 + 100824 \cdot x_2 + 84811 \cdot x_3 + 124173 \cdot x_4|_{2^{17}}$$

Серединой диапазона СОК будет K=23094, для которого C(K)=65517.

Найдем частное от деления X=(5, 4, 3, 5) на Y=(1, 10, 6, 4). Проверим знаки делимого и делителя, для чего вычислим C(X) и C(Y):

C(X)=122770>65517=C(K), число отрицательное,

C(Y)=54<65517=C(K), число положительное.

Поскольку делимое и делитель разных знаков, то результат будет отрицательным. Для делимого найдем противоположное значение, чтобы выполнять деление над абсолютными значениями. Для этого в СОК необходимо из модуля вычесть соответствующий остаток.

$$-X = (p_1 - x_1, p_2 - x_2, \dots, p_n - x_n) = (11-5; 13-4; 17-3; 19-5)$$

Получим |X|=(6, 9, 14, 14). Представления степеней "2" в СОК могут быть вычислены заранее в зависимости от диапазона СОК (наивысшая степень вхождения 2^n равна $[\log_2 K]$) и записаны в память:

$$2^{14} = (5,4,13,6), 2^{13} = (8,2,15,3), 2^{12} = (4,1,16,11), 2^{11} = (2,7,8,15)$$

$$2^{10} = (1,10,4,17), 2^9 = (6,5,2,18), 2^8 = (3,9,1,9), 2^7 = (7,11,9,14)$$

$$2^6 = (9,12,13,7), 2^5 = (10,6,15,13), 2^4 = (5,3,16,16), 2^3 = (8,8,8,8)$$

$$2^2 = (4,4,4,4), 2^1 = (2,2,2,2), 2^0 = (1,1,1,1)$$

Наивысшая возможная степень частного при выполнении деления равна размерности делимого. Для определения необходимо, последовательно умножая делитель на 2^1, найти число, для которого зна-

чения функции ядра удовлетворяют выражению $C(|X|) \leq C(2^i|Y|)$.

$$C(2^6|Y|) = 4155 < C(|X|) = 8264 < C(2^7|Y|) = 8331$$

По формуле (2) вычислим $\Delta_1 = X - 2^7 \cdot Y$:

$$\Delta_1 = (6,9,14,14) - (7,11,9,14) \cdot (1,10,6,4) = (10,3,11,15), \Delta_1 < 0.$$

Значит, 2^7 не входит в представление частного Q.

Проверим 2^6, вычислив $\Delta_2 = X - 2^6 \cdot Y$:

$$\Delta_2 = (6,9,14,14) - (9,12,13,7) \cdot (1,10,6,4) = (8,6,4,5), \Delta_2 > 0.$$

Значит, 2^6 входит в представление частного Q.

Проверим 2^5, вычислив $\Delta_3 = \Delta_2 - 2^5 \cdot Y$:

$$\Delta_3 = (8,6,4,5) - (10,6,15,13) \cdot (1,10,6,4) = (9,11,16,10), \Delta_3 > 0.$$

Значит, 2^5 входит в представление частного Q.

Проверим 2^4, вычислив $\Delta_4 = \Delta_3 - 2^4 \cdot Y$:

$$\Delta_4 = (9,11,16,10) - (5,3,16,16) \cdot (1,10,6,4) = (4,7,5,3), \Delta_4 > 0.$$

Значит, 2^4 входит в представление частного Q.

Проверим 2^3, вычислив $\Delta_5 = \Delta_4 - 2^3 \cdot Y$:

$$\Delta_5 = (4,7,5,3) - (8,8,8,8) \cdot (1,10,6,4) = (7,5,8,9), \Delta_5 > 0.$$

Значит, 2^3 входит в представление частного Q.

Проверим 2^2, вычислив $\Delta_6 = \Delta_5 - 2^2 \cdot Y$:

$$\Delta_6 = (7,5,8,9) - (4,4,4,4) \cdot (1,10,6,4) = (3,4,1,12), \Delta_6 > 0.$$

Значит, 2^2 входит в представление частного Q.

Проверим 2^1, вычислив $\Delta_7 = \Delta_6 - 2^1 \cdot Y$:

$$\Delta_7 = (3,4,1,12) - (2,2,2,2) \cdot (1,10,6,4) = (1,10,6,4), \Delta_7 > 0.$$

Значит, 2^1 входит в представление частного Q.

Проверим 2^0, вычислив $\Delta_8 = \Delta_7 - 2^0 \cdot Y$:

$$\Delta_8 = (1,10,6,4) - (1,1,1,1) \cdot (1,10,6,4) = (0,0,0,0), \Delta_7 = 0.$$

Значит, 2^0 входит в представление частного Q.

Таким образом,

$$|Q| = 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 127.$$

Т.к. результат должен быть отрицательным, то Q=-127. Проверим $-\frac{2921}{23} = -127$.

