# Distributional Analyses of Euclidean Algorithms

Viviane Baladi[*] Brigitte Vallée [†]

December 1st, 2003

**Abstract**

We provide a complete analysis of the standard Euclidean algorithm and two of its "fast" variants, the nearest-integer and the odd-quotient algorithm. For a whole family of costs, including the number of iterations, we show that the distribution of the cost is asymptotically normal, and obtain the optimal speed of convergence. Precisely, we establish both local and central limit theorems, which characterize respectively distribution functions and their cumulative versions. Our results widely extend earlier results of Hensley (1994) regarding the number of steps of the standard algorithm and even in this particular case provide improved error estimates. We view an algorithm as a dynamical system restricted to rational inputs, and combine tools imported from dynamics, such as transfer operators, with various other techniques: Dirichlet series, Perron's formula, quasi-powers theorems, and the saddle-point method. Such dynamical analyses had previously been used to perform the average-case analysis of algorithms. The present (dynamical) analysis in distribution relies on a novel approach based on bivariate transfer operators and builds upon recent results of Dolgopyat (1998) by providing pole-free regions for certain associated Dirichlet series.

## 1 Introduction

According to Knuth [25, p. 335], "we might call Euclid's method the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day". Since addition and multiplication of rational numbers both require gcd calculations, Euclid's algorithm is a basic building block of computer algebra systems and multi-precision arithmetic libraries, and, in many such applications, most of the time is indeed spent in computing gcd's. The classic books by Schönhage, H. Cohen, Knuth, von zur Gathen and Jürgen further illustrate the central rôle of this algorithm in computational number theory and related applications.

Although its design is quite clear, the Euclidean algorithms have not yet been completely analysed. We consider here three (discrete) Euclidean algorithms (the standard Euclidean algorithm, the centered and the odd-quotient algorithms) and their (continuous) versions, the continued fraction algorithms. We allow in general a unit cost $c$ incurred at each step that is of moderate growth (i.e., at most logarithmic) and precisely describe the asymptotic distribution of the total cost $C(x)$ of an execution of the Euclidean Algorithm on the input $x$. As a technical preparation, we first do so when $x$ is real (and trajectories are truncated, see Theorem 1), then consider the case where $x$ is randomly (uniformly) drawn from rational inputs with denominator and numerator less than $N$. Our first main result, Theorem 3, is a central limit theorem (CLT): it states that the distribution of $C$ is asymptotically Gaussian, with expectation and variance asymptotically proportional to $\log N$. Theorem 3 gives the best possible speed of convergence to the Gaussian law, of order $O(1/\sqrt{\log N})$. Furthermore, the constants $\mu(c)$ and $\delta^2(c)$ that intervene in the main terms of the expectation and the variance appear to be computable constants with $\mu(c)$ even admitting a closed form. Our second main result, Theorem 4, is a local limit theorem (LLT) which holds for any lattice cost $c$ (i.e., a nonzero cost whose values belong to a set of the form $L\mathbf{N}$, with $L > 0$). Note that any integer cost is lattice.

Three special instances of our results are of major interest.

(*i*) Digit-cost $c(m) \equiv 1$. This plainly yields as total cost the number of steps of our three Euclidean algorithms, for which normality results. In this special case, the LLT was previously proved by Hensley [20], in the particular case of the Standard Euclidean Algorithm, but with a worse speed of convergence.

(*ii*) Digit-cost, $c(m) = c_k(m)$, the characteristic function of a digit $k$. We then characterize the frequencies of each digit as Gaussian, a result which is itself new.

* CNRS UMR 7586, Institut de Mathématiques de Jussieu, F-75251 Paris, France.

† CNRS UMR 6072, GREYC, Université de Caen, F-14032 Caen, France .

(*iii*) Digit-cost $c(m) = \lfloor \log_2 m \rfloor$. This gives the length of the binary encoding of a continued fraction representation, also proved to obey Gaussian fluctuations. This analysis is of interest in relation to the information content of continued fraction representations and to the boolean complexity of the Euclidean algorithm, for which a complete analysis is still lacking.

A full version of this extended abstract [4], titled "Euclidean Algorithms are Gaussian" is available from the ArXiv

## 2 Methodological Outlook

**2.1 Three Euclidean algorithms and their dynamical systems.** Three Euclidean algorithms will be analyzed; each of them is related to a Euclidean division. These algorithms possess similar properties, with various parameters described in Figure 1. They form a class which will be denoted by $\mathcal{E}$.

Let $v \geq u \geq 1$ be integers. The classical division, corresponding to the standard Euclidean algorithm $\mathcal{G}$, $v = mu + r$ produces an integer $m \geq 1$ and an integer remainder $r$ such that $0 \leq r < u$. The centered division (centered algorithm $\mathcal{K}$) requires $v \geq 2u$ and takes the form $v = mu+s$, with integer $s \in [-u/2, +u/2[$. Letting $s = \epsilon r$, with $\epsilon = \pm 1$ (and $\epsilon = +1$ if $s = 0$), it produces an integer remainder $r$ such that $0 \leq r \leq u/2$, and an integer $m \geq 2$. The odd division (odd algorithm $\mathcal{O}$) produces an odd quotient: it is of the form $v = mu + s$ with $m$ odd and integer $s \in [-u, +u[$. Letting $s = \epsilon r$, with $\epsilon = \pm 1$ (and $\epsilon = +1$ if $s = 0$), it produces an integer remainder $r$ with $0 \leq r \leq u$, and an odd integer $m \geq 1$. In the three cases, the divisions are defined by pairs $q = (m, \epsilon)$, which are called the digits. (See Figure 1.)

For the present purposes, since the pair $(du, dv)$ produces the same sequence of digits as $(u, v)$, up to multiplying all remainders $r$ by $d$, we may consider the rational $u/v$, instead of the integer pair $(u, v)$. Then, rationals $u/v$ belong to interval $\mathcal{I}$, and the division expressing the pair $(u, v)$ as a function of $(r, u)$ is replaced by a linear fractional transformation (LFT) $h$ that expresses the rational $u/v$ as a function of $r/u$.

To summarize, on the input $(u, v)$, each algorithm produces a sequence of pairs $((m_1, \epsilon_1), \ldots, (m_p, \epsilon_p))$ and thus builds a specific continued fraction

$$\text{(2.1)} \qquad \frac{u}{v} = \cfrac{1}{m_1 + \cfrac{\epsilon_1}{m_2 + \cfrac{\epsilon_2}{\ddots + \cfrac{\epsilon_{P-1}}{m_P}}}},$$

of depth $P$, decomposing it also as

$$\text{(2.2)} \qquad (u/v) = h_1 \circ h_2 \circ \ldots \circ h_p(0) = h(0),$$

with $h_i \in \mathcal{H}, 1 \leq i \leq p-1$, and $h_p \in \mathcal{F}$. The "generic" set $\mathcal{H}$ contains LFTs of the form $h(x) = 1/(m + \epsilon x)$ with $(m, \epsilon) \in \mathcal{A}$. The LFTs appearing in the final step belong to a subset $\mathcal{F} \subset \mathcal{H}$ of the form $h(x) = 1/(m+\epsilon x)$ with $(m, \epsilon) \in \mathcal{A} \cap \mathcal{B}$. (See Figure 1)

We associate to each algorithm a dynamical system of the interval, i.e., a transformation $T : \mathcal{I} \to \mathcal{I}$. For nice and elementary surveys on interval dynamics, see [5, 26, 11]. The interval $\mathcal{I}$ has already been defined (see Figure 1) and $T$ extends the map defined on rationals by the equality $T(u/v) = r/u$ where $r$ is the remainder of the Euclidean division on $(u, v)$. Then,

$$T(x) := \left| \frac{1}{x} - A\left(\frac{1}{x}\right) \right|, \quad x \neq 0, \quad T(0) = 0,$$

where the function $A$ depends on the algorithm and is defined in Figure 1. Note also that $\mathcal{H}$ is just the set of inverse branches of our map $T : \mathcal{I} \to \mathcal{I}$. Furthermore, each $h \in \mathcal{H}$ maps $\mathcal{I}$ into $\mathcal{I}$, and the set of the inverse branches of the iterate $T^k$ is exactly the set $\mathcal{H}^k$; its elements are called the inverse branches of depth $k$. Each interval $h(\mathcal{I})$ for $h$ of depth $k$ is called a fundamental interval of depth $k$, and, for any $n \geq 1$, the union of all fundamental intervals of depth $n$ is exactly $\mathcal{I}$. Each dynamical system is strongly contracting, and the contraction ratio satisfies

$$\text{(2.3)} \qquad \rho := \lim_{n \to \infty} \left(\max\{|h'(x)|; h \in \mathcal{H}^n, x \in \mathcal{I}\}\right)^{1/n} < 1.$$

**2.2 Costs of truncated real trajectories.** The trajectory $\mathcal{T}(x) = (x, T(x), T^2(x), \ldots, T^n(x), \ldots)$ is entirely described by the infinite sequence of digits $(m_1(x), m_2(x), m_3(x), \ldots, m_n(x), \ldots)$, through

$$m_i(x) := \begin{cases} A\left(\frac{1}{T^{i-1}(x)}\right) & \text{if} \quad T^{i-1}(x) \neq 0, \\ \infty & \text{if} \quad T^{i-1}(x) = 0, \end{cases}$$

When $x$ is rational, the trajectory $\mathcal{T}(x)$ reaches 0 in finitely many steps, and the largest $p$ for which $m_p(x)$ is finite is the depth of the trajectory (or of the rational). For $x \in \mathcal{I}$, it is usual to consider the truncated trajectory $\mathcal{T}_n(x) := (x, Tx, \ldots, T^n x)$ together with its truncated encoding $(m_1(x), m_2(x), \ldots, m_n(x))$, which keeps track of the first $n$ stages of the process, and then let the truncation degree $n$ tend to $\infty$.

