О среднем числе шагов в алгоритме Евклида

А. В. Устинов*

УДК 511.17+519.681

1 Обозначения

1. Запись $[x_0; x_1, \ldots, x_s]$ означает цепную дробь

$$x_0 + \cfrac{1}{x_1 + \ddots + \cfrac{1}{x_s}}$$

длины s с формальными переменными x_0, x_1, …, x_s.

2. Для рационального r обычно (если не сделано дополнительных оговорок) будет использоваться каноническое разложение в цепную дробь $r = [t_0; t_1, \ldots, t_s]$ длины $s = s(r)$, где $t_0 = [r]$ (целая часть r), t_1, …, t_s — неполные частные (натуральные числа) и $t_s \geqslant 2$ при $s \geqslant 1$.

3. Если A — некоторое утверждение, то $[A]$ означает 1, если A истинно, и 0 в противном случае.

4. Для натурального q через $\delta_q(a)$ будем обозначать характеристическую функцию делимости на q:

$$\delta_q(a) = [a \equiv 0 \pmod p] = \begin{cases} 1, & \text{если } a \equiv 0 \pmod q, \\ 0, & \text{если } a \not\equiv 0 \pmod q. \end{cases}$$

2 Введение

Детальный анализ алгоритма Евклида приводит к различным задачам о статистических свойствах конечных цепных дробей (см. [2, разд. 4.5.3]). Если на вход алгоритма подается пара натуральных чисел c и d ($c < d$), то основной интерес представляет число выполняемых делений, которое совпадает с $s(c/d)$ — количеством неполных частных в цепной дроби

$$c/d = [0; t_1, \ldots, t_s].$$

Впервые вопрос о поведении величины $s(c/d)$ в среднем был исследован Хейльбронном. В 1968 г. он (см. [6]) доказал асимптотическую формулу

$$\frac{1}{\varphi(d)} \sum_{\substack{1 \leqslant c \leqslant d \\ (c,d)=1}} s(c/d) = \frac{2 \log 2}{\zeta(2)} \log d + O(\log^4 \log d).$$

*Работа выполнена при поддержке фонда INTAS, грант № 03-51-5070 и проекта ДВО РАН 06-III-A-01-017

Позднее Портер (см. [9]) для того же среднего получил асимптотическую формулу с двумя значащими членами

$$\frac{1}{\varphi(d)} \sum_{\substack{1\leqslant c\leqslant d\\(c,d)=1}} s(c/d) = \frac{2\log 2}{\zeta(2)} \log d + C_P - 1 + O(d^{-1/6+\varepsilon}),$$

где

$$C_P = \frac{\log 2}{\zeta(2)} \left(3\log 2 + 4\gamma - 4\frac{\zeta'(2)}{\zeta(2)} - 2 \right) - \frac{1}{2}$$

— константа, получившая название константы Портера (её окончательный вид был найден Ренчем, см. [8]).

При усреднении по обоим параметрам c и d вероятностными и эргодическими методами получены следующие результаты. Диксон [5] показал, что для любого положительного ε найдётся такая константа $c_0 > 0$, что

$$\left| s(c/d) - \frac{12\log 2}{\pi^2} \log d \right| < (\log d)^{1/2+\varepsilon}$$

для всех пар чисел (c, d) лежащих в области $1 \leqslant c \leqslant d \leqslant R$, за исключением, быть может, $R^2 \exp(-c_0(\log R)^{\varepsilon/2})$ пар. Хенсли [7] уточнил результат Диксона и доказал, что разность между величиной $s(a/b)$ и ее средним значением асимптотически имеет нормальное распределение, параметры которого можно указать явно. В частности, Хенсли доказал асимптотическую формулу для второго момента величины $s(c/d)$. Позднее Валле [10] были доказаны асимптотические формулы для математического ожидания, дисперсии и моментов более высокого порядка со степенными понижениями в остаточных членах (см. [4]).

При фиксированном значении d, для дисперсии величины $s(c/d)$ известна лишь правильная с точностью до константы оценка, принадлежащая Быковскому [1]:

$$\frac{1}{d} \sum_{c=1}^{d} \left(s\left(\frac{c}{d}\right) - \frac{2\log 2}{\zeta(2)} \log d \right)^2 \ll \log d.$$

Она получена методами аналитической теории чисел, опирающимися на оценки сумм Клостермана.

