О среднем числе шагов в алгоритме Евклида с нечетными неполными частными

А. В. Устинов*

1 Три быстрых варианта алгоритма Евклида и статистики Гаусса — Кузьмина

Среди различных модификаций алгоритма Евклида обычно выделяют три «быстрых» варианта (см. [13]), основанных на различных способах деления с остатком: классический алгоритм Евклида

$$a = bq + r, \quad q = \lfloor a/b \rfloor, \quad 0 \leqslant r < b;$$

алгоритм с выбором минимального по модулю остатка

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = \left\lceil \frac{a}{b} - \frac{1}{2} \right\rceil, \quad -\frac{b}{2} < r \leqslant \frac{b}{2};$$

алгоритм с нечетными неполными частными

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = 2\left\lceil \frac{a}{2b} \right\rceil - 1, \quad -b < r \leqslant b.$$

Число шагов в быстрых вариантах в наихудшем случае и в среднем есть $O(\log N)$ (при a, $b \ll N$).

К «медленным» относят: алгоритм вычитанием, алгоритм с делением «по избытку» и алгоритм с четными неполными частными. Для них число шагов в среднем имеет порядок $\log^2 N$, а в наихудших случаях может быть порядка N (более подробная информация и библиография могут быть найдены в [13]).

Каждый из трех быстрых алгоритмов приводит к разложению чисел в соответствующие цепные дроби. Классический алгоритм:

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{}{\ddots + \cfrac{1}{a_s}}} = [a_0; a_1, \ldots, a_s] \tag{1}$$

где a_0 — целое, a_1, …, a_s — натуральные и $a_s \geqslant 2$ при $s \geqslant 1$. (Другой вариант обеспечить однозначность разложения — это требовать, чтобы последнее неполное частное было равно единице.) Алгоритм с выбором минимального по модулю остатка:

$$\frac{a}{b} = a_0 + \cfrac{\varepsilon_1}{a_1 + \cfrac{\varepsilon_2}{a_2 + \cfrac{}{\ddots + \cfrac{\varepsilon_l}{a_l}}}}, \tag{2}$$

*Работа выполнена при поддержке гранта Президента РФ № МД-2339.2010.1, фонда «Династия», фонда РФФИ, гранты № 09-01-12129 офи-м, 10-01-98001-р-сибирь-а, 09-01-00371-а, проекта ДВО № 09-I-П4-03

где a_0 — целое, $a_1, \ldots, a_l$ — натуральные, $\varepsilon_k = \pm 1$, $a_k \geqslant 2$ $(1 \leqslant k \leqslant l)$, $a_k + \varepsilon_{k+1} \geqslant 2$ $(1 \leqslant k < l)$, и $\varepsilon_l = -1$ при $l \geqslant 1$ и $a_l = 2$. Алгоритм с нечетными неполными частными:

$$\frac{a}{b} = a_0 + \cfrac{\varepsilon_1}{a_1 + \cfrac{\varepsilon_2}{a_2 + \ddots + \cfrac{\varepsilon_h}{a_h}}} = \left\langle a_0; \frac{\varepsilon_1}{a_1}, \frac{\varepsilon_2}{a_2} \ldots, \frac{\varepsilon_h}{a_h} \right\rangle, \tag{3}$$

где a_0 — нечетное целое, $a_1, \ldots, a_h$ — нечетные натуральные, $\varepsilon_k = \pm 1$, $a_k + \varepsilon_{k+1} \geqslant 1$ $(1 \leqslant k < h)$, и $\varepsilon_h = 1$ при $h \geqslant 1$ и $a_h = 1$. Длины разложений рационального числа a/b в дроби вида (1)–(3) будем соответственно обозначать $s(a/b)$, $l(a/b)$ и $h(a/b)$.

С вычислительной точки зрения естественно возникает задача об исследовании средних значений функций $s(a/b)$, $l(a/b)$ и $h(a/b)$. Вопрос о средней длине классических цепных дробей впервые был исследован Хейльбронном. В 1968 г. элементарными методами он доказал асимптотическую формулу (см. [8])

$$\frac{1}{\varphi(b)} \sideset{}{^*}\sum_{a=1}^{b} s(a/b) = \frac{2\log 2}{\zeta(2)} \cdot \log b + O(\log^4 \log b)$$

(здесь и далее знак звездочки суммах означает, что переменная суммирования пробегает приведенную систему вычетов). В 1975 г. Портер, используя оценки сумм Клостермана, для того же среднего получил асимптотическую формулу с двумя значащими членами (см. [10])

$$\frac{1}{\varphi(b)} \sideset{}{^*}\sum_{a=1}^{b} s(a/b) = \frac{2\log 2}{\zeta(2)} \cdot \log b + C_P - 1 + O_\varepsilon(b^{-1/6+\varepsilon}), \tag{4}$$

