УДК 511

С. Л. Амбарян

Алгоритм деления с неограниченной точностью

(Представлено академиком В.С.Закаряном 18/I 2001)

Точность выполнения арифметических операций на вычислительных системах / персональных компьютерах имеет чрезвычайно важное значение. Можно привести множество примеров, когда данная разрядная сетка не обеспечивает требуемую точность решения поставленной задачи. Кроме того, некоторые исследователи науки и техники (теория чисел, криптография, комбинаторика, теория бесконечных рядов, дифференциальные уравнения, интегральное исчисление, атомная физика, разные направления механики, астрономия и др.) в своих исследованиях, требующих высокой точности, просто лишены возможности непосредственно использовать большие преимущества персональных компьютеров из-за ограничений разрядной сетки. Поэтому в связи с широким распространением и усовершенствованием персональных компьютеров разработка эффективных алгоритмов и программно-аппаратных средств реализации арифметики многократной точности (кратко а.м.т.) имеет хорошую перспективу [1-3].

Вопросы арифметики однократной, двойной и многократной точности исследованы многими авторами, проблемы, история и библиография, посвященные им, великолепно изложены в [1]. А. Шенхаге и Ф. Штрассен разработали изящный алгоритм, который умножение (деление) двух n-разрядных чисел выполняет за 0 (n log n log log n) шагов [2].

Представление цифр-чисел в *а.м.т.* можно осуществить по-разному. Нами принят следующий подход.

a. Машинное слово процессора вычислительной системы / персонального компьютера состоит из четного числа двоичных разрядов, равного 2(k + 1) (см. рис.1.), один из которых выделен для знака целого числа с фиксированной точкой (точка фиксирована после младшего разряда).

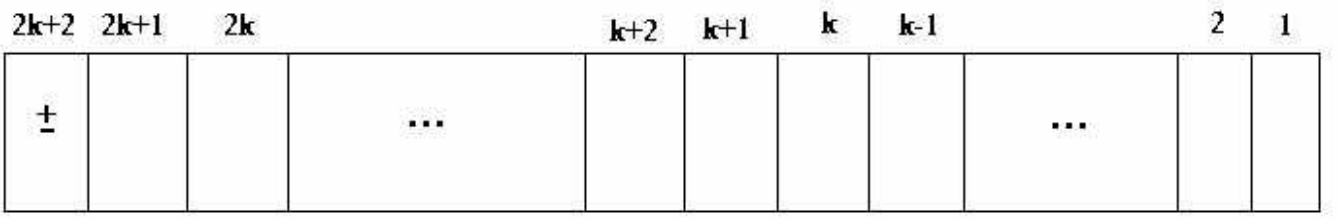

Рис. 1.

b. Основанием системы счисления p выбрано целое число из отрезка $[2, 2^k]$.

c. Каждая цифра *а.м.т.* представлена в одном полуслове как целое положительное число.

d. Числа *а.м.т.* представлены как числа с плавающей точкой. Первое полуслово выделено для знака числа, второе полуслово - для порядка числа и, наконец, начиная с третьего полуслова в последовательных адресах оперативной памяти представлены цифры числа (дробная часть) *а.м.т.* (см. рис. 2.).

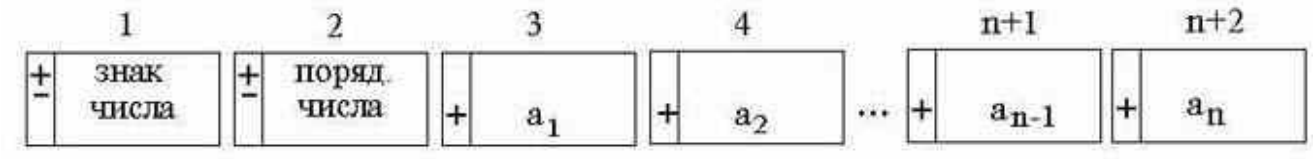

Рис. 2.