Развивая подход, предложенный в [1], в настоящей работе для среднего значения

$$E(R) = \frac{2}{[R]([R]+1)} \sum_{d\leqslant R} \sum_{c\leqslant d} s(c/d) \tag{1}$$

при $R \geqslant 2$ доказывается асимптотическая формула с лучшим понижением в остаточном члене, чем в результате Портера, а именно:

$$E(R) = \frac{2\log 2}{\zeta(2)} \log d + B + O(R^{-1/2} \log^{1/2} R), \tag{2}$$

где

$$B = C_P - 1 + \frac{\log 2}{\zeta(2)} \left(2\frac{\zeta'(2)}{\zeta(2)} - 1 \right).$$

3 О цепных дробях

Следуя работе [1], обозначим через $\mathcal{M}$ множество всех целочисленных матриц

$$S = \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix} = \begin{pmatrix} P(S) & P'(S) \\ Q(S) & Q'(S) \end{pmatrix}$$

с определителем $\det S = \pm 1$, у которых

$$1 \leqslant Q \leqslant Q', \quad 0 \leqslant P \leqslant Q, \quad 1 \leqslant P' \leqslant Q'.$$

Для вещественного $R > 0$ через $\mathcal{M}(R)$ будем обозначать конечное подмножество в $\mathcal{M}$, состоящее из всех матриц S с дополнительным условием $Q' \leqslant R$.

Отметим два свойства множества $\mathcal{M}$ (см. [1]).

1°. Каждому конечному (непустому) набору натуральных чисел $(q_1, \ldots, q_s)$ можно поставить в соответствие матрицу $S \in \mathcal{M}$ по правилу

$$S = S(q_1, \ldots, q_s) = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_s \end{pmatrix}.$$

При этом

$$S = \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix},$$

где

$$\frac{P}{Q} = [0; q_1, \ldots, q_{s-1}] \quad \text{и} \quad \frac{P'}{Q'} = [0; q_1, \ldots, q_s]$$

(здесь последние неполные частные могут быть и единицами).

Отображение

$$(q_1, \ldots, q_s) \to S(q_1, \ldots, q_s)$$

является биекцией между множеством всех конечных наборов натуральных чисел и множеством $\mathcal{M}$.

2°. Если $Q < Q'$ и $(Q, Q') = 1$, то имеются ровно две пары

$$(P, P') \quad \text{и} \quad (Q - P, Q' - P'),$$

дополняющие в качестве первой строки вторую (Q, Q') до матрицы из $\mathcal{M}$. Кроме того, если

$$\frac{Q}{Q'} = [0; q_s, \ldots, q_1] = [0; q_s, \ldots, q_1 - 1, 1] \qquad (q_1 \geqslant 2),$$

то соответствующие матрицы имеют вид

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_s \end{pmatrix} = \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_1 - 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_s \end{pmatrix} = \begin{pmatrix} Q - P & Q' - P' \\ Q & Q' \end{pmatrix}.$$

При $Q = Q'$ существует только одна матрица $S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ из $\mathcal{M}$.

В следующей лемме для рациональных чисел $r \in (0, 1]$ будет использоваться (единственное) разложение в цепную дробь с единицей на конце:

$$r = [0; t_1, \ldots, t_s, 1] \qquad (s \geqslant 0).$$

Оно удобнее канонического разложения тем, что единообразно описывает все такие числа, включая $r = 1$.

Лемма 1. *Пусть c и d — натуральные числа, $1 \leqslant c \leqslant d$ и*

$$\frac{c}{d} = [0; t_1, \ldots, t_{s-1}, t_s, 1] \qquad (s \geqslant 0). \tag{3}$$

Тогда уравнение

$$S \cdot \begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}, \tag{4}$$

в котором неизвестными являются числа k, $l \in \mathbb{N}$ $(k \leqslant l)$ и матрица $S \in \mathcal{M}$, имеет s решений.

Доказательство. Если $k/l = [0; q_1, \dots, q_m, 1]$ $(m \geqslant 0)$,

$$S = \begin{pmatrix} 0 & 1 \\ 1 & z_1 \end{pmatrix} \dots \begin{pmatrix} 0 & 1 \\ 1 & z_n \end{pmatrix}$$

и числа c, d определены равенством (4), то

$$\frac{c}{d} = [0; z_1, \dots, z_n, q_1, \dots, q_m, 1].$$

Поэтому из условий (3), (4) и свойства 1° множества $\mathcal{M}$ вытекает, что для некоторого j $(1 \leqslant j \leqslant s)$

$$S = \begin{pmatrix} 0 & 1 \\ 1 & t_1 \end{pmatrix} \dots \begin{pmatrix} 0 & 1 \\ 1 & t_j \end{pmatrix}, \qquad \frac{k}{l} = [0; t_{j+1}, \dots, t_s, 1].$$

Значит, количество решений уравнения (4) совпадает с числом способов, которыми можно выбрать j в пределах от 1 до s и равно s. □

4 О математическом ожидании

Для действительного $R \geqslant 1$ положим

$$\sigma(R) = \sum_{d \leqslant R} \sum_{c \leqslant d} s(c/d).$$

Тогда, в соответствии с (1),

$$E(R) = \frac{2}{[R]([R]+1)} \cdot \sigma(R). \tag{5}$$

Поэтому, чтобы доказать основные результат (2) , для суммы $\sigma(R)$ нужно будет получить асимптотическую формулу с 2 значащими членами.