где ε — любое положительное и

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

— константа, получившая название константы Портера (её окончательный вид был найден Ренчем, см. [9]). При усреднении по обоим параметрам можно доказать более точную формулу (см. [4])

$$\frac{2}{R(R+1)} \sum_{b \leqslant R} \sideset{}{^*}\sum_{a=1}^{b} s(a/b) = \frac{2\log 2}{\zeta(2)} \cdot \log R + \widetilde{C}_P - 1 + O(R^{-1} \log R^4), \tag{5}$$

где

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

Для цепных дробей вида (2) и (3) аналоги результата Хейльбронна были доказаны Ригером (см. [11, 12]). В работе [7] Балади и Валле эргодическими методами доказали двучленные асимптотические формулы

$$\frac{2}{R(R+1)} \sum_{b \leqslant R} \sideset{}{^*}\sum_{a=1}^{b} l(a/b) = \frac{2\log \varphi}{\zeta(2)} \cdot \log R + \widetilde{C}_l + O(R^{-\gamma}),$$

$$\frac{2}{R(R+1)} \sum_{b \leqslant R} \sideset{}{^*}\sum_{a=1}^{b} h(a/b) = \frac{3\log \varphi}{\zeta(2)} \cdot \log R + \widetilde{C}_h + O(R^{-\gamma}),$$

где $\varphi = (1+\sqrt{5})/2$ — «золотое сечение» и $\gamma > 0$. В той же работе был поставлен вопрос о нахождении констант $\widetilde{C}_l$ и $\widetilde{C}_h$.

Оказывается, что вопрос о поведении в среднем функций $l(a/b)$ и $h(a/b)$ можно свести к анализу классического алгоритма Евклида, если воспользоваться статистиками Гаусса — Кузьмина. Это позволяет для средних значений $l(a/b)$ и $h(a/b)$ доказать формулы, аналогичные (4) и (5), а для констант $\widetilde{C}_l$ и $\widetilde{C}_h$ получить представления через сингулярные ряды.

Для рационального $a/b = [0; a_1, \ldots, a_s, 1] \in [0,1]$ и действительных $x \in [0,1]$ статистиками Гаусса — Кузьмина называются числа (см. [1])

$$s_x(a/b) = \#\{j : 0 \leqslant j \leqslant s, [0; a_{j+1}, \ldots, a_s, 1] \leqslant x\}. \tag{6}$$

В частности, $s_1(a/b) = s+1$ — длина работы классического алгоритма Евклида, примененного к паре чисел (a,b) (при этом подразумевается, что на первом шаге переменные переставляются, а на следующих шагах уже происходят деления с остатком, см. [3]).

Для дальнейших рассуждений оказывается удобным распространить определение статистик Гаусса — Кузьмина на произвольные $x > 0$:

$$s_x(a/b) = \#\{(j,t) : 0 \leqslant j \leqslant s, 0 \leqslant t < a_j, [t; a_{j+1}, \ldots, a_s, 1] \leqslant x\} \tag{7}$$

(здесь считаем, что $a_0 = +\infty$). Для конечных цепных дробей выбрана запись с единицей на конце, чтобы новое определение (7) совпадало со старым (6) не только при $x \in [0,1)$, но и при $x = 1$.

Для средних значений статистик Гаусса — Кузьмина выполняются равенства (доказательства из работ [4, 5] остаются справедливыми при произвольном положительном x)

$$\frac{1}{\varphi(b)} \sideset{}{^*}\sum_{a=1}^{b} s_x(a/b) = \frac{2\log(1+x)}{\zeta(2)} \log b + C_P(x) + O(b^{-1/6} \log^{7/6+\varepsilon} b), \tag{8}$$

$$\frac{2}{R(R+1)} \sum_{b \leqslant R} \sum_{a=1}^{b} s_x(a/b) = \frac{2\log(1+x)}{\zeta(2)} \log R + \widetilde{C}_P(x) + O(R^{-1} \log^4 R), \tag{9}$$

где

$$C_P(x) = \frac{2\log(1+x)}{\zeta(2)} \left(2\gamma - 2\frac{\zeta'(2)}{\zeta(2)} - \frac{\log(1+x)}{2} + \log x - 1\right) + \tag{10}$$
$$+ \frac{2}{\zeta(2)}(h_1(x) + h_2(x)) + \frac{x^2}{x+1},$$
$$\widetilde{C}_P(x) = C_P(x) + \frac{2\log(1+x)}{\zeta(2)} \left(\frac{\zeta'(2)}{\zeta(2)} - \frac{1}{2}\right),$$

