ЖУРНАЛ
ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОЙ ФИЗИКИ

Том 19 Май 1979 Июнь № 3

НАУЧНЫЕ СООБЩЕНИЯ

УДК 519.6:511

НЕКОТОРЫЕ ОЦЕНКИ, СВЯЗАННЫЕ С АЛГОРИТМОМ ЕВКЛИДА

С. А. АБРАМОВ

(Москва)

Число делений в алгоритме Евклида может быть оценено сверху по количеству цифр в записи меньшего из двух данных чисел в позиционной системе счисления с некоторым основанием q. Исследуется зависимость свойств этих оценок от значения q. Кроме этого исследуется освобождение памяти в процессе применения алгоритма Евклида.

1. Пусть применение алгоритма Евклида к натуральным числам a_0, a_1, $a_0>a_1$, требует m делений, включая последнее деление, дающее нулевой остаток. Получающиеся при этом неполные частные обозначим $q_1, \ldots, q_m$, а ненулевые остатки $a_2, \ldots, a_m$. Положим $a_{m+1}=0$. По известной теореме Ляме [1],

$$a_1 \geqslant u_{m+1}, \tag{1}$$

где u_{m+1} – число Фибоначчи с номером $m+1$. Из неравенства (1) легко выводится

$$m+1<\log_{(1+\sqrt{5})/2}(1+a_1)+\log_{(1+\sqrt{5})/2}\sqrt{5}=\log_{(1+\sqrt{5})/2}(1+a_1)+1.672275... \tag{2}$$

Для практического применения оценки (2) логарифм заменяют количеством цифр натурального числа a_1 в некоторой позиционной системе. Если целое q, большее единицы,– основание системы, то получается

$$m \leqslant ([\log_{(1+\sqrt{5})/2}q]+1)([\log_q a_1]+1)=([\log_{(1+\sqrt{5})/2}q]+1)\,n_q(a_1), \tag{3}$$

где $n_q(a_1)$ – количество цифр a_1 в q-ичной системе.

Для наиболее распространенных систем – двоичной и десятичной – получается следующее:

$$\log_{(1+\sqrt{5})/2}2=1.440..., \qquad m \leqslant 2n_2(a_1),$$

$$\log_{(1+\sqrt{5})/2}10=4.784..., \qquad m \leqslant 5n_{10}(a_1).$$

Для упрощения записи примем обозначение $c_q=[\log_{(1+\sqrt{5})/2}q]+1$. Оценка (3) запишется в виде $m \leqslant c_q n_q(a_1)$.

При любом q оценка (3) является более грубой, чем (2). Выбрав критерий качества оценки, можно рассуждать о том, какая из оценок (3) для двух разных значений q предпочтительнее. То, что, выбрав два значения q, мы можем получить оценки, во многом отличающиеся друг от друга, показывает уже сравнение выписанных оценок для $q=2$ и $q=10$.

Для достаточно больших a_1 десятичная оценка лучше двоичной. Но двоичная оценка допускает локализацию в следующем смысле: для $i=1, 2, \ldots, m-2$ выполнено $a_i \geqslant 2a_{i+2}$ (и даже $a_i>2a_{i+2}$; доказательство: $a_i=q_{i+1}a_{i+1}+a_{i+2} \geqslant a_{i+2}+a_{i+2}>2a_{i+2}$). Утверждение же $a_i \geqslant 10a_{i+5}$, вообще говоря, неверно (пример $a_0=49$, $a_1=30$, $i=1$). Двоичная оценка допускает улучшение: на самом деле выполнено неравенство (это

будет доказано ниже) $m<2n_2(a_1)$; но пример $a_0=13$, $a_1=8$ показывает, что в десятичной оценке нельзя знак $\leqslant$ заменить на $<$.