Через $\lambda(d)$ обозначим число решений уравнения

$$kQ + lQ' = d$$

относительно неизвестных k, l, Q и Q' таких, что

$$1 \leqslant k \leqslant l, \quad 1 \leqslant Q \leqslant Q', \quad (Q, Q') = 1. \tag{6}$$

Через $N^*(R)$ обозначим число решений неравенства

$$kQ + lQ' \leqslant R$$

относительно неизвестных k, l, Q, Q', связанных условиями (6); другими словами

$$N^*(R) = \sum_{d \leqslant R} \lambda(d).$$

Лемма 2. *Пусть* $R \geqslant 1$. *Тогда*

$$\sigma(R) = 2N^*(R) - \left[\frac{R}{2}\right] \cdot \left[\frac{R+1}{2}\right].$$

Доказательство. Из первого утверждения леммы 1 вытекает, что сумма

$$\sum_{c\leqslant d} s(c/d)$$

равна числу решений уравнения

$$\begin{pmatrix} * & * \\ Q & Q' \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} * \\ d \end{pmatrix}, \tag{7}$$

где

$$\begin{pmatrix} * & * \\ Q & Q' \end{pmatrix} \in \mathcal{M}, \quad 1 \leqslant k \leqslant l.$$

Если $Q' \geqslant 2$, то по свойству 2° множества $\mathcal{M}$ для пары (Q, Q') существует ровно две пары чисел (P, P'), которые дополняют строку (Q, Q') до матрицы из $\mathcal{M}$. Значит, в этом случае число решений уравнения (7) равно $2\lambda(d)$. Если же $Q' = 1$, то $Q = 1$, и число решений уравнения (7) совпадает с числом решений уравнения $k + l = d$, где $1 \leqslant k \leqslant l$, равным $[d/2]$.

Таким образом,

$$\sum_{d\leqslant R}\sum_{c\leqslant d} s(c/d) = \sum_{d\leqslant R}\left(2\lambda(d) - \left[\frac{d}{2}\right]\right) =$$
$$= 2\sum_{d\leqslant R}\lambda(d) - \left[\frac{R}{2}\right]\cdot\left[\frac{R+1}{2}\right] = 2N^*(R) - \left[\frac{R}{2}\right]\cdot\left[\frac{R+1}{2}\right].$$

□

5 Вспомогательные утверждения

Лемма 3. *При $R \geqslant 1$ для суммы*

$$\Phi(R) = \sum_{Q'\leqslant R}\sum_{Q\leqslant Q'} \frac{1}{Q'(Q+Q')} \tag{8}$$

справедлива асимптотическая формула

$$\Phi(R) = \log 2\,(\log R + \log 2 + \gamma) - \frac{\zeta(2)}{2} + O\left(\frac{1}{R}\right).$$

Доказательство. Заметим, что

$$\Phi(R) = \log 2 \sum_{Q'\leqslant R}\frac{1}{Q'} + \sigma_0 + O\left(\frac{1}{R}\right), \tag{9}$$

где

$$\sigma_0 = \sum_{Q'=1}^{\infty}\frac{1}{Q'}\left(\sum_{Q=1}^{Q'}\frac{1}{Q+Q'} - \log 2\right). \tag{10}$$

Для суммы σ_0 известно точное значение (см. [8]):

$$\sigma_0 = \log^2 2 - \frac{\zeta(2)}{2}. \tag{11}$$

Подставляя его в формулу (9), приходим к утверждению леммы. □

Лемма 4. *При $\xi \geqslant 2$ для суммы*

$$F(\xi) = \sum_{n<\xi} \sum_{m\leqslant n} \frac{1}{m}\left(\frac{1}{n} - \frac{1}{m+n}\right) - \sum_{n<\xi} \sum_{\substack{m\leqslant n \\ m+n>\xi}} \frac{1}{m}\left(\frac{1}{\xi} - \frac{1}{m+n}\right) \tag{12}$$