а функции $h_1(x)$ и $h_2(x)$ задаются абсолютно сходящимися сингулярными рядами

$$h_1(x) = \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{m=1}^{n} \frac{x}{n+mx} - \log(1+x)\right), \quad h_2(x) = \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{\frac{n}{x} \leqslant m < \frac{n}{x}+n} \frac{1}{m} - \log(1+x)\right).$$

В статье [6] доказано, что $l(a/b) = s_{\varphi-1}(a/b)$. Поэтому результаты о средних значениях $l(a/b)$ (и формулы для вторых констант в асимптотических формулах) получаются подстановкой $x = \varphi - 1$ в формулы (8) и (9).

В настоящей статье доказывается, что при $b \geqslant 1$, $b/2 \leqslant a < b$, $(a,b) = 1$, $aa^\star \equiv 1 \pmod b$, $1 \leqslant a^\star < b$ выполняется тождество

$$h\left(\frac{a^\star}{b}\right) + h\left(\frac{b-a^\star}{b}\right) = s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right).$$

Поэтому равенства (8) и (9) приводят к следующему результату.

Теорема . *Справедливы асимптотические формулы*

$$\frac{1}{\varphi(b)}\sideset{}{^*}\sum_{a=1}^{b} h(a/b) = \frac{3\log\varphi}{\zeta(2)}\log b + C_h + O(b^{-1/6}\log^{7/6+\varepsilon} b),$$

$$\frac{2}{R(R+1)}\sum_{b\leqslant R}\sum_{a=1}^{b} h(a/b) = \frac{3\log\varphi}{\zeta(2)}\log R + \widetilde{C}_h + O(R^{-1}\log^4 R),$$

где

$$C_h = \frac{1}{2}(C_P(\varphi) + C_P(\varphi-1)),$$

$$\widetilde{C}_h = \frac{1}{2}(\widetilde{C}_P(\varphi) + \widetilde{C}_P(\varphi-1)) = C_h + \frac{3\log\varphi}{\zeta(2)}\left(\frac{\zeta'(2)}{\zeta(2)} - \frac{1}{2}\right),$$

и функция $C_P(x)$ определена равенством (10).

2 Разложения в дуальные дроби

Наряду с разложениями вида (3) будем рассматривать дуальные (перевернутые) дроби

$$\left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_2}{a_1}\right\rangle^\star = \cfrac{\varepsilon_{h+1}}{a_h + \ddots + \cfrac{\varepsilon_2}{a_1}}$$

с теми же ограничениями на параметры: a_j — нечетные натуральные числа $(1 \leqslant j \leqslant h)$, $\varepsilon_j = \pm 1$ $(2 \leqslant j \leqslant h+1)$, $\varepsilon_{j+1} + a_j > 0$ $(1 \leqslant j < h)$.

Лемма 1. *Рациональное число p/q представимо дуальной дробью тогда и только тогда, когда $p/q \in (\varphi-2, \varphi)$; представление дуальной дробью единственно.*

Доказательство. Необходимость условия $p/q \in (\varphi-2,\varphi)$ следует из неравенств

$$\varphi - 2 = \left\langle 0; \frac{-1}{3}, \frac{-1}{3}, \dots\right\rangle^\star < \left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_2}{a_1}\right\rangle^\star < \left\langle 0; \frac{1}{1}, \frac{-1}{3}, \frac{-1}{3}, \dots\right\rangle^\star = \varphi.$$

Для доказательства его достаточности опишем алгоритм разложения. При $\varepsilon_{h+1} = -1$

$$-\frac{1}{\varphi^2} = \varphi - 2 < \frac{p}{q} < 0, \quad -\frac{q}{p} > \varphi^2,$$

и для некоторого нечетного $a_h > \varphi^2 - \varphi = 1$, определяемого однозначно, число $-a_h - q/p$ будет лежать в интервале $(\varphi-2,\varphi)$. Если же $\varepsilon_{h+1} = 1$, то $q/p > 1/\varphi$ и для некоторого нечетного $a_h \geqslant \frac{1}{\varphi} + \frac{1}{\varphi^2} = 1$, также определяемого однозначно, число $q/p - a_h$ также попадет в интервал $(\varphi-2,\varphi)$. Таким образом в каждом из случаев однозначно находится пара (ε_{h+1}, a_h), для которой $\varepsilon_{h+1} + a_h > 0$ и осуществляется переход к дроби $\frac{r}{p} = \pm\frac{q}{p} - a_h \in (\varphi-2,\varphi)$.