Ограничение пункта b равносильно тому, что в одном машинном слове «свободно» помещается двузначное число а. м. т. При соблюдении данного ограничения максимальное число, которое может получиться в результате арифметических операций однократной точности в одном машинном слове, не менее чем $2p^2 - 1$, т.е. $2p^2 - 1 \le \max u \le 2 \cdot 2^{2k} - 1$.

Дадим определение допустимых арифметических операций однократной точности.

Определение. *Арифметическую операцию с однократной точностью будем называть* ***допустимой****, если исходные, промежуточные и окончательные результаты не превышают* $2 \cdot 2^{2k} - 1$.

Пусть даны два n-разрядных положительных целых числа a и b по основанию p.

$$a = a_1 a_2 \dots a_n,\ a_1 \ne 0 \ \text{ и } b = b_1 b_2 \dots b_n,\ b_1 \ne 0;$$
$$A_k = p \cdot A_{k-1} + a_k,\ A_0 = 0 \ \text{ и } B_k = p \cdot B_{k-1} + b_k,\ B_0 = 0;\ k = 1,2, \dots,n. \tag{1}$$

Рассмотрим операцию деления над числами неограниченной (произвольно высокой) точности в *а. м. т.*

Определим число c как

$$c = a / b = = q_0, c_1, c_2 \dots c_n;\ \ q_0 = [a / b] = [A_n / B_n];$$
$$\text{где } 0 \le a_k, b_k, c_k < p;\ \ k = 1,2,\dots,n.$$

При $A_k > B_k$ рассмотрим представление A_k через B_k в форме

$$A_k = q_k \cdot B_k + r_k,\ \ 0 \le r_k < B_k,\ \ 1 \le q_k < p;\ k = 1,2,\dots,n. \tag{2}$$

При $A_k < B_k$ рассмотрим представление A_{k+1} через B_k в форме

$$A_{k+1} = q_k \cdot B_k + r_k,\ \ 0 \le r_k < B_k,\ \ 1 \le q_k < p;\ k \ge 2. \tag{2a}$$

В представлении (2) r_k и r_{k-1} связаны между собой рекуррентным соотношением

$$r_k = pr_{k-1} + a_k - q_k b_k + p(q_{k-1} - q_k)B_{k-1},$$
$$\text{где } q_k \le q_{k-1},\ \ k = 1,2,\dots,n. \tag{3}$$

При $q_k \ne q_{k-1}$ (т.е. $q_{k-1} = q_k + 1$, может быть кроме k = 2) будем иметь

$$r_k = pr_{k-1} + a_k - q_k b_k + pB_{k-1};\ k = 2,3,\dots,n. \tag{3a}$$

При $q_k = q_{k-1} = q$ (см. теорему 4) получим

$$r_k = pr_{k-1} + a_k - qb_k;\ k = 3,4,\ldots,n. \qquad (3b)$$

Требуется при помощи допустимых арифметических операций эффективно (быстро) определить значение q_0.

В этих обозначениях справедлива следующая лемма.

Лемма 1. $q - 1 \le q_0 \le q$.

Доказательство. $c = a / b = a_1a_2,a_3\ldots a_n / b_1b_2,b_3\ldots b_n =$

$$= (A_2 + x) / (B_2 + y) = q + (r + x - qy) / (B_2 + y), \text{ где } q = q_2,\ r = r_2 \text{ и } 0 < x, y < 1.$$

Очевидно, что $|(r + x - qy) / (B_2 + y)| < 1$, действительно, это следует из следующих цепочек неравенств:

$$0 \le r + x - qy \le r + x \le B_2 - 1 + x \le B_2 + y,$$

$$0 \ge r + x - qy \ge - qy \ge -q > - B_2 \ge -B_2 - y.$$

Таким образом,

$$q_0 = \begin{cases} q, & \text{если } r + x - qy \ge 0, \\ q - 1, & \text{если } r + x - qy < 0. \end{cases}$$

Следствие 1. *Если* $q = 0$, *то* $q_0 = 0$;

если $q \le r$, *то* $q_0 = q$.