справедлива асимптотическая формула

$$F(\xi) = \log 2(\log \xi + H) + O\left(\frac{\log \xi}{\xi}\right), \tag{13}$$

где

$$H = \frac{\log 2}{2} + \gamma - 1.$$

Доказательство. Подстановка $x = 1$ в лемму 10 из работы [3] приводит к равенству (13) с константой

$$H = \gamma - \frac{\zeta'(2)}{\zeta(2)} - \frac{\log 2}{2} - 1 + \frac{1}{\log 2}\left(\sigma_0 + \frac{\zeta(2)}{2}\right),$$

где σ_0 задается рядом (10). Подставляя в последнюю формулу значение σ_0 из (11), приходим к утверждению леммы. □

Пусть $\rho(x) = 1/2 - \{x\}$ и

$$h(x) = \sum_{n=1}^{\infty} \frac{\rho(nx)}{n^2}.$$

6 Асимптотическая формула для математического ожидания

Обозначим через $N(R)$ число решений неравенства

$$kQ + lQ' \leqslant R \tag{14}$$

относительно неизвестных

$$1 \leqslant k \leqslant l, \quad 1 \leqslant Q \leqslant Q'. \tag{15}$$

Теорема . *Пусть $R \geqslant 2$. Тогда*

$$N(R) = \frac{\log 2}{2} R^2 \log R + \frac{R^2}{4}\left(\log 2(3\log 2 + 4\gamma - 3) - \zeta(2)\right) + O(R^{3/2}\log^{1/2} R).$$

Доказательство. Введем параметр U, лежащий в пределах $1 \leqslant U \leqslant R$. Через $N_1(R,U)$ обозначим число решений неравенства (14) с ограничениями (15), удовлетворяющих дополнительному условию $Q' \leqslant U$. Число решений, для которых $Q' > U$ обозначим через $N_2(R,U)$. Таким образом,

$$N(R) = N_1(R,U) + N_2(R,U). \tag{16}$$

Для нахождения $N_1(R,U)$ заметим, что при фиксированных Q и Q' число решений неравенства (14) относительно переменных k и l равно числу целых точек на плоскости Okl, лежащих в области

$$0 < k \leqslant l, \quad kQ + lQ' \leqslant R.$$

Значит,

$$N_1(R,U) = \sum_{Q'\leqslant U} \sum_{Q\leqslant Q'} \left(\int_0^R dl \int_0^l dk[kQ + lQ' \leqslant R] + O\left(\frac{R}{Q'}\right)\right) =$$

$$= \frac{R^2}{2} \sum_{Q'\leqslant U} \sum_{Q\leqslant Q'} \frac{1}{Q'(Q+Q')} + O(RU) = \frac{R^2}{2}\Phi(U) + O(RU),$$

где $\Phi(R)$ задается равенством (8). По лемме 3

$$N_1(R,U)=\frac{\log 2}{2}R^2\log U+\frac{R^2}{2}\left(\log 2(\log 2+\gamma)-\frac{\zeta(2)}{2}\right)+O(RU)+O(R^2U^{-1}). \qquad (17)$$

Пусть $R_1=RU^{-1}$. Для величины $N_2(R,U)$ аналогично находим

$$N_2(R,U)=\sum_{l\leqslant R_1}\sum_{k\leqslant l}\left(\int_U^R dQ'\int_0^{Q'}dQ[kQ+lQ'\leqslant R]+O\left(\frac{R}{l}\right)\right)=$$
$$=\sum_{l\leqslant R_1}\sum_{k\leqslant l}\int_U^R dQ'\int_0^{Q'}dQ\,[kQ+lQ'\leqslant R]+O(R^2U^{-1}).$$

Для подсчета двойного интеграла сделаем последовательно замены переменных $w=kQ+lQ'$, $\xi=wU^{-1}$, $y=Q'U^{-1}$. Тогда получим

$$\int_U^R dQ'\int_0^{Q'}dQ\,[kQ+lQ'\leqslant R]=\frac{1}{k}\int_U^R dQ'\int_0^R dw\,\left[\frac{w}{k+l}\leqslant Q'\leqslant\frac{w}{l}\right]=$$
$$=\frac{U^2}{k}\int_1^{R_1}dy\int_0^{R_1}d\xi\left[\frac{\xi}{k+l}\leqslant y\leqslant\frac{\xi}{l}\right]=\frac{U^2}{k}\int_0^{R_1}\xi\left(\frac{1}{l}-\max\left\{\frac{1}{k+l},1\right\}\right)[\xi\geqslant l]d\xi=$$
$$=\frac{U^2}{k}\int_0^{R_1}\xi\left(\frac{1}{l}-\frac{1}{k+l}\right)[\xi\geqslant k+l]d\xi+\frac{U^2}{k}\int_0^{R_1}\xi\left(\frac{1}{l}-\frac{1}{\xi}\right)[l\leqslant\xi<k+l]d\xi.$$