Данное устройство деления чисел, представленных в СОК, поясняется фиг. 1-4.

На фиг. 1 представлена общая структурная схема устройства, которая содержит вход делимого 1, вход делителя 2, блок вычисления позиционных характеристик 3, блок уточнения аппроксимационного ряда 4, блок вывода частного 5 и выход частного 6. Входы делимого 1 и делителя 2 подключены к первому и второму входам блока вычисления позиционных характеристик 3. С первого выхода блока вычисления позиционных характеристик 3 значение знака результата поступает на первый вход блока вывода частного 5. Со второго выхода блока вычисления позиционных характеристик 3 на второй вход блока вывода частного 5 поступает сигнал "|X|<|Y|", т.е. что результат деления равен 0. С третьего выхода блока вычисления позиционных характеристик 3 на третий вход блока вывода частного 5 поступает сигнал "|X|=|Y|", т.е. что результат деления равен ±1 в зависимости от знаков входных чисел. С четвертого и шестого выходов блока вычисления позиционных характеристик 3 на первый и третий входы блока уточнения аппроксимационного ряда 4 поступают абсолютные значения делимого |X| и делителя |Y|. С пятого выхода блока вычисления позиционных характеристик 3 на второй вход блока уточнения аппроксимационного ряда 4 поступает значение функции ядра абсолютного значения делимого C(|X|). С первого выхода блока уточнения аппроксимационного ряда 4 на четвертый вход блока вывода частного 5 поступает сигнал окончания перебора степеней "2", входящих в представление частного Q. Со второго выхода блока уточнения аппроксимационного ряда 4 на пятый вход блока вывода частного 5 поступают степени "2", входящие в представление частного Q. Первый выход блока вывода частного 5 является выходом частного 6.

На фиг. 2 представлена схема блока вычисления позиционных характеристик 3, которая содержит инверторы делимого 7 и делителя 14, блоки умножения на константы 8, 11, 15, 18, блоки сложения 9, 12, 16, 19, блоки определения знака 10 и 17, мультиплексоры 13 и 20, элемент XOR 21, блок сравнения 22.

На входы делимого 1 и делителя 2 поступают значения делимого X и делителя Y, представленные в СОК, т.к. $(x_1, x_2, ..., x_n)$ и $(y_1, y_2, ..., y_n)$. В инверторах делимого 7 и делителя 14 вычисляются противоположные значения -X и -Y соответственно. В СОК для получения противоположного значения -X необходимо из модуля вычесть соответствующий остаток $(p_1-x_1, p_2-x_2, ..., p_n-x_n)$. Затем числа X и -X, Y и -Y в блоках умножения на константы 8, 11, 15, 18 соответственно умножаются на константы значений функции ядра ортогональных базисов СОК $C(B_i)$, т.е. в каждом блоке происходит параллельное умножение остатков на $C(B_i)$ по формуле (3). Значения произведений с блоков умножения на константы 8, 11, 15, 18 подаются на входы блоков сложения 9, 12, 16, 19 соответственно, на выход которых подаются младшие N бит суммы, что соответствует нахождению остатка по модулю 2^N в формуле (3), а N определяется за-

ранее по алгоритму 1 при построении функции ядра.

На первые входы блоков определения знака 10 и 17 поступают значения делимого и делителя со входов делимого 1 и делителя 2 соответственно. На вторые входы блоков определения знака 10 и 17 поступают значения функции ядра C(X) и C(Y) с выходов блоков сложения 9 и 16 соответственно. В блоках определения знака 10 и 17 происходит сравнение значений функции ядра и остатков по одному из оснований с серединой диапазона K СОК по алгоритму 2. Значения знаков X и Y с выходов блоков определения знака 10 и 17 поступают на входы элемента XOR 21, а также на управляющие входы мультиплексоров 13 и 20 соответственно. Выход элемента XOR 21 является первым выходом блока вычисления позиционных характеристик 21.

На первый и второй информационные входы мультиплексора 13 поступают значение функции ядра C(X) с выхода блока сложения 9 и значение делимого X с входа делимого 1. На третий и четвертый информационные входы мультиплексора 13 поступают значение функции ядра C(-X) с выхода блока сложения 12 и значение -X с выхода инвертора 7. Первый выход мультиплексора 13 подключен ко второму входу блока сравнения 22 и пятому выходу блока вычисления позиционных характеристик 3 и передает значение функции ядра от абсолютного значения делимого C(|X|). Второй выход мультиплексора 13 подключен к первому входу блока сравнения 22 и является четвертым выходом блока вычисления позиционных характеристик 3 и передает абсолютное значение делимого |X|.