Associate a nonnegative real value $c(m)$ to each digit $m$, and put $c(\infty) = 0$. We may also view $c$ as a function on $\mathcal{H}$, and extend the function $c$ additively to (truncated)

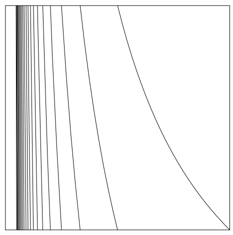
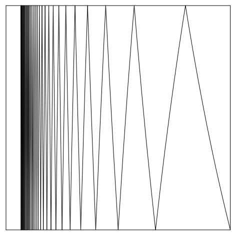
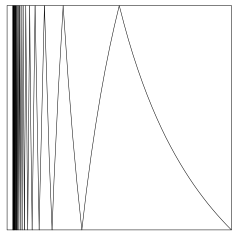
| *Algorithm* | $\mathcal{G}$ | $\mathcal{K}$ | $\mathcal{O}$, |
|---|---|---|---|
| *Interval* | $\mathcal{I} = [0, 1]$ | $\mathcal{I} = [0, 1/2]$ | $\mathcal{I} = [0, 1]$ |
| *Generic Conditions* $\mathcal{A}$ *on pairs* $(m, \epsilon)$ *with* $m \geq 1$, $\epsilon = \pm 1$. | $\epsilon = +1$ | $(m, \epsilon) \geq (2, 1)$ | $m$ odd, $(m, \epsilon) \geq (1, 1)$ |
| *Final conditions* $\mathcal{B}$. | $m \geq 2$ | $\epsilon = +1$ | $\epsilon = +1$ |
| *Graphs of* $T$. |  |  |  |
| *Function* $A(x)$ | Integer part of $x$ | Nearest integer to $x$ | Odd integer nearest to $x$ |
| *Contraction ratio* $\rho$ | $1/\phi^2$ | $1/(\sqrt{2}+1)^2$ | $1/\phi^2$ |
| *Invariant function* $f_1$ | $\frac{1}{\log 2} \frac{1}{1+x}$ | $\frac{1}{\log \phi}[\frac{1}{\phi + x} + \frac{1}{\phi^2 - x}]$. | $\frac{1}{\phi - 1 + x} + \frac{1}{\phi^2 - x}$ |
| *Entropy* | $\frac{\pi^2}{6 \log 2}$ | $\frac{\pi^2}{6 \log \phi}$ | $\frac{\pi^2}{9 \log \phi}$ |

Figure 1: The three Euclidean dynamical systems of class $\mathcal{E}$

trajectories by setting for each $n \geq 1$

$$C^{(n)}(x) := \sum_{i=1}^{n} c(m_i(x)) \,. \tag{2.4}$$

*Here, we consider costs $c$ which are of moderate growth, i.e., they are nonzero and satisfy $c(m) = O(\log m)$. Any triple $(\mathcal{I}, T, c)$ formed with a dynamical system of $\mathcal{E}$ and a cost $c$ of moderate growth will be called of $\mathcal{EMG}$–type.*

Some special cases are particularly interesting: if $c = c_m$ is the characteristic function of a fixed digit $m$, then $C^{(n)}$ is just the number of occurrences of $m$ amongst the first $n$ digits of the *CF*-expansion; if $c$ is the binary length of the digit, then $C^{(n)}$ is closely related to the length of a standard encoding of the trajectory $\mathcal{T}_n$. We shall refer to $c$ as a "digit-cost" and to $C$ as the associated "total cost". The cost $C$ is a sum (of $c$) over time-iterates, and it is of great importance to characterize its probabilistic behavior, as the truncation degree tends to $\infty$.

The density transformer, also known as the Perron-Frobenius operator,

$$\mathbf{H}_1[f](x) = \sum_{h \in \mathcal{H}} |h'(x)| \cdot f \circ h(x) \tag{2.5}$$

was introduced early in the study of continued fractions (see, e.g., the works of Lévy Khinchin, Kuzmin, Wirsing, Babenko, and Mayer). It describes the density of $T(X)$ when $X$ has density $f$. The density transformer encapsulates important information on the "dynamics" of the iterative process. Two of its properties, the existence of a unique dominant eigenvalue [Property *UDE*], relative to a density $f_1$, together with a spectral gap separating this eigenvalue from the remainder of the spectrum [Property *SG*] (see Figure 2) entail the applicability of simple and powerful spectral methods, in the $\mathcal{EMG}$–setting: As the truncation degree $n$ tends to $\infty$, the expectation $\mathrm{E}[C^{(n)}]$ of the cost $C^{(n)}$ is asymptotic to $n\widehat{\mu}(c)$, where

$$\widehat{\mu}(c) := \sum_{h \in \mathcal{H}} c(h) \int_{h(\mathcal{I})} f_1(x)\, dx \tag{2.6}$$

is the average of cost $c$ with respect to the dominant eigenfunction $f_1$.

In order to establish more precise results on the distribution of truncated trajectories, and study the speed of convergence, it is standard to use the moment generating function. One then works with a weighted transfer operator, which is a perturbation of the density

| | |
|---|---|
| *UDE* | Unique Dominant Eigenvalue at $(1,0)$ |
| *SG* | Spectral Gap at $(1,0)$ |
| $An_w(1,0)$ | Analyticity of operator with respect to $w$ at 0 for $s=1$ |
| $An_s(1,0)$ | Analyticity of operator with respect to $s$ at 1 for $w=0$ |
| $An_{s,w}(1,0)$ | Analyticity of operator with respect to $(s,w)$ in a neighborhood of $(1,0)$ |
| *SMVL* | Strict Maximum on the Vertical Line attained at $s=\sigma$ $\forall(\sigma,\nu)(\text{reals}), \forall t\neq 0, R(\sigma+it,\nu)<R(\sigma,\nu)$ |
| *UEVL* | Uniform Estimates near the Vertical Bi-Line $\{(s,w); \Re(s)=1, \Re(w)=0\}$: $\forall\xi>0, \exists M>0,\ t_0>0,$ such that $\forall(\sigma,\nu)(\text{real})$ near $(1,0)$ $\forall s=\sigma+it, w=\nu+i\tau, \lvert t\rvert>t_0, \quad \sup\lvert(I-\mathbf{H}_{s,w})^{-1}[1]\rvert\leq M\cdot\lvert t\rvert^{\xi}$ |

Figure 2: Main analytical properties of the operator $\mathbf{H}_{s,w}$ and its spectral radius $R(s,w)$ (on a convenient functional space).

| | Average-case | Distribution |
|---|---|---|
| Truncated real trajectories | *UDE* + *SG* | *UDE* + *SG* + $An_w(1,0)$ + strict convexity of $\log\lambda(1,w)$ at 0 |
| Rational trajectories | *UDE* + *SG* + $An_s(1,0)$ + *SMVL* | *UDE* + *SG* + $An_{s,w}(1,0)$ + *UEVL* + strict convexity of $\log\lambda(s,w)$ at $(1,0)$ |

Figure 3: Properties of the transfer operator useful for analyzing trajectories.

transformer. Quite general weighted transfer operators were introduced by Ruelle, in connection with thermodynamic formalism (see e.g. [34]).
Here, for a given digit-cost $c$, the transfer operator $\mathbf{H}_{1,w}$ depends on a parameter $w$ and is defined by

$$\mathbf{H}_{1,w}[f]=\sum_{h\in\mathcal{H}}\exp[wc(h)]\cdot\lvert h'\rvert\cdot f\circ h, \tag{2.7}$$

so that $\mathbf{H}_{1,0}=\mathbf{H}_1$. When $c$ is of $\mathcal{MG}$–type, the operator is well–defined and analytic with respect to $w$ when $w$ is near 0 [Property $An_w(1,0)$]. Then, perturbation theory [24] entails that the two properties *UDE* and *SG* extend to the operator $\mathbf{H}_{1,w}$ with a dominant eigenvalue $\lambda(1,w)$ and a spectral gap. If the digit-cost is non constant, the pressure function $\Lambda(1,w):=\log\lambda(1,w)$ is furthermore strictly convex. Finally, (see Figure 3) for non constant digit–costs of class $\mathcal{MG}$, this leads to a proof that, for any probability with smooth density, the asymptotic distribution of the total cost is Gaussian. The dominant terms of the expectation and the variance involve the first derivatives of function $\Lambda(1,w)$.

**Theorem 1.** *For a triple of $\mathcal{EMG}$ type with non-constant $c$ and any initial probability on $\mathcal{I}$ with a $\mathcal{C}^1$ density, there are $\widehat{\mu}(c)>0$ and $\widehat{\delta}(c)>0$ so that for any $n$, and any $Y\in\mathbb{R}$*

$$\mathbb{P}\left[x \ \middle|\ \frac{C^{(n)}(x)-\widehat{\mu}(c)n}{\widehat{\delta}(c)\sqrt{n}}\leq Y\right]$$

$$=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{Y}e^{-y^2/2}\,dy+O\left(\frac{1}{\sqrt{n}}\right).$$

*Furthermore, for any $\theta$ satisfying $\theta>r_1$ (where $r_1$ is the subdominant spectral radius of $\mathbf{H}_1$), the mean and the variance satisfy*

$$\mathbb{E}\,[C^{(n)}]=\widehat{\mu}(c)\cdot n+\widehat{\eta}(c)+O(\theta^n),$$

$$\mathbb{V}\,[C^{(n)}]=\widehat{\delta}^2(c)\cdot n+\widehat{\delta}_1(c)+O(\theta^n),$$

$$\text{with}\ \ \widehat{\mu}(c)=\Lambda'_w(1,0), \quad \widehat{\delta}^2(c)=\Lambda''_{w^2}(1,0). \tag{2.8}$$

This Central Limit Theorem (CLT) is quite well-known: for published results, including sometimes the Local Limit Theorem, see for instance [10] or [7] for interval maps, and [1] for a more abstract framework. The proof that we give in Section 3 is based on a compact and versatile Quasi-Powers statement of Hwang (see [23]). It encapsulates the consequences of the two main tools usually applied to get the CLT with speed of convergence: the Lévy continuity theorem for characteristic functions and the Berry-Esseen inequality. Hwang's Theorem includes useful asymptotic expressions (with error terms), for the expectation and variance. We shall also apply this theorem in our analysis of the Euclidean algorithms.