Отсюда

$$N_2(R,U)=U^2\int_0^{R_1}\xi F(\xi)d\xi+O(R^2U^{-1}),$$

где функция $F(\xi)$ определена равенством (12). По лемме 4

$$N_2(R,U)=\frac{\log 2}{2}R^2\left(\log\frac{R}{U}+\frac{\log 2}{2}+\gamma-\frac{3}{2}\right)+O(R^2U^{-1})+O(RU\log R). \qquad (18)$$

Подставляя формулы (17), (18) в равенство (16) и выбирая $U=R^{1/2}\log^{-1/2}R$, приходим к утверждению теоремы. □

Следствие . *Пусть $R\geqslant 2$. Тогда*

$$E(R)=\frac{2\log 2}{\zeta(2)}\log R+\frac{\log 2}{\zeta(2)}\left(3\log 2+4\gamma-2\frac{\zeta'(2)}{\zeta(2)}-3\right)-\frac{3}{2}+O(R^{-1/2}\log^{1/2}R).$$

Доказательство. Подставляя результат теоремы в формулу обращения

$$N^*(R)=\sum_{d\leqslant R}\mu(d)N\left(\frac{R}{d}\right),$$

находим

$$N^*(R)=\frac{\log 2}{2\zeta(2)}R^2\log R+\frac{R^2}{4\zeta(2)}\left(\log 2\left(3\log 2+4\gamma-2\frac{\zeta'(2)}{\zeta(2)}-3\right)-\zeta(2)\right)+O(R^{3/2}\log^{1/2}R).$$

Подстановка этого результата в лемму 2 приводит к равенству

$$\sigma(R)=\frac{\log 2}{\zeta(2)}R^2\log R+\frac{R^2}{2\zeta(2)}\left(\log 2\left(3\log 2+4\gamma-2\frac{\zeta'(2)}{\zeta(2)}-3\right)-\frac{3}{2}\zeta(2)\right)+O(R^{3/2}\log^{1/2}R).$$

Подставляя его в (5), получаем утверждение следствия. □

Замечание. Более сложными методами, основанными на оценках сумм Клостермана, может быть исследована дисперсия

$$D(R) = \frac{2}{[R]([R]+1)} \sum_{d \leqslant R} \sum_{c \leqslant d} \left(s(c/d) - E(R)\right)^2 .$$

Для нее может быть доказана формула

$$\delta_1 \cdot \log R + \delta_0 + O(R^{-1/6} \log^3 R)$$

с абсолютными константами $\delta_1 > 0$ и δ_0. Отметим, что в соответствующем результате работы [4] утверждается лишь существование некоторой константы $\gamma > 0$ вместо $1/6$ в показателе остаточного члена.

Список литературы

[1] Быковский В. А. *Оценка дисперсии длин конечных непрерывных дробей.* — ФПМ, т. 11, вып. 6, 2005, 15–26.

[2] Кнут Д. Э. *Искусство программирования. Т. 2. Получисленные алгоритмы.* — М., Санкт-Петербург, Киев: Вильямс, 2000.

[3] Устинов А. В. *О статистических свойствах конечных цепных дробей.* — Записки научн. семин. ПОМИ, т. 322, СПб., 2005, 186–211.

[4] Baladi V., Vallée B. *Euclidean algorithms are Gaussian.* — J. Number Theory, v. 110, 2005, 331-386.

[5] Dixon J. D. *The Number of Steps in the Euclidean Algorithm.* — J. of Number Theory, v. 2, 1970, 414–422.

[6] Heilbronn H. *On the average length of a class of finite continued fractions.* — in Abhandlungen aus Zahlentheorie und Analysis, Berlin, VEB, 1968, 89–96.

[7] Hensley D. *The Number of Steps in the Euclidean Algorithm.* — J. of Number Theory, v. 49, 1994, 142–182.

[8] Knuth D. E. *Evaluation of Porter's Constant.* — Comp. and Maths. with Appls., v. 2, 1976, 137–139.

[9] Porter J. W. *On a theorem of Heilbronn.* — Mathematika, 1975, v. 22, № 1, 20–28.

[10] Vallée B. *A Unifying Framework for the Analysis of a Class of Euclidean Algorithms.* — Proceedings of LATIN'2000, Lecture Notes in Computer Science 1776, Springer, 343–354.

Хабаровское отделение Института прикладной математики
Дальневосточного отделения Российской академии наук
ustinov@iam.khv.ru