На первый и второй информационные входы мультиплексора 20 поступают значение функции ядра C(Y) с выхода блока сложения 16 и значение делителя Y с входа делителя 2. На третий и четвертый информационные входы мультиплексора 20 поступают значение функции ядра C(-Y) с выхода блока сложения 19 и значение -Y с выхода инвертора 14. Первый выход мультиплексора 20 подключен к третьему входу блока сравнения 22 и передает значение функции ядра от абсолютного значения делителя C(|Y|). Второй выход мультиплексора 20 подключен к четвертому входу блока сравнения 22, является шестым выходом блока вычисления позиционных характеристик 3 и передает абсолютное значение делителя |Y|.

Блок сравнения 22 на основе алгоритма 2 по значениям C(|X|), |X| и C(|Y|), |Y| сравнивает абсолютные значения делимого и делителя и подает на первый выход блока сравнения 22 сигнал в случае "|X|<|Y|", который поступает на второй выход блока вычисления позиционных характеристик 3, подает на второй выход блока сравнения 22 сигнал в случае "|X|=|Y|", который поступает на третий выход блока вычисления позиционных характеристик 3.

На фиг. 3 изображен блок уточнения аппроксимационного ряда 4, который содержит регистр хранения уменьшаемого 23, регистр хранения делителя 24, блок умножения по модулю 25, регистр хранения степеней "2" 26, блок отсчета степеней 27, демультиплексор 28, мультиплексор 29, блок вычитания по модулю 30, блоки умножения на константы 31 и 33, блоки сложения 32 и 34, блок определения знака 35, элемент И 36.

На первый вход регистра хранения уменьшаемого 23 поступает значение |X| с первого входа блока уточнения аппроксимационного ряда 4. Вход регистра хранения делителя 24 является третьим входом блока уточнения аппроксимационного ряда 4 и передает значение |Y| на первый вход блока умножения по модулю 25, в котором осуществляется умножение делителя на степени "2", представленные в СОК, которые поступают с первого выхода регистра хранения степеней "2" 26. Дополнительно степени "2" с первого выхода регистра хранения степеней "2" 26 поступают на второй вход демультиплексора 28, на первый вход которого поступает значение произведения с выхода блока умножения по модулю 25.

Блок отсчета степеней 27 осуществляет определение степени "2", для которой произведение $2^i \cdot |Y| \geq |X|$, и после проводит обратный отсчет степеней для проверки вхождения степени "2" в представление частного Q. Для определения максимальной степени "2" блок отсчета степеней 27 подает на первый выход, соединенный с первым входом регистра хранения степеней "2" 26, значения адреса, начиная с 1, при этом максимальная степень равна $[\log_2 K]$, регистр хранения степеней "2" 26 подает на первый выход степени "2", представленные в СОК. На второй выход, подключенный к управляющему входу демультиплексора 28, подается значение режима работы: прямой или обратный отсчет степеней. В случае прямого отсчета значение произведения с выхода блока умножения по модулю подается на третий выход демультиплексора 28, который подключен ко входу блока умножения на константу 31, в котором происходит умножение на значения функции ядра от ортогональных базисов СОК C(Bi) и последующее их сложение в блоке сложения 32, младшие N бит результата подаются на второй вход блока отсчета степеней 27, где происходит его сравнение со значением функции ядра делимого, которое поступает на первый вход блока отсчета степеней 27 со второго входа блока уточнения аппроксимационного ряда 4. В случае обратного отсчета значение произведения с выхода блока умножения по модулю подается на первый выход демультиплексора 28, на второй выход которого подается значение степени "2". По окончании обратного отсчета на третий выход блока отсчета степеней 27 подается сигнал окончания отсчета.

В блоке вычитания по модулю 30 происходит вычитание по формуле (2) из уменьшаемого, которое подается на первый вход с выхода регистра хранения уменьшаемого 23 произведения с первого выхода демультиплексора 28, которое подается на второй вход блока вычитания по модулю 30. Результат вычитания подается на вход блока умножения на константы 33, откуда через блок сложения 34 поступает на

первый вход блока определения знака 35, второй вход которого подключен к выходу блока вычитания по модулю 30, который также подключен ко второму информационному входу мультиплексора 29. Выход блока определения знака 35 подключен через инвертор к первому выходу элементу И 36, на второй вход которого поступают степени "2" со второго выхода демультиплексора 28 и на управляющий вход мультиплексора 29, первый вход которого соединен с выходом регистра хранения уменьшаемого 23, а выход мультиплексора 29 подключен ко второму входу регистра хранения уменьшаемого 23. Выход элемента И 36 является вторым выходом блока уточнения аппроксимационного ряда 4.

На фиг. 4 изображен блок вывода частного 5, содержащий блок сложения по модулю 37, демультиплексор 38, инвертор 39, регистр хранения "1" в СОК 40, регистр хранения "-1" в СОК 41, мультиплексор частного 42, мультиплексор единицы 43, мультиплексор выбор частного 44, элемент И 45.