**2.3 Continued fractions of rational numbers: Average-case analysis of Euclidean Algorithms.** As already seen, rational trajectories reach 0 in finitely many steps and describe the execution of the Euclidean algorithms. They have been less extensively studied. The above-mentioned results about real inputs do not say anything about the set of rational inputs, since the rationals have zero Lebesgue measure. As it is often the case, the discrete problem is more difficult than its continuous counterpart. However, this problem is of central importance, since it corresponds to the analysis of the Euclidean algorithms: An execution of a Euclidean algorithm on the input $(u, v)$ gives rise to a rational trajectory $\mathcal{T}(u/v)$ which ends at 0, so that the analysis of the algorithm depends on the probabilistic analysis of such rational trajectories. Note that the reference parameter is no longer the truncation degree $n$, but the size $v := \max(u, v)$ of the input $(u, v)$.

We study here the total cost related to an execution of the Euclidean algorithm. The most basic cost is the number of iterations $P(u, v)$, which corresponds to the trivial digit-cost $c = 1$, but we are interested in general total costs $C$ relative to digit–costs $c$ of moderate growth. Now, the trajectory of $(u/v)$ is described by (2.2) and the total cost $C(u, v)$ is of the form

$$(2.9)\quad C(u,v) := \sum_{i=1}^{P(u,v)} c(h_i) \qquad \text{with} \quad P(u,v) := p.$$

The average-case complexity of Euclidean Algorithms is by now well-understood. For the basic total cost $P$, the results have been obtained around 1969, independently by Heilbronn and Dixon for algorithm $\mathcal{G}$, and by Rieger for $\mathcal{K}$. Recently, Vallée [41, 38, 40] used another perturbation of the density transformer, the transfer operator $\mathbf{H}_s$, together with its weighted version $\mathbf{H}_s^{(c)}$ defined as

(2.10)

$$\mathbf{H}_s[f] = \sum_{h\in\mathcal{H}} |h'|^s \cdot f\circ h, \qquad \mathbf{H}_s^{(c)} := \sum_{h\in\mathcal{H}} c(h)\cdot|h'|^s\cdot f\circ h,$$

to analyze Euclidean Algorithms. Note first that operators similar to $\mathbf{H}_s$ appear in the study of discrete-time dynamics over continuous spaces: with $s$ real, they are related, via the Bowen formula, to Hausdorff-dimension of invariant sets (see e.g. [35]). But they are also used in continuous-time dynamics (flows) over continuous spaces, with $s$ complex related to the parameter of the Fourier transform of the continuous-time correlation function (see e.g. [30, 14]). The study of $\mathbf{H}_s$ for $s$ with large imaginary part is indeed related to the speed of decay of correlations for Anosov flows, a very difficult problem only solved recently [14].

Using the operator $\mathbf{H}_s$ in the analysis of Euclidean algorithms leads to a "dynamical analysis" approach that provides a unifying framework for the average-case analysis in the $\mathcal{EMG}$–setting and shows that the rational trajectories have an expected behavior similar to what is observed on truncated real trajectories. More precisely (see [41]), the expectation $\mathbb{E}_N[P]$ of the number of steps $P$ on rational trajectories whose inputs have numerator and denominator less than $N$ is asymptotic to $\mu \log N$, where $\mu = 2/|\lambda'(1)|$, and $\lambda(s)$ is the dominant eigenvalue of the operator $\mathbf{H}_s$. More generally, for a triple of $\mathcal{EMG}$–type, the mean value $\mathbb{E}_N[C]$ of the total cost $C(u/v)$ of trajectory $\mathcal{T}(u/v)$ satisfies

$$\mathbb{E}_N[C] \sim \widehat{\mu}(c)\cdot \mu \log N\,,$$

with $\widehat{\mu}(c)$ the asymptotic mean value (2.6) of real (truncated) trajectories.

We now explain the rôle of the parameter $s$ in the operator, discussing briefly the proof of the above claim. For the discrete algorithms, the relevant parameters are described by generating functions, a common tool in the average-case study of algorithms [17]. As it is usual in number theory contexts, the generating functions are Dirichlet series $S(s)$ where the parameter $s$ "marks" the size $v$ of input $(u, v)$. It turns out that $S(2s)$ can be (easily) expressed with the "quasi-inverse" $(I - \mathbf{H}_s)^{-1}$ of the transfer operator, together with the weighted operator $\mathbf{H}_s^{(c)}$. Hence the asymptotic extraction of the coefficients of $S(s)$ can be achieved by means of Tauberian theorems [13, 36], which yield the desired estimates on mean values of the total costs related to rational trajectories. To check that the hypotheses of the Tauberian theorems are satisfied, analyticity of the operator $\mathbf{H}_s$ at $s = 1$ [Property $An_s(1, 0)$], in conjunction with *UDE* and *SG*, is useful, together with Property *SMVL,* which requires that the spectral radius of the transfer operator $\mathbf{H}_s$ admits a strict maximum on the vertical line $\Re(s) = 1$ at $s = 1$ (see Figures 2 and 3).

**2.4 Euclidean Algorithms: Distributional analysis and dynamical methods.** In view of the average-case results (and the distributional results for truncated real trajectories) just presented, it is natural to ask whether the distribution of the total cost $C(u/v)$ on rational trajectories with $0 < u \le v \le N$ is asymptotically Gaussian (when $N$ tends to $\infty$)? This paper provides a precise answer to this question in the $\mathcal{EMG}$–setting.

Distributional analyses build upon the tools used for the average-case, that is, generating functions. However, they are now bivariate, of the form $S(s,w)$. Like for the average-case analysis, they are of Dirichlet type with respect to the variable $s$, but an extra parameter, $w$, of the type usual in moment generating functions, is needed for non-constant costs. Accordingly, we introduce a two-variable (weighted) transfer operator $\mathbf{H}_{s,w}$ defined by

$$\mathbf{H}_{s,w}[f] = \sum_{h\in\mathcal{H}} \exp[wc(h)] \cdot |h'|^s \cdot f \circ h, \tag{2.11}$$

which is a generalization of all previously introduced transfer operators [see (2.5, 2.7, 2.10) and note that $\mathbf{H}_s^{(c)}$ is just the derivative of $\mathbf{H}_{s,w}$ at $w = 0$]. We shall establish below (4.25) a simple relation between $S(2s,w)$ and the quasi-inverse $(I - \mathbf{H}_{s,w})^{-1}$ of the two-variable operator $\mathbf{H}_{s,w}$,

$$S(2s,w) = \mathbf{F}_{s,w} \circ (I - \mathbf{H}_{s,w})^{-1}[1](0)\,,$$

where the transfer operator $\mathbf{F}_{s,w}$ is relative to the final set $\mathcal{F}$ used in the last step of the algorithm.

In a sense, distributional analyses are obtained by (uniform) perturbation of average-case analyses. Following [17], parameters of combinatorial or number-theoretic structures, provided they remain "simple' ' enough, lead to local deformations (via an auxiliary variable $w$) of the functional relations defining univariate generating functions. Under fairly general conditions, such deformations are amenable to perturbation theory and admit of uniform expansions near singularities.

In this paper, we apply dynamical methods for the first time to the distributional analysis of (discrete) algorithms. This leads to a new facet of the domain: distributional dynamical analysis. We now need uniform estimates of coefficients of bivariate series $S(s,w)$ with respect to the parameter $w$, which "marks" the cost. While Tauberian Theorems sufficed for average-case analyses, they prove insufficient for distributional analyses, since they do not provide (uniform) remainder terms. We then need a more precise "extractor" of coefficients, and the Perron formula is well-suited to this purpose. A sufficient condition for the applicability of Perron's formula is the "uniform" Property *UEVL* on the quasi-inverse of the transfer operator $\mathbf{H}_{s,w}$.

### 2.5 Condition *UNI* and Property *UEVL*.

**Property** *UEVL.* It expresses that, when $(\Re s, \Re w)$ is near the reference point $(1,0)$ with $|\Im s| > t_0$, for some $t_0 > 0$, a uniform power-law estimate $|\Im s|^\xi$, with $\xi$ small, holds on the quasi-inverse $(I - \mathbf{H}_{s,w})^{-1}$ (see Figure 2).
Note that the work of Mayer [28, 29] relative to the standard Euclidean algorithm shows that there is $\alpha > 0$ for which the quasi inverse $(I - \mathbf{H}_{s,0})^{-1}$ is analytic for $\Re s \ge 1 - \alpha$ and $s \ne 1$. However, this property does not suffice and we actually need *UEVL*.

We adapt here powerful methods due to Dolgopyat [14] and we show that the two-variable transfer operator satisfies *UEVL*. In the spirit of Chernov [9], Dolgopyat [14] introduced several "uniform nonintegrability" (*UNI* ) conditions on the dynamical foliations. Then, he proved that the *UNI* Conditions implies *UEVL* Property in the case of one–variable transfer operators $\mathbf{H}_s$ which are related to dynamical systems with a finite number of branches. We have to adapt Dolgopyat's result to our context.

We first give a new formulation of the strongest of Dolgopyat's *UNI* Conditions, only implicit in Section 5 of [14], which expresses that the derivatives of inverse branches of the dynamical system $(\mathcal{I}, T)$ are "not too close", except on a set of "small measure".

