Probabilistic analyses of the plain multiple gcd algorithm

Valérie Berthé

LIAFA, UMR CNRS 7089, Université Paris Diderot, France

Loïck Lhote

GREYC, UMR CNRS 6072, ENSICAEN & Université de Caen Normandie, France

Brigitte Vallée

GREYC, UMR CNRS 6072, Université de Caen Normandie, France

Abstract

Among multiple gcd algorithms on polynomials as on integers, one of the most natural ones performs a sequence of $\ell - 1$ phases (ℓ is the number of inputs), with each of them being the Euclid algorithm on two entries. We present here a complete probabilistic analysis of this algorithm, by providing both the average-case and the distributional analysis, and by handling in parallel the integer and the polynomial cases, for polynomials with coefficients in a finite field. The main parameters under consideration are the number of iterations in each phase and the evolution of the size of the current gcd along the execution. Three phenomena are clearly emphasized through this analysis: the fact that almost all the computations are performed during the first phase, the great difference between the probabilistic behavior of the first phase compared to subsequent phases, and, as can be expected, the great similarity between the integer and the polynomial cases.

Key words: Gcd algorithms, analysis of algorithms, analytic combinatorics, generating functions, transfer operator, dynamical analysis, limit laws, beta law, Perron Formula, Landau Theorem.

⋆ This work was supported by Agence Nationale de la Recherche through three projects: Dyna3S ANR-13-BS02-0003 – ANR BOOLE (ANR 2009 BLAN 0011) – ANR MAGNUM (ANR 2010 BLAN 0204).

Email addresses: berthe@liafa.univ-paris-diderot.fr (Valérie Berthé), loick.lhote@ensicaen.fr (Loïck Lhote), brigitte.vallee@unicaen.fr (Brigitte Vallée).

1. Introduction.

Among arithmetic operations, on polynomials as on integers, the computation of gcd's plays a prominent role. It can even be considered as the fifth main one, with an impressive range of applications, described for instance in von zur Gathen and Gerhard (2003). Let us just quote as an example the fact that in many symbolic computation systems, a large proportion of the time is devoted to the computation of gcd's on numbers, or on polynomials, in order to keep fractions under an irreducible form. Being able to measure the efficiency of a gcd algorithm, and to perform its analysis, is thus crucial.

The plain algorithm. Even for two entries, there is a wide variety of gcd algorithms; see, e.g., (von zur Gathen and Gerhard, 2003) or (Vallée, 2006). In this case, the Euclid algorithm plays a central role. Observe that there are many possible variants, in particular in the integer case with fast gcd algorithms; see (Brent, 1976; Schönhage, 1971; Stehlé and Zimmermann, 2004). For the general case of ℓ entries ($\ell \geq 2$), one of the most natural and basic algorithms consists in performing a succession of $\ell - 1$ phases, with each of them being the Euclid algorithm on two entries, as described in the book (Knuth, 1998).

More precisely, inputs are here either nonnegative integers or univariate polynomials over a finite field $\mathbb{F}_q$. In order to compute the gcd of ℓ inputs $x_1, \ldots, x_\ell$ ($\ell \geq 2$), we consider a sequence of $\ell - 1$ phases, that is, of $\ell - 1$ gcd computations on two entries. Let $y_1 := x_1$, then, for $k \in [2..\ell]$, one successively computes $y_k := \gcd(x_k, y_{k-1}) = \gcd(x_1, x_2, \ldots, x_k)$. The total gcd is $y_\ell := \gcd(x_1, x_2, \ldots, x_\ell)$, and it is obtained after $\ell - 1$ phases. We call it the *plain ℓ-Euclid algorithm.*

This is a straightforward algorithm, which cannot be easily extended for computing Bézout coefficients. We are interested in performing its analysis, making more precise and proving the observations made in Knuth (1998): "In most cases, the length of the partial gcd decreases rapidly during the first few phases of the calculation, and this will make the remainder of the computation quite fast". There are indeed inputs for which $\ell - 1$ phases are required, but, as the probability for two uniformly chosen inputs to be coprime is asymptotically $6/\pi^2$ for integers and $2q/(q-1)$ for polynomials, this algorithm is expected to require in average less steps. We thus do not claim that this naive algorithm is efficient [1] . However, a first step in analysis of algorithms consists in understanding and precisely analyzing even the simplest algorithms; such an analysis is not as trivial as it may first appear and then provides a basis of comparison for other algorithms of the same class.