Степени "2" с пятого входа блока вывода частного 5 поступают на первый вход блока сложения по модулю 37, выход которого соединен с информационным выходом демультиплексора 38, который в зависимости от сигнал окончания отсчета на управляющий вход демультиплексора 38 с четвертого входа блока вывода частного 5 подает результат на второй вход блока сложения по модулю 37 или на второй информационный вход мультиплексора частного 42 и на первый информационный вход мультиплексора частного 42 через инвертор 39. Сигнал знака Q с первого входа блока вывода частного 5 поступает на управляющие входы мультиплексора частного 42 и мультиплексора единицы 43, на первый и второй информационные входы которого поступают сигналы с выходов регистра хранения "1" в СОК 40 и регистра хранения "-1" в СОК соответственно. Выходы мультиплексора частного 42 и мультиплексора единицы 43 подключены к первому и второму информационным входам мультиплексора выбора частного 44, на управляющий вход которого поступает сигнал "|X|=|Y|" с третьего входа блока вывода частного 5. Выход мультиплексора частного 44 подключен к первому входу элемента И 45, на второй вход которого через инвертор поступает сигнал "|X|<|Y|" со второго входа вывода частного 5. Выход элемента И 45 является выходом частного 6.

Рассмотрим предыдущий пример для СОК $\{p_1, p_2, p_3, p_4\}=\{11, 13, 17, 19\}$. Для данной СОК по алгоритму 1 рассчитываются внутренние параметры N=17, w_1= 16, w_2=8, w_3=5, w_4=9. Блоки умножения на константы 8, 11, 15, 18, 31, 33 осуществляют умножения каждого из четырех остатков числа на $C(B_1)$=83408, $C(B_2)$=100824, $C(B_3)$=84811, $C(B_4)$=124173 соответственно. Блоки сложения 9, 12, 16, 19, 32 осуществляют сложение полученных произведений и вывод младших N бит числа. Таким образом, пары блоков умножения на константы с блоками сложения реализуют выполнение формулы $C(X)=|83408\cdot x_1+100824\cdot x_2+84811\cdot x_3+124173\cdot x_4|_2^{17}$. Инверторы находят противоположное значение для числа, представленного в СОК, для чего из модуля вычитают соответствующий остаток.

На вход делимого 1 подается X=(5, 4, 3, 5), которое после вычисления функции ядра блоками умножения на константы 8 и сложения 9 подает значение C(X)=122770 на второй вход блока определения знака 10, на первый вход которого подается X=(5, 4, 3, 5) с входа делимого 1. В блоке определения знака 10 происходит сравнение с K=23094 и C(K)=65517 по алгоритму 2. Значение знака X равно 1 (отрицательное) и поступает на управляющий вход мультиплексора делимого 13 и на первый вход элемента XOR 21. Также значение X=(5, 4, 3, 5) поступает на инвертор 7, результатом которого будет $-X=(p_1-x_1, p_2-x_2, ..., p_n-x_n)$=(6, 9, 14, 14). После вычисления функции ядра блоками умножения на константы 11 и сложения 12 получают C(-X)=8264. На первый информационный вход мультиплексора 13 подается C(X)=122770, на второй информационный вход подается X=(5, 4, 3, 5), на третий информационный вход подается C(-X)=8264, на четвертый информационный вход подается -X=(6, 9, 14, 14). Поскольку делимое отрицательное, то на первый выход мультиплексора 13 подается C(|X|)=8264, а на второй выход - |X|=(6, 9, 14, 14).

Одновременно на вход делителя 2 подается Y=(1, 10, 6, 4), которое после вычисления функции ядра блоками умножения на константы 15 и сложения 16 подает значение C(Y)=54 на второй вход блока определения знака 17, на первый вход которого подается Y=(1, 10, 6, 4) с входа делителя 2. В блоке определения знака 17 происходит сравнение с K=23094 и C(K)=65517 по алгоритму 2. Значение знака Y равно 0 (положительное) и поступает на управляющий вход мультиплексора делителя 20 и на второй вход элемента XOR 21. Также значение Y=(1, 10, 6, 4) поступает на инвертор 14, результатом которого будет -Y=(10, 3, 11, 15). После вычисления функции ядра блоками умножения на константы 18 и сложения 19 получают C(-Y)=130980. На первый информационный вход мультиплексора 20 C(Y)=54, на второй информационный вход подается Y=(1, 10, 6, 4), на третий информационный вход подается C(-Y)=130980, на четвертый информационный вход подается -Y=(10, 3, 11, 15). Поскольку делитель положительный, то на первый выход мультиплексора 20 подается C(|Y|)=54, а на второй выход - |Y|=(1, 10, 6, 4).