**Condition** *UNI.* We introduce a "distance" $\Delta$ between two inverse branches $h$ et $k$ of same depth,

$$\Delta(h,k) = \inf_{x\in\mathcal{I}} \left| \frac{h''}{h'}(x) - \frac{k''}{k'}(x) \right| \tag{2.12}$$

and, for $h$ in $\mathcal{H}^n$, and $\eta > 0$, we denote by $J(h,\eta)$ the union of the fundamental intervals $k(\mathcal{I})$, where $k \in \mathcal{H}^n$ ranges over the $\Delta$-ball of center $h$ and radius $\eta$:

$$J(h,\eta) := \bigcup_{k\in\mathcal{H}^n, \Delta(h,k)\le\eta} k(\mathcal{I}).$$

Recalling that $\rho$ is the contraction ratio defined in (2.3), Condition *UNI* expresses that, for any $a, 0 < a < 1$, the Lebesgue measure of $J(h, \rho^{an})$ (for $h \in \mathcal{H}^n$) is $O(\rho^{an})$, with a uniform $O$–term (with respect to $h, n, a$).

We first prove that all the Systems of $\mathcal{E}$ satisfy Condition *UNI.* This is due to the good properties of their dual systems (see Lemma 7 in [4]).
Then we have to modify Dolgopyat's arguments which prove that *UNI* implies *UEVL*: we must consider dynamical systems which may possess an infinite number of branches, and we work with bivariate weighted transfer operators $\mathbf{H}_{s,w}$ involving a cost function. We finally prove the following theorem, which is the central functional analytic result of the paper and provides Property *UEVL.*

**Theorem 2** [Dolgopyat-type estimates]. *Consider a triple of $\mathcal{EMG}$-type, with contraction ratio $\rho$, and let $\mathbf{H}_{s,w}$ be its weighted transfer operator. For any $\xi > 0$, there is a real neighborhood $\Sigma_1 \times W_1$ of $(1,0)$, and there is a constant $M > 0$, such that, for all $s = \sigma + it$, $w = \nu + i\tau$ with $(\sigma, \nu) \in \Sigma_1 \times W_1$ and $|t| \geq 1/\rho^2$,*

$$\sup_{x \in \mathcal{I}} \left| (I - \mathbf{H}_{s,w})^{-1}[1](x) \right| \leq M \cdot |t|^{\xi}. \tag{2.13}$$

Dolgopyat was interested in the decay of correlations relative to flows. Later on, Pollicott and Sharp used Dolgopyat's bounds together with Perron's formula to find error terms in some asymptotic estimates for geodesic flows on surfaces of variable negative curvature (see e.g. [31]). Note that they work with univariate Dirichlet series with positive coefficients whereas we need uniform estimates on coefficients of bivariate Dirichlet series with complex cofficients. To the best of our knowledge, the present paper is the first instance where these powerful tools are applied to distributional analyses in discrete combinatorics. This paper can also be viewed in essence as a realization of Hensley's prophecy in [20]: "This suggests that [our results] might be sharpened considerably. Perhaps, what is needed is a deeper understanding of the function $\lambda(s)$ and the [transfer] operators".

**2.6 Our main results.** With Dolgopyat estimates and Perron's formula, we obtain the following Central Limit Theorem (see Section 4 for a description of the main steps of the proof).

**Theorem 3.** [Central Limit Theorem for costs.] *Consider a Euclidean Algorithm of the class $\mathcal{E}$. Denote by $\widetilde{\Omega}_N$ the set of pairs $(u,v)$ with $u/v \in \mathcal{I}$ and $0 < v \leq N$, and by $\Omega_N$ the set of coprime pairs of $\Omega_N$. For any cost $c$ of moderate growth, there is $\alpha > 0$ so that :*
*$(a)$ The distribution of the total cost $C$ on $\Omega_N, \widetilde{\Omega}_N$ is asymptotically Gaussian, with speed of convergence $O(1/\sqrt{\log N})$, i.e., there exist two constants $\mu(c) > 0$ and $\delta(c) > 0$ such that, for any $N$, and any $y \in \mathbb{R}$*

$$\mathbb{P}_N \left[ (u,v) \;\middle|\; \frac{C(u,v) - \mu(c) \log N}{\delta(c)\sqrt{\log N}} \leq y \right]$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-x^2/2}\, dx + O\left( \frac{1}{\sqrt{\log N}} \right).$$

*$(b)$ The mean and the variance satisfy,*

$$\mathbb{E}_N[C] = \mu(c) \log N + \eta(c) + O(N^{-\alpha}),$$
$$\mathbb{V}_N[C] = \delta^2(c) \log N + \delta_1(c) + O(N^{-\alpha}).$$

*$(c)$ In the special case $c \equiv 1$, the constants $\mu := \mu(1)$, $\delta^2 := \delta^2(1)$ involve the first two derivatives of the pressure function $\Lambda(s)$:*

$$\mu = \frac{2}{|\Lambda'(1)|} > 0, \quad \delta^2 = \frac{2|\Lambda''(1)|}{|\Lambda'(1)^3|} > 0. \tag{2.14}$$

*In particular, $2/\mu$ is the entropy for $(T, f_1 dx)$. In the general case, $\mu(c) = \mu \cdot \widehat{\mu}(c)$, and*

$$\delta^2(c) = \widehat{\mu}^2(c) \cdot \delta^2 + \mu \cdot \widehat{\delta}^2(c) + \mu^2 \cdot \widehat{\mu}(c) \cdot \chi(c) > 0,$$

*where $\widehat{\mu}(c)$, $\widehat{\delta}(c)$ are the constants of Theorem 1, and $\chi(c) = \Lambda''_{sw}(1,0)$.*

Note that $\alpha$ depends a priori on the cost $c$ (remark that this was not the case for $\theta$ in Theorem 1). The constant $\chi(c)$ can be viewed as a covariance coefficient between the number of steps $P$ and the cost $c$. Since there exists a closed form for the invariant density $f_1$ for the systems of $\mathcal{E}$, the constants $\mu, \widehat{\mu}(c)$, and thus $\mu(c)$ can be easily computed (see [41]). On the other hand, the constants $\widehat{\delta}(c)$, $\delta$, $\delta(c)$ do not seem to admit a closed form. However, Lhote has proved that they can be computed in polynomial time [27].

With similar methods, we then obtain the following Local Limit Theorem for any lattice cost of moderate growth (see Section 4 for a description of the main steps of the proof). Note that the LLT was previously obtained by Hensley [20], in the particular case of the Standard Euclidean Algorithm and of the trivial cost $c = 1$, and with a worse speed of convergence. His proof used the transfer operator, but in way appreciably different from ours: Hensley approximates discrete measures on rationals by continuous measures, and he obtains distributional results on rational trajectories by approximating them by truncated real trajectories. In particular, he avoids dealing with parameters $s$ of large imaginary parts.

**Theorem 4.** [Local Limit Theorem for lattice costs.] *For any algorithm among $\mathcal{G}$, $\mathcal{K}$, $\mathcal{O}$, and any lattice cost $c$ of span $L > 0$ (i.e., a cost $c$ whose values belong to a subset $L\mathbf{N}$) and of moderate growth, and letting $\mu(c) > 0$ and $\delta^2(c) > 0$ be the constants from Theorem 3, the following holds,*

$$\mathbb{P}_N \left[ -\frac{L}{2} < C(u,v) - \mu(c) \log N - \delta(c) x \sqrt{\log N} \leq \frac{L}{2} \right]$$
$$= \frac{e^{-x^2/2}}{\delta(c)\sqrt{2\pi \log N}} + O\left( \frac{1}{\log N} \right),$$

*with a $O$ uniform for $x \in \mathbb{R}$. The same holds for $\widetilde{\mathbb{P}}_N$ in $\widetilde{\Omega}_N$.*

## 3 Dynamical Analysis of Continued Fraction Expansions of Real Numbers

In this section, we introduce the weighted transfer operator (§3.1) and recall its main properties (§3.2). §3.3 explains (as a useful and exemplary parenthesis) the fundamental rôle this operator plays in the distributional analysis of truncated real trajectories. Theorem 1 is proved using Hwang's Quasi-Power result.

**3.1 Transfer operators of interval maps.** If $\mathcal{I}$ is endowed with an initial probability density with respect to Lebesgue measure $f = f_0$, repeated applications of the map $T$ modify the density, and the flow of successive densities $f_1, f_2, \ldots, f_n, \ldots$ describes the global evolution of the system at time $t = 0, 1, 2, \ldots, n, \ldots$. The operator $\mathbf{H}$ such that $f_1 = \mathbf{H}[f_0]$ and more generally $f_n = \mathbf{H}[f_{n-1}] = \mathbf{H}^n[f_0]$ for all $n$ is called the density transformer, or the Perron-Frobenius operator. It is defined as

$$\mathbf{H}[f](x) := \sum_{h \in \mathcal{H}} |h'(x)| \; f \circ h(x)\,.$$

We consider a digit–cost of $\mathcal{MG}$–type, i.e., a strictly positive digit-cost $c$ defined on $\mathcal{H}$ which satisfies $c(m) = O(\log m)$. Then the series

$$\sum_{h \in \mathcal{H}} \exp[wc(h)] \cdot |h'(x)|^s$$

is convergent when $(\Re s, \Re w)$ belongs to some real neighborhood of $(1, 0)$, or, equivalently to $\Sigma_0 \times W_0$ with

(3.15)
$$\Sigma_0 = ]\sigma_0, +\infty] \ \text{ and } \ W_0 = ]-\infty, \nu_0[ \ \text{ for } \ \sigma_0 > (1/2), \nu_0 > 0.$$

In the sequel, we study properties of trajectories in the $\mathcal{EMG}$–setting. We extend the digit cost $c$ to a cost function, also denoted $c$, on $\mathcal{H}^\star$ by

$$c(h_1 \circ h_2 \circ \ldots \circ h_k) := \sum_{i=1}^{k} c(h_i)$$

and we introduce the two-variable transfer operator $\mathbf{H}_{s,w}$ which extends the transfer operator, via $\mathbf{H}_{1,0} = \mathbf{H}$. It depends on two (complex) parameters $s$ and $w$,

(3.16)
$$\mathbf{H}_{s,w}[f](x) := \sum_{h \in \mathcal{H}} \exp[wc(h)] \cdot |h'(x)|^s \cdot f \circ h(x).$$

The operator $\mathbf{F}_{s,w}$ is defined in a similar way, with $\mathcal{F}$ replacing $\mathcal{H}$. Note that the additive property of costs (together with the multiplicative property of the derivatives) entails

(3.17)
$$\mathbf{H}^n_{s,w}[f](x) := \sum_{h \in \mathcal{H}^n} \exp[wc(h)] \cdot |h'(x)|^s \cdot f \circ h(x)\,.$$

In particular, the quasi-inverse $(I - \mathbf{H}_{s,w})^{-1}$ can be written (formally) as

(3.18)
$$(I - \mathbf{H}_{s,w})^{-1}[f](x) := \sum_{h \in \mathcal{H}^\star} \exp[wc(h)] \cdot |h'(x)|^s \cdot f \circ h(x)\,.$$

We shall recall next some classical properties of the weighted transfer operator.