Согласно следствию, если $r \ge q$, то $q_0 = q$, и поэтому предположим, что $0 \le r < q$. Обозначим через m то минимальное значение k, для которого в (3b) имеет место одно из следующих неравенств:

$$r_m < 0 \ \text{ либо } \ r_m \ge q,$$

тогда справедлива следующая теорема.

Теорема 1(основная теорема). *Если* $r_m < 0$, *то* $q_0 = q - 1$, *или*

если $r_m \ge q$, *то* $q_0 = q$.

Доказательство. Пусть $0 \le r_i < q$, $i = 2,3,\ldots, m - 1$, и для m имеет место условие теоремы, т.е.

$$r_m < 0 \ \text{ либо } \ r_m \ge q.$$

В результате поочередной подстановки значений r_i, $i = 3,4,\ldots,m - 1$, в рекуррентное соотношение (3b) получим

$$0 \le A_{m-2} - q \cdot B_{m-2} + a_{m-1} - qb_{m-1} < q, \ \text{т.е. } 0 \le A_{m-1} - q \cdot B_{m-1} < q.$$

Рассмотрим случай, когда $r_m < 0$; тогда

$$p(A_{m-1} - q \cdot B_{m-1}) + a_m - qb_m < 0,$$

$$A_m - q \cdot B_m \le -1,\ (A_m + 1) / B_m \le q.$$

Из последнего неравенства и леммы 1 следует, что $q_0 = q - 1$.

Пусть теперь $r_m \ge q$, тогда

$$p(A_{m-1} - q \cdot B_{m-1}) + a_m - qb_m \ge q,$$

$$A_m - q(B_m + 1) \ge 0,\ A_m / (B_m + 1) \ge q.$$

из последнего неравенства и леммы 1 следует, что $q_0 = q$. Теорема доказана.

Если не существует такое m, т.е. $0 \le r_i < q$ для всех i = 2,3,…, n, то справедливо следующее следствие.

Следствие 2. $a / b = q + r_n / b,\ 0 \le r_n < q$.

Теперь подробно рассмотрим случай $A_2 < B_2$. Так как имеет место неравенство $p^2 \le A_3 \le p^3 - p - 1$, то необходимо разработать алгоритм, который с помощью допустимых арифметических операций позволяет эффективно определить значения неполного частного $q = q_2$ и остатка $r = r_2$.

Элементарные преобразования приводят к формуле

$$q_2 = q_1 - (q_1 b_2 + r_2 - (pr_1 + a_3)) / B_2,$$
$$q_2 = q_1 -]q_1 b_2 - (pr_1 + a_3)[/B_2, \tag{4}$$

$$\Delta A = q_1 b_2 - (pr_1 + a_3) \text{ через } B_2 \text{ в форме}$$
$$\Delta A = \Delta q + \Delta r / B_2,\ 0 \le \Delta r < B_2,\ -1 \le \Delta q \le p-1. \tag{5}$$

Следует заметить, что $q_1 b_2 \le (2p - 2)(p - 1) < 2p^2 - 1$.

Тогда справедлива следующая теорема.

Теорема 2 (первая теорема о частном и об остатке). *При* $A_2 < B_2$ *значения неполного частного и остатка в (2а) определяются формулами:*

$$q = q_1 - \Delta q \ \textit{и}\ r = 0,\ \textit{при}\ \Delta r = 0;\ \textit{или} \tag{6}$$

$$q = q_1 - (\Delta q + 1) \ \textit{и}\ r = B_2 - \Delta r,\ \textit{при}\ \Delta r \ne 0. \tag{7}$$

Правильность формул (6) и (7) следует из (4) и (5).