Разложение будет конечным, поскольку на каждом шаге уменьшается высота раскладываемого числа ($|r| + |p| < |p| + q$). Единственность представления дуальной дробью следует из однозначности описанного алгоритма. □

Длину разложения рационального числа a/b в дуальную дробь будем далее обозначать через $h^\star(a/b)$.

3 Цепные дроби и матрицы

При изучении статистических свойств конечных цепных дробей ключевую роль (см., например, [4], [5]) играет биекция, которая каждому непустому набору натуральных чисел $(a_1, \dots, a_n)$ (составленному из неполных частных рационального числа) ставит в соответствие матрицу

$$\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \dots \begin{pmatrix} 0 & 1 \\ 1 & a_s \end{pmatrix} \in \mathcal{M},$$

где

$$\mathcal{M} = \left\{ \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix} \in GL_2(\mathbb{Z}) : P \geqslant 0, 1 \leqslant P' \leqslant Q', 1 \leqslant Q \leqslant Q' \right\}. \qquad (11)$$

Для изучения цепных дробей с нечетными неполными частными и дуальных к ним дробей введем отображение Φ, которое будет ставить в соответствие рациональному числу

$$\frac{a}{b} = \left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_2}{a_1} \right\rangle^{\star} \in (\varphi - 2, \varphi)$$

матрицу

$$\Phi(a/b) = \begin{pmatrix} 0 & \varepsilon_{h+1} \\ 1 & a_h \end{pmatrix} \dots \begin{pmatrix} 0 & \varepsilon_2 \\ 1 & a_1 \end{pmatrix}.$$

Отметим основные свойства отображения Φ.

1°. Если $\Phi(a/b) = \left(\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right)$, то

$$\begin{aligned} \frac{P}{Q} &= \left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_3}{a_2} \right\rangle^{\star}, & \frac{P}{P'} &= \left\langle 0; \frac{1}{a_1}, \frac{\varepsilon_2}{a_2} \dots, \frac{\varepsilon_{h-1}}{a_{h-1}} \right\rangle, \\ \frac{P'}{Q'} &= \left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_2}{a_1} \right\rangle^{\star} = \frac{a}{b}, & \frac{Q}{Q'} &= \left\langle 0; \frac{1}{a_1}, \frac{\varepsilon_2}{a_2} \dots, \frac{\varepsilon_h}{a_h} \right\rangle. \end{aligned} \qquad (12)$$

2°. Всякая матрица $S = \left(\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right)$, лежащая в образе отображения Φ однозначно восстанавливается как по строке $(Q\,Q')$ так и по столбцу $\left(\begin{smallmatrix} P' \\ Q' \end{smallmatrix}\right)$. В частности, определитель матрицы S есть функция от отношения P'/Q', которую в дальнейшем будем обозначать через $\Delta(P'/Q')$.

3°. Отображение Φ является биекцией между $\mathbb{Q} \cap (\varphi - 2, \varphi)$ и множеством матриц

$$\mathcal{N} = \left\{ \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix} \in GL_2(\mathbb{Z}) : 1 \leqslant Q \leqslant Q', PQ' - P'Q = \Delta\left(\frac{P'}{Q'}\right), \frac{P'}{Q'} \in (\varphi - 2, \varphi) \right\}.$$

4°. Если $\left(\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right) \in \mathcal{N}$, то $h^{\star}(P'/Q') = h(Q/Q')$.

5°. Если $Q' \geqslant 2$ и

$$\Phi\left(\frac{a}{b}\right) = \begin{pmatrix} * & P' \\ Q & Q' \end{pmatrix} \in \mathcal{M} \cap \mathcal{N},$$

то $\Delta((Q' - P')/Q') = \Delta(P'/Q')$ и

$$\Phi\left(\frac{b-a}{b}\right) = \begin{pmatrix} * & Q' - P' \\ Q' - Q & Q' \end{pmatrix} \in \mathcal{M} \cap \mathcal{N}.$$

6°. При $Q' \geqslant 2$ строка $(Q\,Q')$ и столбец $\left(\begin{smallmatrix} P' \\ Q' \end{smallmatrix}\right)$ могут быть двумя способами дополнены до матрицы из $\mathcal{M}$. При этом в каждой из двух пар полученных

матриц $\left(\left(\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right), \left(\begin{smallmatrix} P'-P & P' \\ Q'-Q & Q' \end{smallmatrix}\right)\right)$ и $\left(\left(\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right), \left(\begin{smallmatrix} Q-P & Q'-P' \\ Q & Q' \end{smallmatrix}\right)\right)$ ровно одна матрица лежит в множестве $\mathcal{N}$.