**3.2 Summary of classical spectral properties of transfer operators** (For more precisions, see e.g. [3, 7, 10, 12, 37]). Let $\mathbf{H}_{s,w}$ be the transfer operator (3.16) associated to a $\mathcal{EMG}$ triple. Let $\Sigma_0$, $W_0$ be the real sets from (3.15). When $(\Re s, \Re w)$ belongs to $\Sigma_0 \times W_0$, the operator $\mathbf{H}_{s,w}$ acts boundedly on the Banach space $\mathcal{C}^1(\mathcal{I})$ endowed with the norm $\|\cdot\|_1$ defined by $\|f\|_1 = \sup|f| + \sup|f'|$. It depends analytically on $(s, w)$. When $w = 0$, we omit the second index in the operator and its associated objects.

$(a)$ *Spectral Dominant Properties and Analyticity.* For real parameters $(s, w) \in \Sigma_0 \times W_0$, the operator $\mathbf{H}_{s,w}$ is quasi-compact [1], satisfies *UDE* and *SG*. Analyticity Property, together with perturbation theory, proves that the dominant eigenvalue $\lambda(s, w)$, the dominant eigenvector $f_{s,w}$, the subdominant spectral radius $r_{s,w}$ are well-defined and analytic when $(s, w)$ is near the real axes.

$(b)$ *Pressure function.* For $(\sigma, \nu) \in \Sigma_0 \times W_0$, the pressure function is defined as $\Lambda(\sigma, \nu) := \log \lambda(\sigma, \nu)$. The first derivatives of $\Lambda$ satisfy

$$\Lambda'(1) = -\int_{\mathcal{I}} \log|T'(x)|\, f_1(x)\, dx < 0\,,$$

$$\Lambda'_w(1, 0) = \sum_{h \in \mathcal{H}} c(h) \int_{h(\mathcal{I})} f_1(x)\, dx,$$

and $\Lambda'(1)$ is the opposite of the entropy of the dynamical system $(T, \mu_1)$ while $\Lambda'_w(1, 0)$ is the average of the cost (with respect to $f_1$), equal to $\widehat{\mu}(c)$ [see (2.6)].

$(c)$ *Strict convexity of the pressure.* The pressure is strictly convex in $s$, i.e., $\Lambda''_{s^2}(\sigma, \nu) > 0$. Also $\Lambda(\sigma + q\nu, \nu)$ is strictly convex as a function of $\nu$ for all fixed $q \neq 0$ and fixed $\sigma$. If $c$ is not constant, the pressure is strictly convex in $w$, i.e., $\Lambda''_{w^2}(\sigma, \nu) > 0$.

$(d)$ *Function $\sigma$.* There is a complex neighborhood $\mathcal{W}$ of 0 and a unique function $\sigma : \mathcal{W} \to \mathbb{C}$ such that $\lambda(\sigma(w), w) = 1$; this function is analytic near 0, and $\sigma(0) = 1$.

$(e)$ *Condition UNI and aperiodicity.* Since the systems of the class $\mathcal{E}$ satisfy the *UNI* Condition, they fulfill

[1] An operator is quasi–compact if the upper part of its spectrum is formed with isolated eigenvalues with finite multiplicity

aperiodicity conditions: First, for any $t \neq 0$, 1 does not belong to $\mathrm{Sp}\,\mathbf{H}_{1+it,0}$ (this is a weak version of the $SMVL$ Condition). Second, if $c$ is a lattice cost with span $L$, for all $t$, and all $\tau$ not multiple of $2\pi/L$, 1 does not belong to $\mathrm{Sp}\,\mathbf{H}_{1+it,i\tau}$. (See Proposition 1 in [4]).

**3.3 Transfer operators and real trajectories.** We now describe the fundamental rôle played by the operator $\mathbf{H}_{1,w}$ in the analysis of truncated real trajectories. We consider any triple of $\mathcal{EMG}$ type, with a non–constant cost $c$. The interval $\mathcal{I}$ is endowed with a probability measure with smooth density $f$, and we are interested in the asymptotic behavior of the distribution of

$$C^{(n)}(x) := \sum_{i=1}^{n} c(h_i)\,.$$

when the truncation degree $n$ tends to $\infty$. [Recall that the $h_i$'s ($1 \le i \le n$) are the first $n$ LFTs used by the trajectory $\mathcal{T}(x)$.] As already mentioned, a very convenient tool is the moment generating function $M_n(w)$ of the cost $C^{(n)}$, defined by

$$M_n(w) := \mathrm{E}[\exp(wC^{(n)})] = \sum_{h\in\mathcal{H}^n} \exp[wc(h)]\cdot\int_{h(\mathcal{I})} f(y)\,dy\,.$$

With the change of variables $y = h(u)$, we can rewrite $M_n(w)$ as:

$$M_n(w) = \sum_{h\in\mathcal{H}^n} \exp[wc(h)]\cdot\int_{\mathcal{I}} |h'(u)|\cdot f\circ h(u)\,du$$

$$= \int_{\mathcal{I}} \mathbf{H}^n_{1,w}[f](u)\,du\,. \tag{3.19}$$

The above relation is fundamental for analysing costs on truncated real trajectories: From Section 3.2 ($a$), (recalling that $r_1$ is the subdominant spectral radius), for any $\theta > r_1$, there is a complex neighborhood $\mathcal{W}$ of 0 on which the operator $\mathbf{H}_{1,w}$ splits as

$$\mathbf{H}_{1,w} = \lambda(1,w)\,\mathbf{P}_{1,w} + \mathbf{N}_{1,w}\,,$$

where $\mathbf{P}_{1,w}$ is the projector on the dominant eigensubspace for the eigenvalue $\lambda(1,w)$, and $\mathbf{N}_{1,w}$ has spectral radius $r_{1,w} \le \theta|\lambda(1,w)|$. Therefore, for any $n \ge 1$

$$\mathbf{H}^n_{1,w}[f](u) = \lambda(1,w)^n\,\mathbf{P}_{1,w}[f](u)\,du + \mathbf{N}^n_{1,w}[f](u)\,,$$

which entails

$$M_n(w) = \left(\lambda(1,w)^n \int_{\mathcal{I}} \mathbf{P}_{1,w}[f](u)\,du\right)(1 + O(\theta^n))\,,$$

with a uniform $O$-term for $w \in \mathcal{W}$. In other words, the moment generating function $M_n(w)$ behaves as a "Quasi-Power", and we are in a position to apply the following result, in order to prove Theorem 1:

**Hwang's Quasi-Power Theorem** [23]. *Assume that the moment generating functions relative to a sequence of functions $\widehat{C}_N$ on probability spaces $\widehat{\Omega}_N$ are analytic in a complex neighborhood $\mathcal{W}$ of 0, where they satisfy*

$$\mathrm{E}_N[\exp(w\widehat{C}_N)] = \exp[\beta_N U(w) + V(w)]\left(1 + O(\kappa_N^{-1})\right)\,,$$

*with $\beta_N$, $\kappa_N \to \infty$ as $N \to \infty$, and $U(w)$, $V(w)$ analytic on $\mathcal{W}$. Assume also that $U''(0) \neq 0$. Then, the mean and the variance satisfy*

$$\mathrm{E}_N[\widehat{C}_N] = \beta_N U'(0) + V'(0) + O(\kappa_N^{-1})\,,$$

$$\mathbb{V}_N[\widehat{C}_N] = \beta_N U''(0) + V''(0) + O(\kappa_N^{-1})\,.$$

*Furthermore, the distribution of $\widehat{C}_N$ on $\widehat{\Omega}_N$ is asymptotically Gaussian, with speed of convergence $O(\kappa_N^{-1} + \beta_N^{-1/2})$.*

For our application to Theorem 1, we set $\widehat{\Omega}_n = (\mathcal{I}, f\,dx)$ for all $n$, $\widehat{C}_n = C^{(n)}$, $\beta_n = n$, $\kappa_n = \theta^{-n}$. Function $U$ equals the pressure function $w \mapsto \Lambda(1,w)$ and $V(w) = \log\left(\int_{\mathcal{I}} \mathbf{P}_{1,w}[f](u)\,du\right)$. Note that, when $c$ is not constant, the function $\Lambda(1,w)$ is strictly convex at $w = 0$, (see Section 3.2) and $U''(0) \neq 0$. Note that $f_1$ is explicitly given in Figure 1 for $\mathcal{G}$, $\mathcal{O}$, and $\mathcal{K}$, so that $\widehat{\mu}(c)$ is computable in these cases. The constants $\widehat{\mu}(c)$ and $\widehat{\delta}(c)$ will appear in Theorem 3. A Local Limit Theorem and a Large Deviations Property hold in this context (see [7, 1]).

## 4 Dynamical Analysis of Continued Fraction Expansions of Rational Numbers

In this section, we turn to rational inputs and Euclidean Algorithms. We introduce in §4.1 Dirichlet series of moment generating functions, which we relate to the quasi-inverse of the weighted transfer operator. We explain (in §4.2) how to use Perron's Formula to extract coefficients of Dirichlet series and why Property *UEVL* is needed for this. Next, in §4.3 we explain why this leads to a uniform quasi-power approximation for the moment generating function of costs. Theorem 3 follows, applying again Hwang's Quasi-Power theorem, and provides the asymptotic Gaussian distribution for costs of moderate growth on rational trajectories. Finally, we focus in §4.4 on lattice costs, and describe how an application of the saddle point method entails our local limit theorem, Theorem 4.