Аналог следствия 1 здесь звучит так: если $q_2 = 1$, то $q_0 = 1$ и если $q_2 = p$, то $q_0 = p - 1$.

Доказанная теорема занимает ключевое место при разработке алгоритмов операции деления в *а.м.т.*

В *а.м.т.* в алгоритме операции деления [1] после определения неполного частного q_0 с точностью единицы ($q - 1 \le q_0 \le q$) вычисляется разность

$$a_t = a_\tau - qb,$$

где $a_t(a_\tau)$ - текущее (предыдущее) значение делимого, и при $a_t < 0$ производится компенсирующее сложение в *а.м.т.*

$$a_t = a_\tau + b,\ 0 < a_t < b.$$

Ниже следует лемма, согласно которой компенсирующее сложение в алгоритме операций деления может отсутствовать.

Лемма 2 (о компенсирующем сложении). *Если неполное частное определено с точностью единицы, то* i-*ый разряд частного с выражается формулой:*

$$c_i = q,\ \text{если } a_\tau > 0 \text{ и } a_t \ge 0,$$

$$c_i = q - 1,\ \text{если } a_\tau > 0 \text{ и } a_t < 0,$$

$$c_i = p + q,\ \text{если } a_\tau < 0 \text{ и } a_t \ge 0,$$

$$c_i = p + q - 1,\ \text{если } a_\tau < 0 \text{ и } a_t < 0;\ i = 1, 2, \ldots, n.$$

Доказательство. Первые два случая очевидны, докажем третий случай, откуда следует и четвертый.

Пусть $a_t = a_\tau - qb < 0$, тогда определение следующей цифры частного достигается при помощи представления

$$p\, a_t / b = q + r / b,\ 0 \le r < b,\ -p < q \le -1,$$

так как $p(a_t + b) / b = p + pa_t / b = p + q + r / b$, откуда и следует утверждение леммы.

Замечание. Отметим, что здесь можно обойтись без использования отрицательных неполных частных ($q < 0$ при $a < 0$), положив $a = -a$ после операции $a = a - qb$.

Пусть, например, ω первоначально принимает значение, равное нулю ($\omega = 0$). Далее ω принимает значение, равное единице ($\omega = 1$), если результат операции $a = a - qb$ окажется отрицательным ($a < 0$), то ω сохраняет это значение до тех пор, пока a заново не станет отрицательным, тогда ω принимает значение, равное нулю ($\omega = 0$) и т.д. Тогда

$$c_i = q,\ \text{если } a \ge 0 \text{ и } \omega = 0,$$

$$c_i = q - 1,\ \text{если } a < 0 \text{ и } \omega = 0,$$

$$c_i = p - q - 1,\ \text{если } a \ge 0 \text{ и } \omega = 1,$$

$$c_i = p - q,\ \text{если } a < 0 \text{ и } \omega = 1;\ i = 1, 2, \ldots, n.$$

Согласно основной теореме и первой теореме о неполном частном и об остатке опишем *алгоритм операции деления в а.м.т.*

Описание алгоритма операции деления. Работа алгоритма операции деления начинается с проверки на нуль делимого a ($a_1 = 0$ или $a_1 \ne 0$) и делителя b ($b_1 = 0$ или $b_1 \ne 0$). Первоначально положим показатель результата e(c) = e(a) – e(b). В дальнейшем показатель делителя b e(b) = 0. При $A_2 \ge B_2$ установить показатель делимого e(a) = 0 и уточнить значение e(c) = e(c) + 1, а при $A_2 < B_2$ установить показатель делимого e(a) = 1.

Алгоритм операции деления неотрицательных целых чисел а.м.т. состоит из следующих шагов.

