ISSN 0001-4346, Mathematical Notes, 2010, Vol. 88, No. 4, pp. 574–584. © Pleiades Publishing, Ltd., 2010.
Original Russian Text © A. V. Ustinov, 2010, published in Matematicheskie Zametki, 2010, Vol. 88, No. 4, pp. 594–604.

The Mean Number of Steps in the Euclidean Algorithm with Odd Partial Quotients

A. V. Ustinov[*]
Khabarovsk Branch, Institute of Applied Mathematics,
Russian Academy of Sciences

Received April 13, 2010

Abstract—The length of the continued-fraction expansion of a rational number with odd partial quotients is expressed via the Gauss–Kuz'min statistics for the classical continued fraction. This has made it possible to prove asymptotic formulas, similar to those already known for the classical Euclidean algorithm, for the mean length of the Euclidean algorithm with odd partial quotients.

DOI: 10.1134/S0001434610090300

Key words: *Euclidean algorithm, Gauss–Kuz'min statistics, continued-fraction expansion, dual fraction, partial quotient.*

Dedicated to the memory of A. A. Karatsuba

1. THREE FAST VERSIONS OF THE EUCLIDEAN ALGORITHM AND GAUSS–KUZ'MIN STATISTICS

Three "fast" versions are usually singled out from among the different modifications of the Euclidean algorithm (see [1]); they are based on differentt methods of division with remainder:

- the classical Euclidean algorithm

$$a = bq + r, \qquad q = \left\lfloor \frac{a}{b} \right\rfloor, \quad 0 \le r < b;$$

- the algorithm with least absolute value remainder

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

- the algorithm with odd partial quotients

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

In the fast versions, the mean number of steps in the worst case is $O(\log N)$ (for $a, b \ll N$).

The "slow" algorithms are: the algorithm with subtraction, the "excess" division algorithm, and the algorithm with even partial quotients. For them, the mean number of steps is of the order of $\log^2 N$ and, in the worst case, can be of the order of N (for more detailed information and bibliography, see [1]).

Each of of three fast algorithms involves the expansion of numbers in the corresponding continued fractions. The classical algorithm is:

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

[*] E-mail: ustinov@iam.khv.ru

where a_0 is an integer, $a_1, \dots, a_s$ are natural numbers, and $a_s \geq 2$ for $s \geq 1$. (Another way to ensure the uniqueness of the continued-fraction expansion is to require that the last partial quotient be equal to 1.) The algorithm with least absolute value remainder is:

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

where a_0 is an integer $a_1, \dots, a_l$ are natural numbers, $\varepsilon_k = \pm 1$, $a_k \geq 2$, $1 \leq k \leq l$, $a_k + \varepsilon_{k+1} \geq 2$, $1 \leq k < l$, and $\varepsilon_l = -1$ for $l \geq 1$ and $a_l = 2$. The algorithm with odd partial quotients is:

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

where a_0 is an odd integer, $a_1, \dots, a_h$ are odd natural numbers, $\varepsilon_k = \pm 1$, $a_k + \varepsilon_{k+1} \geq 1$, $1 \leq k < h$, and $\varepsilon_h = 1$ for $h \geq 1$ and $a_h = 1$. The lengths of expansions of a rational number a/b in fractions of the form (1)–(3) will be denoted, respectively, by $s(a/b)$, $l(a/b)$, and $h(a/b)$.

From the computational point of view, the problem of studying the mean values of the functions $s(a/b)$, $l(a/b)$, and $h(a/b)$ naturally arises. The mean length of classical continued fractions was first studied by Heilbronn. In 1968, using elementary methods, he proved the asymptotic formula (see [2])

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

(here and elsewhere, the sign $*$ on the sums means that the summation variable ranges over a given system of residues). In 1975, using estimates of Kloosterman sums for the same mean, Porter obtained the following asymptotic formula with two significant terms (see [3]):

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

where ε is any positive number and

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

is a constant known as the *Porter constant* (its final form was obtained by Wrench; see [4]). By averaging over both parameters, one can prove the more exact formula (see [5])

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

where

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

For continued fractions of the form (2) and (3), analogs of Heilbronn's result were proved Rieger (see [6], [7]). In [8], using ergodic methods, Baladi and Valée proved the two-term asymptotic formulas

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

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

where $\varphi = (1+\sqrt{5})/2$ is the "golden section" and $\gamma > 0$. In the same paper, the problem of the determination of the constants $\widetilde{C}_l$ and $\widetilde{C}_h$ was posed.