**4.1 Dirichlet series and transfer operators.** We restrict now our study to rational inputs $x = (u/v) \in \mathcal{I}$ in the $\mathcal{EMG}$–setting. We will see, with (4.26), that it is sufficient to consider the sets

$$\Omega := \{(u,v);\ \frac{u}{v} \in \mathcal{I}, v > 0, \gcd(u,v) = 1\},$$

$$\Omega_N := \{(u,v) \in \Omega; v \le N\},$$

as the possible inputs. Precisely, we deal with the probabilistic model relative to $\Omega_N$ endowed with uniform probability $\mathbb{P}_N$.

Our tool to study the distribution of the total cost $C(u,v)$, associated to a digit-cost $c$ and defined in (2.9), is its *moment generating function* on $\Omega_N$,

$$\text{(4.20)} \qquad \mathbb{E}_N[\exp(wC)] := \frac{\Phi_w(N)}{\Phi_0(N)},$$

where $\Phi_w(N)$ is the cumulative value of $\exp(wC)$ on $\Omega_N$,

(4.21)

$$\Phi_w(N) := \sum_{(u,v)\in\Omega_N} \exp[wC(u,v)], \quad \Phi_0(N) = |\Omega_N|.$$

To analyse the moment generating function $\mathbb{E}_N[\exp(wC)]$ of the cost $C$ on $\Omega_N$, it then suffices to estimate the functions $\Phi_w(N)$, asymptotically in $N \to \infty$, and uniformly in $w$ in a complex neighborhood of 0. Extending the principles defined in [38, 40, 41], we replace the sequence of moment generating functions by a single bivariate Dirichlet series, henceforth called the Dirichlet-moment generating function:

(4.22)

$$S(s,w) := \sum_{(u,v)\in\Omega} \frac{1}{v^s} \exp[wC(u,v)] = \sum_{n\ge 1} \frac{c_n(w)}{n^s},$$

$$\text{where } c_n(w) := \sum_{(u,v)\in\Omega, v=n} \exp[wC(u,v)].$$

Then, the relation

$$\text{(4.23)} \qquad \sum_{n\le N} c_n(w) = \Phi_w(N)$$

shows that the moment generating function (4.20) is related to partial sums of the coefficients of series $S(s,w)$.

As we previously did in Section 3.3 for truncated real trajectories, we aim to relate the moment generating function of costs on rational trajectories to the weighted transfer operator. Since each inverse branch of any depth is a linear fractional transformation

$$h(x) = (ax+b)/(cx+d),$$

with $a, b, c, d$ coprime integers, with determinant $ad - bc = \pm 1$, and denominator $D[h]$ related to $|h'|$ through

$$D[h](x) := |cx+d| = |\det h|^{1/2}\, |h'(x)|^{-1/2} = |h'(x)|^{-1/2},$$

the transfer operator can be alternatively defined by

(4.24)

$$\mathbf{H}_{s,w}[f](x) = \sum_{h\in\mathcal{H}} \exp[wc(h)] \frac{1}{D[h](x)^{2s}}\ f \circ h(x).$$

An execution of the Euclidean algorithm on an input $(u,v)$ of $\Omega$ performing $p$ steps uniquely decomposes the rational $(u/v)$ in a unique way as

$$\frac{u}{v} = h_1 \circ h_2 \circ \ldots \circ h_p(0) = h(0),$$

with $h_i \in \mathcal{H}, 1 \le i \le p-1$ and $h_p \in \mathcal{F}$. Thus, each Euclidean algorithm defines a map $(u,v) \mapsto h$ which is a bijection between the sets $\Omega$ and $\mathcal{H}^\star \times \mathcal{F}$. In view of (4.24,4.22,3.18), the relations

$$v = D[h](0), \quad C(u,v) = c(h) = \sum_{i=1}^{p} c(h_i), \quad P(u,v) = p.$$

provide the desired expression for the Dirichlet moment generating function $S(s,w)$ in terms of the transfer operators $\mathbf{H}_{s,w}$ and $\mathbf{F}_{s,w}$:

$$\text{(4.25)} \qquad S(2s,w) = \mathbf{F}_{s,w} \circ (I - \mathbf{H}_{s,w})^{-1}[1](0).$$

With the set $\widetilde{\Omega}$ of all pairs $(u,v)$ with $(u/v) \in \mathcal{I}$, we may define a Dirichlet moment generating function $\widetilde{S}(s,w)$. Since each element $(u',v')$ can be written in a unique way as $(du,dv)$ with coprime $(u,v)$, and $C(u,v) = C(u',v')$, one has

$$\text{(4.26)} \qquad \widetilde{S}(2s,w) = \zeta(2s) S(2s,w)$$

Using well-known properties of the Riemann zeta function $\zeta(s)$, all our results for $\widetilde{\Omega}_N$ will follow from those on $\Omega_N$.

In view of (4.20, 4.22, 4.23), the relations (4.25), (4.26) connecting the Dirichlet moment generating function with the transfer operator are the analogues for rational trajectories of the relation (3.19) for the truncated real trajectories. In the case of rational trajectories, we have to work with the quasi-inverse and extract the coefficients of Dirichlet series. This is why the discrete problem, which we wish to solve here, is more difficult to solve than the continuous problem. The sequel of the Section motivates and summarizes informally the main steps of our work.

**4.2 Perron's formula and Dolgopyat's estimates.** We wish to evaluate the sum $\Phi_w(N)$ of the first $N$ coefficients of the Dirichlet series $S(2s,w)$. Our first main tool towards this goal is the Perron Formula of order two (see [15]), which is valid for a Dirichlet series $F(s) = \sum_{n\geq 1} a_n n^{-s}$ and a vertical line $\Re s = D > 0$ inside the domain of convergence of $F$,

$$\Psi(T) := \sum_{n\leq T} a_n (T-n) = \frac{1}{2i\pi}\int_{D-i\infty}^{D+i\infty} F(s)\frac{T^{s+1}}{s(s+1)}\,ds\,.$$

Applying it to the Dirichlet series $S(2s,w)$, we find

$$\Psi_w(T) := \sum_{n\leq T} c_n(w)(T-n) = \frac{1}{2i\pi}\int_{D-i\infty}^{D+i\infty} S(2s,w)\frac{T^{2s+1}}{s(2s+1)}\,ds\,. \tag{4.27}$$

Thus, Perron's formula gives us information on $\Psi_w(N)$, which is just a Cesaro sum of the $\Phi_w(Q)$:

$$\Psi_w(N) = \sum_{Q\leq N}\sum_{n\leq Q} c_n(w) = \sum_{Q\leq N}\Phi_w(Q)\,.$$

We shall explain in the next subsection below how to transfer information from $\Psi_w$ to $\Phi_w$.

Now, we first discuss the choice of $D$. In view of (4.25) and Section 3.2, for any fixed $w$ (near 0), the domain of convergence of $S(2s,w)$ is limited by the rightmost values of $s$ for which the transfer operator $\mathbf{H}_{s,w}$ (acting on $\mathcal{C}^1(\mathcal{I})$) admits 1 as an eigenvalue. Section 3.2 $(d)$ also shows that $s \mapsto S(2s,w)$ has a possible pole at $s = \sigma(w)$, where $\sigma(w)$ is the unique complex number near 1 for which $\lambda(\sigma(w),w) = 1$. In particular, the integral in (4.27) is well-defined if $D > \sup_w(\Re\sigma(w))$.

It is next natural to modify the integration contour $\Re s = D$ into a contour containing $\sigma(w)$ as a unique pole of $S(2s,w)$. This is possible (for a quadrilateral contour) if there is $\alpha > 0$ and a neighborhood $\mathcal{W}$ of 0 for which the following is true:

- $(i)$ for all $w \in \mathcal{W}$, the Dirichlet series $S(2s,w)$ admits $s = \sigma(w)$ as a unique pole in the strip $|\Re s - 1| \leq \alpha$.
- $(ii)$ On the left vertical line $\Re s = 1-\alpha$, the series $S(2s,w)$ is $O(|\Im s|^{\xi})$, with a small $\xi$, and a uniform $O$-term (with respect to $w \in \mathcal{W}$), so that it is possible to control the integral (4.27) on the left vertical line $\Re s = 1-\alpha$, in a uniform way with respect to $w$.

These two properties are clear consequences of Property *UEVL*. And Theorem 2 proves that Property *UEVL* holds in the $\mathcal{EMG}$–setting.

**4.3 Asymptotic normality and Quasi-Power estimates.** Perron's Formula (4.27) combined with the fundamental relation (4.25), together with Property *UEVL* will provide the following estimate for the Cesaro sum $\Psi_w$ of $\Phi_w$, as $T \to \infty$,

$$\Psi_w(T) := \sum_{n\leq T} c_n(w)(T-n) = \frac{E(w)}{\sigma(w)(2\sigma(w)+1)}T^{2\sigma(w)+1}\left[1+O(T^{-2\alpha})\right], \tag{4.28}$$

where $E(w)$ is the residue of $S(2s,w)$ at the pole $s = \sigma(w)$, and the $O$–term is uniform on $\mathcal{W}$ when $T \to \infty$. Note that $\sigma$ and $E$ are analytic on a complex neighborhood of $w = 0$. It does not seem easy to transfer the information (4.28) on $\Psi_w(T)$ to estimates on $\Phi_w(T)$; we proceed in three steps to prove asymptotic normality of the cost $C$:

*First Step.* We introduced a smoothed model, i.e., the probabilistic model $(\overline{\Omega}_N, \overline{\mathbb{P}}_N)$ defined as follows: For any integer $N$, set $\overline{\Omega}_N = \Omega_N$; next, choose uniformly an integer $Q$ between $N - \lfloor N^{1-2\alpha}\rfloor$ and $N$, and draw uniformly an element $(u,v)$ of $\Omega_Q$. Slightly abusing language, we refer to the function $C$ in the model $(\overline{\Omega}_N, \overline{\mathbb{P}}_N)$ as the "smoothed cost." Now, we appeal to a classical result that is often used in number theory contexts (see Lemma 10 in [4]), and we then deduce from (4.28) the following quasi-power estimates for the moment generating function of the "smoothed" version of the cost $C$,

$$\frac{\overline{\mathbb{E}}_N[\exp(wC)]}{[1+O(N^{-\alpha})]} = \exp\left(2[\sigma(w)-\sigma(0)]\log N + \log\frac{E(w)}{E(0)\sigma(w)}\right), \tag{4.29}$$

where the $O$-term is uniform in $w$.