Нетрудно усмотреть, что для достаточно больших a_1 выполнено $c_q n_q(a_1)<c_p n_p(a_1)$, если $(1-\{\log_{(1+\sqrt{5})/2}q\})/\log_{(1+\sqrt{5})/2}q$ меньше аналогичной величины для p (в этом случае для достаточно больших a_1 будет выполняться неравенство $c_q(\log_q a_1+1)<c_p\log_p a_1$). Пользуясь этим, упорядочим значения $c_2,\ldots,c_{10}$ по мере убывания точности оценки $m\leqslant c_q n_q(a_1)$ для достаточно больших a_1: $c_4=3$, $c_{10}=5$, $c_9=5$, $c_6=4$, $c_8=5$, $c_5=4$, $c_7=5$, $c_3=3$, $c_2=2$.

Ясно, что для любого q найдется Q такое, что для любого натурального $p>Q$ оценка $m\leqslant c_p n_p(a_1)$ для больших a_1 более точна, чем $m\leqslant c_q n_q(a_1)$.

Не так просто в общем случае устанавливается возможность локализации оценки и улучшения. В этом пункте будет показано, что класс оценок вида (3), допускающих локализацию, совпадает с классом оценок этого же вида, допускающих улучшение. Будут сформулированы необходимые и достаточные условия, которым должно подчиняться q для принадлежности соответствующей оценки этому классу.

По индукции с использованием равенства $a_i=q_{i+1}a_{i+1}+a_{i+2}$ для $i=1, 2,\ldots,m$ может быть доказано

$$a_1=Q_{i-1}(q_2,\ldots,q_i)a_i+Q_{i-2}(q_2,\ldots,q_{i-1})a_{i+1}, \tag{4}$$

где $Q_0, Q_1,\ldots$ – многочлены Эйлера:

$$Q_0=1,\qquad Q_1(x_1)=x_1,$$

$$Q_n(x_1,\ldots,x_n)=x_nQ_{n-1}(x_1,\ldots,x_{n-1})+Q_{n-2}(x_1,\ldots,x_{n-2}).$$

Поскольку для любого набора натуральных $q_2,\ldots,q_i$ имеет место $Q_{i-1}(q_2,\ldots,q_i)\geqslant Q_{i-1}(1,\ldots,1)=u_i$, как следствие получаем, что для $i=1, 2,\ldots,m$ верно неравенство $a_1\geqslant u_ia_i+u_{i-1}a_{i+1}$ и тем более

$$a_1\geqslant u_ia_i. \tag{5}$$

Замечание. Если $a_0=u_{m+2}$, $a_1=u_{m+1}$, то (4) превращается в известное тождество для чисел Фибоначчи:

$$u_{m+1}=u_iu_{m-i+2}+u_{i-1}u_{m-i+1}.$$

Соотношения (4), (5) позволяют описать все q, для которых оценка (3) допускает локализацию.

Теорема 1. *Пусть $i\geqslant 2$. Для каждого действительного $\varepsilon>0$ можно подобрать такие натуральные a_0 и a_1, что алгоритм Евклида в применении к ним потребует не менее $i-1$ делений и при этом будет выполнено $a_1/a_i<u_i+\varepsilon$.*

Доказательство. Выберем N настолько большим, чтобы выполнялось $u_{i-1}/N<\varepsilon$, и рассмотрим последовательность чисел, заданную рекуррентно:

$$v_1=1,\qquad v_2=N,\qquad v_n=v_{n-1}+v_{n-2}.$$

Положим теперь $a_0=v_{i+2}$, $a_1=v_{i+1}$. Имеем $q_1=\ldots=q_{i-1}=1$ и, в силу (4),

$$a_i=u_ia_i+u_{i-1}\quad\text{и}\quad \frac{a_1}{a_i}=u_i+\frac{u_{i-1}}{N}<u_i+\varepsilon.$$

Сопоставление утверждения теоремы 1 с неравенством (5) позволяет получить два следствия.

Следствие 1. Для $i\geqslant 2$ и для любых a_0, a_1 таких, что алгоритм Евклида не заканчивается после $i-1$ делений, имеет место неравенство $a_1/a_i\geqslant u_i$. В то же время можно подобрать такие a_0 и a_1, что алгоритм Евклида не заканчивается после $i-1$ делений и $a_1/a_i<u_i+1$.