It turns out that the question of the mean behavior of the functions $l(a/b)$ and $h(a/b)$ can be reduced to the analysis of the classical Euclidean algorithm if we use Gauss–Kuz'min statistics. This allows us to prove formulas for the mean values of $l(a/b)$ and $h(a/b)$ similar to (4) and (5), while, for the constants $\widetilde{C}_l$ and $\widetilde{C}_h$, we can obtain representations in terms of singular series.

For a rational number $a/b = [0; a_1, \dots, a_s, 1] \in [0,1]$ and a real number $x \in [0,1]$, by *Gauss–Kuz'min statistics* we mean the numbers (see [9])

$$s_x\left(\frac{a}{b}\right) = \#\{j : 0 \le j \le s,\ [0; a_{j+1}, \dots, a_s, 1] \le x\}. \tag{6}$$

In particular, $s_1(a/b) = s+1$ is the work length of the classical Euclidean algorithm applied to a pair of numbers (a,b) (here we assume that, at the first step, the variables are transposed, while, at the following steps, division with remainder occurs; see [10]).

For subsequent arguments, it is convenient to extend the definition of Gauss–Kuz'min statistics to an arbitrary $x > 0$:

$$s_x\left(\frac{a}{b}\right) = \#\{(j,t) : 0 \le j \le s,\ 0 \le t < a_j,\ [t; a_{j+1}, \dots, a_s, 1] \le x\} \tag{7}$$

(here we assume that $a_0 = +\infty$). For a finite continued fraction, we have chosen the expression with 1 at the end so that the new definition (7) coincides with the old one (6) not only for $x \in [0,1)$, but also for $x = 1$.

For the mean values of the Gauss–Kuz'min statistics, the following relations hold (the proofs from [5], [11] remain valid for an arbitrary positive x):

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

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

where

$$\begin{aligned} C_P(x) &= \frac{2\log(1+x)}{\zeta(2)}\left(2\gamma - 2\frac{\zeta'(2)}{\zeta(2)} - \frac{\log(1+x)}{2} + \log x - 1\right) \\ &\quad + \frac{2}{\zeta(2)}(h_1(x) + h_2(x)) + \frac{x^2}{x+1}, \end{aligned} \tag{10}$$

$$\widetilde{C}_P(x) = C_P(x) + \frac{2\log(1+x)}{\zeta(2)}\left(\frac{\zeta'(2)}{\zeta(2)} - \frac{1}{2}\right), \tag{11}$$

while the functions $h_1(x)$ and $h_2(x)$ are given by the absolutely convergent singular series

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

$$h_2(x) = \sum_{n=1}^{\infty} \frac{1}{n}\left(\sum_{n/x \le m < n/x+n} \frac{1}{m} - \log(1+x)\right).$$

In [12], it was proved that $l(a/b) = s_{\varphi-1}(a/b)$. Therefore, results on the mean values of $l(a/b)$ (and formulas for the second constants in the asymptotic formulas) can be obtained by substituting $x = \varphi - 1$ into formulas (8) and (9).

In the present paper, it is proved that, for

$$b \geq 1, \quad \frac{b}{2} \leq a < b, \quad (a,b)=1, \quad aa^\star \equiv 1 \pmod{b}, \quad 1 \leq a^\star < b,$$

the following identity holds:

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

Therefore, relations (8) and (9) imply the following result.

Theorem. *The following asymptotic formulas hold*:

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

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

where

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

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

and the functions $C_P(x)$, $\widetilde{C}_P(x)$ are given by relations (10), (11).

2. DUAL-FRACTION EXPANSIONS

Along with continued-fraction expansions of the form (3), we also consider dual (inverted) fractions

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

with the same constraints on the parameters: the a_j are odd natural numbers, $1 \leq j \leq h$, $\varepsilon_j = \pm 1$, $2 \leq j \leq h+1$, $\varepsilon_{j+1} + a_j > 0$, $1 \leq j < h$.

Lemma 1. *A rational number p/q can be expressed as a dual fraction if and only if $p/q \in (\varphi-2, \varphi)$; the representation by a dual fraction is unique.*

Proof. *Necessity* The necessity of the condition $p/q \in (\varphi-2,\varphi)$ follows from the inequalities

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

To prove its *sufficiency*, let us describe the expansion algorithm. For $\varepsilon_{h+1} = -1$, we have

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

and, for some odd number $a_h > \varphi^2 - \varphi = 1$ uniquely defined, $-a_h - q/p$ will lie in the interval $(\varphi-2, \varphi)$. But if $\varepsilon_{h+1} = 1$, then $q/p > 1/\varphi$ and, for some odd number

$$a_h \geq \frac{1}{\varphi} + \frac{1}{\varphi^2} = 1,$$

also uniquely defined, $q/p - a_h$ will also lie in the interval $(\varphi-2,\varphi)$. Thus, in each case, the pair (ε_{h+1}, a_h) is uniquely defined; for it, $\varepsilon_{h+1}+a_h>0$ and the passage to the fraction

$$\frac{r}{p} = \pm\frac{q}{p} - a_h \in (\varphi-2,\varphi)$$

is carried out.

The expansion is finite, because the height of the expanded number decreases at each step

$$|r| + |p| < |p| + q.$$

The uniqueness of the representation by a dual fraction is a consequence of the uniqueness of the algorithm under consideration. □

In what follows, the length of the dual-fraction expansion of a rational number a/b will be denoted by $h^\star(a/b)$.

3. CONTINUED FRACTIONS AND MATRICES

A key role in the study of the statistical properties of finite continued fractions (see, for example, [5], [11]) is played by the bijection which, to each nonempty collection of natural numbers $(a_1,\dots,a_n)$ (composed of partial quotients of a rational number), assigns the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_s \end{pmatrix} \in \mathscr{M},$$

where

$$\mathscr{M} = \left\{ \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) : P \ge 0,\ 1 \le P' \le Q',\ 1 \le Q \le Q' \right\}. \tag{12}$$

In order to study continued fractions with odd partial quotients and the corresponding dual fractions, we introduce the mapping Φ assigning to the rational number

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

the matrix

$$\Phi\left(\frac{a}{b}\right) = \begin{pmatrix} 0 & \varepsilon_{h+1} \\ 1 & a_h \end{pmatrix} \cdots \begin{pmatrix} 0 & \varepsilon_2 \\ 1 & a_1 \end{pmatrix}.$$

Note the main properties of the mapping Φ.

1°. If

$$\Phi\left(\frac{a}{b}\right) = \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix},$$

then

$$\begin{aligned} \frac{P}{Q} &= \left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_3}{a_2} \right\rangle^\star, & \frac{P}{P'} &= \left\langle 0; \frac{1}{a_1}, \frac{\varepsilon_2}{a_2}, \dots, \frac{\varepsilon_{h-1}}{a_{h-1}} \right\rangle, \\ \frac{P'}{Q'} &= \left\langle 0; \frac{\varepsilon_{h+1}}{a_h}, \dots, \frac{\varepsilon_2}{a_1} \right\rangle^\star = \frac{a}{b}, & \frac{Q}{Q'} &= \left\langle 0; \frac{1}{a_1}, \frac{\varepsilon_2}{a_2}, \dots, \frac{\varepsilon_h}{a_h} \right\rangle. \end{aligned} \tag{13}$$

2°. Any matrix

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

lying in the image of the mapping Φ can be uniquely reconstructed from both the row $(Q\ Q')$ and the column $\binom{P'}{Q'}$. In particular, the determinant of the matrix S is a function of the ratio P'/Q'; in what follows, this function will be denoted by $\Delta(P'/Q')$.

3°. The mapping Φ is a bijection between $\mathbb{Q}\cap(\varphi-2,\varphi)$ and the set of matrices

$$\mathscr{N}=\left\{\begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix}\in \mathrm{GL}_2(\mathbb{Z}) : 1\le Q\le Q',\ PQ'-P'Q=\Delta\biggl(\frac{P'}{Q'}\biggr),\ \frac{P'}{Q'}\in(\varphi-2,\varphi)\right\}.$$

4°. If

$$\begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix}\in\mathscr{N},$$

then $h^\star(P'/Q')=h(Q/Q')$.

5°. If $Q'\ge 2$ and

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

then $\Delta((Q'-P')/Q')=\Delta(P'/Q')$ and

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

6°. For $Q'\ge 2$, the row $(Q\ Q')$ and the column $\binom{P'}{Q'}$ can be complemented to a matrix from $\mathscr{M}$ in two ways. Furthermore, in each of the two pairs of resulting matrices

$$\begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix},\quad \begin{pmatrix} P'-P & P' \\ Q'-Q & Q' \end{pmatrix}\qquad\text{and}\qquad \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix},\quad \begin{pmatrix} Q-P & Q'-P' \\ Q & Q' \end{pmatrix},$$

exactly one matrix lies in the set $\mathscr{N}$.

Property 1° is verified by induction.

Property 2° immediately follows from property 1°.

In property 3°, the fact that the mapping Φ is injective follows from Lemma 1 and the equality $P'/Q'=a/b$. To prove surjectivity, consider an arbitrary matrix

$$S=\begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix}\in\mathscr{N}$$

and set

$$\widetilde{S}=\Phi(P'/Q')=\begin{pmatrix} \widetilde{P} & P' \\ \widetilde{Q} & Q' \end{pmatrix}\in\mathscr{N}.$$

Then $\det S=\det\widetilde{S}=\Delta(P'/Q')$, and, for some integer t, the following relations hold: $\widetilde{P}=P+tP'$, $\widetilde{Q}=Q+tQ'$. But $1\le Q,\widetilde{Q}\le Q'$; therefore, $t=0$ and $S=\widetilde{S}$.

Property 4° follows from property 3° and relations (13).

In order to prove property 5°, we first note that, for $Q' = 2$, there is exactly one matrix

$$S = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

lying in $\mathscr{M} \cap \mathscr{N}$. For it, the assertion of the lemma is obvious; therefore, we can assume that $Q' \geq 3$. By property 2°, the column $\binom{Q'-P'}{Q'}$ can be complemented to some matrix

$$\widetilde{S} = \begin{pmatrix} * & Q' - P' \\ \widetilde{Q} & Q' \end{pmatrix} \in \mathscr{N}.$$

By definition (12), this matrix lies in the set $\mathscr{M}$ and $1 \leq \widetilde{Q} < Q'$. Here $\widetilde{Q} \neq Q$, because $Q' - P' \neq P'$. Since $\det S = \pm \det \widetilde{S}$, it follows that $QP' \equiv \pm \widetilde{Q}P' \pmod{Q'}$, and $\widetilde{Q} = Q' - Q$. Hence we have

$$\det S \equiv P'Q \equiv \det \widetilde{S} \pmod{Q'} \qquad \text{and} \qquad \Delta((Q' - P')/Q') = \Delta(P'/Q').$$

Property 6° follows from property 2°.

4. REDUCTION TO GAUSS–KUZ'MIN STATISTICS

Lemma 2. *Suppose that $b \geq 2$, $b/2 \leq a < b$, $(a, b) = 1$. Then*

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

Proof. Suppose that $a/b = [0; 1, a_1, \dots, a_s, 1]$, $(s \geq 0)$. To each k between the limits $0 \leq k \leq s$, we assign a quadruple of numbers (u_k, v_k, p_k, q_k) defined by the equalities $(u_k, v_k) = (p_k, q_k) = 1$,

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

Define the multiset (its elements may occur over and over) $A = A_1 \cup A_2 \cup A_3$, where

$$\begin{aligned} A_1 &= \{(u_k, v_k, p_k, q_k) : 0 \leq k \leq s\}, \\ A_2 &= \biggl\{(u_k, v_k, p_k, q_k) : 0 \leq k \leq s,\ u_k \leq \frac{v_k}{2},\ \frac{p_k}{q_k} < \frac{1}{\varphi}\biggr\}, \\ A_3 &= \biggl\{(u_k, v_k, p_k, q_k) : 0 \leq k \leq s,\ v_k \geq 2,\ \frac{p_k}{q_k} < \frac{1}{\varphi}\biggr\}. \end{aligned}$$

Here the multiplicity of occurrence of each quadruple in the set A is equal to the sum of the number of times this quadruple appears in A_1, A_2, and A_3.

To the expansion

$$\frac{a}{b} = \biggl\langle 0; \frac{1}{b_h}, \frac{\varepsilon_h}{b_{h-1}}, \dots, \frac{\varepsilon_2}{b_1} \biggr\rangle^\star$$

and the number j between the limits $2 \leq j \leq h$, we assign the quadruple of numbers $(\alpha_j, \beta_j, \lambda_j, \mu_j)$ specified by the conditions $\alpha_j, \beta_j, \mu_j > 0$, $(\alpha_j, \beta_j) = (\lambda_j, \beta_j) = 1$,

$$\frac{\alpha_j}{\beta_j} = \biggl\langle 0; \frac{1}{b_j}, \frac{\varepsilon_{j+1}}{b_{j+1}}, \dots, \frac{\varepsilon_h}{b_h} \biggr\rangle, \qquad \frac{\lambda_j}{\mu_j} = \biggl\langle 0; \frac{\varepsilon_j}{b_{j-1}}, \dots, \frac{\varepsilon_2}{b_1} \biggr\rangle^\star. \tag{14}$$

Let B denote the set of all such quadruples:

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

Here $B = B_1 \cup B_2 \cup B_3$, where

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

Let $\widetilde{B}$, $\widetilde{B}_1$, $\widetilde{B}_2$, and $\widetilde{B}_3$ denote the similar sets constructed from the dual-fraction expansion of $(b-a)/b$.

By the definition of the Gauss–Kuz'min statistics,

$$\#(A_1 \cup A_2) = s_\varphi\biggl(\frac{a}{b}\biggr) - 1, \qquad \#A_3 = s_{\varphi-1}\biggl(\frac{a}{b}\biggr) - 1.$$

In addition,

$$\#B = h^\star\biggl(\frac{a}{b}\biggr) - 1, \qquad \#\widetilde{B} = h^\star\biggl(\frac{b-a}{b}\biggr) - 1.$$

Therefore, in order to prove the lemma, it suffices to verify that the sets A and $B \cup \widetilde{B}$ are of equal cardinality. To do this, let us find mappings f_i, $i = 1,2,3$, that establish one-to-one correspondences from A_i into $B_i \cup \widetilde{B}_i$:

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

For example, if $(u,v,p,q) \in A_1$, then, for some u' and v',

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

where each of the factors lies in $\mathscr{M}$. If

$$\begin{pmatrix} u' & v' \\ u & v \end{pmatrix} \in \mathscr{N},$$

then $(u,v,p,q) \in B_1$, but if

$$\begin{pmatrix} u' & v' \\ u & v \end{pmatrix} \notin \mathscr{N},$$

then

$$\begin{pmatrix} u-u' & v-v' \\ u & v \end{pmatrix} \in \mathscr{N}$$

(see property 6°),

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

and $(u,v,p,q)\in\widetilde{B}_1$. Moreover, each quadruple $(\alpha,\beta,\lambda,\mu)\in B_1\cup\widetilde{B}_1$ will lie in the image of f_1. Thus, if $(\alpha,\beta,\lambda,\mu)\in B_1$, then (the factors lie in $\mathscr{N}$)

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

The first factor also lies in the set $\mathscr{M}$, and the matrices

$$\begin{pmatrix}* & \lambda\\ * & \mu\end{pmatrix}\qquad\text{and}\qquad\begin{pmatrix}* & a\\ * & b\end{pmatrix}$$

can be transformed into matrices from $\mathscr{M}$ by changing the first columns (see property 6°). Hence $(\alpha,\beta,\lambda,\mu)\in A_1$.

But if $(\alpha,\beta,\lambda,\mu)\in\widetilde{B}_1$, then

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

In the last equality, each of the factors (perhaps, after replacing the elements marked by an asterisk) will lie in $\mathscr{M}$, and hence, also in this case, $(\alpha,\beta,\lambda,\mu)\in A_1$.

The fact that f_2 and f_3 are bijective is verified in a similar way from the equalities

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

which allow transforming the products of matrices from $\mathscr{M}$ into the products of matrices from the set $\mathscr{N}$, and conversely. □

Example. For the fraction $5/7=[0;1,2,1,1]$, the sets A_1, A_2, and A_3 are of the form

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

The elements of A_1 are in one-to-one correspondence with the decompositions of the matrix

$$\begin{pmatrix}3 & 5\\ 4 & 7\end{pmatrix}=\Psi(1,2,1,1)$$

into the product of the elements of $\mathscr{M}$:

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

From the expansion $5/7=\langle 0;1/1,1/1,1/1,-1/3\rangle^\star$ we find the set

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

whose elements correspond to the decompositions of the matrix

$$\begin{pmatrix}2 & 5\\ 3 & 7\end{pmatrix}=\Phi\left(\frac{5}{7}\right)$$

into the product of the matrices from $\mathscr{N}$:

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

Here

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

Similarly, from the fraction $2/7=\langle 0;1/3,1/1,1/1\rangle^\star$, we construct the set

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

whose elements correspond to the decomposition of the matrix

$$\begin{pmatrix}1&2\\3&7\end{pmatrix}=\Phi\left(\frac{2}{7}\right)$$

into the product of matrices from $\mathscr{N}$:

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

Here

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

We can easily see that $f_i(A_i)=B_i\cup\widetilde{B}_i$, $i=1,2,3$.

5. MAIN RESULTS

Lemma 3. *Suppose that* $b\ge 2$, $(a,b)=1$, $1\le a,a^\star<b$, $aa^\star\equiv 1 \pmod b$. *Then*

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

Proof. Complementing the columns $\binom{a}{b}$ and $\binom{b-a}{b}$ to matrices from $\mathscr{N}$, we obtain the matrices

$$\begin{pmatrix}*&a\\b-a^\star&b\end{pmatrix},\qquad\begin{pmatrix}*&b-a\\a^\star&b\end{pmatrix}$$

for $\Delta(a/b)=1$ and the matrices

$$\begin{pmatrix}*&a\\a^\star&b\end{pmatrix},\qquad\begin{pmatrix}*&b-a\\b-a^\star&b\end{pmatrix}$$

for $\Delta(a/b)=-1$. In each case, the assertion of the lemma follows from property 4°. □

Proof of the theorem. Using Lemmas 2 and 3, we obtain

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

If $a/b = [0; 1, a_1, a_2, \dots, a_s, 1]$, then $(b-a)/b = [0; a_1+1, a_2, \dots, a_s, 1]$. Therefore, by the definition of the Gauss–Kuz'min statistics, we have

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

where χ_I is the characteristic function of the interval I. In particular,

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

Hence

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

and, therefore,

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

Using relations (8) and (9), we obtain the assertion of the theorem. □

ACKNOWLEDGMENTS

This work was supported by the Presidential grant no. MD-2339.2010.1, by the Dynasty Foundation, by the Russian Foundation for Basic Research (grants no. 09-01-12129-ofi-m, no. 10-01-98001-r-sibir'-a, and no. 09-01-00371-a), as well as by the DVO grant no. 09-I-P4-03.

REFERENCES

1. B. Vallée, "Dynamical analysis of the class of Euclidean algorithms," Theoret. Comput. Sci. **297** (1-3), 447–486 (2003).
2. H. Heilbronn, "On the average length of the class of finite continued fractions," in *Number Theory and Analysis*, Papers in Honor of Edmund Landau (Plenum, New York, 1969), pp. 87–96.
3. J. W. Porter, "On a theorem of Heilbronn," Mathematika **22** (1), 20–28 (1975).
4. D. E. Knuth, "Evaluation of Porter's constant," Comput. Math. Appl. **2** (2), 137–139 (1976).
5. A. V. Ustinov, "Asymptotic behaviour of the first and second moments for the number of steps in the Euclidean algorithm," Izv. Ross. Akad. Nauk Ser. Mat. **72** (5), 189–224 (2008) [Russian Acad. Sci. Izv. Math. **72** (5), 1023–1059 (2008)].
6. G. J. Rieger, "Über die mittlere Schrittanzahl bei Divisionsalgorithmen," Math. Nachr. **82** (1), 157–180 (1978).
7. G. J. Rieger, "Ein Heilbronn–Satz für Kettenbrüche mit ungeraden Teilnennern," Math. Nachr. **101** (1), 295–307 (1981).
8. V. Baladi and B. Vallée, "Euclidean algorithms are Gaussian," J. Number Theory **110** (2), 331–386 (2005).
9. M. O. Avdeeva, "On the statistics of partial quotients of finite continued fractions," Funktsional. Anal. Prilozhen. **38** (2), 1–11 (2004) [Functional Anal. Appl. **38** (2), 79–87 (2004)].
10. Donald E. Knuth, *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms* (Addison-Wesley, Reading, Mass., 1969; Mir, Moscow, 2000).
11. A. V. Ustinov, "On the number of solutions of the congruence $xy \equiv l (\operatorname{mod} q)$ under the graph of a twice continuously differentiable function," Algebra Anal. **20** (5), 186–216 (2008) [St. Petersbg. Math. J. **20** (5), 813–836 (2008)].
12. A. V. Ustinov, "The mean number of steps in the Euclidean algorithm with least absolute value remainders," Mat. Zametki **85** (1), 153–156 (2009) [Math. Notes **85** (1–2), 142–145 (2009)].