Свойство 1° проверяется по индукции.

Свойство 2° непосредственно следует из свойства 1°.

В свойстве 3° инъективность отображения Φ следует из леммы 1 и равенства $P'/Q' = a/b$. Для доказательства сюръективности рассмотрим произвольную матрицу $S = \left(\begin{smallmatrix} P & P' \\ Q & Q' \end{smallmatrix}\right) \in \mathcal{N}$ и положим $\widetilde{S} = \Phi(P'/Q') = \left(\begin{smallmatrix} \widetilde{P} & P' \\ \widetilde{Q} & Q' \end{smallmatrix}\right) \in \mathcal{N}$. Тогда $\det S = \det \widetilde{S} = \Delta(P'/Q')$, и для некоторого целого t выполняются равенства $\widetilde{P} = P + tP'$, $\widetilde{Q} = Q + tQ'$. Но $1 \leqslant Q, \widetilde{Q} \leqslant Q'$, следовательно, $t = 0$ и $S = \widetilde{S}$.

Свойство 4° вытекает из свойства 3° и равенств (12).

Для доказательства свойства 5° сначала заметим, что при $Q' = 2$ есть ровно одна матрица $S = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$, лежащая в $\mathcal{M} \cap \mathcal{N}$. Для нее утверждение леммы очевидно, поэтому можно считать, что $Q' \geqslant 3$. Согласно свойству 2°, столбец $\left(\begin{smallmatrix} Q'-P' \\ Q' \end{smallmatrix}\right)$ можно дополнить до некоторой матрицы $\widetilde{S} = \left(\begin{smallmatrix} * & Q'-P' \\ \widetilde{Q} & Q' \end{smallmatrix}\right) \in \mathcal{N}$. По определению (11) эта матрица лежит в множестве $\mathcal{M}$ и $1 \leqslant \widetilde{Q} < Q'$. При этом $\widetilde{Q} \neq Q$, так как $Q' - P' \neq P'$. Поскольку $\det S = \pm \det \widetilde{S}$, то $QP' \equiv \pm \widetilde{Q} P' \pmod{Q'}$, и $\widetilde{Q} = Q' - Q$. Значит $\det S \equiv P'Q \equiv \det \widetilde{S} \pmod{Q'}$ и $\Delta((Q'-P')/Q') = \Delta(P'/Q')$.

Свойство 6° следует из свойства 2°.

4 Сведение к статистикам Гаусса — Кузьмина

Лемма 2. *Пусть $b \geqslant 2$, $b/2 \leqslant a < b$, $(a, b) = 1$. Тогда*

$$h^\star\left(\frac{a}{b}\right) + h^\star\left(\frac{b-a}{b}\right) = s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right).$$

Доказательство. Пусть $a/b = [0; 1, a_1, \ldots, a_s, 1]$ ($s \geqslant 0$). Каждому k в пределах $0 \leqslant k \leqslant s$ будем ставить в соответствие четверку чисел (u_k, v_k, p_k, q_k), определяемую равенствами $(u_k, v_k) = (p_k, q_k) = 1$,

$$\frac{u_k}{v_k} = [0; a_k, \ldots, a_1, 1], \qquad \frac{p_k}{q_k} = [0; a_{k+1}, \ldots, a_s, 1].$$

Определим мультимножество (его элементы могут повторяться) $A = A_1 \cup A_2 \cup A_3$, где

$$\begin{aligned} A_1 &= \{(u_k, v_k, p_k, q_k) : 0 \leqslant k \leqslant s\}, \\ A_2 &= \{(u_k, v_k, p_k, q_k) : 0 \leqslant k \leqslant s, u_k \leqslant v_k/2, p_k/q_k < 1/\varphi\}, \\ A_3 &= \{(u_k, v_k, p_k, q_k) : 0 \leqslant k \leqslant s, v_k \geqslant 2, p_k/q_k < 1/\varphi\}. \end{aligned}$$

При этом кратность вхождения каждой четверки в множество A равна сумме кратностей, с которыми эта четверка входит в A_1, A_2 и A_3.