Следствие 2. Оценка для числа делений $m\leqslant c_q n_q(a_1)$ допускает локализацию, т. е. $a_1/a_{c_q+1}\geqslant q$ тогда и только тогда, когда

$$u_{c_q+1}\geqslant q. \tag{6}$$

Возвращаясь к оценке $m \leqslant 5n_{10}(q_1)$, видим, что она не допускает локализации: $u_6=8<10$. Оценка $m \leqslant 2n_2(a_1)$ допускает локализацию, так как $u_3=2$. Приведем список всех значений q, не превосходящих 10, для которых оценка (3) допускает локализацию: 2, 3, 5, 7, 8.

Теорема 2. *Оценка $m \leqslant c_q n_q$ допускает локализацию тогда и только тогда, когда для некоторого натурального t выполнено*

$$\left(\frac{1+\sqrt{5}}{2}\right)^{t-1} < q \leqslant u_{t+1}.$$

В этом случае $c_q=t-1$, т. е. $m \leqslant (t-1)n_q(a_1)$.

Доказательство выводится из следствия 2 и из неравенства

$$\left(\frac{1+\sqrt{5}}{2}\right)^{t-1} < u_{t+1} < \left(\frac{1+\sqrt{5}}{2}\right)^{t},$$

справедливого для всех натуральных t.

Теорема 3. *Пусть оценка $m \leqslant c_q n_q(a_1)$ не допускает локализации. Тогда она неулучшаема в следующем смысле: можно подобрать такие a_0, a_1, что применение к ним алгоритма Евклида потребует точно $c_q n_q(a_1)$ делений.*

Доказательство. По теореме 2 найдется натуральное t такое, что

$$u_t < q < \left(\frac{1+\sqrt{5}}{2}\right)^{t-1}.$$

Берем $a_0=u_{t+1}$, $a_1=u_t$. Тогда $n_q(a_1)=1$, $c_q=[\log_{(1+\sqrt{5})/2} q]+1=t-1$; число делений равно $t-1$.

Теорема 4. *Пусть оценка $m \leqslant c_q n_q(a_1)$ допускает локализацию. Тогда она улучшаема: справедливо неравенство $m < c_q n_q(a_1)$.*

Доказательство. Пусть $q^{s-1} \leqslant a_1 < q^s$ для некоторого натурального s. Проведем индукцию по s:

1) $s=1$; используя (6) и (1), получаем

$$u_{c_q+1} \geqslant q > a_1 \geqslant u_{m+1},$$

откуда $c_q > m$, что и требуется;

2) $s>1$; если $c_q > m$, то доказывать нечего; иначе, в силу того что оценка допускает локализацию, имеем $a_{c_q+1} < q^{s-1}$.

По предположению индукции,

$$m - c_q < c_q n_q(a_{c_q+1}),$$

отсюда получаем

$$m < c_q(n_q(a_{c_q+1})+1) \leqslant c_q n_q(a_1).$$

Доказательство завершено.

2. Из неравенства $a_i > 2a_{i+2}$ следует, что переход от пары чисел a_i, a_{i+1} к паре a_{i+1}, a_{i+2} понижает суммарное количество цифр в двоичной записи чисел по крайней мере на 1, т. е. с каждым шагом алгоритма Евклида заведомо освобождается 1 бит памяти выполняющего этот алгоритм. Освобождающаяся память может быть занята под другие вычисления. Известно несколько алгоритмов, которые выполняются шаг за шагом параллельно с алгоритмом Евклида, например построение для двух целых чисел a_0 и a_1 таких целых чисел s и t, что $a_0 s + a_1 t = \text{НОД}(a_0, a_1)$. Для получения s и t последовательно строятся s_0, t_0; s_1, t_1; ... такие, что $a_0 s_i + a_1 t_i = a_i$. Ясно, что $s_0=t_1=1$, $s_1=t_0=0$ и для $i=2, 3, \ldots, m$ выполнено

$$s_i = (-1)^i Q_{i-2}(q_2, \ldots, q_{i-1}), \qquad t_i = (-1)^{i+1} Q_{i-1}(q_1, \ldots, q_{i-1}).$$

Частный случай этого алгоритма – алгоритм обращения натурального a в поле вычетов по простому модулю p при $a<p$: $ps+at=1$,– влечет $at\equiv 1 \pmod p$, значение s здесь интереса не представляет.