Поскольку знаки у делимого X и делителя Y разные, на выход элемента XOR 21 подается сигнал 1, т.е. результат отрицательный. В блоке сравнения 22 на основе алгоритма 2 сравниваются C(|X|)=8264 и |X|=(6, 9, 14, 14) с C(|Y|)=54 и |Y|=(1, 10, 6, 4), поступающими с мультиплексоров 13 и 20. Поскольку C(|X|)=8264>C(|Y|)=54, то |X|>|Y| и на выходы "|X|<|Y|" и "|X|=|Y|" подаются 0.

Таким образом, на первый выход блока вычисления позиционных характеристик 3 подается знак результата 1, на второй и третий выходы подаются нули, что означает невыполнение условий "|X|<|Y|" и "|X|=|Y|". На четвертый, пятый и шестой выходы подаются соответственно значения |X|=(6, 9, 14, 14),

C(|X|)=8264 и |Y|=(1, 10, 6, 4).

На вход регистра хранения делимого 24 подается |Y|=(1, 10, 6, 4). Блок отсчета степеней 27 подает на первый выход адрес степени "2^1", представленной в СОК, которая хранится в регистре хранения степеней "2" 26. Значение (2, 2, 2, 2) подается на второй вход блока умножения по модулю 25, на первый вход которого подается (1, 10, 6, 4). Результат (2, 7, 12, 8) под действием сигнала на управляющий вход демультиплексора 28 подается на блоки умножения на константу 31 и сложения 32, в которых вычисляется значение функции ядра C(2|Y|)=116. В блоке отсчета степеней 27 данное значение сравнивается с C(|X|)=8264, которое поступает на первый вход, и поскольку 116<8264, продолжается прямой отсчет степеней. Данный отсчет продолжается до 2^7, для которого C(2^7|Y|)=8331. После этого блок отсчета степеней 27 переходит в обратный отсчет и подает соответствующий сигнал на управляющий вход демультиплексора 28.

Блок отсчета степеней 27 подает на первый выход адрес степени "2^7", представленной в СОК, которая хранится в регистре хранения степеней "2" 26. Значение (7, 11, 9, 14) подается на второй вход блока умножения по модулю 25, на первый вход которого подается (1, 10, 6, 4). Результат (7, 6, 3, 18) под действием сигнала на управляющий вход демультиплексора 28 подается на второй вход блока вычитания по модулю 30, на первый вход которого подается |X|=(6, 9, 14, 14). Результат Δ_1=(10, 3, 11, 15) подается на блоки умножения на константу 33 и сложения 34, в которых вычисляется значение функции ядра C(Δ_1)=130980, которое поступает на первый вход блока определения знака 35, на второй вход которого поступает значение Δ_1, поскольку число C(Δ_1)>C(K), то Δ_1<0 и 2^7 не входит в представление частного Q. На выход блока определения знака 35 подается 1, которая поступает на управляющий вход мультиплексора 29, перезаписывая значение |X| в регистре хранения уменьшаемого 23. Также 1 с выхода блока определения знака 35 подается на инвертированный первый вход элемента И 36, обнуляя значение степени "2^7", подаваемой со второго выхода демультиплексора 28.

Далее блок отсчета степеней 27 подает на первый выход адрес степени "2^6", представленной в СОК, которая хранится в регистре хранения степеней "2" 26. Значение (9, 12, 13, 7) подается на второй вход блока умножения по модулю 25, на первый вход которого подается (1, 10, 6, 4). Результат (9, 3, 10, 9) под действием сигнала на управляющий вход демультиплексора 28 подается на второй вход блока вычитания по модулю 30, на первый вход которого подается |X|=(6, 9, 14, 14). Результат Δ_2=(8, 6, 4, 5) подается на блоки умножения на константу 33 и сложения 34, в которых вычисляется значение функции ядра C(Δ_2)=4093, которое поступает на первый вход блока определения знака 35, на второй вход которого поступает значение Δ_2, поскольку число C(Δ_2)<C(K), то Δ_2>0 и 2^6 входит в представление частного Q. На выход блока определения знака 35 подается 0, которая поступает на управляющий вход мультиплексора 29, записывая значение Δ_2 в регистре хранения уменьшаемого 23. Также 0 с выхода блока определения знака 35 подается на инвертированный первый вход элемента И 36, пропуская значение степени "2^6", подаваемой со второго выхода демультиплексора 28, на второй выход блока уточнения аппроксимационного ряда 4.