*Second Step.* Now, we are again in the framework of Hwang's Theorem, and we get that the smoothed version of cost $C$ follows an asymptotic Gaussian distribution, with a speed of convergence in $O(1/\sqrt{\log N})$, together with precise informations about the asymptotic behavior of the expectation $\overline{\mathbb{E}}_N[C]$ and the variance $\overline{\mathbb{V}}_N[C]$. The function $U$ of Hwang's Theorem is equal to $U(w) = 2\sigma(w)$ where $\sigma$ is defined in Section 3.2 $(d)$.

*Third Step.* We prove that the distributions of $C$ on $\overline{\Omega}_N$ and on $\Omega_N$ are $N^{-2\alpha}$–close, i.e., for all $(u,v) \in \Omega_N$,

$$|\,\mathbb{P}_N(u,v) - \overline{\mathbb{P}}_n(u,v)| = O(N^{-2\alpha})$$

so that the distribution of $C$ on $\Omega_N$ is also asymptotically Gaussian, with a speed of convergence in

$O(1/\sqrt{\log N})$. The closeness of distributions, together with the polynomial worst–case complexity of the algorithms of $\mathcal{E}$ now provides precise information about the asymptotic behavior of the expectation $\mathbb{E}_N[C]$ and the variance $\mathbb{V}_N[C]$. The constants that appear in the main tems of the expectation and the variance are equal respectively to

$$\mu(c) = 2\sigma'(0), \qquad \delta^2(c) = 2\sigma''(0). \tag{4.30}$$

This ends our sketch of the proof of Theorem 3.

**4.4 Local Limit Theorem and Saddle Point Method.** We summarize now the proof of Theorem 4. It deals with any lattice cost $c$ of moderate growth. It is sufficient to consider costs $C$ relative to costs $c$ with span $L = 1$, in the smoothed model, and our starting point is the relation

$$\overline{\mathbb{P}}_N[C(u,v) = \ell] = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-i\tau\ell}\cdot\overline{\mathbb{E}}_N[e^{i\tau C}]\,d\tau\,.$$

Since we are looking for an LLT result, the convenient scale of the problem is $n := \log N$, and we set

$$\ell = p_x(n) := \mu(c)n + \delta(c)x\sqrt{n}, \qquad q_x(n) := \lfloor p_x(n)\rceil\,.$$

(Here $\lfloor\cdot\rceil$ denotes the nearest integer function.) We consider

$$\begin{aligned} I_n &:= 2\pi\sqrt{\log N}\cdot\overline{\mathbb{P}}_N[C(u,v) = q_x(\log N)] \\ &= \sqrt{n}\int_{-\pi}^{+\pi}\exp[-i\tau q_x(n)]\cdot\overline{\mathbb{E}}_N[e^{i\tau C}]\,d\tau\,. \end{aligned} \tag{4.31}$$

Our strategy is to decompose the integration interval $[-\pi, +\pi]$ into a neighborhood of zero, $[-\upsilon, \upsilon]$, and its complement $|\tau| \in (\upsilon, \pi]$. This gives rise to two integrals $I_n^{(0)}$ and $I_n^{(1)}$.

*Integral* $I_n^{(0)}$. The estimate (4.29), together with Relations (4.30), proves that the main part of the integrand $\exp[-i\tau q_x(n)]\cdot\overline{\mathbb{E}}_N[e^{i\tau C}]$ is

$$\exp[2n(\sigma(i\tau) - 1 - i\tau\sigma'(0))]\cdot\exp[-i\tau x\delta(c)\sqrt{n}]\,.$$

Since the function $z \mapsto \sigma(z) - 1 - z\sigma'(0)$ has a saddle point at $z = 0$, the saddle point method entails the following estimate for the integral $I_n^{(0)}$,

$$I_n^{(0)} = \sqrt{2\pi}\,\frac{e^{-x^2/2}}{\delta(c)} + O\left(\frac{1}{\sqrt{n}}\right)\,.$$

*Integral* $I_n^{(1)}$. On the other hand, when $|\tau| \in [\upsilon, \pi]$, Dolgopyat's estimates and aperiodicity results (see $(e)$ of 3.2), entail the following: For some $\beta > 0$,

$(i)$ The Dirichlet series $S(2s, i\tau)$ is analytic in the strip $|\Re s - 1| \le \beta$,

$(ii)$ On the left vertical line $\Re s = 1 - \beta$, the series $S(2s, i\tau)$ is $O(|\Im s|^{\xi})$, with a small $\xi$, and a uniform $O$-term (with respect to $\tau$), so that it is possible to control the integral (4.27) on the left vertical line $\Re s = 1 - \beta$.

Then, using the Perron formula as in 4.3 proves that that the second part $I_n^{(1)}$ is a $O(N^{-\gamma})$ for some $\gamma > 0$.

This ends our sketch of the proof of Theorem 4.

## 5 Conclusions

This article has presented a unified approach to a large body of results relative to Euclid's algorithm and its major (fast) variants. We recapitulate here some of its consequences, relations to the vast existing literature on the subject, as well as extensions and open questions. It should be stressed that most of the improvements can eventually be traced to the existence of pole-free strips for Dirichlet series of cost parameters, a fact that precisely devolves from our extension of Dolgopyat's estimates to continued fraction systems.

First our methods lead to extremely precise estimates of the moments of costs, and in particular the number of steps, a much studied subject. Our estimates, when specialized to the mean number of steps, yield

$$\mathbb{E}_N[C] = \mu\log n + \eta + O(N^{-\gamma}); \tag{5.32}$$

see above Theorem 3, Parts $(b)$ and $(c)$. In the case of the standard algorithm, this covers the original estimates of Dixon and Heilbronn in 1969–1970 (the main term), as well as Porter's 1975 improvement (the second term, $\eta$), while providing the right shape of the error term $[O(N^{-\gamma})]$, for which Porter further showed that one could take $\gamma = (1/6) - \epsilon$ in the case of the standard algorithm. We refer the reader to the accounts by Knuth [25] and Finch [16] for more material on this classical topic. Our formula (5.32) also extends Rieger's analyses (first published around 1980, see [32, 33]) of the centered algorithm and the odd algorithm. Note that, in our perspective, the second-order constant $\eta$ comes out as a spectral quantity. It is an open problem to derive an explicit form starting from our expressions (e.g., such a form involving $\zeta'(2)$ is known under the name of Porter's constant in the standard case).

In sharp contrast to the mean value case, variances do not seem to be amenable to elementary methods. The first-order estimate has been given by Hensley (1994) in the paper [20] that first brought functional analysis to the field. Our formula,

$$\mathbb{V}_N[C] = \delta^2\log n + \delta_1 + O(N^{-\gamma}), \tag{5.33}$$

stated in Theorem 3 can be viewed as a precise form of Hensley's estimate relative to the standard algorithm, one that also extends to the odd and centered algorithms. (Incidentally, the quantity $\delta$, called Hensley's constant [16], is not recognized to be related to classical constants of analysis, though it is now known to be polynomial-time computable thanks to a recent study of Lhote [27]; the nature of $\delta_1$ is even more obscure.) Note that the complex-analytic properties of the moment generating functions provided by the functional-analytic methods furnish similarly strong estimates for moments of arbitrarily high order (our Theorem 3), a fact which also appears to be new.

Regarding distributional results, several points are worthy of note. Dixon in his 1970 paper had already obtained exponential tail bounds and these were further improved, albeit in a still fairly qualitative way by Hensley in his 1994 study (see his Theorem 1 in [20]). Our approach gives much more precise information on the distribution, as we now explain.

For simplicity, let us specialize once more the discussion to the number of steps. First, regarding the central region of the Local Limit Theorem (Theorem 4), the nature of the error terms obtained ($O(N^{-\gamma_0})$) and the fact that the saddle point method lends itself to the derivation of full asymptotic expansions (see, e.g., Henrici's book [19]) entail the existence of a *full asymptotic expansion* associated with the Gaussian approximation of Theorem 4, namely,

$$\mathbb{P}_N[\cdot] = \frac{e^{-x^2/2}}{\delta\sqrt{2\pi\log N}} \cdot \Sigma_r(\log N) \tag{5.34}$$

where

$$\Sigma_r(\log N) := 1 + \sum_{k=1}^{r} \frac{c_r}{(\log N)^{r/2}} + O\left(\log^{-(r+1)/2} N\right)$$

involves a computable numeric sequence $\{c_j\}$, (the argument of $\mathbb{P}_N$ being that of Theorem 4). This expansion is valid for $x$ in any compact set of $\mathbb{R}$.

Regarding large deviations, Lemma 11 (quasi-powers for smoothed costs) implies that $\overline{\overline{\mathbb{E}}}_N[\exp(wC)]$ is of the form of a quasi-power, provided $w$ stays in a small enough fixed neighbourhood of 0. By a standard argument (originally due to Cramér and adapted to the quasi-powers framework by Hwang [21, 22, 23]) and Lemma 14, this implies the existence of a large deviation rate function, that is, of a function $I(y)$ such that, for the right tail corresponding to $y \geq 0$, there holds

$$\lim_{N\to\infty} \frac{1}{\log N} \log \mathbb{P}_N[C > (1+y)\mu \log N] = -I(y), \tag{5.35}$$

with $I(y)$ defined on an interval $[0, \delta]$ for some $\delta > 0$. In other words, the probability of exceeding the mean by $y\mu\log N$ is exponentially small in the scale of the problem, being of the form

$$\exp[-I(y)\log N] = N^{-I(y)}.$$

.A simplified version of (5.35) is then: the probability of observing a value at $z$ or more standard deviations from the mean is bounded by a quantity that decays like $e^{-C_1 z^2}$ (Hensley's notations [20]). Analogous properties naturally hold for the left tail. Cramer's technique of "shifting the mean" and use of the resulting "shifted" quasi-powers lead in fact to very precise quantitative versions of (5.35) in the style of Hwang—thereby providing optimal forms of tail inequalities *à la* Dixon–Hensley.