Выведем оценку объема памяти, необходимого для применения последнего алгоритма. Пусть для записи чисел выбрана двоичная система. Будет показано, что $2n_2(p)+4$ разрядов достаточно для решения задачи. Сохраняя введенную в начале статьи систему обозначений, считаем, что $a_0=p$, $a_1=a$. При выводе оценки основную роль будет играть

Теорема 5. *Для* $i=0, 1, \ldots, m$ *имеют место неравенства* $n_2(|t_i|)+n_2(a_i)\leqslant n_2(a_0)+1$, $n_2(|t_i|)+n_2(q_i)+n_2(a_{i+1})\leqslant n_2(a_0)+2$.

Доказательство. Используя тот факт, что $a_0=Q_m(q_1, \ldots, q_m)$, $|t_i|=Q_{i-1}(q_1, \ldots, q_{i-1})$, $a_{i+1}=Q_{m-i-1}(q_{i+2}, \ldots, q_m)$, имеем

$$n_2(|t_i|)+n_2(a_i)=([\log_2 |t_i|]+1)+([\log_2 a_i]+1)\leqslant$$

$$\leqslant \log_2 |t_i| a_i+2=\log_2 Q_{i-1}(q_1, \ldots, q_{i-1}) Q_{m-i}(q_{i+1}, \ldots, q_m)+2<\log_2 a_0+2.$$

Поскольку $n_2(|t_i|)+n_2(a_i)$ – целое число, то выполнено $n_2(|t_i|)+n_2(a_i)\leqslant[\log_2 a_0]+2=n_2(a_0)+1$. Далее

$$n_2(|t_i|)+n_2(q_i)+n_2(a_{i+1})\leqslant \log_2 |t_i| q_i a_{i+1}+3=$$

$$=\log_2 Q_{i-1}(q_1, \ldots, q_{i-1}) q_i Q_{m-i-1}(q_{i+2}, \ldots, q_m)\leqslant \log_2 a_0+3,$$

и, аналогично предыдущему, получаем, что

$$n_2(|t_i|)+n_2(q_i)+n_2(a_{i+1})\leqslant[\log_2 a_0]+3=n_2(a_0)+2.$$

Теорема доказана.

Деля «уголком» a_i на a_{i+1}, можно неполное частное q_{i+1} и остаток a_{i+2} получать на том месте, где располагалось a_i: разрядов, занятых a_i, заведомо хватит на это. Для вычисления $|t_{i+2}|=q_{i+1}|t_{i+1}|+|t_i|$ используем место, занятое под $|t_i|$ и q_{i+1}: цифры числа q_{i+1} начиная с младшей при вычислении произведения «столбиком» становятся одна за другой ненужными. Если память выполняющего алгоритм – это упорядоченная последовательность двоичных разрядов, то желательно, чтобы каждое из рассматриваемых чисел занимало несколько последовательных разрядов. Можно при четном i рассматриваемые числа расположить так:

(7)
$$\underbrace{|\overleftarrow{t_i}|\alpha\overrightarrow{a_i}}_{n_2(a_0)+2\text{ разрядов}}\quad\underbrace{\overleftarrow{a_{i+1}}\alpha|\overrightarrow{t_{i+1}}|}_{n_2(a_0)+2\text{ разрядов}}$$

Надписанная стрелка $\rightarrow$ означает, что цифры числа идут подряд (слева направо) начиная со старшей цифры, стрелка $\leftarrow$ означает обратный порядок; буквой α всюду обозначены группы не представляющих интереса цифр. При нечетном i величины с индексами i и $i+1$ меняются местами.

