ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

МОДУЛЯРНЫЕ МЕТОДЫ И АЛГОРИТМЫ ДЕЛЕНИЯ НА ОСНОВЕ СПУСКА ФЕРМА И ИТЕРАЦИЙ НЬЮТОНА

Червяков Н.И., Лавриненко И.Н., Лобес М.В.

В статье рассмотрены методы и алгоритмы деления на основе спуска Ферма и итераций Ньютона. Проведена их сравнительная оценка и определены диапазоны эффективного применения.

Введение. Постановка задачи

Главными целями процесса развития вычислительных средств были и остаются повышение их производительности и обеспечение высокой информационной и технической надежности. Как показывают многочисленные исследования, позиционная система свои возможности в этом направлении исчерпала. В связи с этим в последнее время проявляется значительный интерес к непозиционным системам счисления, а именно к системе остаточных классов, обладающей высоким уровнем естественного параллелизма при выполнении арифметических операций, высокой точностью, надежностью, способностью к самокоррекции. Однако широкое применение этой системы связано с трудностями, возникающими при реализации таких операций, как, например, деление. Операция деления в системе остаточных классов (как и в позиционной системе), является наиболее сложной и длинной [1]. Таким образом, для построения машинной арифметики на базе системы остаточных классов очень важным является вопрос разработки эффективного алгоритма для выполнения операции деления.

Модулярный метод и алгоритм деления на основе спуска Ферма

До последнего времени одним из самых эффективных модулярных методов деления считался итерационный метод спуска Ферма [2-3], суть которого заключается в следующем:

1. Делитель b переводится в обобщенную позиционную систему, то есть представляется в виде

$$b = b_{n+1}\prod_{i=1}^{n} p_i + b_n\prod_{i=1}^{n-1} p_i + \ldots + b_3 p_1 p_2 + b_2 p_1 + b_1 a_1,$$

где $p_1, p_2 \ \ldots \ p_n$ – основания системы и определяется наиболее значимая ненулевая цифра b_p этого представления (на основе представления ортогональных базисов в обобщенной позиционной системе [4]).

2. Определяется приблизительный делитель $\bar{b} = Q \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{k-1}$, где k – номер наиболее значимой ненулевой цифры представления делителя в обобщенной позиционной системе, Q определяется из таблицы, хранимой в памяти.

3. Вычисляется начальное приближение частного $q_1 = \left\lfloor a_0 / \bar{b} \right\rfloor$, где a_0 – делимое и значения $a_1 = a_0 - b \cdot q_1$.

4. Цикл из r итераций, в процессе которых вычисляются значения $q_i = \left\lfloor a_{i-1} / \bar{b} \right\rfloor$ и $a_i = a_{i-1} - b \cdot q_i$ при $i = 2;3 \ldots r$. Выполнение итераций продолжается до тех пор не будет выполнено условие $q_i = 0$, либо до $a_i = 0$.

5. Определяется частное от деления $q = q_1 \cdot q_2 \cdot \ldots \cdot q_{r-1} + q'_r$, где

$$q_r = \begin{cases} q_r, если \quad q_r \neq 0 \, и \, a_r = 0 \\ 1, если \quad q_r = 0 \, и \, a_{r-1} \geq b \, для \quad любых \quad \bar{b} \neq 0. \\ 0, во \quad всех \quad остальных \quad случаях \end{cases}$$

Рассмотренный итерационный модулярный метод общего деления на основе метода спуска Ферма является эффективным, простым в реализации. Он может быть легко модифицирован на язык кольцевых операций системы остаточных классов. Представленная в частном ошибка при выполнении итераций уменьшается до нуля. Так, если допустимая ошибка задана не выше 0,1; то достаточно провести всего четыре итерации.

Недостатком метода деления на основе спуска Ферма является то, что в случае если разрядности делимого и делителя отличаются значительно, то для вычисления округленного частного может потребоваться много итераций. В связи с этим возникла необходимость разработки алгоритма деления лишенного подобного недостатка.

Метод и алгоритм целочисленного деления на основе итераций Ньютона

Для реализации итераций Ньютона необходимо использование расширенной системы остаточных классов, которая определяет вычислительный диапазон для промежуточных значений, равный приблизительно квадрату от соответству-

ющего нормального диапазона. Для этого система оснований выбирается специальным образом. Пусть $q_1, q_2, ..., q_{2n}$ – простые числа, для которых выполняется условие

$$1 < q_1 < q_2 < ... < q_{2n-1} < q_{2n}, \quad (1)$$

где $n \in Z, \quad n \geq 1$. Разобьем эти числа на две группы следующим образом:

$$p_1 = q_1, \quad p_2 = q_3, \quad p_3 = q_5 \quad ... \quad p_n = q_{2n-1}; \quad (2)$$

$$p_{n+1} = q_2, \quad p_{n+2} = q_4, \quad p_{n+3} = q_6 \quad ... \quad p_{2n} = q_{2n}. \quad (3)$$