Разложению

$$\frac{a}{b} = \left\langle 0; \frac{1}{b_h}, \frac{\varepsilon_h}{b_{h-1}}, \ldots, \frac{\varepsilon_2}{b_1} \right\rangle^\star$$

и номеру j в пределах $2 \leqslant j \leqslant h$ будем ставить в соответствие четверку чисел $(\alpha_j, \beta_j, \lambda_j, \mu_j)$, определяемую условиями $\alpha_j, \beta_j, \mu_j > 0$, $(\alpha_j, \beta_j) = (\lambda_j, \beta_j) = 1$,

$$\frac{\alpha_j}{\beta_j} = \left\langle 0; \frac{1}{b_j}, \frac{\varepsilon_{j+1}}{b_{j+1}}, \ldots, \frac{\varepsilon_h}{b_h} \right\rangle, \qquad \frac{\lambda_j}{\mu_j} = \left\langle 0; \frac{\varepsilon_j}{b_{j-1}}, \ldots, \frac{\varepsilon_2}{b_1} \right\rangle^\star. \tag{13}$$

Через B обозначим множество всех таких четверок:

$$B = \{(\alpha_j, \beta_j, \lambda_j, \mu_j) : 2 \leqslant j \leqslant h\}.$$

При этом $B = B_1 \cup B_2 \cup B_3$, где

$$\begin{aligned} B_1 =&\{(\alpha,\beta,\lambda,\mu) \in B : 0 < \lambda/\mu \leqslant 1\},\\ B_2 =&\{(\alpha,\beta,\lambda,\mu) \in B : 1 < \lambda/\mu < \varphi\},\\ B_3 =&\{(\alpha,\beta,\lambda,\mu) \in B : \varphi - 2 < \lambda/\mu < 0\}. \end{aligned}$$

Через $\widetilde{B}$, $\widetilde{B}_1$, $\widetilde{B}_2$ и $\widetilde{B}_3$ обозначим аналогичные множества, построенные из разложения $(b-a)/b$ в дуальную дробь.

По определению статистик Гаусса — Кузьмина

$$\#(A_1 \cup A_2) = s_\varphi(a/b) - 1, \quad \#A_3 = s_{\varphi-1}(a/b) - 1.$$

Кроме того,

$$\#B = h^\star(a/b) - 1, \quad \#\widetilde{B} = h^\star((b-a)/b) - 1.$$

Поэтому для доказательства леммы достаточно проверить равномощность множеств A и $B \cup \widetilde{B}$. Для этого укажем отображения f_i ($i = 1, 2, 3$), которые устанавливают взаимно однозначные отображения из A_i в $B_i \cup \widetilde{B}_i$:

$$\begin{aligned} f_1(u,v,p,q) =&(u,v,p,q),\\ f_2(u,v,p,q) =&(u,v-u,p+q,q),\\ f_3(u,v,p,q) =&(v-u,v,-p,p+q). \end{aligned}$$

Например, если $(u,v,p,q) \in A_1$, то для некоторых u' и v'

$$\begin{pmatrix} u' & v' \\ u & v \end{pmatrix} \begin{pmatrix} * & p \\ * & q \end{pmatrix} = \begin{pmatrix} * & a \\ * & b \end{pmatrix},$$

где каждый из сомножителей лежит в $\mathcal{M}$. Если при этом $\left(\begin{smallmatrix} u' & v' \\ u & v \end{smallmatrix}\right) \in \mathcal{N}$, то $(u,v,p,q) \in B_1$, если же $\left(\begin{smallmatrix} u' & v' \\ u & v \end{smallmatrix}\right) \notin \mathcal{N}$, то $\left(\begin{smallmatrix} u-u' & v-v' \\ u & v \end{smallmatrix}\right) \in \mathcal{N}$ (см. свойство 6°),

$$\begin{pmatrix} u-u' & v-v' \\ u & v \end{pmatrix} \begin{pmatrix} * & p \\ * & q \end{pmatrix} = \begin{pmatrix} * & b-a \\ * & b \end{pmatrix},$$

и $(u,v,p,q) \in \widetilde{B}_1$. При этом каждая четверка $(\alpha,\beta,\lambda,\mu) \in B_1 \cup \widetilde{B}_1$ будет лежать в образе f_1. Так если $(\alpha,\beta,\lambda,\mu) \in B_1$, то (сомножители лежат в $\mathcal{N}$)

$$\begin{pmatrix} \alpha' & \beta' \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} * & \lambda \\ * & \mu \end{pmatrix} = \begin{pmatrix} * & a \\ * & b \end{pmatrix}.$$

Первый сомножитель лежит и в множестве $\mathcal{M}$, а матрицы $\left(\begin{smallmatrix} * & \lambda \\ * & \mu \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} * & a \\ * & b \end{smallmatrix}\right)$ можно превратить в матрицы из $\mathcal{M}$, изменив первые столбцы (см. свойство 6°). Значит, $(\alpha,\beta,\lambda,\mu) \in A_1$.