Преобразование содержимого первых $n_2(a_0)+2$ двоичных разрядов в (7) для перехода от величин с индексом i к величинам с индексом $i+2$ происходит так:

$$|\overleftarrow{t_i}|\alpha\overrightarrow{q_{i+1}}\alpha\overrightarrow{a_{i+2}}$$

$$|\overleftarrow{t_i}|\alpha\overleftarrow{q_{i+1}}\overrightarrow{a_{i+2}}$$

$$|\overleftarrow{t_{i+2}}|\alpha\overrightarrow{a_{i+2}}$$

Теорема 5 гарантирует, что места для этого преобразования хватит.

Если самое последнее значение $|t_m|$ окажется справа (т. е. m нечетно), то t_m — отрицательное число и для нахождения обратного элемента к a надо еще вычесть $|t_m|$ из p. Это обстоятельство, однако, вовсе не вынуждает помнить значение p до конца вычислений: легко усматривается, что $p=t_{m+1}$.

Автор благодарит В. Д. Поддерюгина за ряд советов.

Поступила в редакцию 3.05.1978

Цитированная литература

1. *Д. Кнут.* Искусство программирования для ЭВМ. Т. 2. М., «Мир», 1977.

УДК 517.988.8

О ПРОЕКЦИОННО-ИТЕРАТИВНЫХ МЕТОДАХ РЕШЕНИЯ ОПЕРАТОРНЫХ УРАВНЕНИЙ

ФАМ КИ АНЬ

(Воронеж)

Методом неподвижных точек квазинерастягивающих операторов доказывается ряд усиленных теорем о сходимости проекционно-итеративных методов (п.и.м.)

1. Рассмотрим операторное уравнение вида

$$x=T(x, x), \tag{1}$$

где нелинейное отображение T действует из $E\times E$ в E, а (E, d) — некоторое метрическое пространство с метрикой d.

Для решения уравнения (1) применяется п.и.м. (см. [1, 2]), суть которого заключается в отыскании последовательностей $\{u_n\}$, $\{v_n\}$, удовлетворяющих условию

$$u_n=T(u_n, v_n), \qquad v_n=T_k(u_n, v_{n-1}), \tag{2}$$

где $T_1(x, y)=T(x, y)$, $T_i(x, y)=T(x, T_{i-1}(x, y))$, $i=2, 3, \ldots, k$.

Для дальнейшего нам необходимо

Определение 1. Непрерывное отображение $T : D\times D\to D$, где D — замкнутое множество метрического пространства (E, d), называется отображением типа (α, β, g), если выполнены следующие условия.

Условие А. Уравнение (1) разрешимо, т. е. множество $F=\{x\in D : T(x, x)=x\}$ не пусто.

Условие Б. Существуют непрерывная функция $g : D\times F\to[0, \infty)$ и положительные константы α, β: $\alpha+\beta\leqslant 1$ такие, что:

а) $g(x, p)=0$, $x\in D$, $p\in F$, тогда и только тогда, когда $x=p\in F$;

б) для всех x, $y\in D$ и для всякого $p\in F$ имеем $g(T(x, y), p)\leqslant\alpha g(x, p)+\beta g(y, p)$;

в) если $F=\{p\}$ (т. е. F состоит только из одного элемента), то из условия $g(x, p)\to 0$ следует $d(x, p)\to 0$.

Условие В. Для всякого $y\notin F$ и для всех $x\in D$ существуют $q=q(x, y)\in F$ такие, что

$$g(T(x, y), q)<\alpha g(x, q)+\beta g(y, q).$$

Условие Г. Существует $p\in F$ такое, что из условия $d(x, p)\to\infty$ следует $g(x, p)\to\infty$.

Теорема 1. *Пусть T — отображение типа (α, β, g), при этом если $\alpha+\beta=1$, то отображение T предполагается компактным; выполнены условия* В *и* Г.