Тогда $p_1, p_2 \cdots p_{2n}$ – основания расширенной системы, а $p_1, p_2 \cdots p_n$ – основания базовой системы; $p_{n+1}, p_{n+2} \cdots p_{2n}$ – основания расширения базовой системы до расширенной;

$$P = \prod_{i=1}^{2n} p_i, \quad M = \prod_{i=1}^{n} p_i, \quad \overline{M} = \prod_{i=n+1}^{2n} p_i \; -$$

соответствующие диапазоны.

Алгоритм деления, основанный на итерациях Ньютона, состоит из двух этапов: вычисление целочисленной обратной величины для делителя b по отношению к нормальному диапазону и нахождение частного [5-6].

Для вычисления обратной величины $\lfloor M/b \rfloor$ используется метод итераций Ньютона. Применяя схему итераций Ньютона

$$z_{i+1} = z_i - f(z_i)/f'(z_i) \quad (4)$$

для $f(z_i) = M/z_i - b$ и $f'(z_i) = -M/z_i^2$, получаем следующую рекурсию $z_{i+1} = z_i + \left(\left(M \cdot z_i - b \cdot z_i^2\right)/M\right) = z_i \cdot (2M - b \cdot z_i)/M$. В системе остаточных классов используется только целочисленное деление, поэтому окончательная версия примет вид:

$$Z_{i+1} = \left\lfloor \frac{Z_i(2M - bZ_i)}{M} \right\rfloor = 2Z_i - \left\lceil \frac{bZ_i^2}{M} \right\rceil. \quad (5)$$

В качестве начального приближения можно выбрать $z_1 = 2$ и продолжать вычисления до тех пор, пока выполняется условие $z_{i+1} \neq z_i$. При $z_{i+1} = z_i$ вычисления прекращаются, и проверяется условие:

$$t = M - b \cdot z_{i+1} - b < 0. \quad (6)$$

Если это условие верное, то обратная величина будет равна $\lfloor M/b \rfloor = z_{i+1}$, иначе $\lfloor M/b \rfloor = z_{i+1} + 1$.

Второй этап деления a на b состоит в нахождении частного из равенства $q = \lfloor (a \cdot z_{i+1})/M \rfloor$. Если $g = r - b > 0$, то $\lfloor a/b \rfloor = q + 1$, иначе $\lfloor a/b \rfloor = q$.

Для того, чтобы обосновать сходимость процесса нахождения обратной величины $\lfloor M/b \rfloor$, нужно сначала доказать вспомогательное неравенство:

$$b/M \cdot (M/b - Z_i)^2 \leq M/b - Z_{i+1} < b/M(M/b - Z_i)^2 + 1. \quad (7)$$

Оно следует из определения оператора $\lceil X \rceil$ (наименьшее целое число превосходящее X, то есть $X \leq \lceil X \rceil < X + 1$):

$$M/b - Z_{i+1} = M/b - 2Z_i + \left\lfloor bZ_i^2 / M \right\rfloor <$$

$$< M/b - 2Z_i + bZ_i^2/M + 1 = b/M(M/b - Z_i)^2 + 1.$$

Аналогично доказывается левая часть выражения (7).

Алгоритм нахождения обратной величины $\lfloor M/b \rfloor$ конечен для любого значения b, удовлетворяющего условию $1 \leq b < M$.

При $Z_1 = 2$ и $b > \lfloor 3M/4 \rfloor$ итерации останавливаются на значениях $Z_2 = Z_3 = 0$.

При условии $\lfloor M/2 \rfloor < b \leq \lfloor 3M/4 \rfloor$ алгоритм останавливается на $Z_2 = Z_3 = 1$.

При условии $1 \leq b \leq \lfloor M/2 \rfloor \leq M/2$ можно показать индукцией по i, что $M/b - Z_i \geq 0$: для $i = 1 \Rightarrow M/b - Z_1 \geq M/M/2 - 2 = 0$; для $i > 1$ с учетом левой части выражения (7) $\Rightarrow M/b - Z_{i+1} \geq b/M(M/b - Z_i)^2 \geq 0$.