Аналогично проверяются остальные степени. Наконец, блок отсчета степеней 27 подает на первый выход адрес степени "2^0", представленной в СОК, которая хранится в регистре хранения степеней "2" 26. Значение (1, 1, 1, 1) подается на второй вход блока умножения по модулю 25, на первый вход которого подается (1, 10, 6, 4). Результат (1, 10, 6, 4) под действием сигнала на управляющий вход демультиплексора 28 подается на второй вход блока вычитания по модулю 30, на первый вход которого подается Δ_7=(1, 10, 6, 4) с выхода регистра хранения уменьшаемого. Результат Δ_8=(0, 0, 0, 0) подается на блоки умножения на константу 33 и сложения 34, в которых вычисляется значение функции ядра C(Δ_2)=0, которое поступает на первый вход блока определения знака 35, на второй вход которого поступает значение Δ_8, поскольку число C(Δ_2)<C(K), то Δ_8>0 и 2^0 входит в представление частного Q. На выход блока определения знака 35 подается 0, которая поступает на управляющий вход мультиплексора 29, записывая значение Δ_8 в регистре хранения уменьшаемого 23. Также 0 с выхода блока определения знака 35 подается на инвертированный первый вход элемента И 36, пропуская значение степени "2^0", подаваемой со второго выхода демультиплексора 28, на второй выход блока уточнения аппроксимационного ряда 4. Поскольку отсчет закончен, на третий выход блока отсчета степеней 27 подается сигнал окончания отсчета.

В блоке вывода частного 4 происходит формирование итогового частного. На первый вход блока сложения по модулю 37 последовательно поступают степени "2", входящие в представление частного Q, на второй вход блока сложения по модулю 37 поступает сумма ранее полученных степеней. Так число "2^7" после логического умножения с нулем равно (0, 0, 0, 0), поступая на первый вход, складывается с (0, 0, 0, 0). Далее 2^6=(9, 12, 13, 7) складывается с (0, 0, 0, 0). 2^5=(10, 6, 15, 13) складывается с 2^6=(9, 12, 13, 7), 2^4=(5, 3, 16, 16) складывается с 2^6+2^5=(8, 5, 11, 1), 2^3=(8, 8, 8, 8) складывается с $2^6+2^5+2^4$=(2, 8, 10, 17), 2^2=(4, 4, 4, 4) складывается с $2^6+2^5+2^4+2^3$=(10, 3, 1, 6), 2^1=(2, 2, 2, 2) складывается с $2^6+2^5+2^4+2^3+2^2$=(3, 7, 5, 10), 2^0=(1, 1, 1, 1) складывается с $2^6+2^5+2^4+2^3+2^2+2^1$=(5, 9, 7, 12) и результат (6, 10, 8, 13) под действием сигнала окончания отсчета четвертого входа блока вывода частного 5 на управляющий вход демультиплексора 38 поступает на вход инвертора 39, где находится противоположное значение (5, 3, 9, 6), по-

ступающее на первый вход мультиплексора частного 42, на второй вход которого поступает (6, 10, 8, 13) со второго выхода демультиплексора 38. Поскольку на управляющие входы мультиплексора частного 42 и мультиплексора единицы 43 поступает сигнал, что результат отрицательный, на выход данных мультиплексоров подаются значение (5, 3, 9, 6) с инвертора 39 и (10, 12, 16, 18) с регистра хранения "-1" в СОК. Под действием сигнала "|X|=|Y|" (в данном случае 0) с третьего входа блока вывода частного 5 на управляющий вход мультиплексора выбора частного 44 на выход подается значение (5, 3, 9, 6) с инвертора 39, и поскольку сигнал "|X|<|Y|" (в данном случае 0) с второго входа блока вывода частного 5 инвертируется вторым входом элемента И 45, то на выход частного 6 подается значение (5, 3,9, 6), которое соответствует значению -127.

Реализация всего устройства возможна с использованием программируемых логических интегральных схем (ПЛИС) и может использоваться как отдельное устройство или как сопроцессор для выполнения немодульных операций.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Устройство деления чисел, представленных в системе остаточных классов, содержащее входы делимого и делителя, блок вычисления позиционных характеристик, блок уточнения аппроксимационного ряда, блок вывода частного и выход частного,

при этом вход делимого и вход делителя соединены с первым и вторым входами блока вычисления позиционных характеристик;

первый, второй и третий выходы блока вычисления позиционных характеристик соединены с первым, вторым и третьим входами блока вывода частного;

четвертый и шестой выходы блока вычисления позиционных характеристик соединены с первым и третьим входами блока уточнения аппроксимационного ряда, первый и второй выходы которого соединены с четвертым и пятым входами блока вывода частного, выход которого является выходом частного; и

блок вычисления позиционных характеристик содержит два инвертора, четыре блока умножения на константы, четыре блока сложения, два мультиплексора, элемент XOR и блок сравнения,

при этом значение делимого, представленное в СОК, с первого входа поступает на вход первого блока умножения на константы и на вход первого инвертора, выход которого подключен ко входу второго блока умножения на константы;

выходы первого и второго блоков умножения на константы подключены ко входам первого и второго блоков сложения, выходы которых соединены с первым и третьим входами первого мультиплексора;

значение делителя, представленное в СОК, со второго входа блока вычисления позиционных характеристик поступает на вход третьего блока умножения на константы и на вход второго инвертора, выход которого подключен ко входу четвертого блока умножения на константы;