State of the art. To the best of our knowledge, the plain ℓ–Euclid algorithm has not been yet analyzed. Its analysis was proposed as an exercise in the second edition of the "Art of Computer Programming" (Knuth, 1998), and quoted as a difficult one (HM48). However, the exercise disappears in the third edition..... The situation contrasts with the case $\ell = 2$, where the classical Euclid algorithm and all its main variants running on integers or on polynomials are now precisely analyzed. See (Berthé and Nakada, 2000; Friesen and Hensley, 1996; Knopfmacher and Knopfmacher, 1988; Ma and von zur Gathen, 1990) for analyses on polynomials; see (Heilbronn, 1969; Dixon, 1970) for the first analyses on integers and (Hensley, 1994; Vallée, 2006; Baladi and Vallée, 2005; Lhote

[1] Nevertheless, we will show that this algorithm is in fact not as "stupid" as it seems to be...

and Vallée, 2008) for more recent ones, involving distributional analyses. Here, in all these previous studies, the size of an input is defined as the *maximum* size of its components; and the size is the degree of the polynomial, or the logarithm of the integer. The same probabilistic behavior appears in both cases (polynomials and integers): with respect to the input size, the mean number of iterations is linear, and the arithmetic complexity is quadratic. Furthermore, the distribution of the number of iterations is asymptotically Gaussian.

There exists also a probabilistic algorithm proposed in von zur Gathen and Shparlinski (2006) for computing gcd's. It replaces a gcd computation on ℓ entries by a unique gcd on two random linear combinations of the initial input. The approach is different: we perform here a probabilistic analysis of a deterministic algorithm where the distribution of the inputs is chosen a priori, whereas the algorithm developed in von zur Gathen and Shparlinski (2006) is probabilistic, designed as requiring few steps, and handles the worst-case. In Section 10, we return to the comparison between the two strategies, and make more precise the comparison done in (von zur Gathen and Shparlinski, 2006, Section 3).

Results. We provide two studies which perform in parallel the two complete analyses (in the average-case and also in distribution) for the two types of inputs (polynomials and integers).

For the analysis of the plain Euclid algorithm, it is natural to choose, as the total size of the input, the *sum of the size* of its components, instead of the maximum of the sizes of its components, as it was usually the case in previous studies. Observe first that changing the total size of the input yields a different probabilistic behavior, even for $\ell = 2$. Indeed, in the case $\ell = 2$, and with respect to this new total size, the mean number of iterations is proven to remain linear, but the distribution of number of iterations is now asymptotically uniform (instead of being Gaussian).

In the case $\ell \geq 3$, our analysis exhibits a strong difference between the first phase and the following phases. In the first phase, the number of iterations has a linear mean and follows a beta law (the same as the law followed by the minimum of $\ell - 1$ reals i.i.d. in the unit interval) which reduces to the uniform law for $\ell = 2$. In the following phases, the number of iterations is constant on the average and follows a geometric law. These results were expected, according to the previous remark of Knuth, but our analysis exhibits a more precise phenomenon, since we indeed show that, in most cases, *almost all the calculation* is done during the first phase.

Methods. On both types of inputs (polynomials or integers), our methods are typical in the *Analytic Combinatorics* domain, as it described in the book (Flajolet and Sedgewick, 2009). We first perform a combinatorial step, and build generating functions that describe the problem: we transfer, with formal tools, operations on structures (polynomials, integers) into operations on generating functions. Then, in a second analytical step, we view the generating functions as functions of the complex variable, and a good knowledge of their singularities (position, and nature) provides asymptotic estimates of their coefficients, and thus the probabilistic behavior of the algorithm.
The analysis in the polynomial case is a typical instance of classical analytic combinatorics: we deal with power generating functions, built in Section 4, and the main analytic tool is the Cauchy formula used in Section 5. As could be expected, the integer case

is more difficult to handle, in each of the two steps, and combines analytic combinatorics and dynamical systems: it can be viewed as an instance of the dynamical analysis methodology described, for instance, in (Vallée, 2006); in the first step, the generating functions are now built with dynamical tools, namely with the transfer operator of the dynamical system which underlies the Euclid algorithm (i.e., the dynamical system defined by the Gauss map), and these generating functions are now of Dirichlet type (see Section 7), as usual in this context; in the analytical step, performed in Section 8, the main tools are now the Perron formula, together with functional analysis.

Plan of the paper. We begin in Section 2 by describing our general framework: the algorithm, its main parameters, some basic facts in analysis of algorithms, with a focus on limit laws. Along the paper, we stress the strong analogy between the polynomial and the integer cases, and we keep the same order of presentation in both cases. We start with the polynomial case where the analysis is more standard. Sections 3, 4, 5 are devoted to the polynomial case, and Sections 6, 7, 8 to the integer case. Sections 3 and 6 state the main results, respectively in the polynomial and in the integer case. Sections 4 and 7 perform the *combinatorial* steps and build the adequate generating functions, Sections 5 and 8 perform the *analytic* steps. The proofs in the integer case rely on a general version of a theorem due to Landau (1924), which seems to be not very well-known; this is why we describe in Section 9 a version of this result which is well adapted to our context, and provide its proof. We then conclude the paper with Section 10.