Следовательно, выполняются неравенства $bZ_i \leq M$, $\frac{bZ_i}{M} \leq 1$, $\frac{bZ_i}{M} \cdot Z_i \leq Z_i$. Из которых следует справедливость оценки

$$Z_{i+1} = 2Z_i - \left\lceil \frac{2Z_i^2}{M} \right\rceil \geq 2Z_i - Z_i = Z_i. \quad (8)$$

Это означает, что последовательность монотонно возрастает и условие остановки алгоритма $Z_{i+1} = 2Z_i - \left\lceil \frac{bZ_i^2}{M} \right\rceil$ будет в итоге достигнуто.

На обоих этапах разработанного метода и алгоритма деления главной операцией является операция масштабирования числом M, которая может быть выполнена на основе разработанного метода представления ортогональных базисов в обобщенной позиционной системе [4].

На первом этапе алгоритма деления условие остановки алгоритма $z_{i+1} = z_i$. Два целых числа a и b в системе представлении равны тогда и только тогда, когда равны их соответствующие компоненты: $a_i = b_i$. При

реализации в ЭВМ проверка на равенство для каждой компоненты может быть выполнена в двоичном коде с помощью логической операции *AND*.

Кроме того, для выполнения корректирующего шага на обоих этапах разработанного метода деления на базе итераций Ньютона необходима одна операция сравнения. Она может быть выполнена на основе представления в обобщенной позиционной системе [4].

Для того чтобы ускорить процесс нахождения обратной величины M/b нужно в качестве начального приближения вместо значения $Z_1 = 2$ выбрать ближайшую степень двойки. То есть выбрать начальное значение в виде $Z_1 = 2^K$, где K определяется из условия $\lfloor M/2^{K+1} \rfloor < b \le \lfloor M/2^K \rfloor$.

Сравнительная оценка методов деления на основе спуска Ферма и итераций Ньютона

Методы Ферма и Ньютона являются итерационными. Поэтому их сравнение нужно проводить по двум критериям:

- по числу операций, выполняемых за одну итерацию;
- по общему числу выполняемых итераций.

Эти методы имеют различную структуру, и число повторений входящих в них циклов зависит от разных параметров. По этой причине выполнить их точную сравнительную оценку по общему числу операций затруднительно, поэтому она была проведена приближенно. Для этого на рисунках, изображающих схемы алгоритмов Ферма и Ньютона были пронумерованы шаги, которые соответствуют по виду и по числу выполняемых арифметических операций. В результате этой оценки был сделан вывод о том, что алгоритмы Ферма и Ньютона при условии выполнения только одной итерации имеют приблизительно одинаковую вычислительную сложность.

Сравнительная оценка общего количества итераций, выполняемых в алгоритмах Ферма и Ньютона, приведена на рис.1-2.

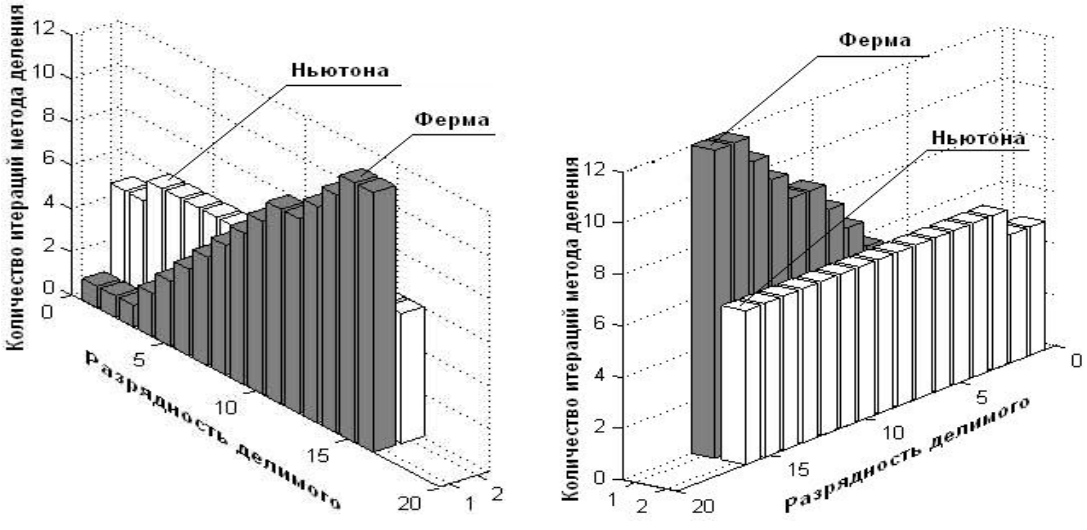

Рис. 1. Оценка числа итераций методов Ферма и Ньютона в зависимости от разрядности делимого