Similar properties hold for other costs measures, like the ones detailed in the introduction. Of particular interest is the statistics of the number of digits assuming a particular value, for which estimates parallel to (5.32), (5.33), (5.34), and (5.35) are also seen to hold. For instance, the frequency of occurrence of digit $m$ in the expansion of a rational number has mean

$$\sim \log_2\left(1 + \frac{1}{m(m+2)}\right),$$

and it exhibits Gaussian fluctuations. It is again unknown to us, which of the involved constant (beyond the mean value factor) may be related to classical constants of analysis. The spectral forms of our Lemma 12 may at least provide a starting point for such investigations.

A major challenge is to derive distributional information that are so to speak "superlocal". By this, we mean the problem of estimating the behaviour of the number of steps and other cost measures over fractions of denominator *exactly* equal to $N$, i.e., rationals belonging to $\Omega_N \setminus \Omega_{N-1}$. In view of what is known in the average-case [16, 25], we expect arithmetical properties of $N$ to come into the picture. The analytical difficulty in this case stems from the fact that a further level of "unsmoothing" (how to go from $\Omega_N$ to $\Omega_N \setminus \Omega_{N-1}$?) would be required.

**Further works.** Our dynamical approach provides a general framework, where it seems possible to answer other questions about distributional analysis. For instance, all the questions that we solve for rational trajectories can be asked for the periodic trajectories. A periodic trajectory is produced by a quadratic number, and the reference parameter is related to the length of the geodesics on the modular surface. In a forthcoming paper, and following the same principles as in [30, 31, 39], we prove that the distribution of costs on periodic trajectories can be studied in a similar way as here, replacing the quasi–inverse $(I - \mathbf{H}_{s,w})^{-1}$ by $\det(I - \mathbf{H}_{s,w})$.

**Open problems.** We also ask various questions about Euclidean algorithms: for instance, what happens for other Euclidean algorithms of the Fast Class (in particular for the Binary algorithm [6, 38])? The extension of our results to cost functions that are still "small" but take into account the boolean cost (also known as the bit complexity) of each arithmetic operation is on our agenda. Note that an average-case analysis is already known to be possible via operator techniques [2, 41]. On another register, the extension to "large" costs is likely to lead us to the realm of stable laws: see for instance Gouezel and Vardi's works [18, 42] for occurrences of these laws in continued fraction related matters.

**Acknowledgements.** During his thesis, Hervé Daudé made experiments providing evidence for the Gaussian limit property of the number of steps. Joint work with Eda Cesaratto [8] involved an extensive use of the weighted transfer operator, and some of the ideas that we shared on that occasion proved very useful for the present paper. We have had many stimulating discussions with Philippe Flajolet regarding the saddle-point method and the notion of smoothed costs. Finally, we thank Sébastien Gouëzel who found a mistake in a previous version. This work has been supported in part by two CNRS Mathstic grants and by the European Union under the Future and Emerging Technologies programme of the Fifth Framework (Alcom-ft Project IST-1999-14186).

## References

[1] Aaronson, J., and Denker, M., Local limit theorems for partial sums of stationary sequences generated by Gibbs-Markov maps, *Stoch. Dyn.* 1 (2001) 193–237

[2] Akhavi, A. and Vallée, B., Average bit–complexity of Euclidean Algorithms, Proceedings ICALP'00, *Lecture Notes Comp. Science* 1853, 373–387, Springer, 2000.

[3] Baladi, V., *Positive Transfer operators and decay of correlations,* Advanced Series in non linear dynamics, vol 16, World Scientific, 2000.

[4] Baladi, V. and Vallée, B. Euclidean Algorithms are Gaussian, available from the ArXiv

[5] Boyarsky, A. and Gora, P., *Laws of Chaos, Invariant Measures and Dynamical Systems in One Dimension*, Probability and its applications, Birkhauser, 1997.

[6] Brent, R.P. Analysis of the Binary Euclidean algorithm, *Algorithms and Complexity, New Directions and Recent Results,* J.F. Traub, ed., Academic Press, 1976.

[7] Broise, A., Transformations dilatantes de l'intervalle et théorèmes limites, *Asterisque* 238, pp. 5–109, Société Mathématique de France , 1996.

[8] Cesaratto, E., and Vallée, B. Hausdorff dimension of sets defined by constraints on digits related to large additive costs, Les Cahiers du GREYC, 2003, submitted.

[9] Chernov, N. *Markov approximations and decay of correlations for Anosov flows,* Ann. of Math. (2) 147 (1998) 269–324.

[10] Collet, P., Some ergodic properties of maps of the interval, *Dynamical systems, Proceedings of the first UNESCO CIMPA School on Dynamical and Disordered Systems* (Temuco, Chile, 1991), Hermann, 1996.

[11] Collet, P., and Eckmann, J.-P., *Iterated Maps on the Interval as Dynamical Systems,* Birkhauser, Boston, 1990.

[12] Chazal, F., Maume, V., Statistical properties of General Markov dynamical sources: applications to information theory, To appear in DMTCS, 2004.

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

[14] Dolgopyat, D., On decay of correlations in Anosov flows, *Ann. of Math.,* 147 (1998) pp. 357–390.

[15] Ellison, W. and Ellison, F., *Prime Numbers,* Hermann, Paris, 1985.

[16] Finch, S. R., *Mathematical Constants*, Cambridge University Press, 2003.

[17] Flajolet, P. and Sedgewick, R., *Analytic Combinatorics*, Book in preparation, see also the *Rapports de Recherche INRIA* 1888, 2026, 2376, 2956.

[18] Gouezel, S. Central limit theorem and stable laws for intermittent maps, *Prob. Theory and Applications* (2003), to appear.

[19] Henrici, P., *Applied and Computational Complex Analysis*, vol. 2, John Wiley, 1974.

[20] Hensley, D., The number of steps in the Euclidean algorithm, *Journal of Number Theory,* 49, 2 (1994) pp. 142–182.

[21] Hwang, H.-K., *Théorèmes limite pour les structures combinatoires et les fonctions arithmétiques,* PhD thesis, Ecole Polytechnique, Dec. 1994.

[22] Hwang, H.-K., Large deviations for combinatorial distributions: I. Central limit theorems, *The Annals of Applied Probability* 6 (1996) 297–319.

[23] Hwang, H.-K., On convergence rates in the central limit theorems for combinatorial structures, *European Journal of Combinatorics,* 19 (1998) pp. 329–343.

[24] Kato, T., *Perturbation Theory for Linear Operators,* Springer-Verlag, 1980.

[25] Knuth, D.E., *The Art of Computer programming,* Volume 2, 3rd edition, Addison Wesley, Reading, Massachusetts, 1998.

[26] Lasota, A. and Mackey, M., *Chaos, Fractals and Noise; Stochastic Aspects of Dynamics,* Applied Mathematical Science 97, Springer, 1994.

[27] Lhote, L., Computation of a Class of Continued Fraction Constants, hese Proceedings.

[28] Mayer, D. H., On the thermodynamic formalism for the Gauss map, *Comm. Math. Phys.,* 130 (1990) pp. 311–333.

[29] Mayer, D. H., The thermodynamic formalism approach to Selberg's zeta function for $PSL(2,\mathbb{Z})$, *Bull. Amer. Math. Soc.,* 25 (1991) pp. 55–60.

[30] Parry, W., and Pollicott, M., *Zeta Functions and the Periodic Orbit Structure of Hyperbolic Dynamics,* Astérisque, 187–188, 1990.

[31] Pollicott, M., and Sharp, R. Exponential error terms for growth functions on negatively curved surfaces, *Amer. J. Math.,* 120 (1998) pp. 1019–1042.

[32] Rieger, G. J., Über die mittlere Schrittanzahl bei Divisionalgorithmen, *Math. Nachr.* (1978) 157–180.

[33] Rieger, G. J.,, Über die Schrittanzahl beim Algorithmus von Harris und dem nach nächsten Ganzen, *Archiv der Mathematik* 34 (1980), 421–427.

[34] Ruelle, D., *Thermodynamic formalism,* Addison Wesley, 1978.

[35] Ruelle, D., Repellers for real analytic maps, *Ergodic Theory Dynamical Systems,* 2 (1982) 99–10.

[36] Tenenbaum, G., *Introduction to analytic and probabilistic number theory,* Cambridge University Press, 1995.

[37] Vallée, B., Dynamical sources in information theory: fundamental intervals and word prefixes, *Algorithmica,* 29 (2001) pp 262–306.

[38] Vallée, B., Dynamics of the Binary Euclidean Algorithm: Functional Analysis and Operators, *Algorithmica,* (1998) 22 (4) pp. 660–685.

[39] Vallée, B., Dynamique des fractions continues à contraintes périodiques, *Journal of Number Theory* (1998) 2, 183–235.

[40] Vallée, B., Dynamical Analysis of a Class of Euclidean Algorithms, *Theoretical Computer Science* vol 297/1-3 (2003) pp 447–486

[41] Vallée, B., Digits and Continuants in Euclidean Algorithms. Ergodic Versus Tauberian Theorems, *Journal de Théorie des Nombres de Bordeaux,* 12 (2000) pp. 531–570.

[42] Vardi, I., A relation between Dedekind sums and Kloosterman sums, *Duke Math. J.* 55 (1987), 189–197.