This paper is an extended version of a previous short paper (Berthé et al., 2013) which appeared in the Proceedings of the ISSAC'2013 Conference. For the polynomial case, we provide here two proofs which do not appear in the short version (namely the proofs of Proposition 11 and Theorem 5), and we develop thoroughly the analysis in the integer case: the average-case analysis was only briefly described in the short version, and the distributional analysis provided here is completely new.

2. General framework.

2.1. The ℓ-Euclid algorithm.

There are two main rings endowed with a Euclidean division: the ring $\mathbb{F}_q[X]$ of polynomials over the finite field $\mathbb{F}_q$ with q elements, and the ring $\mathbb{Z}$ of integers. In each case, there is a Euclidean algorithm which performs a gcd computation between two entries, with a sequence of Euclidean divisions, as recalled in Figure 1. The quantity $\gcd(a_1, a_2)$ is the last nonzero remainder a_{r+1}. It can be chosen monic (in the polynomial case) or positive (in the integer case). The number of *steps* (here equal to r) is one of the main parameters of interest.

On an ℓ-uple $(x_1, x_2, \ldots, x_\ell)$ of nonzero entries (polynomials or integers), the *plain ℓ-Euclid algorithm* computes their greatest common divisor y via a sequence of $\ell - 1$ gcd computations between two entries, which yields

$$y_1 := x_1, \quad y_k = \gcd(x_k, y_{k-1}) = \gcd(x_1, x_2, \ldots, x_k) \text{ for } k \in [2..\ell].$$

The total gcd $y_\ell := \gcd(x_1, x_2, \ldots, x_\ell)$ is thus obtained after $\ell - 1$ *phases*.

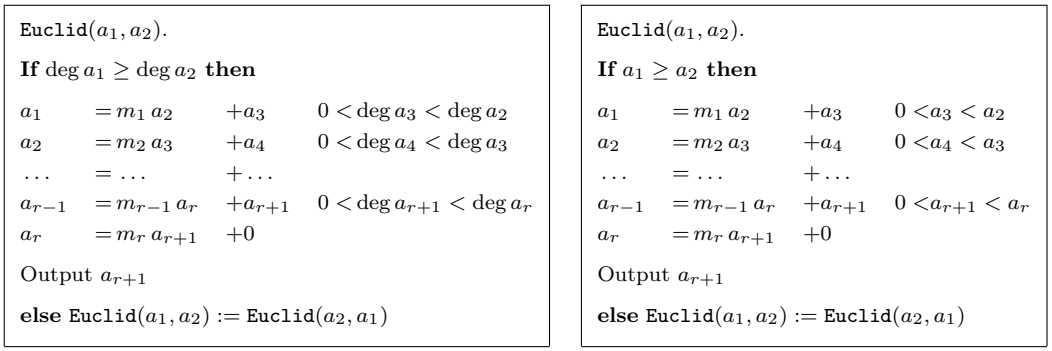


Fig. 1. Description of the Euclid algorithm on two inputs, for polynomials on the left, and for integers on the right.

This paper aims at precisely understanding the random behavior of the plain algorithm. Since the algorithm is a succession of phases, it is important to describe each phase of index k ($k \in [1..\ell - 1]$), with the following parameters:

(a) the number L_k of iterations, i.e., of divisions, performed during the k-th phase,

(b) the size[2] D_k of the gcd y_k at the beginning of the k-th phase.

Remark 1. The variable L_k always takes positive values whereas the variable D_k may take the value zero. When unifying the treatments of both variables, we sometimes will have to study the variable $L_k - 1$ in order to compare it more efficiently with D_k.

We are also interested in the analysis of the following *global parameters*:

(c) the *total number of iterations* $L := L_1 + L_2 + \ldots + L_k$,

(d) the algorithm may be interrupted as soon as $y_k = 1$ and Π is the number of *useful phases*, namely

$$\Pi = 0 \text{ if } y_1 = 1 \text{ and } \Pi := \max\{k \mid y_k \neq 1\} \text{ if } y_1 \neq 1;$$

(e) the total number $\tilde{L}$ of divisions of the interrupted algorithm is defined as

$$\tilde{L} = 0 \text{ if } \Pi = 0 \text{ and } \tilde{L} := L_1 + L_2 + \ldots + L_\Pi \text{ if } \Pi > 0.$$

2.2. Probabilistic analysis.

For each type (polynomials or integers), an input for the ℓ–Euclid algorithm is an ℓ-uple $\underline{x} := (x_1, x_2, \ldots, x_\ell)$ of entries, and the set of all possible inputs is denoted in a generic way by Ω. Furthermore, there is a size d which defines a mapping $\mathrm{d} : \Omega \to \mathbb{N}$, and, for an input $\underline{x} \in \Omega$, the integer $\mathrm{d}(\underline{x})$ is closely related to the space that is occupied by $\underline{x}$. The set Ω_n gathers the inputs of size n. This is a finite subspace of Ω which is endowed with the uniform probability denoted by $\mathbb{P}_n$. Now, each parameter X of interest, here $X \in \{L_k, D_k, \Pi, L\}$, is studied via its *restriction* X_n to each Ω_n that gives rise to a random integer variable (defined on Ω_n).