Если же $(\alpha,\beta,\lambda,\mu) \in \widetilde{B}_1$, то

$$\begin{pmatrix} \alpha' & \beta' \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} * & \lambda \\ * & \mu \end{pmatrix} = \begin{pmatrix} * & b-a \\ * & b \end{pmatrix}, \quad \begin{pmatrix} \alpha-\alpha' & \beta-\beta' \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} * & \lambda \\ * & \mu \end{pmatrix} = \begin{pmatrix} * & a \\ * & b \end{pmatrix}.$$

В последнем равенстве каждый из сомножителей (быть может после замены элементов, помеченных звездочками) будет лежать в $\mathcal{M}$, а значит, и в этом случае $(\alpha,\beta,\lambda,\mu) \in A_1$.

Биективность f_2 и f_3 проверяется аналогично исходя из равенств

$$\begin{pmatrix} u' & v' \\ u & v \end{pmatrix} \begin{pmatrix} p' & p \\ q' & q \end{pmatrix} = \begin{pmatrix} u' & v'-u' \\ u & v-u \end{pmatrix} \begin{pmatrix} p'+q' & p+q \\ q' & q \end{pmatrix},$$

$$\begin{pmatrix} u' & v' \\ u & v \end{pmatrix} \begin{pmatrix} p' & p \\ q' & q \end{pmatrix} = \begin{pmatrix} v'-u' & v' \\ v-u & v \end{pmatrix} \begin{pmatrix} -p' & -p \\ p'+q' & p+q \end{pmatrix},$$

которые произведения матриц из $\mathcal{M}$ позволяют переводить в произведения матриц из множества $\mathcal{N}$ и наоборот. □

Пример. Для дроби $5/7 = [0; 1, 2, 1, 1]$ множества A_1, A_2 и A_3 имеют вид

$$A_1 = \{(1,1,2,5), (1,3,1,2), (3,4,1,1)\}, \quad A_2 = A_3 = \{(1,3,1,2)\}.$$

Элементы A_1 находятся во взаимно однозначном соответствии с разложениями матрицы $\left(\begin{smallmatrix}3 & 5\\ 4 & 7\end{smallmatrix}\right) = \Psi(1,2,1,1)$ в произведение элементов $\mathcal{M}$:

$$\begin{pmatrix}3 & 5\\ 4 & 7\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 3 & 5\end{pmatrix} = \begin{pmatrix}1 & 2\\ 1 & 3\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix} = \begin{pmatrix}2 & 3\\ 3 & 4\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}.$$

По разложению $5/7 = \left\langle 0; \frac{1}{1}, \frac{1}{1}, \frac{1}{1}, \frac{-1}{3}\right\rangle^\star$ находится множество

$$B = \{(1,1,2,5), (1,2,3,2), (2,3,-1,3)\},$$

элементам которого соответствуют разложения матрицы $\left(\begin{smallmatrix}2 & 5\\ 3 & 7\end{smallmatrix}\right) = \Phi(5/7)$ в произведение матриц из $\mathcal{N}$:

$$\begin{pmatrix}2 & 5\\ 3 & 7\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 2 & 5\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & 3\\ 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2\\ 2 & 3\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 3\end{pmatrix}.$$

При этом

$$B_1 = \{(1,1,2,5)\}, \quad B_2 = \{(1,2,3,2)\}, \quad B_3 = \{(2,3,-1,3)\}.$$

Аналогично по дроби $2/7 = \left\langle 0; \frac{1}{3}, \frac{1}{1}, \frac{1}{1}\right\rangle^\star$ строится множество

$$\widetilde{B} = \{(1,3,1,2), (3,4,1,1)\},$$

элементы которого соответствуют разложения матрицы $\left(\begin{smallmatrix}1 & 2\\ 3 & 7\end{smallmatrix}\right) = \Phi(2/7)$ в произведение матриц из $\mathcal{N}$:

$$\begin{pmatrix}1 & 2\\ 3 & 7\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 3 & 4\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}.$$

При этом

$$\widetilde{B}_1 = \{(1,3,1,2), (3,4,1,1)\}, \quad \widetilde{B}_2 = \widetilde{B}_3 = \emptyset.$$

Легко видеть, что $f_i(A_i) = B_i \cup \widetilde{B}_i$ $(i = 1, 2, 3)$.