выходы третьего и четвертого блоков умножения на константы подключены ко входам третьего и четвертого блоков сложения, выходы которых соединены с первым и третьим входами второго мультиплексора;

первые выходы первого и второго мультиплексоров подключены ко второму и третьему входам блока сравнения, первый и второй выходы которого являются вторым и третьим выходами блока вычисления позиционных характеристик;

первый выход первого мультиплексора дополнительно соединен с пятым выходом блока вычисления позиционных характеристик;

выход элемента XOR является первым выходом блока вычисления позиционных характеристик; и

блок уточнения аппроксимационного ряда содержит регистр хранения уменьшаемого, блок вычитания по модулю, мультиплексор, регистр хранения степеней "2", блок отсчета степеней и элемент И,

при этом выход блока вычитания по модулю соединен со вторым входом мультиплексора, выход которого соединен со вторым входом регистра хранения уменьшаемого;

третий выход блока отсчета степеней является первым выходом блока уточнения аппроксимационного ряда;

выход элемента И является вторым выходом блока уточнения аппроксимационного ряда; и

блок вывода частного содержит блок сложения по модулю, демультиплексор, инвертор, регистр хранения "1" в СОК, регистр хранения "-1" в СОК, мультиплексор частного, мультиплексор единицы и мультиплексор выбора частного,

при этом первый вход блока сложения по модулю является пятым входом блока вывода частного;

второй вход блока сложения по модулю подключен к первому выходу демультиплексора, а выход соединен со входом демультиплексора, управляющий вход которого подключен к четвертому входу блока вывода частного, а второй выход - ко второму входу и через инвертор к первому входу мультиплексора частного, выход которого соединен с первым входом мультиплексора выбора частного, второй вход которого соединен с выходом мультиплексора единицы, первый и второй входы которого соединены с регистрами хранения "1" и "-1" в СОК соответственно;

управляющие входы мультиплексора частного и мультиплексора единицы соединены с первым входом блока вывода частного;

управляющий вход мультиплексора выбора частного подключен к третьему входу блока вывода частного,

отличающееся тем, что пятый выход блока вычисления позиционных характеристик соединен со вторым входом блока уточнения аппроксимационного ряда;

в блок вычисления позиционных характеристик введены первый и второй блоки определения знака;

в блоках умножения на константы производится умножение на ортогональные базисы СОК

$$C(B_i) = \frac{B_i \cdot C_P}{P} - \frac{w_i}{p_i},$$

где $B_i = P_i \cdot \left|P_i^{-1}\right|_{p_i}$, $P_i = P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ - мультипликативная инверсия,

$P = \prod_{i=1}^{n} p_i$ - рабочий диапазон СОК с модулями p_1, p_2, ..., p_n;

в блоках суммирования происходит вычисление функции ядра

$$C(X) = \left|\sum_{i=1}^{n} C(B_i) \cdot x_i\right|_{C_P},$$

которая подбирается из условия монотонности и отсутствия критических ядер,

где $C_P=2^N$ - максимальный диапазон функции ядра, а

веса w_i характеризует конкретную функцию ядра,

при этом на выход блоков сложения подаются N младших бит суммы;

выходы первого и третьего блоков сложения дополнительно соединены со вторыми входами первого и второго блоков определения знака, первые входы которых соединены с первым и вторым входами блока вычисления позиционных характеристик, а выходы соединены с управляющими входами первого и второго мультиплексоров соответственно, и с первым и вторым входами элемента XOR;

первый и второй входы блока вычисления позиционных характеристик дополнительно соединены со вторыми входами первого и второго мультиплексора, четвертые входы которых соединены с выходами первого и второго инверторов;

вторые выходы первого и второго мультиплексоров соединены с первым и четвертым входами блока сравнения и четвертым и шестым выходами блока вычисления позиционных характеристик; и

в блок уточнения аппроксимационного ряда введен регистр хранения делителя, блок умножения по модулю, демультиплексор, два блока умножения на константу, два блока сложения и блок определения знака,

при этом блок отсчета степеней во время прямого отсчета вычисляет максимальную степень частного, а во время обратного отсчета последовательно передает адреса степеней "2" в порядке убывания на первый вход регистра хранения степеней "2", выход которого подключен ко второму входу блока умножения по модулю и второму входу демультиплексора, на управляющий вход которого поступает сигнал со второго выхода блока отсчета степеней, а на первый вход - сигнал с выхода блока умножения по модулю, первый вход которого соединен с выходом регистра хранения делителя, вход которого является третьим входом блока уточнения аппроксимационного ряда, первый вход которого подключен к первому входу регистра хранения уменьшаемого, а второй вход подключен к первому входу блока отсчета степеней;

третий выход демультиплексора подключен ко входу первого блока умножения на константы, выход которого подключен ко входу первого блока сложения, выход которого подключен ко второму входу блока отсчета степеней;