Шаг 1. Пр. «Опр. e(c), e(a) = 0/1, e(b) = 0»;

2. i = 1;

3. $(q,r) = A_{2+e(a)} / B_2$;

4. Если $r \ge q$, то идти к 17;

5. Пр. «Уточнение значения q»;

6. Если $r \geq 0$, то идти к 17;
7. $q = q - 1$;
8. $m = k - (3 + e(a))$;
9. Пр. «$c_i = q$, $c_{i+j} = p - 1$; $j = 1,2,\ldots,m$»;
10. Если $m = 0$, то идти к 15;
11. $q = q + 1$;
12. $a = a - qb$;
13. $e(a) = e(a) + m$;
14. $a = a + b$; идти к 16;
15. $a = a - qb$;
16. $e(a) = e(a) + 1$; идти к 3;
17. $c_i = q$;
18. $a = a - qb$;
19. Пр. «Опр. e(a) и $c_{i+j} = 0$, $j = 1,2,\ldots e(a)$».
20. $i = i + 1$, если $i \leq n$, то идти к 3.
21. End.

Помимо того, что описанный алгоритм исключает компенсирующее сложение (при $a - qb < 0$) [1], он имеет и другие преимущества. Перейдем к строгому изложению некоторых из них.

Теорема 3. *Если для некоторого* $i = 1,2,\ldots,n$ *и некоторого* $k = m + 3 + e(a) \geq 3$ *в (3b) имеет место одно из следующих неравенств:* $r_m < 0$ *либо* $r_m \geq q$, *тогда:*

Случай 1. Если $r_k < 0$, *то* $c_i = q - 1$ *и за этой цифрой следует не менее т цифр* $c_{i+j} = p - 1$; $j = 1,2,\ldots,m$.

Случай 2. Если $r_k \geq q$, *то* $c_i = q$ *и за этой цифрой следует не менее т цифр* $c_{i+j} = 0$; $j = 1,2,\ldots,m$.

Доказательство.

Случай 1. Пусть $r_k < 0$, тогда $0 \leq r_{k-1} < q_{k-1} = q$ и $q_k = q - 1$;

$$c = a / b > A_k / (B_k + 1) = (q_k B_k + r_k) / (B_k + 1) = q_k + (r_k - q_k) / (B_k + 1) =$$

$$= q_k + (pr_{k-1} + a_k - q_k b_k + pB_{k-1} - q_k) / (B_k + 1) \geq$$

$$\geq q_k + (pB_{k-1} - q_k(b_k + 1)) / (B_k + 1) = q_k + 1 - (q_k + 1)(b_k + 1) / (B_k + 1) \geq$$

$$\geq q_k + 1 - (q_k + 1) / (B_{k-1} + 1) = q - q / (B_{k-1} + 1) \geq q - q / (p^{m+1+e(a)} + 1) \geq$$

$$\geq q - q/(p^{m+1} + 1); \quad c > (q - 1) + 1 - q / (p^{m+1}+1),$$

откуда следует утверждение теоремы по первой части.

При $m = 0$ из последнего неравенства следует, что

$$c > (q - 1) + 1 - (p - 1) / (p + 1) = (q - 1) + 2 / (p + 1),$$

т.е. $c_i = q - 1$ и за ним следует цифра $c_{i+1} \geq 1$.

Случай 2. Пусть теперь $r_k \geq 0$, тогда $0 \leq r_{k-1} < q_{k-1} = q$ и $q_k = q$;

$$c = a / b < (A_k + 1) / B_k = (q_k B_k + r_k + 1) / B_k = q_k + (r_k + 1) / B_k =$$

$$= q_k + (pr_{k-1} + a_k - q_k b_k + 1) / B_k \leq q_k + (pr_{k-1} - q_k b_k + 1) / B_k \leq$$

$$\le q_k + (pr_{k-1} + a_k + 1) / B_k \le q_k + pq_{k-1} / B_k \le q_k + q_{k-1} / B_k =$$

$$= q + q / B_k \le q + q / p^{m+1+e(a)} \le q + q / p^{m+1} \le q + (p - 1)/p^{m+1};$$

$$c < q + (p - 1) / p^{m+1};$$

откуда следует утверждение теоремы по второй части.