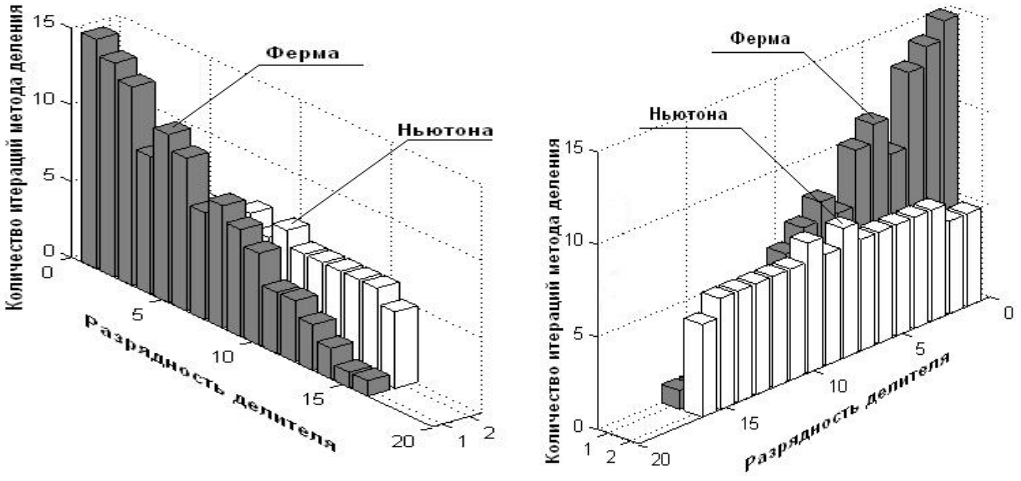

Рис. 2. Оценка числа итераций методов Ферма и Ньютона в зависимости от разрядности делителя

Эта оценка проводилась на основе компьютерного моделирования в системе MATLAB.

В первом случае (см. рис. 1) значение делителя фиксировалось, а значение делимого менялось.

Во втором случае (см. рис. 2), наоборот, неизменным оставалось значение делимого, делитель принимал различные значения.

Проведенная сравнительная оценка показывает, что количество итераций метода Ферма растет вместе с ростом разницы между разрядностями делимого и делителя. Количество итераций метода Ньютона от этого не зависит. Поэтому, если разница между разрядностями делимого и делителя является достаточно большой, то в этом случае отличный результат дает применение метода Ньютона. Однако если разница небольшая, то выгоднее применять для выполнения операции деления метод Ферма.

В таблице 1 приведена оценка числа итераций методов Ферма и Ньютона для случая, когда в качестве делителя выбиралось шестиразрядное число, а разрядность делимого изменялась. Оценка выполнена с помощью программ, разработанных в среде MATLAB, реализующих методы Ферма и Ньютона.

Таблица 1. Оценка числа итераций методов деления Ферма и Ньютона

Разрядность делимого	Число итераций метода		$\approx F/N$
	Ферма (F)	Ньютона(N)	
8	5	6	0,8
16	12	6	2
32	25	6	4,2
64	53	6	8,8
128	105	6	17,5
256	203	6	33,8
512	411	6	68,5
1024	829	6	138,2

Выводы

Проведенная сравнительная оценка показала, что методы деления Ферма и Ньютона при условии выполнения только одной итерации имеют приблизительно одинаковую вычислительную сложность. Если выполняется деление чисел одинаковой разрядности или если их разрядность отличается незначительно, то для достижения лучшего результата выгоднее применение метода Ферма. Если разрядности делимого и делителя отличаются незначительно, огромное преимущество по времени выполнения деления дает применение метода Ньютона.

Литература

1. Галушкин А.И., Червяков Н.И. Нейрокомпьютеры в остаточных классах. М.: Радиотехника, 2003. – 270 с.
2. Червяков Н.И., Лавриненко И.Н., Лавриненко С.В., Мезенцева О.С. Методы и алгоритмы округления, масштабирования и деления чисел в модулярной арифметике // Труды Юбилейной МНТК «50 лет модулярной арифметике» в рамках V МНТК «Электроника и информатика-2005». М.: 2006. – С. 291-310.
3. Лавриненко И.Н. Деление чисел, представленных в системе остаточных классов // ИКТ. Т.3, №3, 2005. – С. 6-9.
4. Червяков Н.И. Методы масштабирования модулярных чисел, используемые при цифровой обработке сигналов // ИКТ. Т.4, №3, 2006. – С. 15-23.
5. Червяков Н.И., Лобес М.В. Целочисленное деление в системе остаточных классов // Материалы III МНТК «Инфокоммуникационные технологии в науке, производстве и образовании». Ч.III. Изд. СевКавГТУ, 2008. – С. 198-204.
6. Червяков Н.И., Лобес М.В. Алгоритм целочисленного деления в системе остаточных классов // ИКТ. Т.5, №4, 2007. – С. 8-13.