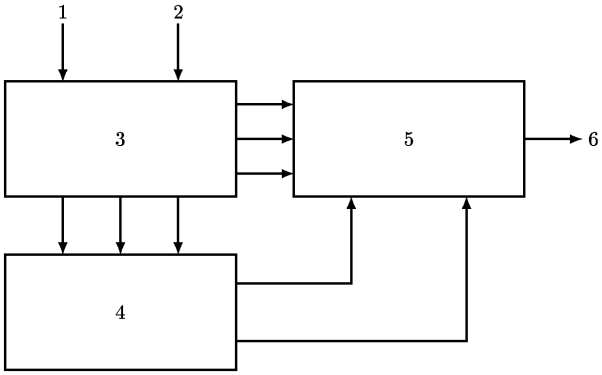
выход регистра хранения уменьшаемого подключен к первому входу мультиплексора и первому входу блока вычитания по модулю, выход которого подключен ко входу второго блока умножения на константы и второму входу блока определения знака;

выход второго блока умножения на константы подключен ко входу второго блока сложения, выход которого подключен к первому входу блока определения знака, выход которого подключен к управляющему входу мультиплексора и через инвертор к первому входу элемента И, второй вход которого соединен со вторым выходом демультиплексора, первый выход которого подключен ко второму входу блока вычитания по модулю;

в блок вывода частного дополнительно введен элемент И, первый вход которого соединен с выходом мультиплексора выбора частного, а второй вход - через инвертор со вторым входом блока вывода частного; и

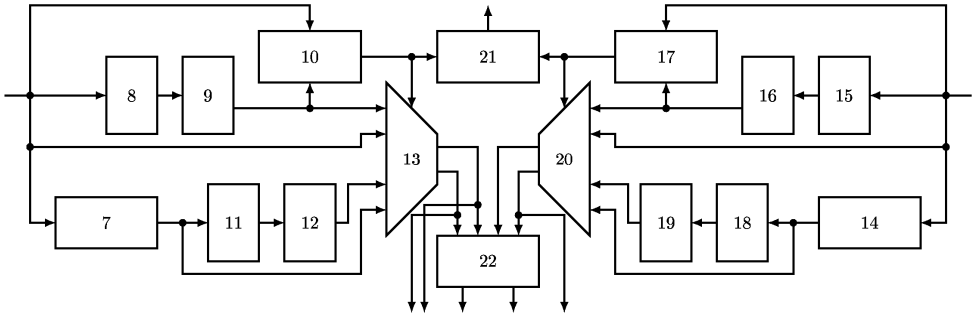
выход элемента И является выходом частного.

Общая структурная схема устройства



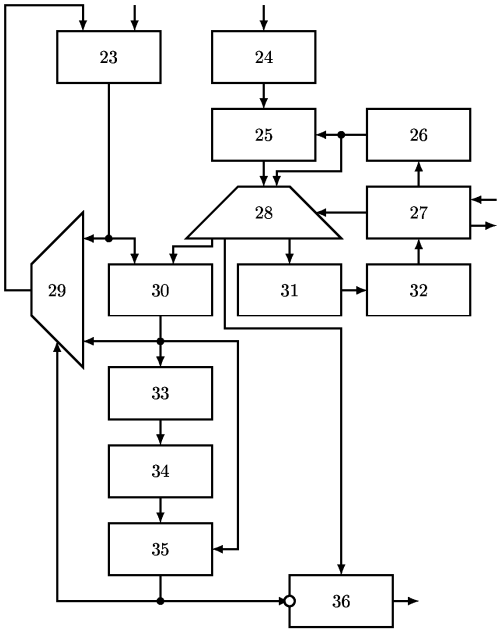
Фиг. 1

Блок вычисления позиционных характеристик



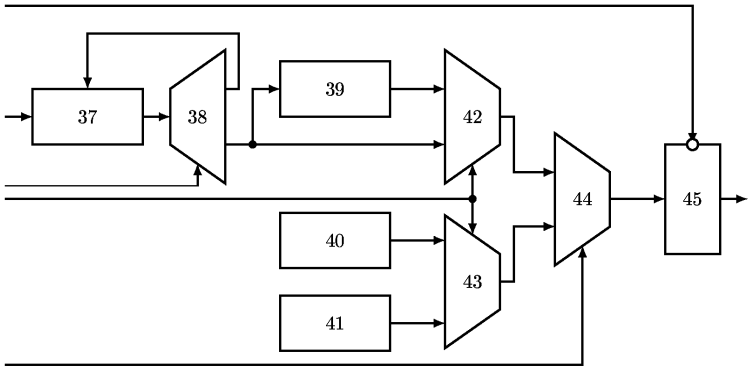
Фиг. 2

Блок уточнения аппроксимационного ряда



Фиг. 3

Блок вывода частного



Фиг. 4

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2