5 Основные результаты

Лемма 3. *Пусть* $b \geqslant 2$, $(a, b) = 1$, $1 \leqslant a, a^\star < b$, $aa^\star \equiv 1 \pmod b$. *Тогда*

$$h^\star\left(\frac{a}{b}\right) + h^\star\left(\frac{b-a}{b}\right) = h\left(\frac{a^\star}{b}\right) + h\left(\frac{b-a^\star}{b}\right).$$

Доказательство. Дополняя столбцы $\left(\begin{smallmatrix}a\\ b\end{smallmatrix}\right)$ и $\left(\begin{smallmatrix}b-a\\ b\end{smallmatrix}\right)$ до матриц из $\mathcal{N}$, при $\Delta(a/b) = 1$ получим матрицы $\left(\begin{smallmatrix}* & a\\ b-a^\star & b\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}* & b-a\\ a^\star & b\end{smallmatrix}\right)$, а при $\Delta(a/b) = -1$ — матрицы $\left(\begin{smallmatrix}* & a\\ a^\star & b\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}* & b-a\\ b-a^\star & b\end{smallmatrix}\right)$. В любом случае утверждение леммы вытекает из свойства 4°. □

Доказательство теоремы. Применяя леммы 2 и 3, находим

$$\sum_{a=1}^{b}{}^{*} h\left(\frac{a}{b}\right) = \sum_{a=1}^{b}{}^{*} h\left(\frac{a^\star}{b}\right) = \sum_{a=1}^{b}{}^{*} h^\star\left(\frac{a}{b}\right) =$$
$$= \sum_{b/2\leqslant a\leqslant b}{}^{*} \left(h^\star\left(\frac{a}{b}\right) + h^\star\left(\frac{b-a}{b}\right)\right) = \sum_{b/2\leqslant a\leqslant b}{}^{*} \left(s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right)\right).$$

Если $a/b = [0; 1, a_1, a_2, \ldots, a_s, 1]$, то $(b-a)/b = [0; a_1+1, a_2, \ldots, a_s, 1]$. Поэтому, по определению статистик Гаусса — Кузьмина

$$s_x\left(\frac{a}{b}\right) - s_x\left(\frac{b-a}{b}\right) = \chi_{[0,\{x\}]}\left(\frac{a}{b}\right) + \chi_{[0,x]}\left(\frac{b-a}{b}\right) - \chi_{[0,\{x\}]}\left(\frac{b-a}{b}\right) - \chi_{[0,x]}\left(\frac{a}{b-a}\right),$$

где χ_I — характеристическая функция отрезка I. В частности,

$$s_\varphi\left(\frac{a}{b}\right) = s_\varphi\left(\frac{b-a}{b}\right), \quad s_{\varphi-1}\left(\frac{a}{b}\right) = s_{\varphi-1}\left(\frac{b-a}{b}\right).$$

Значит,

$$\sum_{a=1}^{b}{}^{*}\, h\left(\frac{a}{b}\right) = \frac{1}{2}\sum_{a=1}^{b}{}^{*}\left(s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right)\right),$$

а следовательно и

$$\sum_{1\leqslant a\leqslant b} h\left(\frac{a}{b}\right) = \frac{1}{2}\sum_{1\leqslant a\leqslant b}\left(s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right)\right).$$

Применяя равенства (8) и (9), приходим к утверждению теоремы.

Список литературы

[1] Авдеева М. О. О статистиках неполных частных конечных цепных дробей. — *Функц. анализ и его прил.* **38**: 2 (2004), 1–11.

[2] Быковский В. А., Устинов А. В Статистика траекторий частиц в однородной задаче Синая для двумерной решетки. — *Функц. анализ и приложения*, **42**: 3 (2008), 10–22.

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

[4] Устинов А. В. Асимптотическое поведение первого и второго моментов для числа шагов в алгоритме Евклида. — *Известия РАН*, **72**: 5 (2008), 189–224.

[5] Устинов А. В. О числе решений сравнения $xy \equiv l \pmod q$ под графиком дважды непрерывно дифференцируемой функции. — *Алгебра и анализ*, **20**: 5 (2008), 186–216.

[6] Устинов А. В. О среднем числе шагов в алгоритме Евклида с выбором минимального по модулю остатка. — *Мат. заметки*, **85**: 1 (2009), 153–156.

[7] Baladi V., Vallée B. Euclidean algorithms are Gaussian. — *J. Number Theory*, **110** (2005), 331–386.

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

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

[10] Porter J. W. On a theorem of Heilbronn. — *Mathematika*, **22**:1 (1975), 20–28.

[11] Rieger G. J. Über die mittlere Schrittanzahl bei Divisionsalgorithmen. — *Math. Nachr.*, **82** (1978), 157–180.

[12] Rieger G. J. Ein Heilbronn-Satz für Kettenbrüche mit ungeraden Teilnennern. — *Math. Nachr.*, **101** (1981), 295–307.

[13] Vallée B. Dynamical analysis of a class of Euclidean algorithms. — *Theoret. Comput. Sci.*, **297** (2003), 447–486.