При $m = 0$ из последнего неравенства следует, что

$$c < q + (p - 1) / p,$$

т.е. $c_i = q$ и за ним следует цифра $c_{i+1} \le p - 2$.

Теорема полностью доказана.

Теорема 4 (вторая теорема о частном и об остатке). *Если для некоторого* $k \ge 3$ *(в (3b)) имеет место неравенство* $0 \le r_k < q_k$, *то* $0 \le r_{k-1} < q_{k-1}$ *и* $q_{k-1} = q_k$.

Доказательство. Прежде всего докажем, что $q_{k-1} = q_k = q$. Если $q_{k-1} \ne q_k$, то из (3a) следует, что

$$a_k = q_k b_k + r_k - p(r_{k-1} + B_{k-1}) \le q_k b_k + q_k - p(r_{k-1} + B_{k-1}) \le$$

$$\le q_k(b_k + 1) - p(r_{k-1} + B_{k-1}) \le p(q_k - r_{k-1} - B_{k-1}) \le 0, \text{ т.е. } a_k < 0,$$

что противоречит определению a_k.

Предположим, что утверждение теоремы неверно и $r_{k-1} < 0$, тогда

$$a_k = q_k b_k + r_k - pr_{k-1}, \text{ так как}$$

$$qb_k + r_k \ge 0, \text{ то } a_k \ge -pr_{k-1} \ge p,$$

что противоречит определению a_k.

Пусть теперь $r_{k-1} \ge q$, тогда

$$a_k = q_k b_k + r_k - pr_{k-1} = -(p(r_{k-1} - q) + (p - b_k)q - r_k), \text{ так как}$$

$$p(r_{k-1} - q) \ge 0 \text{ и } (p - b_k)q - r_k \ge 0, \text{ то } a_k < 0,$$

что противоречит определению a_k. Теорема доказана.

Ереванский научно-исследовательский
институт математических машин

Литература

1. *Кнут Д.* Искусство программирования для ЭВМ. Получисленные алгоритмы. М.: Мир, 1977.
2. *Schonhage A., Strassen V.* Computing, Archiv für elektronisches Rechnen, 7 (1971), Fasc. 3-4.
3. *Амбарян С. Л.* Эффективные алгоритмы выполнения арифметических операций в арифметике с многократной точностью. Пакет программ а.м.т. (ПП-АМТ) в среде Visual C++. Ереванский научно-исследовательский институт математических машин (ЕрНИИММ), Ереван, 1998.

Ս. Լ. Համբարյան

Անսահմանափակ ճշտությամբ բաժանման ալգորիթմ

Թվաբանական գործողությունների կատարումը հաշվողական համակարգերում/ անհատական համակարգիչներում իրականացվում է որոշակի թվով թվանշաններ ունեցող թվերի հետ, որի հետևանքով՝ ընդհանուր դեպքում, բացառվում է տվյալ խնդրի լուծման ճշտության ապահովումը:

Բազմապատիկ ճշտությամբ թվաբանությունում թվի թվանշանների քանակի վրա, գործնականում, սահմանափակում չի դրվում:

Աշխատանքում հետազոտված է բազմապատիկ ճշտությամբ թվաբանությունում բաժանման գործողության կատարման խնդիրը:

Ապացուցված են մի շարք թեորեմներ, որոնք հնարավորություն են տալիս մշակել բավականաչափ արդյունավետ ու պարզ կառուցվածք ունեցող բաժանման գործողության կատարման ալգորիթմ:

Ա. Շենխագենի և Ֆ. Շտրասսենի բաժանման՝ բազմապատկման միջոցով հայտնի ալգորիթմը, ներկա պահին ունի լավագույն գնահատականը. 0 (n log n log log n), սակայն իրականացման համար պահանջվում է ավելի բարդ կառուցվածք: