Dynamics of the Binary Euclidean Algorithm:

Functional Analysis and Operators.

Brigitte Vallée
GREYC, Université de Caen, 14032 Caen Cedex, France.
e–mail : Brigitte.Vallee@info.unicaen.fr

Abstract. *We provide here a complete average–case analysis of the binary continued fraction representation of a random rational whose numerator and denominator are odd and less than N. We analyse the three main parameters of the binary continued fraction expansion, namely the height, the number of steps of the binary Euclidean algorithm, and finally the sum of the exponents of powers of 2 contained in the numerators of the binary continued fraction. The average values of these parameters are shown to be asymptotic to $A_i \log N$, and the three constants A_i are related to the invariant measure of the Perron-Frobenius operator linked to this dynamical system. The Binary Euclidean algorithm has been previously studied in 1976 by Brent who provided a partial analysis of the number of steps, based on a heuristic model and some unproven conjecture. Our methods are quite different, not relying on unproven assumptions, and more general, since they allow us to study all the parameters of the binary continued fraction expansion.*

0. Introduction. The Euclidean algorithms find the greatest common divisor (gcd) of two integers. The classical Euclidean algorithm uses divisions and exchanges, and is based on the two relations

$$\gcd(u,v) = \gcd(v \bmod u, u), \qquad \gcd(u,v) = \gcd(v,u).$$

The behaviour of the classical algorithm is now well–understood. Heilbronn [Hei] and Dixon [Di] have independently shown that the average number D_N of Euclidean divisions on a random rational input with numerator and denominator less than N is asymptotically logarithmic,

$$D_N \sim \frac{12 \log 2}{\pi^2} \log N.$$

Here, we focus on the binary Euclidean algorithm which operates on pairs of odd integers. It performs only subtractions, right binary shifts and exchanges. Let the symbol $\mathrm{Val}_2\,(u)$ denote the dyadic valuation of the integer u, i.e., the largest exponent b such that 2^b divides u; then, the binary Euclidean algorithm is based on the relations

$$\gcd(u,v) = \gcd\Big(\frac{v-u}{2^{\mathrm{Val}_2\,(v-u)}}, v\Big), \qquad \gcd(u,v) = \gcd(v,u).$$

Unlike the classical Euclidean algorithm, no divisions are required, so that each iteration of the binary gcd algorithm is faster than an iteration of the classical gcd algorithm. We consider here the average number of operations (subtractions, shifts, and exchanges) that are performed on a random rational with numerator and denominator odd and less than N, and we show that each of these numbers have an average that grows logarithmically.

The binary Euclidean algorithm operates on pairs of odd integers that belong to the set

$$\Omega := \{(u,v);\ u, v \,\text{odd},\ 0 < u \le v\}. \tag{1}$$

as follows:

Binary Euclidean Algorithm (u, v)

Input: $(u, v) \in \Omega$;

While $u \neq v$ **do**

  While $u < v$ **do**

    $b := \mathrm{Val}_2\,(v - u)$; (2)

    $v := (v - u)/2^b$;

  Exchange u and v;

Output: u (or v).

This algorithm has two nested loops: The external loop corresponds to an exchange. Between two exchanges, there is a sequence of iterations that constitutes the internal loop. This sequence consists in subtractions and shifts and can be written as

$$v = u + 2^{b_1} v_1, \qquad v_1 = u + 2^{b_2} v_2, \qquad v_2 = u + 2^{b_3} v_3, \qquad \ldots \qquad v_{\ell-1} = u + 2^{b_\ell} v_\ell, \tag{3}$$

with $v_\ell < u$. Then we exchange u and v_ℓ. If $x = x_0$ denotes the rational u/v at the beginning of an internal loop, the global result of the sequence (3) of the internal loops followed by the last exchange is the rational $x_1 = v_\ell/u$ defined by

$$x_0 = \frac{1}{a + 2^k x_1},$$

where a is an odd integer equal to

$$a = 1 + 2^{b_1} + 2^{b_1+b_2} + 2^{b_1+b_2+b_3} + \ldots + 2^{b_1+b_2+b_3+\ldots+b_{\ell-1}},$$

while the exponent k is equal to $k = b_1 + b_2 + \ldots + b_\ell$. Then the antecedents of the rational x_1 can be written as $x_0 = h(x_1)$, where all the possible functions h are of the form

$$h(x) := \frac{1}{a + 2^k x}, \qquad \text{with } a \text{ odd, } 1 \leq a < 2^k, \text{ and } k \geq 1. \tag{4}$$

Thus the rational u/v has a unique binary continued fraction expansion

$$\frac{u}{v} = \cfrac{1}{a_1 + \cfrac{2^{k_1}}{a_2 + \cfrac{2^{k_2}}{\ddots \quad \ddots + \cfrac{2^{k_{r-1}}}{a_r + 2^{k_r}}}}}. \tag{5}$$

We study three parameters of this continued fraction:

(i) The height or the depth (i.e., the number of exchanges); here, it is equal to r.

(ii) The total number of operations that are necessary to obtain the expansion; if $p(a)$ denotes the number of 1's in the binary expansion of the integer a, it is equal to $p(a_1) + p(a_2) + \ldots + p(a_r)$, where the a_i's are the denominators of the binary continued fraction.

(iii) The total sum of exponents of 2 in the numerators of the binary continued fraction: here, it is equal to $k_1 + k_2 + \ldots + k_r$.

Our main results (Theorems 1 and 2) describe the average values of these three parameters:

Main result. *The expectations of the main parameters of the Binary Continued Fraction on the set*

$$\Omega_N := \{(u,v);\ u, v\,\text{odd},\ 0 < u \le v \le N\} \tag{6}$$

are all asymptotically equal to $A_i \log N$. The constants A_i are related to the dominant spectral properties of the operator $\mathcal{V}_2$

$$\mathcal{V}_2[f](x) := \sum_{k\ge 1} \sum_{\substack{a\ \text{odd},\\ 1\le a<2^k}} \Big(\frac{1}{a+2^k x}\Big)^2 f\Big(\frac{1}{a+2^k x}\Big), \tag{7}$$

defined on a suitable Hardy space of holomorphic functions inside a disk that contains the real segment $]0,1]$. Denote by f_2 the dominant eigenvector of $\mathcal{V}_2$ relative to the dominant eigenvalue $\lambda = 1$, with the normalization condition $\int_0^1 f_2(t)dt = 1$, and by F_2 the integral of f_2 such that $F_2(0) = 0$. Then the three constants can be expressed with f_2 and F_2, as follows:

$$A_1 = \frac{2}{\pi^2 f_2(1)}, \qquad A_2 = \frac{2}{\pi^2 f_2(1)} \Big[\sum_{\substack{a\ \text{odd}\\ a\ge 1}} \frac{1}{2^{k_a}} F_2\Big(\frac{1}{a}\Big)\Big] \qquad A_3 = 2A_2, \tag{8}$$

(Here k_a denotes the integer part of $\log_2 a$).

Remark: The relation between A_1, A_2, A_3 in (8) is the one to be expected if, at each depth of the process, the decomposition described in the sequence (3)

$$v = au + 2^k r, \quad \text{with } a \text{ odd less than } 2^k \text{ and } r < u,$$

has the same behaviour as at the beginning of the process: when (u,v) is uniformly distributed in Ω_N, the average values $E[p_N]$ of $p(a)$ and $E[k_N]$ of the exponent k satisfy $E[k_N] \simeq 2E[p_N]$.

The methods developed here use quite varied tools: generating functions, Ruelle operators, Tauberian methods, functional analysis. First, we use classical tools in the average–case analysis of algorithms [Fl], [FS]: we introduce the generating functions related to the three parameters to be analyzed; as is usual in the context of analytic number theory, these generating functions are Dirichlet series. Second, we prove that these generating functions are closely linked to the operator $\mathcal{V}_s$,

$$\mathcal{V}_s[f](x) := \sum_{k\ge 1} \sum_{\substack{a\ \text{odd},\\ 1\le a<2^k}} \Big(\frac{1}{a+2^k x}\Big)^s f\Big(\frac{1}{a+2^k x}\Big). \tag{9}$$

This operator contains all the information on the dynamics of the algorithm. In the context of dynamical systems [Ru], it is called the Ruelle operator relative to the system. More precisely, the generating functions involve the quasi–inverse operator $\Lambda_s := (I - \mathcal{V}_s)^{-1}$, and the expectations to be studied are partial sums of coefficients of these Dirichlet series, so the main results of the paper will come from the application of Tauberian Theorems [De], provided that they *can* be applied. This will be the case as soon as the operator $\mathcal{V}_s$ when acting in a suitable Banach space has a "spectral gap", i.e., a unique dominant eigenvalue separated from the remainder of the spectrum by a gap. When acting on a Hardy space of holomorphic functions relative to a suitable disk, the operator $\mathcal{V}_s$ is proven to be compact and positive (in the sense of Krasnoselsky) [Kr] for real values of parameter s, and then it has a spectral gap. Since Tauberian theorems link the asymptotics of coefficients to the dominant singularity of the function, the constants A_i involve the dominant singularity of the quasi–inverse $(I - \mathcal{V}_s)^{-1}$, i.e. the dominant spectral objects of the Ruelle operator $\mathcal{V}_s$.

These "dynamical" methods have been already used in other domains of algorithmic number theory, mainly in the study of the classical Euclidean algorithm, or related algorithms [Ma1], [He$_i$] ($1 \le i \le 4$), [Va$_i$] ($1 \le i \le 3$), [DFV]. In particular, the author [FV] uses them to obtain an alternative proof of the results of Heilbronn and Dixon about the logarithmic behaviour of the Classical Euclidean algorithm. Recently, the author [Va4] has extended similar methods in the general context of information theory, where she describes algorithmic properties of dynamical sources. In all previous works, the functional analysis to be used is simpler, because the Ruelle operators act on a suitable Banach space of holomorphic functions defined in an open disk and continuous on the boundary. Here, the powers of 2 introduce singularities on the boundary of the domain, and make the functional space more difficult to deal with.

Our methods are quite different from those used by Brent. In fact, Brent [Br1] analysed an extension of the algorithm to a continuous (probabilistic) model. There, the input is a real number x in $]0,1]$ and the line (2) of the previous algorithm algorithm is modified.

Continuous Probabilistic Binary Euclidean Algorithm (x)

Input: x (real) $\in]0,1]$;

While $x \neq 1$ **do**

If $x = \dfrac{u}{v}$ for some $(u,v) \in \Omega$, then $b := \mathrm{Val}_2(\dfrac{1}{x} - 1)$

else choose an integer $b \ge 1$ with $\Pr[b = k] = 2^{-k}$;

$y := \dfrac{1}{2^b}(\dfrac{1}{x} - 1)$;

if $y < 1$ then $x := y$ else $x := \dfrac{1}{y}$;

Brent studies the average number of internal loops and introduces the operator $\mathcal{B}_2$

$$\mathcal{B}_2[f](x) := \sum_{b \ge 1} \left(\frac{1}{1+2^b x}\right)^2 f\left(\frac{1}{1+2^b x}\right) + \sum_{b \ge 1} \left(\frac{1}{x+2^b}\right)^2 f\left(\frac{x}{x+2^b}\right),$$

that transforms densities: if f is the initial density on $]0,1]$, then $\mathcal{B}_2[f]$ is the density on $]0,1]$ after one internal step of the algorithm, and $\mathcal{B}_2^\ell[f]$ is the density on $]0,1]$ after ℓ internal steps of the algorithm. Brent conjectures that there exists a limit density for the algorithm, i.e. a function g_2 such that

$$\lim_{\ell \to \infty} \mathcal{B}_2^\ell[f] = g_2, \tag{10}$$

then he makes an (essential) heuristic hypothesis: the rationals have a "typical" behaviour inside the reals, so that the restriction to the rationals of the limit (real) density defined in (10) is also the limit (rational) density. Then, he can prove the following

Theorem (Brent). *Under the conjecture and the heuristic hypothesis, the average number K_N or $\tilde{K}_N$ of total iterations of the Binary Euclidean Algorithm on the set $\Omega_N := \{(u,v);\ u, v \,\text{odd},\ 0 < u \le v \le N\}$, or on the set $\tilde{\Omega}_N := \{(u,v);\ u, v\,\text{odd},\ 0 < u \le v \le N, \gcd(u,v) = 1\}$ satisfies*

$$\tilde{K}_N \sim K_N \sim \frac{1}{M} \ \log N \qquad \textit{with} \quad M = \log 2 - \frac{1}{2}\int_0^1 \log(1-x)\, g_2(x) dx. \tag{11}$$

Here, g_2 denotes the fixed point of the operator $\mathcal{B}_2$

$$\mathcal{B}_2[f](x) := \sum_{b \ge 1} \left(\frac{1}{1+2^b x}\right)^2 f\left(\frac{1}{1+2^b x}\right) + \sum_{b \ge 1} \left(\frac{1}{x+2^b}\right)^2 f\left(\frac{x}{x+2^b}\right), \tag{12}$$

such that $\int_0^1 g_2(t)dt = 1$.

So, the main differences between both methods, Brent's method and ours, are the following:

(i) We operate a *proven* transfer from the continuous model to the discrete model by means of Tauberian Theorems.

(ii) Brent's operator

$$\mathcal{B}_s[f](x) := \sum_{b\geq 1} \Big(\frac{1}{1+2^b x}\Big)^s f\Big(\frac{1}{1+2^b x}\Big) + \sum_{b\geq 1} \Big(\frac{1}{x+2^b}\Big)^s f\Big(\frac{x}{x+2^b}\Big), \tag{13}$$

is *less powerful* than the operator $\mathcal{V}_s$ since it can be used only in the study of the second parameter (the total number of steps).

(iii) For proving Brent's conjecture, one can try to exhibit a "spectral gap" for $\mathcal{B}_s$. This seems difficult because it is not clear for instance whether $\mathcal{B}_s$ is compact on a suitable Banach space: another expression of $\mathcal{B}_s$, namely

$$\mathcal{B}_s[f](x) = \mathcal{U}_s[f](x) + \frac{1}{x^s}\mathcal{U}_s[f](\frac{1}{x}), \qquad \text{with} \qquad \mathcal{U}_s[f](x) := \sum_{k\geq 1} \Big(\frac{1}{1+2^k x}\Big)^s f\Big(\frac{1}{1+2^k x}\Big), \tag{14}$$

involves both x and $1/x$ and suggests that the behaviour of $\mathcal{B}_s$ is more intricate.

Plan of the paper. We first introduce the generating functions that are involved in the study of the first parameter (the height), and we exhibit their link with the Ruelle operator $\mathcal{V}_s$. Then, we state precisely the properties of the operator $\mathcal{V}_s$ on a suitable Banach space (compacity, nuclearity, positivity), and we show that the hypotheses of Tauberian Theorems are fulfilled. We deduce the first result on the average behaviour of the height. Then, we show how to slightly modify the previous framework so as to study the other parameters linked to the numerators and the denominators of the binary continued fraction. The properties of the operator $\mathcal{V}_s$ which have been previously stated allow us to easily obtain the asymptotic behaviour of their average values. Finally, we relate our work with Brent's paper and we describe the principles on which numerical computations could be performed.

An extended abstract of these results (without proofs) has been presented at ANTS'98 [Va6].

1. The average height of a binary continued fraction.

Here, we introduce the generating functions that describe the height of binary continued fraction and we relate them to the dynamical operator. Consider the following sets

$$\Omega := \{(u,v);\ u,v\,\text{odd},\ 0 < u \leq v\},\quad \tilde{\Omega} := \{(u,v);\ u,v\,\text{odd},\ 0 < u \leq v, \gcd(u,v)=1\},$$

$$\Omega_N := \{(u,v);\ u,v\,\text{odd},\ 0 < u \leq v \leq N\},$$

$$\tilde{\Omega}_N := \{(u,v);\ u,v\,\text{odd},\ 0 < u \leq v \leq N,\ \gcd(u,v)=1\}, \tag{15}$$

for the possible inputs of the Binary Euclidean algorithm, and we denote by $\Omega^{[\ell]}$, $\tilde{\Omega}^{[\ell]}$, $\Omega_N^{[\ell]}$, $\tilde{\Omega}_N^{[\ell]}$ the subsets of Ω, $\tilde{\Omega}$, Ω_N, $\tilde{\Omega}_N$ for which the algorithm performs exactly ℓ exchanges. Equivalently, the height of the binary continued fraction is equal to ℓ. We study the average number of exchanges

$\tilde{E}_N$ of the algorithm on $\tilde{\Omega}_N$ and the average number of iterations E_N of the algorithm on Ω_N. These quantities satisfy

$$\tilde{E}_N := \frac{1}{|\tilde{\Omega}_N|} \sum_{\ell \geq 0} \ell \ |\tilde{\Omega}_N^{[\ell]}| \qquad E_N := \frac{1}{|\Omega_N|} \sum_{\ell \geq 0} \ell \ |\Omega_N^{[\ell]}|, \tag{16}$$

and we wish to evaluate their asymptotic behaviour (for $N \to \infty$). The operator $\mathcal{V}_s$ defined in (9) plays a central rôle for evaluating the costs. It can be written, in a shorthand notation, as

$$\mathcal{V}_s[f](x) := \sum_{h \in \mathcal{L}} \frac{1}{D[h](x)^s} \ f \circ h(x). \tag{17}$$

Here, $D[h]$ denotes the denominator of the linear fractional transformation (LFT) h, defined for $h(x) = (ax+b)/(cx+d)$ with a, b, c, d coprime integers by

$$D[h](x) = |cx + d| = \sqrt{\frac{|\det h|}{|h'(x)|}}, \tag{18}$$

that can be extended in a natural way on a complex neighborhood of $]0, 1]$. The sum is taken over the set $\mathcal{L}$ that contains all the linear fractional transformations h which express the possible antecedents of a rational x as a function of x; These h are defined in (4) and are called LFT's of height 1. More generally, the multiplicativity of D, defined in (18),

$$D[h \circ g](x) = D[h](g(x)) \, D[g](x)$$

proves that the ℓ-th iterate of $\mathcal{V}_s$ uses all the LFT's h of $\mathcal{L}^\ell$; they are of the form $h = h_1 \circ h_2 \circ \ldots \circ h_\ell$ with $h_i \in \mathcal{L}$ and express all the ℓ-th possible iterates of x_0 as a function of x_0. These LFT's are called LFT's of height ℓ, and

$$\mathcal{V}_s^\ell[f](x) := \sum_{h \in \mathcal{L}^\ell} \frac{1}{D[h](x)^s} \ f \circ h(x). \tag{19}$$

Since the ℓ-th iterate of $\mathcal{V}_s$ generates all the LFT's of height ℓ, the operator $\mathcal{V}_s$ can be viewed as a "generating" operator, and this explains why usual generating functions can be easily expressed with it.

Proposition 1. *The average number of exchanges $\tilde{E}_N$ of the Binary Euclidean algorithm on $\tilde{\Omega}_N$ is a ratio where the numerator and the denominator involves the partial sums of the Dirichlet series $F(s)$ and $G(s)$, defined from the quasi–inverse $\Lambda_s := (I - \mathcal{V}_s)^{-1}$,*

$$F(s) := \Lambda_s[1](1) = (I - \mathcal{V}_s)^{-1}[1](1), \qquad G(s) := \Lambda_s^2 \circ \mathcal{V}_s[1](1) = (I - \mathcal{V}_s)^{-2} \circ \mathcal{V}_s[1](1).$$

In the same vein, the average number of exchanges E_N of the algorithm on Ω_N is a ratio where the numerator and the denominator involves the partial sums of the Dirichlet series $\tilde{\zeta}(s)F(s)$, and $\tilde{\zeta}(s)G(s)$, where $\tilde{\zeta}(s)$ is the Riemann function relative to odd numbers,

$$\tilde{\zeta}(s) := \sum_{v \text{ odd}} \frac{1}{v^s} = (1 - \frac{1}{2^s})\zeta(s). \tag{20}$$

Proof. Consider an element (u,v) of $\tilde{\Omega}^{[\ell]}$ $(\ell \geq 0)$; since the Binary Euclidean algorithm performs ℓ exchanges on this input, there exists exactly one linear fractional transformation h of height ℓ such that $u/v = h(1)$. Then, from (19) and for any $\ell \geq 0$,

$$\mathcal{V}_s^\ell[f](1) = \sum_{h \in \mathcal{L}^\ell} \frac{1}{D[h](1)^s} \; f \circ h(1) = \sum_{(u,v) \in \tilde{\Omega}^{[\ell]}} \frac{1}{v^s} f(\frac{u}{v}). \tag{21}$$

When using the Riemann series $\tilde{\zeta}$ relative to odd numbers defined in (20), we obtain, for (21), a sum over $\Omega^{[\ell]}$,

$$\mathcal{V}_s^\ell[f](1) = \frac{1}{\tilde{\zeta}(s)} \sum_{(u,v) \in \Omega^{[\ell]}} \frac{1}{v^s} f(\frac{u}{v}). \tag{22}$$

Now, the sum over all the possible heights $(\ell \geq 0)$ of (21) or (22) gives two formal expressions of the quasi–inverse

$$(I - w\mathcal{V}_s)^{-1}[f](1) = \sum_{\ell \geq 0} w^\ell \, \mathcal{V}_s^\ell[f](1) = \sum_{\ell \geq 0} w^\ell \sum_{(u,v) \in \tilde{\Omega}^{[\ell]}} \frac{1}{v^s} f(\frac{u}{v}) = \frac{1}{\tilde{\zeta}(s)} \sum_{\ell \geq 0} w^\ell \sum_{(u,v) \in \Omega^{[\ell]}} \frac{1}{v^s} f(\frac{u}{v}). \tag{23}$$

The differentiation of (23) with respect to w gives

$$(I - w\mathcal{V}_s)^{-2} \circ \mathcal{V}_s[f](1) = \sum_{\ell \geq 1} \ell w^{\ell-1} \sum_{(u,v) \in \tilde{\Omega}^{[\ell]}} \frac{1}{v^s} f(\frac{u}{v}) = \frac{1}{\tilde{\zeta}(s)} \sum_{\ell \geq 1} \ell w^{\ell-1} \sum_{(u,v) \in \Omega^{[\ell]}} \frac{1}{v^s} f(\frac{u}{v}). \tag{24}$$

We now choose $f = 1$, and $w = 1$, and we denote by $\tilde{\nu}_v^{[\ell]}$ (resp. $\nu_v^{[\ell]}$) the number of elements of $\tilde{\Omega}^{[\ell]}$ (resp. $\Omega^{[\ell]}$) whose second component is equal to v; then, the average numbers of iterations described in (16) are of the form

$$\tilde{E}_N = \frac{\sum_{\ell \geq 0} \ell \; \sum_{v \leq N} \tilde{\nu}_v^{[\ell]}}{\sum_{\ell \geq 0} \sum_{v \leq N} \tilde{\nu}_v^{[\ell]}}, \qquad E_N = \frac{\sum_{\ell \geq 0} \ell \; \sum_{v \leq N} \nu_v^{[\ell]}}{\sum_{\ell \geq 0} \sum_{v \leq N} \nu_v^{[\ell]}}. \tag{25}$$

On the other hand, the Dirichlet series that generate the quantities $\nu_v^{[\ell]}$ and $\tilde{\nu}_v^{[\ell]}$ to be studied,

$$F(s) := \sum_{v \geq 1} \frac{1}{v^s} \sum_{\ell \geq 0} \tilde{\nu}_v^{[\ell]} = \frac{1}{\tilde{\zeta}(s)} \sum_{v \geq 1} \frac{1}{v^s} \sum_{\ell \geq 0} \nu_v^{[\ell]}, \tag{26}$$

$$G(s) := \sum_{v \geq 1} \frac{1}{v^s} \sum_{\ell \geq 0} \ell \; \tilde{\nu}_v^{[\ell]} = \frac{1}{\tilde{\zeta}(s)} \sum_{v \geq 1} \frac{1}{v^s} \sum_{\ell \geq 0} \ell \; \nu_v^{[\ell]}, \tag{27}$$

are expressed in terms of the operator $\mathcal{V}_s$ as

$$F(s) := (I - \mathcal{V}_s)^{-1}[1](1) \qquad G(s) := (I - \mathcal{V}_s)^{-2} \circ \mathcal{V}_s[1](1). \tag{28}$$

Relations (25), (26), (27), (28) then prove the proposition. ■

Thus, the asymptotic evaluations of $\tilde{E}_N$ and E_N (for $N \to \infty$) are possible if we can apply the following Tauberian theorem [De] to the Dirichlet series $F(s)$, $\tilde{\zeta}(s)F(s)$, $G(s)$, $\tilde{\zeta}(s)G(s)$.

Tauberian Theorem. [Delange] *Let $F(s)$ be a Dirichlet series with non negative coefficients such that $F(s)$ converges for $\Re(s) > \sigma > 0$. Assume that*

(i) $F(s)$ is analytic on $\Re(s) = \sigma, s \neq \sigma$, and

(ii) for some $\gamma \geq 0$

$$F(s) = \frac{A(s)}{(s-\sigma)^{\gamma+1}} + C(s),$$

where A, C are analytic at σ, with $A(\sigma) \neq 0$.

Then, as $N \to \infty$,

$$\sum_{n \leq N} a_n = \frac{A(\sigma)}{\sigma\Gamma(\gamma+1)} \; N^\sigma \log^\gamma N \quad [1 + \epsilon(N)], \quad \epsilon(N) \to 0.$$

In the remainder of the paper, we show that the Tauberian Theorem applies to the Dirichlet series defined in (26) and (27) with $\sigma = 2$, and respectively $\gamma = 0$ and $\gamma = 1$. This will prove the logarithmic behaviour of the height. We first examine the case of function $F(s)$ defined in (26).

Lemma 1. *The Tauberian Theorem applies to $F(s)$ and $\tilde\zeta(s)F(s)$ with $\sigma = 2$ and $\gamma = 0$. It applies more generally (with the same parameters) to $\Lambda_s[f](1)$ for functions f that satisfy $|xf'(x)| \leq K$ for $x \in]0, 1]$.*

Proof. First, the Dirichlet series $F(s) := \Lambda_s[1](1)$ defined in (26) is closely linked to the $\tilde\zeta$ function defined in (22),

$$F(s) := (I - \mathcal{V}_s)^{-1}[1](1) = 1 + \frac{1}{2\tilde\zeta(s)} \sum_{v \text{ odd}} \frac{v-1}{v^s} = \frac{1}{2}[\frac{\tilde\zeta(s-1)}{\tilde\zeta(s)} + 1]. \tag{29}$$

It is then clear that the Tauberian Theorem applies to $F(s)$ and $\tilde\zeta(s)F(s)$, with $\sigma = 2$ and $w = 0$. More generally, the Dirichlet series $\Lambda_s[f](1) := (I - \mathcal{V}_s)^{-1}[f](1)$ can also be expressed, with (23), as a function of $\tilde\zeta(s-1)/\tilde\zeta(s)$. If $xf'(x)$ is bounded in $]0, 1]$, the comparison between the Riemann sum and the integral gives

$$\sum_{\substack{u \text{ odd} \\ u<v}} \frac{1}{v} f(\frac{u}{v}) = \frac{1}{2} \int_0^1 f(x)dx + O(\frac{\log v}{v}),$$

where the constant in the O depends on f. Then

$$\Lambda_s[f](1) := (I - \mathcal{V}_s)^{-1}[f](1) = \frac{\tilde\zeta(s-1)}{2\tilde\zeta(s)} \int_0^1 f(x)dx + \frac{R(f,s)}{\tilde\zeta(s)} \;, \tag{30}$$

where $R(f, s)$ has no poles on the plane $\{s \,|\, \Re(s) > 1\}$. ■

2. The operator $\mathcal{V}_s$.

If we wish to apply the Tauberian Theorem to $G(s)$ and $\tilde\zeta(s)G(s)$, with $\sigma = 2$ and $\gamma = 1$, we need to study the operator $\mathcal{V}_s$ when acting in a suitable functional space. It appears that the convenient space is a Hardy space $\mathcal{H}^2(\mathcal{D})$ relative to some disk $\mathcal{D}$ that contains the interval $]0, 1]$. On this space, the operator is compact, even nuclear, and its spectrum is thus discrete (Proposition 2). Furthermore, for real values of the parameter s, the operator satisfies strong positivity properties that entail the existence of dominant spectral objects (dominant eigenvalue, dominant eigenvector, projection on the dominant eigensubspace) (Proposition 4). Finally, we exhibit a maximum property of the spectral radius (Proposition 5). All these properties allow us to prove that the hypotheses of the Tauberian Theorems are fulfilled (Proposition 6), and we thus obtain the logarithmic behaviour of the height of the binary continued fraction (Theorem 1).

The operator $\mathcal{V}_2$ does not act on the Banach space of analytic functions defined in a complex neighborhood of $[0,1]$, since, for instance, the function $\mathcal{V}_2[1]$ is not bounded in the neighborhood of 0. On the other side, the operator $\mathcal{V}_2$ acts on the Banach space $\mathcal{L}^1([0,1])$, since, one has:

$$\int_0^1 |\mathcal{V}_2[f](t)|dt \leq \sum_{k\geq 1} \sum_{\substack{a \text{ odd}, \\ 1\leq a<2^k}} \int_0^1 (\frac{1}{a+2^k t})^2 \; |f(\frac{1}{a+2^k t})|dt.$$

Now, using in each term the change of variable defined by the LFT's of (4), $h : x \to 1/(a+2^k x)$, and denoting by F the integral of $|f|$ such that $F(0)=0$,

$$\int_0^1 |\mathcal{V}_2[f](t)|dt \leq \sum_{k\geq 1} \sum_{\substack{a \text{ odd}, \\ 1\leq a<2^k}} \frac{1}{2^k}[F(\frac{1}{a}) - F(\frac{1}{a+2^k})] = F(1) = \int_0^1 |f(t)|dt. \tag{31}$$

But the space $\mathcal{L}^1([0,1])$ seems too large, and, in the following, the main problem is to find a suitable Banach space "between" analytic functions and integrable ones, on which the operators $\mathcal{V}_s$ act (for s near 2) with "good" spectral properties. The Hardy space relative to a suitable disk containing the interval $]0,1[$ will be convenient.

We consider the open disk $\mathcal{D}$ of diameter $\mathcal{J} :=]0,2\rho[$ defined by some fixed number ρ with $(1/2) < \rho < 1$, the boundary δ of $\mathcal{D}$, and the circle δ_r of center ρ and radius r. We work with the space of the functions defined in $\mathcal{D}$, that are analytic inside $\mathcal{D}$ and such that the quantity

$$||f||_2^2 = \text{Sup}_{\;0\leq r<\rho} \; \frac{1}{2\pi\rho} \int_{\delta_r} |f(z)|^2 \; |dz|$$

is finite. Such functions f are thus defined almost everywhere on δ, and one has also

$$||f||_2^2 := \frac{1}{2\pi\rho} \int_{\delta} |f(z)|^2 \; |dz|. \tag{32}$$

This set of functions is classically denoted by $\mathcal{H}^2(\mathcal{D})$ and is called the Hardy space of order two associated to the disk $\mathcal{D}$. The quantity $||f||_2$ defined in (32) is a norm which endows $\mathcal{H}^2(\mathcal{D})$ with a Banach space structure, and a Hilbert space structure. The Fejer-Riesz inequality [Du]

$$\int_0^1 |f(x)|^2 dx \leq \pi ||f||_2^2$$

proves that the restriction of an element $f \in \mathcal{H}^2(\mathcal{D})$ to the unit interval belongs to $\mathcal{L}^2([0,1])$, and thus to $\mathcal{L}^1([0,1])$.

The operator $\mathcal{V}_s$ is the sum of the component operators $\mathcal{V}_{s,a,k}$

$$\mathcal{V}_{s,a,k}[f](z) := (\frac{1}{a+2^k z})^s f(\frac{1}{a+2^k z}). \tag{33}$$

Each component operator is a so–called composition operator of the form $f \to h^s\ f \circ h$, where h defined in (4) is an analytic function which maps $\mathcal{D}$ inside $\mathcal{D}$. Such operators are studied in an extensive way by several authors (Schwartz [Sc], Shapiro and Taylor [ST], Shapiro [Sh1], [Sh2]) who relate the properties of the operator and the position of the image $h(\mathcal{D})$ with respect to the boundary of $\mathcal{D}$. More precisely, they prove the following fact: when acting on $\mathcal{H}^2(\mathcal{D})$, a composition operator is compact as soon as h maps the closure $\bar{\mathcal{D}}$ of the disk $\mathcal{D}$ inside $\mathcal{D}$. It is then moreover nuclear of order 0 (in the sense of Grothendieck cf [Gr1], [Gr2]). Here, since ρ is chosen strictly greater than $1/2$, each component operator is thus compact and nuclear of order 0, and we prove now that the same properties hold for the operator $\mathcal{V}_s$ itself:

Proposition 2. *For $\Re(s) > 3/2$, the operator $\mathcal{V}_s$ acts on the space $\mathcal{H}^2(\mathcal{D})$ and is compact on this space. Its spectrum is thus discrete with an accumulation point at 0. Moreover, $\mathcal{V}_s$ is nuclear of order 0 on this space.*

Proof. In the proof, we make use of an inequality due to Gabriel ([Ga], quoted in [Sh]).

Gabriel's inequality. *If γ is a convex curve in the closed disk $\bar{\mathcal{D}}$, then, for every $f \in \mathcal{H}^2(\mathcal{D})$, one has:*

$$\int_\gamma |f(z)|^2\ |dz| \leq 2 \int_\delta |f(z)|^2\ |dz|. \tag{34}$$

We use also the following property [Sc]:

Property. *An operator T is compact on $\mathcal{H}^2(\mathcal{D})$ iff for every norm bounded sequence (f_n) in $\mathcal{H}^2(\mathcal{D})$ which converges to zero uniformly on compact subsets of $\mathcal{D}$, the image sequence $T(f_n)$ converges to zero in norm.*

Since each LFT $z \to 1/(a+2^k z)$ maps $\mathcal{D}$ inside itself (for $a < 2^k$), each component operator $\mathcal{V}_{s,a,k}$ acts on $\mathcal{H}^2(\mathcal{D})$. Using the change of variables defined by the LFT h,

$$h : z \to \frac{1}{a+2^k z}, \tag{35}$$

we obtain for each component operator defined in (33),

$$||\mathcal{V}_{s,a,k}[f]||_2^2 = \frac{1}{2\pi\rho}\ \frac{1}{2^k} \int_{h(\delta)} |u|^{2\sigma-2}\ |f(u)|^2\ |du|, \tag{36}$$

with $\sigma := \Re(s)$. For $\sigma > 1$, one has, with (34),

$$||\mathcal{V}_{s,a,k}[f]||_2^2 \leq \frac{1}{2\pi\rho}\ \frac{1}{2^k}(\frac{1}{a})^{2\sigma-2} \int_{h(\delta)} |f(u)|^2\ |du| \leq (\frac{1}{a})^{2\sigma-2}\frac{2}{2^k}\ ||f||_2^2. \tag{37}$$

Then, the operator $\mathcal{V}_{s,a,k}$ is bounded, and its norm satisfies

$$||\mathcal{V}_{s,a,k}|| \leq (\frac{1}{a})^{\sigma-1}\frac{1}{(\sqrt{2})^{k-1}}. \tag{38}$$

The LFT defined in (35) maps the disk $\bar{\mathcal{D}}$ inside $\mathcal{D}$ (this is why ρ is chosen greater than $1/2$), so that the property, together with inequality (37), shows that $\mathcal{V}_{s,a,k}$ is compact.

Now, the operator $\mathcal{V}_s$ is itself bounded and compact, as the sum of the compact operators $\mathcal{V}_{s,a,k}$ (for indices (a,k) such that $k > k_a$). This sum forms a convergent series for $\sigma > (3/2)$, since the norm of $\mathcal{V}_s$ satisfies, with (38),

$$||\mathcal{V}_s|| \leq \sum_{a\,\mathrm{odd}} (\frac{1}{a})^{\sigma-1} \sum_{k>k_a} \frac{1}{(\sqrt{2})^{k-1}}. \tag{39}$$

Since k_a is the integer part of $\log_2 a$, the internal sum is at most equal to

$$\frac{2}{\sqrt{2}-1}\,\frac{1}{\sqrt{a}},$$

and, finally, for $\sigma > (3/2)$,

$$||\mathcal{V}_s|| \leq \frac{2}{\sqrt{2}-1}\;\tilde{\zeta}(\sigma - \frac{1}{2}). \tag{40}$$

We study now the nuclearity of $\mathcal{V}_s$. We first recall this notion introduced by Grothendieck [Gr1], [Gr2]. Let B be a Banach space and $B^\star$ its dual space. An operator $\mathcal{M} : B \to B$ is nuclear of order 0 if it admits a representation

$$\mathcal{M}[f] = \sum_{i\in I} \mu_i\; e_i^\star(f)\; e_i \quad \text{for all } f \in B,$$

with $e_i \in B$, $e_i^\star \in B^\star$ such that $||e_i|| = ||e_i^\star|| = 1$ and the μ_i are p-summable for all $p > 0$ (i.e., $\sum |\mu_i|^p < +\infty$). Most of matrix algebra can be extended to such operators; in particular, one can define their trace, and also the analogue of their characteristic polynomial known as the Fredholm determinant.
From Shapiro's work, we know that each component operator $\mathcal{V}_{s,a,k}$ defined in (33) is nuclear on $\mathcal{H}^2(\mathcal{D})$ (for $2^k > a$). More precisely, its spectrum consists in a geometric progression which involves the unique fixed point $x_{a,k}$ of the LFT $x \to 1/(a + 2^k x)$ inside $\mathcal{D}$, under the form

$$\mathrm{Sp}\,\mathcal{V}_{s,a,k} = \{\lambda_n := x_{a,k}^s\;(2^k\,x_{a,k}^2)^n, \quad n \in \mathbf{N}\}.$$

The inequality $x_{a,k}^2 \leq 2^{-k}$ proves that the sequence $(\lambda_n)_{n\in\mathbf{N}}$ is element of ℓ^p for every $p > 0$; in particular, the trace is well-defined and satisfies

$$\mathrm{Tr}\,\mathcal{V}_{s,a,k} = \frac{x_{a,k}^{s-1}}{a}. \tag{41}$$

Then each operator $\mathcal{V}_{s,a,k}$ is nuclear of order 0. The inequality $x_{a,k}^2 \leq 2^{-k}$ proves that the expressions in (41) define a convergent series when summing over indices (a,k) that satisfy $a \leq 2^k$. Then $\mathcal{V}_s$ is also nuclear of order 0 on $\mathcal{H}^2(\mathcal{D})$. ■

It appears that the image of the space $\mathcal{H}^2(\mathcal{D})$ by the operator $\mathcal{V}_s$ is contained in a very particular subspace $\mathcal{G}$ of $\mathcal{H}^2(\mathcal{D})$, where singularities are concentrated at $z = 0$ and involve only logarithmic terms proportional to $\log z$ or periodic terms satisfying $C(z) = C(2z)$. In particular, all the eigenfunctions of $\mathcal{V}_s$ belong to $\mathcal{G}$, and satisfy the hypothesis of Lemma 1. These facts will play a central rôle in the proofs of Propositions 4 and 5.

Proposition 3. *The image of the space $\mathcal{H}^2(\mathcal{D})$ by the operator $\mathcal{V}_s$ is contained in the subset $\mathcal{G}$ of $\mathcal{H}^2(\mathcal{D})$,*

$$\mathcal{G} := \{f \ \mid f \in \mathcal{H}^2(\mathcal{D}), \quad f(z) = A\log_2 z + B(z) + C(z)\}$$

where B and C are analytic inside $\mathcal{D}$; furthermore, B is continuous in $\bar{\mathcal{D}}$ and satisfies $B(0) = 0$; C is continuous inside $\bar{\mathcal{D}} \setminus \{0\}$, satisfies $C(2z) = C(z)$, and is bounded on the real segment $\mathcal{J}$.

Proof. We remark that the operator $\mathcal{V}_s$ can be expressed in terms of the operator $\mathcal{U}_s$ only

$$\mathcal{U}_s[f](z) := \sum_{k\geq 1} (\frac{1}{1+2^k z})^s f(\frac{1}{1+2^k z}),$$

under the form

$$\mathcal{V}_s[f](z) = \sum_{a \text{ odd}} \frac{1}{a^s}\, \mathcal{U}_s[f_a]\ (\frac{2^{k_a}}{a} z), \tag{42}$$

where f_a is defined by $f_a(x) := f(x/a)$, and k_a is the integer part of $\log_2 a$. We thus begin by proving that $\mathcal{U}_s[f]$ is element of $\mathcal{G}$ when f is element of $\mathcal{H}^2(\mathcal{D})$, with precise expressions of components $\tilde{A}$, $\tilde{B}$ and $\tilde{C}$ of $\mathcal{U}_s[f]$ as functions of f. The important relation

$$\mathcal{U}_s[f](z) = \frac{1}{(1+2z)^s} f(\frac{1}{1+2z}) + \mathcal{U}_s[f](2z) \tag{43}$$

first shows that $\tilde{A} = -f(1)$, then gives the precise expression of $\tilde{B}$,

$$\tilde{B}(z) = \sum_{k\geq 0} [f(1) - \frac{1}{(1+2^{-k}z)^s} f(\frac{1}{1+2^{-k}z})]$$

which shows the continuity of $\tilde{B}$ inside the disk $\bar{\mathcal{D}}$. Then

$$\tilde{C}(z) := \mathcal{U}_s[f](z) - \tilde{A}\log_2 z - \tilde{B}(z)$$

is a function of $\mathcal{H}^2(\mathcal{D})$ that satisfies

$$\tilde{C}(z) = f(1)\log_2 z + \sum_{k\leq 0} [\frac{1}{(1+2^k z)^s} f(\frac{1}{1+2^k z}) - f(1)] + \sum_{k\geq 1} \frac{1}{(1+2^k z)^s} f(\frac{1}{1+2^k z})$$

and then $\tilde{C}(z) = \tilde{C}(2z)$.

We now come back to the operator $\mathcal{V}_s$ itself, with (42): we provide precise expressions of components A, B and C of $\mathcal{V}_s[f]$ as functions of f. First,

$$A = -\sum_{a \text{ odd}} \frac{1}{a^s} f(\frac{1}{a});$$

Second, $B(z) = \displaystyle\sum_{a \text{ odd}} \sum_{k\geq 0} [\frac{1}{a^s} f(\frac{1}{a}) - \frac{1}{(a+2^{k_a-k}z)^s} f(\frac{1}{a+2^{k_a-k}z})]$.

Remark that these expressions define convergent series because the restriction of f to $[0,1]$ belongs to $\mathcal{L}^2([0,1])$. Finally,

$$C(z) := \mathcal{V}_s[f](z) - A\log_2 z - B(z)$$

satisfies $C(z) = C(2z)$. It is thus of the form

$$C(z) = \sum_{\ell\in\mathbf{Z}} c_\ell z^{s_\ell} \qquad \text{with} \qquad s_\ell := \frac{2i\pi\ell}{\log 2}, \qquad \ell \in \mathbf{Z},$$

and, the expression

$$||z^{s_\ell}||_2^2 = \int_{-\pi/2}^{+\pi/2} \exp[\frac{-4\pi\ell}{\log 2}\theta]\, d\theta = \frac{\log 2}{4\pi\ell}\,[\alpha^{2\ell} - \alpha^{-2\ell}] \ \text{ with } \ \alpha := \exp[\pi^2/\log 2],$$

shows that the series $\sum_{\ell\in\mathbf{Z}} |c_\ell|\, z^{|\ell|}$ has a radius of convergence at least equal to α. In particular, (c_ℓ) belongs to ℓ^1 and C is bounded on $\bar{\mathcal{J}}$. ■

We describe now the spectral properties of the operator $\mathcal{V}_s : \mathcal{H}^2(\mathcal{D}) \to \mathcal{H}^2(\mathcal{D})$, for real values of parameter s. We show strong positivity properties for this operator, so that we can use Krasnoselsky's theorem, and exhibit dominant spectral properties for operators $\mathcal{V}_s$ when restricted to real values of parameter s.

Proposition 4. *For real $s > 3/2$, the operator $\mathcal{V}_s : \mathcal{H}^2(\mathcal{D}) \to \mathcal{H}^2(\mathcal{D})$ has a unique positive dominant eigenvalue $\lambda(s)$. For $s = 2$, one has $\lambda(s) = 1$.*

Proof. We follow the lines of Mayer's work [Ma$_i$] that we adapt in our context. We consider the real Banach space $\mathcal{H}_{\mathbf{R}}$ formed with elements f of $\mathcal{H}^2(\mathcal{D})$ which are real on the real segment $\mathcal{J}$. For real s, $\mathcal{V}_s$ acts on $\mathcal{H}_{\mathbf{R}}$. We denote by $\mathcal{H}_+$ the subset of $\mathcal{H}_{\mathbf{R}}$ formed with elements f which are positive on the real segment $\mathcal{J}$. For real s, $\mathcal{V}_s$ acts on $\mathcal{H}_+$, and $\mathcal{H}_+ \subset \mathcal{H}_{\mathbf{R}}$ is a cone (proper and reproducing in the sense of Krasnoselsky). We recall that the cone $\mathcal{H}_+$ is proper if
(i) $\mu\mathcal{H}_+ \subset \mathcal{H}_+$ for $\mu > 0$
(ii) $\mathcal{H}_+ \cap -\mathcal{H}_+ = \{0\}$
and reproducing if $\mathcal{H}_{\mathbf{R}} = \mathcal{H}_+ - \mathcal{H}_+$.

Lemma 2. *The cone $\mathcal{H}_+$ is reproducing.*

Proof. We prove that any function f of $\mathcal{H}_{\mathbf{R}}$ can be written as the difference of two functions of $\mathcal{H}_+$. Consider the set $\mathcal{Z}$ of the zeroes of f. It is denumerable. Moreover, since f belongs to $\mathcal{H}_{\mathbf{R}}$, f satisfies $f(\bar{z}) = \bar{f}(z)$ and the set $\mathcal{Z}$ is invariant by $z \to \bar{z}$. Recall that the Blaschke function (see for instance [Pa]) B associated to the set $\mathcal{Z}$ is an element of $\mathcal{H}_\infty(\mathcal{D})$, such that $||B||_\infty \le 1$, and whose set of zeroes is exactly $\mathcal{Z}$. Here, the Blaschke function satisfies $B(\bar{z}) = \bar{B}(z)$. Moreover, Riesz's Theorem proves the decomposition $f(z) = g(z)B(z)$ where $g(z)$ has no zeroes on $\mathcal{D}$ and $||g||_2 = ||f||_2$. In particular, g is real on the real segment $\mathcal{J}$ and keeps there the same sign. We may suppose it strictly positive on $\mathcal{J}$. (If not, we change g to $-g$ and B to $-B$). On the real segment $\mathcal{J}$, we have

$$g(x) = \frac{f(x)}{B(x)} = |\frac{f(x)}{B(x)}| \ge |f(x)| \ge -f(x),$$

and thus $f(x) + g(x) \ge 0$. Finally we obtain the decomposition $f(z) = [f(z) + g(z)] - g(z)$. ■

The interior of the cone, denoted by $\mathcal{H}_+^*$, is formed with elements f of $\mathcal{H}^2(\mathcal{D})$ which are strictly positive on the real segment $\mathcal{J}$. Since $\mathcal{J} \subset]0,2[$, the cone $\mathcal{H}_+^*$ contains the function

$$u_0(z) := 1 - \log_2 z \tag{44}$$

which plays the role of a reference function: it is a "typical" function of the set $\mathcal{G}$ of Proposition 3.

We show that the operator $\mathcal{V}_s$ is u_0–positive with respect to the cone $\mathcal{H}_+$: for any non-zero element f of $\mathcal{H}_+$, there exists an integer p such that $\mathcal{V}_s^p[f]$ is u_0 upper–bounded and u_0 lower–bounded; more precisely, there exist p and two constants α and β, strictly positive such that

$$\alpha\ u_0(x) \leq \mathcal{V}_s^p[f](x) \leq \beta\ u_0(x)$$

for any x in $\mathcal{J}$. The upper bound is clear since the components C are bounded on $\mathcal{J}$. For the lower bound, it is sufficient to prove the following result:

Lemma 3. *For real $s > 3/2$, for any non-zero element f of $\mathcal{H}_+$, there exists an integer p such that the function $\mathcal{V}_s^p[f]$ has a non-zero logarithmic component $A_p \log_2 z$.*

Proof. The relation

$$\mathcal{V}_s[f](z) - \mathcal{V}_s[f](2z) = \frac{1}{(1+2z)^s} f(\frac{1}{1+2z}) + \mathcal{V}_s[f](1+2z) \tag{45}$$

when applied at $z = 0$ proves that the logarithmic component A_1 of $\mathcal{V}_s[f]$ equals

$$-A_1 = f(1) + \mathcal{V}_s[f](1). \tag{46}$$

More generally, the component A_p of $\mathcal{V}_s^p[f]$ equals to

$$-A_p = \mathcal{V}_s^{p-1}[f](1) + \mathcal{V}_s^p[f](1).$$

If all the components A_p are zero, then all the terms $\mathcal{V}_s^p[f](1)$ are zero. The expressions (21) and the positivity of f show that f is identically zero on the rationals; since f is continuous on $\mathcal{J}$, f is zero. ■

Then, we use Krasnoselsky's theorem: Since $\mathcal{V}_s : \mathcal{H}_{\mathbf{R}} \rightarrow \mathcal{H}_{\mathbf{R}}$ is a compact u_0–positive operator with respect to the proper and reproducing cone $\mathcal{H}_+$, the restriction of $\mathcal{V}_s$ to the real Banach space $\mathcal{H}_{\mathbf{R}}$ has a unique positive dominant eigenvalue $\lambda(s)$ strictly positive. One can choose the dominant eigenvector f_s in the set $\mathcal{H}_+^* \cap \mathcal{G}$, which means that f_s is strictly positive on $\mathcal{J}$ and of the form $A\log_2(z) + B(z) + C(z)$. Moreover, a direct calculation using the nuclearity (and the trace formula) proven in Proposition 1 shows that the spectra of the two operators, the operator $\mathcal{V}_s : \mathcal{H}^2(\mathcal{D}) \rightarrow \mathcal{H}^2(\mathcal{D})$ and its restriction to $\mathcal{H}_{\mathbf{R}}$, are the same. Finally, the operator $\mathcal{V}_s : \mathcal{H}^2(\mathcal{D}) \rightarrow \mathcal{H}^2(\mathcal{D})$ has itself dominant spectral properties.

Consider now the special case $s = 2$. The relation (31)

$$\int_0^1 |\mathcal{V}_2[f](t)|dt \leq \int_0^1 |f(t)|dt$$

proves that any eigenvalue of $\mathcal{V}_2$ is at most 1 in absolute value. Furthermore, the equality

$$\int_0^1 |\mathcal{V}_2[f](t)|dt = \int_0^1 |f(t)|dt \tag{47}$$

holds for any element f of $\mathcal{H}_+^*$ and proves that $\mathcal{V}_2$ preserves probability distributions. When applied to the dominant eigenvector f_2, it proves that the dominant eigenvalue $\lambda(2)$ equals 1. ■

From Propositions 2 and 4, we deduce the existence of a spectral gap for $\mathcal{V}_s$.

Corollary 1. *For real $s > 3/2$, the operator $\mathcal{V}_s$ has on $\mathcal{H}^2(\mathcal{D})$ a "spectral gap": there is a gap between the dominant eigenvalue $\lambda(s)$ (which is positive and simple) and the remainder of the spectrum, i.e. the supremum*

$$\nu(s) := Sup\{|\mu| \mid \mu \in \mathrm{Sp}\,\mathcal{V}_s,\ \mu \neq \lambda(s)\}$$

is strictly less than $\lambda(s)$.

We prove now a maximum property for the spectral radius which appears to be analogous of those proven in [Fa], [Po] or [Va3] in other contexts.

Proposition 5. *For s complex on the punctured plane $\{\Re(s) \geq 2, s \neq 2\}$, the operator $\mathcal{V}_s : \mathcal{H}^2(\mathcal{D}) \to \mathcal{H}^2(\mathcal{D})$ has a spectral radius strictly less than 1.*

Proof. There are three main steps in the proof.
(i) On each line $\{\Re(s) = \sigma > 2\}$, any eigenvalue of $\mathcal{V}_s$ is less than $\lambda(\sigma)$ in absolute value.
(ii) On the line $\{\Re(s) = 2, s \neq 2\}$, any eigenvalue of $\mathcal{V}_s$ is strictly less than 1 in absolute value.
(iii) The function $\lambda(s)$ is strictly decreasing along the real axis.
(i) We denote by σ the real part of s. Let λ be an eigenvalue of $\mathcal{V}_s$ and $f \in \mathcal{G}$ an eigenvector relative to λ. One denotes by $f_\sigma \in \mathcal{G}$ the dominant eigenvector of $\mathcal{V}_\sigma$ relative to $\lambda(\sigma)$. Since f_σ is strictly positive on $\mathcal{J}$, it has a component A strictly negative (adapt the proof of Lemma 3); one chooses $A = -1$; furthermore, the function μ defined on $\mathcal{J}$ by

$$\mu(x) := \frac{f(x)}{f_\sigma(x)} \tag{48}$$

can be extended to $\bar{\mathcal{J}}$ and one may suppose that its modulus is at most equal to 1, and equal to 1 at x_0. If $x_0 \neq 0$, one has

$$|\lambda|\,|f(x_0)| = |\mathcal{V}_s[f](x_0)| \leq \sum_{h\in\mathcal{L}} \frac{1}{D[h](x_0)^\sigma}\ |f\circ h(x_0)| \leq \sum_{h\in\mathcal{L}} \frac{1}{D[h](x_0)^\sigma}\ f_\sigma \circ h(x_0) = \lambda(\sigma) f_\sigma(x_0), \tag{49}$$

and the definition of x_0 proves the inequality $|\lambda| \leq \lambda(\sigma)$. If $x_0 = 0$, the modulus of the logarithmic component of f_s equals 1; we obtain the same inequality as in (49) when choosing x_1 near 0

$$|\lambda|\ |f(x_1)| \leq \lambda(\sigma) f_\sigma(x_1) \qquad \text{and then} \qquad |\lambda|\,|\frac{f(x_1)}{\log_2 x_1}| \leq \lambda(\sigma)\frac{f_\sigma(x_1)}{|\log_2 x_1|}.$$

Then we take the limits of the two members for $x_1 \to 0$.
(ii) If we suppose now the equality $|\lambda| = \lambda(\sigma)$ and $x_0 \neq 0$, we deduce, for all $h \in \mathcal{L}$, the equality $|f\circ h(x_0)| = f_\sigma \circ h(x_0)$. Thus f is not bounded near 0, and its logarithmic component A is not zero; This is also true if $x_0 = 0$. The identity $-A = (1+\lambda)f(1)$ derived from (46) shows that $f(1)$ is not zero. We work now on the particular line $\{\Re(s) = 2, s \neq 2\}$. Suppose that s is on this line, f is an eigenvector of $\mathcal{V}_s$ relative to $\lambda = 1$, such that $f(1) \neq 0$. Then the function $s \to \Lambda_s[f](1) := (I - \mathcal{V}_s)^{-1}[f](1)$ is singular at the point s. From (30), this Dirichlet series is expressed as a function of $\tilde{\zeta}(s-1)/\tilde{\zeta}(s)$,

$$\Lambda_s[f](1) := (I - \mathcal{V}_s)^{-1}[f](1) = \frac{\tilde{\zeta}(s-1)}{2\tilde{\zeta}(s)} \int_0^1 f(x)dx + \frac{R(f,s)}{\tilde{\zeta}(s)}\ ,$$

where $R(f,s)$ has no poles on the plane $\{s \mid \Re(s) > 1\}$. Then $\Lambda_s[f](1)$ has no singularity on the line $\{s,\ \Re(s) = 2, s \neq 2\}$, since the only singularity of $\tilde{\zeta}(s-1)/\tilde{\zeta}(s)$ on the line $\{s,\ \Re(s) = 2\}$ is $s = 2$. (iii) The existence of the "spectral gap" proves also the equality

$$\lambda(s) = \lim_{\ell \to \infty} (\sum_{h \in \mathcal{L}^\ell} \frac{1}{D[h](1)^s})^{1/\ell}. \tag{50}$$

Amongst all the rationals of height ℓ, the rational which has the least denominator equals $(2^{\ell-1}+1)/(2^\ell+1)$. Then, for $h \in \mathcal{L}^\ell$, one has $D[h](1) > 2^\ell$, and we deduce

$$\lambda(s+t) \le (\frac{1}{2})^t\ \lambda(s) \ \text{ for any real numbers } s > 3/2 \text{ and } t > 0. \qquad \blacksquare$$

We finally prove that all the properties that we have established for $\mathcal{V}_s : \mathcal{H}^2(\mathcal{D}) \to \mathcal{H}^2(\mathcal{D})$ are sufficient to apply the Tauberian theorems.

Proposition 6. *The conditions of the Tauberian Theorem hold for $G(s)$ and $\tilde{\zeta}(s)G(s)$, with $\sigma = 2$ and $\gamma = 1$.*

Proof. Proposition 5 shows that the quasi–inverse operator Λ_s is regular in the punctured plane $\Re(s) \ge 2, s \neq 2$, and the hypothesis (i) of the Theorem is fulfilled.
Consider now the hypothesis (ii). Corollary 1 proves that the operator $\mathcal{V}_2 : \mathcal{H}^2(\mathcal{D}) \to \mathcal{H}^2(\mathcal{D})$ has a spectral gap. Then, it admits a spectral decomposition of the form $\mathcal{P}_2 + \mathcal{N}_2$, where $\mathcal{P}_2$ is the projection on the dominant eigensubspace. By Perturbation theory, this decomposition extends for $\mathcal{V}_s$ to a (complex) neighborood of $s = 2$, the dominant eigenvalue $\lambda(s)$ is analytic there, and one has, for all $\ell \ge 1$, and for $z \in \mathcal{D}$,

$$\mathcal{V}_s^\ell[f](z) = \lambda(s)^\ell f_s(z) e_s[f] + \mathcal{N}_s^\ell[f](z) \tag{51}$$

where f_s is the dominant eigenvector of $\mathcal{V}_s$ and e_s the projector on the dominant eigensubspace, with the normalization condition $e_s[f_s] = 1$. The corresponding projector e_2 satisfies the equality $e_2[f] = \int_0^1 f(x)dx$. This results from the equalities (47) and (51). One deduces from (51) expressions for the powers of the quasi–inverse

$$\Lambda_s^p[f](z) := (I - \mathcal{V}_s)^{-p}[f](z) = \frac{f_s(z)e_s[f]}{(1-\lambda(s))^p} + (I - \mathcal{N}_s)^{-p}[f](z). \tag{52}$$

Now, using the derivability of $s \to \lambda(s)$ at $s = 2$ and the equality $e_2[f] = \int_0^1 f(x)dx$, we obtain the decomposition of the Dirichlet series of Proposition 1 near $s = 2$

$$F(s) := \Lambda_s[1](1) = \frac{-1}{\lambda'(2)} \frac{f_2(1)}{(s-2)} + C(s), \tag{53}$$

and

$$G(s) := \Lambda_s^2 \circ \mathcal{V}_s[1](1) = \frac{1}{\lambda'(2)^2} \frac{f_2(1)}{(s-2)^2} + D(s), \tag{54}$$

where $C(s)$ and $D(s)$ are analytic at $s = 2$. Then $G(s)$ satisfies the hypothesis (i) of the Tauberian Theorem. The comparison of (29) and (53) at $s = 2$ proves

$$\frac{f_2(1)}{\lambda'(2)} = \frac{1}{2\tilde{\zeta}(2)}, \quad \text{i.e.} \quad \frac{-1}{\lambda'(2)} = \frac{2}{\pi^2 f_2(1)}. \qquad \blacksquare(55)$$

From Proposition 6, and relations (53), (54), (55), we thus deduce our first main result:

Theorem 1. *The average number E_N or $\tilde{E}_N$ of exchanges of the Binary Euclidean Algorithm on the set $\Omega_N := \{(u,v);\ u, v\,\mathrm{odd},\ 0 < u \le v \le N\}$, or on the set $\tilde{\Omega}_N := \{(u,v);\ u, v\,\mathrm{odd},\ 0 < u \le v \le N, \gcd(u,v) = 1\}$ satisfies*

$$E_N \sim \tilde{E}_N \sim \frac{2}{\pi^2 f_2(1)}\ \log N$$

where f_2 is the fixed point of the operator $\mathcal{V}_2$

$$\mathcal{V}_2[f](x) := \sum_{k\ge 1} \sum_{\substack{a \text{ odd}, \\ 1 \le a < 2^k}} \Big(\frac{1}{a+2^k x}\Big)^2 f\Big(\frac{1}{a+2^k x}\Big),$$

defined by the normalization condition $\int_0^1 f_2(t)dt = 1$.

3. The average cost of the Binary Euclidean Algorithm.

The study of the other two parameters of the binary continued fraction involves a more general operator

$$\mathbf{V}_{w,s}[f](x) := \sum_{h\in\mathcal{L}} \frac{w^{c(h)}}{D[h](x)^s}\ f\circ h(x). \tag{56}$$

where each term involves a "cost" $c(h)$ associated the LFT h. As in (17), the sum is taken on the set $\mathcal{L}$ of the LFT's defined in (4), of the form $h(x) = 1/(a + 2^k x)$, and $D[h]$ is the denominator of h, defined in (18). We shall consider two different costs

$$c^{(2)}(h) := p(a) = \text{the number of 1 in the binary expansion of } a \tag{57}$$

$$\text{or}\quad c^{(3)}(h) := k = \text{the exponent of 2 used as the numerator of the continued fraction}, \tag{58}$$

and thus two different operators $\mathbf{V}^{(i)}_{w,s}$. In both cases, the "multiplicative" property of D gives the expression of the r–th iterate of $\mathbf{V}_{w,s}$ as a sum over the set $\mathcal{L}^r$ of the LFT of height r. This expression now involves the cost $c(h)$ of a LFT $h := h_1 \circ h_2 \circ \ldots \circ h_r$ of $\mathcal{L}^r$, defined as the sum of the costs of each factor h_i,

$$\mathbf{V}^r_{w,s}[f](x) := \sum_{h\in\mathcal{L}^r} \frac{w^{c(h)}}{D[h](x)^s}\ f\circ h(x). \tag{59}$$

This expression is completely analogous to (19) and we can now follow the same principles as in Proposition 1, where the operator $w\mathcal{V}_s$ is replaced by the generalized operator $\mathbf{V}_{w,s}$. In particular, the method involves the quasi–inverse $(I - \mathbf{V}_{w,s})^{-1}$ and its derivative with respect to w

$$\frac{d}{dw}(I - \mathbf{V}_{w,s})^{-1} = (I - \mathbf{V}_{w,s})^{-1} \circ \frac{d}{dw}\mathbf{V}_{w,s} \circ (I - \mathbf{V}_{w,s})^{-1}$$

at $w = 1$. Furthermore, we remark that $\mathbf{V}_{1,s}$ equals $\mathcal{V}_s$, and, for each cost $c^{(i)}$, we use the notation

$$\mathbf{V}^{(i)}_s := \frac{d}{dw}\mathbf{V}^{(i)}_{w,s}|_{w=1}.$$

Finally we obtain:

Proposition 7. *The average values of the last two parameters of the algorithm on $\tilde{\Omega}_N$ are ratios where the numerators and the denominators involve the partial sums of the Dirichlet series $F(s)$ and $G^{(i)}(s)$, defined from the quasi–inverse $\Lambda_s := (I - \mathcal{V}_s)^{-1}$,*

$$F(s) := \Lambda_s[1](1), \qquad G^{(i)}(s) := \Lambda_s \circ \mathbf{V}_s^{(i)} \circ \Lambda_s [1](1).$$

The operator $\mathbf{V}_s^{(i)}$ depends on the parameter. For the parameter "number of iterations", it is defined by

$$\mathbf{V}_s^{(2)}[f](x) = \sum_{k\geq 1} \sum_{\substack{a \text{ odd},\\ 1\leq a<2^k}} \frac{p(a)}{(a+2^k x)^s} \, f(\frac{1}{a+2^k x})$$

where $p(a)$ denotes the number of 1 in the binary expansion of a. For the parameter "total sum of exponents in the numerators", it is defined by

$$\mathbf{V}_s^{(3)}[f](x) = \sum_{k\geq 1} \sum_{\substack{a \text{ odd},\\ 1\leq a<2^k}} \frac{k}{(a+2^k x)^s} \, f(\frac{1}{a+2^k x}).$$

In the same vein, the average values of the last two parameters of the algorithm on Ω_N are ratios where the numerators and the denominators involve the partial sums of the Dirichlet series $\tilde{\zeta}(s)F(s)$, and $\tilde{\zeta}(s)G^{(i)}(s)$, where $\tilde{\zeta}(s)$ is the Riemann function relative to odd numbers.

So, the asymptotic evaluations (for $N \to \infty$) of the average costs are possible since the Tauberian theorem can be applied to the previous Dirichlet series:

Proposition 8. *The conditions of the Tauberian Theorem hold for $G^{(2)}(s)$ and $G^{(3)}(s)$ with $\sigma = 2$ and $\gamma = 1$.*

Proof. We remark first that the operator $\mathbf{V}_s^{(i)}$ is a sum of component operators $\mathbf{V}_{s,a,k}^{(i)}$ whose norm satisfies

$$||\mathbf{V}_{s,a,k}^{(i)}|| \leq \frac{1}{a^{\sigma-1}} \frac{k}{\sqrt{2}^{k-1}}$$

(adapt the sequence of relations (36), (37), (38)). Then, when taking the sum over indices (a, k) that satisfy $2^k > a$, the component operators form a convergent series for $\sigma > 3/2$. Then the operator $\mathbf{V}_s^{(i)}$ is regular at $s = 2$. Thus, the relation (52) when applied with $p = 1$ to $f = 1$ and then to $\mathbf{V}_2^{(i)}[f_2]$ (which are elements of $\mathcal{H}^2(\mathcal{D})$), proves that $G^{(i)}(s)$ can be written as

$$G^{(i)}(s) = \frac{1}{(s-2)^2} \frac{1}{\lambda'(2)^2} \, f_2(1)\, H^{(i)}(s) + L^{(i)}(s) \tag{60}$$

where $H^{(i)}$ and $L^{(i)}$ are holomorphic near $s = 2$. Moreover, the value of $H^{(i)}(s)$ at $s = 2$ is equal to

$$I^{(i)} := \int_0^1 \mathbf{V}_2^{(i)}[f_2](x)dx.$$

For $i = 2$,

$$\mathbf{V}_2^{(2)}[f](x) = \sum_{k\geq 1} \sum_{\substack{a \text{ odd},\\ a<2^k}} \frac{p(a)}{(a+2^k x)^2} \, f(\frac{1}{a+2^k x}).$$

Then we obtain

$$I^{(2)} := \int_0^1 \mathbf{V}_2^{(1)}[f_2](x)dx = \sum_{k\geq 1} \sum_{\substack{a \text{ odd}, \\ a<2^k}} \frac{p(a)}{2^k} \, [F_2(\frac{1}{a}) - F_2(\frac{1}{a+2^k})],$$

where F_2 is the integral of f_2 such that $F_2(0) = 0$. In the right member, each term $F_2(1/a)$ (for an integer $a > 1$) is multiplied by the factor

$$p(a) \, [\sum_{k>k_a} \frac{1}{2^k}] - (p(a) - 1) \, \frac{1}{2^{k_a}}.$$

Then

$$I^{(2)} = 1 + \sum_{a \text{ odd}>1} \frac{1}{2^{k_a}} F_2(\frac{1}{a}) = \sum_{a \text{ odd}} \frac{1}{2^{k_a}} F_2(\frac{1}{a}). \tag{61}$$

For $i = 3$,

$$\mathbf{V}_2^{(3)}[f](x) = \sum_{k\geq 1} \sum_{\substack{a \text{ odd}, \\ a<2^k}} \frac{k}{(a+2^k x)^2} \, f(\frac{1}{a+2^k x}).$$

Then we obtain

$$I^{(3)} := \int_0^1 \mathbf{V}_2^{(2)}[g_2](x)dx = \sum_{k\geq 1} \sum_{\substack{a \text{ odd}, \\ a<2^k}} \frac{k}{2^k} \, [F_2(\frac{1}{a}) - F_2(\frac{1}{a+2^k})]$$

In the right member, each term $F_2(1/a)$ (for an integer $a > 1$) is multiplied by the factor

$$\sum_{k>k_a} \frac{k}{2^k} - \frac{k_a}{2^{k_a}} = \frac{k_a + 2}{2^{k_a}} - \frac{k_a}{2^{k_a}} = \frac{2}{2^{k_a}},$$

and

$$I^{(3)} = 2 + 2 \sum_{a \text{ odd}>1} \frac{1}{2^{k_a}} F_2(\frac{1}{a}) = 2 \sum_{a \text{ odd}} \frac{1}{2^{k_a}} F_2(\frac{1}{a}).. \tag{62}$$

Thus, comparing (61) and (62),

$$I^{(3)} = 2I^{(2)},$$

and Proposition 8 is proved with (60) and (55). ∎

We thus deduce our second result

Theorem 2. *The average number K_N or $\tilde{K}_N$ of total iterations of the Binary Euclidean Algorithm on the set $\Omega_N := \{(u,v);\ u, v \,\text{odd},\ 0 < u \leq v \leq N\}$, or on the set $\tilde{\Omega}_N := \{(u,v);\ u, v \,\text{odd},\ 0 < u \leq v \leq N, \gcd(u,v) = 1\}$ satisfies*

$$\tilde{K}_N \sim K_N \sim \frac{2}{\pi^2 f_2(1)} [\sum_{a \text{ odd}} \frac{1}{2^{k_a}} F_2(\frac{1}{a})] \quad \log N,$$

where f_2 is the fixed point of the operator $\mathcal{V}_2$

$$\mathcal{V}_2[f](x) := \sum_{k\geq 1} \sum_{\substack{a \text{ odd}, \\ 1\leq a<2^k}} (\frac{1}{a+2^k x})^2 \, f(\frac{1}{a+2^k x}),$$

such that $F_2(x) := \int_0^x f_2(t)dt$ satisfies $F_2(1) = 1$. Here, k_a is the integer part of $\log_2 a$.
The average number P_N or $\tilde{P}_N$ of the sum of exponents of 2 used in the numerators of the binary continued fraction expansions on the set Ω_N or on the set $\tilde{\Omega}_N$ satisfies

$$\tilde{P}_N \sim P_N \sim \frac{4}{\pi^2 f_2(1)}[\sum_{a \text{ odd}} \frac{1}{2^{k_a}} F_2(\frac{1}{a})] \quad \log N.$$

4. Relations with other analyses and numerical computations.

There now exist three different expressions for the asymptotics of the average number of iterations.
(i) In this work, we have obtained a proven expression that involves the fixed point f_2 of the operator $\mathcal{V}_2$ and its integral F_2, defined by $F_2(x) := \int_0^x f_2(t)dt$, with the normalization condition $F_2(1) = 1$,

$$K_N \sim A_2 \log N \quad \text{with} \quad A_2 = \frac{2}{\pi^2 f_2(1)}[\sum_{a \text{ odd}} \frac{1}{2^{k_a}} F_2(\frac{1}{a})], \tag{63}$$

(ii) We recall that Brent [Br1] analyses this parameter by using the operator $\mathcal{B}_2$ defined in (12). He obtained in [Br3] a conjectural–heuristic expression that involves the fixed point g_2 of the operator $\mathcal{B}_2$, with the normalization condition $\int_0^1 g_2(t)dt = 1$,

$$K_N \sim \frac{1}{M} \log N \quad \text{with} \quad M = \log 2 - \frac{1}{2}\int_0^1 \log(1-x)\, g_2(x)dx. \tag{64}$$

(iii) On the other hand, we proved in [Va5], without heuristic hypothesis, but under a "spectral" conjecture on $\mathcal{B}_s$ analogous to our Corollary 1 for $\mathcal{V}_s$, that

$$K_N \sim B \log N \quad \text{with} \quad B = \frac{4}{\pi^2\, g_2(1)}. \tag{65}$$

We remove the heuristic hypothesis when using Tauberian Theorems which lead to a *proven* transfer from the continuous model (the reals) to the discrete one (the rationals).

We did not succeed in proving the equality of the three constants $A_2, (1/M), B$, but Brent [Br3] made extensive computations that show the numerical concordance of the last two estimates (64) and (65) to 44 decimal places. The common numerical value is

$$1.0185012157614367170.....$$

In the same paper, Brent [Br3] exhibits a relation between the three operators $\mathcal{V}_s$, $\mathcal{B}_s$ and $\mathcal{U}_s$ defined in (14)

$$(\mathcal{V}_s - I)\, \mathcal{U}_s = \mathcal{V}_s\ (\mathcal{B}_s - I).$$

However, this does not seem sufficient to obtain the equality between the constant A_2 of (63) and the constant B of (65).

Simulations. At present, we have not yet computed numerically the dominant eigenfunction of the operator $\mathcal{V} := \mathcal{V}_2$, but we have carried out under the Maple system various batches of a few thousand simulations on numbers of the order of 10^{100}. These rough simulations suggest that

$$A_1 = 0.555 \pm 0.005, \quad A_2 = 1.015 \pm 0.005, \quad A_3 = 2.025 \pm 0.005.$$

Such empirical values are consistent with the numerical value computed by Brent, namely $A_2 \simeq 1.01850$. They are also basically in fair agreement with the theoretical prediction that $A_3 = 2 * A_2$.

Principles of the (future) computation. We explain now the principles of the (future) computation that should be very similar to those used in [DFV] or [Va3]. The idea is to approximate the operator $\mathcal{V}$ by a sequence of truncated operators acting on finite–dimensional subspaces generated by Taylor polynomials of functions at the point $z = 1$ together with the log function. These truncated operators are represented by finite matrices and their spectral characteristics may be expected to provide reasonably good approximations to the corresponding spectral characteristics of $\mathcal{V}$. More precisely, we examine the transforms

$$h_j(x) := \mathcal{V}[(x-1)^j](x) \quad = \sum_{a \text{ odd}} \sum_{k > k_a} \frac{1}{(a+2^k x)^2} \left(\frac{1}{a+2^k x} - 1\right)^j . \tag{66}$$

By the binomial theorem, we find

$$h_j(x) = \sum_{\ell=0}^{j} \binom{j}{\ell} (-1)^{j-\ell}\ \mathcal{V}_{2+\ell}[1](x). \tag{67}$$

The function $x \to \mathcal{V}_s[1](x)$ is itself easily expanded at the point $x = 1$. We start with

$$\mathcal{V}_s[1](x) = \sum_{a \text{ odd} > 1} \left(\frac{1}{a + 2^{k_a}(x-1)}\right)^s = \sum_{a \text{ odd} > 1} \frac{1}{a^s} \sum_{\ell=0}^{\infty} (-1)^\ell \binom{s+\ell-1}{\ell} (\frac{2^{k_a}}{a})^\ell (x-1)^\ell .$$

When using the modified ζ function

$$\tilde{\zeta}(s,t) := \sum_{a \text{ odd}>1} \frac{2^{k_a t}}{a^{s+t}}, \tag{68}$$

we obtain

$$\mathcal{V}_s[1](x) = \sum_{\ell=0}^{\infty} (-1)^\ell \binom{s+\ell-1}{\ell} \tilde{\zeta}(s,\ell)\ \ (x-1)^\ell .$$

Since the logarithmic component of $\mathcal{V}_s[1]$ equals $-[1+\mathcal{V}_s[1](1)] = -[1+\tilde{\zeta}(s,0)]$, the function $\mathcal{V}_s[1]$ is now expanded at the point $x = 1$ under the form

$$\mathcal{V}_s[1](x) = -\frac{1+\tilde{\zeta}(s,0)}{\log 2} \log x + \tilde{\zeta}(s,0) + \sum_{\ell=1}^{\infty} (-1)^\ell \left[\binom{s+\ell-1}{\ell} \tilde{\zeta}(s,\ell) - \frac{1+\tilde{\zeta}(s,0)}{\ell \log 2}\right] (x-1)^\ell . \tag{69}$$

When replacing the expression (69) in (67), we obtain $h_j(x)$ as a function of $\log x$ and polynomials $(x-1)^i$. Furthermore,

$$h_{-1}(x) := \mathcal{V}[\log x](x) \quad = \sum_{a \text{ odd}>1} \left(\frac{1}{a+2^{k_a}(x-1)}\right)^2 \log\left(\frac{1}{a+2^{k_a}(x-1)}\right)$$

$$= -\sum_{a \text{ odd}>1} \frac{\log a}{a^2} \left(\frac{1}{1+\frac{2^{k_a}}{a}(x-1)}\right)^2 + \sum_{a \text{ odd}>1} \frac{1}{a^2} \left(\frac{1}{1+\frac{2^{k_a}}{a}(x-1)}\right)^2 \log\left(\frac{1}{1+\frac{2^{k_a}}{a}(x-1)}\right).$$

When using the derivative $\tilde{\zeta}'(s,t)$ of the modified ζ function $\tilde{\zeta}(s,t)$ with respect to s

$$\tilde{\zeta}'(s,t) = -\sum_{a\,\mathrm{odd}>1} \log a\,\frac{2^{k_a t}}{a^{s+t}}, \tag{70}$$

we obtain

$$\mathcal{V}[\log x](x) = \tilde{\zeta}'(2,0) + \sum_{\ell=1}^{\infty}(-1)^{\ell}(x-1)^{\ell}\ (\ell+1)[(H_{\ell+1}-1)\,\tilde{\zeta}(2,\ell) + \tilde{\zeta}'(2,\ell)],$$

which involves the ℓ-th harmonic number H_ℓ. Since the logarithmic component of $\mathcal{V}_2[\log x]$ equals $B := -\mathcal{V}_2[\log x](1) = -\tilde{\zeta}'(2,0)$, the function $\mathcal{V}[\log x]$ is now expanded at the point $x = 1$ under the form

$$h_1(x) := \mathcal{V}[\log x](x) = -\frac{\tilde{\zeta}'(2,0)}{\log 2}\log x + \tilde{\zeta}'(2,0) +$$

$$+\sum_{\ell=1}^{\infty}(-1)^{\ell}(x-1)^{\ell}\ [(H_{\ell+1}-1)(\ell+1)\,\tilde{\zeta}(2,\ell) + (\ell+1)\,\tilde{\zeta}'(2,\ell) - \frac{\tilde{\zeta}'(2,0)}{\ell\log 2}].$$

Thus, viewed as acting on series expansions at $z = 1$, the operator $\mathcal{V}$ is expressed by an infinite matrix $M = (M_{i,j})$, where $M_{i,j}$ is the coefficient of $(x-1)^i$ in $\mathcal{V}[(x-1)^j]$. The index -1 corresponds to logarithmic terms. For each m, the finite matrix $T^{[m]}$ is defined as the square submatrix obtained from $(M_{i,j})$ by restricting the indices to $-1 \le i,j < m$, and accordingly it may be viewed as operating on the linear subspace generated by the logarithmic function together with polynomials of degree less than m. For that reason, we refer to the $T^{[m]}$ as truncated operators. The $T^{[m]}$ provide a sequence of approximations to operator $\mathcal{V}$ so that their eigenvalues and eigenfunctions may be expected to provide reasonably good approximations to the corresponding spectral characteristics of $\mathcal{V}$. If $\lambda^{[m]}$ denotes the dominant eigenvalue of $T^{[m]}$, the corresponding eigenfunction $p^{[m]}$ (which is a combination of a logarithmic term and a polynomial of degree at most equal to $m-1$) can give a reasonably good approximation of the eigenfunction f_2. The main differences with the previous computations in [DFV] or in [Va3] are the following.

(i) The coefficients $M_{i,j}$ involve the modified ζ function defined in (68) together with its derivative defined in (70) instead of the classical one in our previous computations.

(ii) One must take into account the logarithmic terms.

Acknowledgements. I wish to thank Hervé Daudé, Pierre Ducos, Henri Laville, Pascal Porée, Luc Vallée for our discussions of 1992 which began this work. Many thanks to Philippe Flajolet for his help in Mellin transforms. I would like to thank Richard Brent for his interest, for six months of regular e–mail, and his extensive computations for verifying my first conjecture. Finally, I wish to thank Don Knuth for his encouragement.

5. Bibliographic references.

[Br1] Richard P. Brent. *Analysis of the binary Euclidean algorithm*, Algorithms and Complexity, New directions and recent results, ed. by J.F. Traub, Academic Press 1976, pp 321–355

[Br2] Richard P. Brent. Unpublished, cf [Kn, 4.5.2]

[Br3] Richard P. Brent. *Further analysis of the binary Euclidean Algorithm*, feb 98, Resarch Report, Oxford University.

[DFV] Hervé Daudé, Philippe Flajolet, and Brigitte Vallée. *An analysis of the Gaussian Algorithm for Lattice Reduction*, ANTS '1994, Lecture Notes in Computer Science 877, pp 144-158. Extended version in Combinatorics, Probability and Computing (1997) 6, pp 397-433.

[De] Hubert Delange. *Généralisation du Théorème d'Ikehara.* Ann. Sc. ENS, (1954) 71, pp 213–242.

[Di] John G. Dixon. *The number of steps in the Euclidean algorithm*, Journal of Number Theory 2 (1970) pp 414-422.

[Du] Peter L. Duren. *Theory of H^p spaces,* Academic Press, New York, 1970.

[Fa] Christian Faivre. *Distribution of Lévy constants for quadratic numbers*, Acta Arithmetica, LXI. 1 (1992), pp 13-34.

[Fl] Philippe Flajolet. *Analytic analysis of algorithms*, In Proceedings of the 19th International Colloquium "Automata, Languages and Programming", Vienna, July 1992, W. Kuich, editor, Lecture Notes in Computer Science 623, pp 186–210

[FS] Philippe Flajolet and Robert Sedgewick. *Analytic Combinatorics*, Book in preparation (1999), see also INRIA Research Reports 1888, 2026, 2376, 2956.

[FV] Philippe Flajolet and Brigitte Vallée. *Continued Fraction Algorithms, Functional Operators and Structure Constants*, Theoretical Computer Science 194 (1998), pp 1-34.

[Ga] R. M. Gabriel. *Some results concerning the moduli of regular functions along the curves of certain types*, Proc. London Math. Soc. 28 (1928) pp 121-127.

[Gr1] Alexandre Grothendieck. *Produits tensoriels topologiques et espaces nucléaires*, Mem. Am. Math. Soc. 16 (1955)

[Gr2] Alexandre Grothendieck. *La théorie de Fredholm*, Bull. Soc. Math. France 84 pp 319-384.

[Hei] H. Heilbronn. *On the average length of a class of continued fractions*, Number Theory and Analysis, ed. by P. Turan, New-York, Plenum, 1969, pp 87-96.

[He1] Doug Hensley. *The distribution of badly approximable rationals and continuants with bounded digits II*, Journal of Number Theory, 34 pp 293-334 (1990)

[He2] Doug Hensley. *The Hausdorff dimensions of some continued fraction Cantor sets*, Journal of Number theory 33, (1989) pp 182-198

[He3] Doug Hensley. *Continued Fraction Cantor sets, Hausdorff dimension, and functional analysis*, Journal of Number Theory 40 (1992) pp 336-358.

[He4] Doug Hensley. *A polynomial time algorithm for the Hausdorff dimension of a continued fraction Cantor set*, Journal of Number Theory 58 No 1, May 1996, pp 9–45.

[Kn] D.E. Knuth. *The Art of Computer Programming*, Vol 2, third edition (1997), Sec. 4.5.2.

[Kr] M. Krasnoselsky. *Positive solutions of operator equations*, Chap. 2 P. Noordhoff, Groningen. (1964)

[Ma1] Dieter H. Mayer. *Continued fractions and related transformations*, In Ergodic Theory, Symbolic Dynamics and Hyperbolic Spaces, M. K. Tim Bedford and C. Series, Eds. Oxford University Press, 1991, pp. 175–222.

[Ma2] Dieter H. Mayer. *Spectral properties of certain composition operators arising in statistical mechanics*, Commun. Math. Phys. 68, 1-8 (1979)

[Pa] Jonathan R. Partington. *An introduction to Hankel operators*, London Mathematical Society Student Texts. 13, Cambridge University Press (1988).

[Po] Mark Pollicott. *A complex Ruelle-Perron-Frobenius Theorem and two counterexamples*, Ergod. Th. and Dynm. Sys (1984), 4, pp 135–146

[Ru] David Ruelle. *Thermodynamic formalism.* Addison Wesley (1978)

[Sc] H. Schwartz. *Composition operators in $\mathcal{H}^p$*, Ph.D. Thesis, Univ. of Tomedo.

[ST] Joel Shapiro, P.D. Taylor, *Compact, nuclear, and Hilbert–Schmidt composition operators on $\mathcal{H}^2$*, Indiana Univ. Math. J. (1973) 23, pp 471-496

[Sh1] Joel Shapiro. *Composition operators and classical function theory*, Universitext: tracts in mathematics, Springer-Verlag, 1993.

[Sh2] Joel Shapiro. *Compact composition operators on spaces of boundary regular holomorphic functions*, Proceedings of the AMS, 100, (1997), pp 49-57

[Va1] Brigitte Vallée. *Opérateurs de Ruelle–Mayer généralisés et analyse des algorithmes de Gauss et d'Euclide*, Acta Arithmetica LXXXI.2 (1997) pp 101-144 .

[Va2] Brigitte Vallée. *Algorithms for computing signs of 2×2 determinants: dynamics and average-case algorithms*, Proceedings of the 8 th Annual European Symposium on Algorithms, ESA'97, pp 486–499, LNCS 1284, Springer Verlag.

[Va3] Brigitte Vallée. *Fractions continues à contraintes périodiques*, Les Cahiers du GREYC 1997, Université de Caen, to appear in Journal of Number Theory.

[Va4] Brigitte Vallée. *Dynamical systems and average–case analysis of general tries*, Les cahiers du GREYC 1997, Université de Caen; also in Proceedings of RALCOM'97, Santorini Island, October 1997.

[Va5] Brigitte Vallée. Unpublished, cf [Kn, 4.5.2]

[Va6] Brigitte Vallée. *The complete analysis of the Binary Euclidean Algorithm*, Proceedings of ANTS'98, to appear in LNCS.