Such a random variable X_n can be studied in a (usual) probabilistic way, via its expectation, its variance, or its distribution. For a random variable X defined on Ω, we often omit the reference to the space Ω_n when it is clear, and instead of writing $\mathbb{E}_n[X_n]$ for the mean

[2] The size will be defined later in Section 3 for polynomials and in Section 6 for integers.

of X_n on the finite set Ω_n, we simply write $\mathbb{E}_n[X]$. In the same vein, instead of writing $\mathbb{P}_n[X_n > m]$ for the probability of the event $[X_n > m]$, we simply write $\mathbb{P}_n[X > m]$.

Figure 2 below provides a table for the notation introduced so far.

$\mathrm{d}(x)$	size of the input x
$\underline{x}$	a generic input for the ℓ-Euclid Algorithm
Ω	set of the inputs for the ℓ-Euclid Algorithm
Ω_n	subset of the inputs of size n for the ℓ-Euclid Algorithm
k	index of a phase
L_k	number of iterations during the k-th phase
D_k	size of the gcd at the beginning of the k-th phase
Π	number of useful phases
L	total number of divisions of the interrupted algorithm

Fig. 2. Table of notation for the main parameters.

Analysis of algorithms focuses on the *asymptotic* probabilistic behavior of the sequence X_n, when the size n becomes large. Average-case analysis is devoted to the study of the expectations: it deals with the sequence $\mathbb{E}_n[X]$ for $n \to \infty$, and provides first interesting results on the sequence X_n. However, the study of the distribution of X_n gives a more precise knowledge, as will be seen in the next section.

2.3. Distributional analysis and limit laws.

Consider a sequence (X_n) of random variables, each of them with integer nonnegative values. We are interested in events of type $[X_n \leq m]$ and wish to evaluate their probability

$$\varpi_n(m) := \mathbb{P}_n[X_n \leq m],$$

which exactly defines the distribution of the variable X_n. As we focus on the asymptotics, we study the sequence ϖ_n of distribution functions for $n \to \infty$. When it exists, the limit ϖ of the sequence ϖ_n defines the *asymptotic distribution* of the variable X. We also say that the law defined by ϖ is the *asymptotic law* for X.

There are two main possible cases for the limit ϖ: in the first case, the limit law ϖ is discrete, and arises directly from the definition of X_n, whereas, in the second case, there is a continuous limit which arises after a convenient normalization. We will meet the two cases in the present study, according to the index k of the phase. For the first phase ($k = 1$), we will meet a continuous limit law (namely the beta law), whereas, for the subsequent phases ($k \geq 2$), there will be discrete limit laws (closely related to geometric laws); see Theorem 3 and Theorem 14 for precise statements. In their book (Flajolet and Sedgewick, 2009), Flajolet and Sedgewick describe various combinatorial schemes that lead to discrete or continuous limit laws.

Discrete limit. When the limit ϖ exists and is discrete, it is defined on integer values. The functions ϖ_n and their limit ϖ are nondecreasing functions. This implies that the convergence of the sequence (ϖ_n) to the limit ϖ is uniform, and the sequence (ε_n) defined as

$$\varepsilon_n := \sup_{m \in \mathbb{N}} |\varpi_n(m) - \varpi(m)|$$

tends to zero and provides the speed of convergence.

Continuous limit. In this case, the sequence (ϖ_n) will be convergent after a suitable normalization: we write the integer m as a function of the expectation M_n and the standard deviation σ_n as

$$m = M_n + x\sigma_n, \qquad \text{and we thus set} \qquad x := x(m,n) = \frac{m - M_n}{\sigma_n}.$$

We now study the normalized random variable $\check{X}_n$ associated with X_n by the equality of the events $[X_n = m] = [\check{X}_n = x(m,n)]$. And we are interested in the distribution $\check{\varpi}_n$ of $\check{X}_n$, and its (possible) limit $\check{\varpi}$ when $n \to \infty$. If this limit exists, this means

$$\check{\varpi}(x) := \lim_{n\to\infty} \check{\varpi}_n(x) = \lim_{n\to\infty} \varpi_n \left(\frac{m - M_n}{\sigma_n} \right),$$

and we will say that the law $\check{\varpi}$ is the limit law of the sequence (X_n). In the same vein as before, the functions $\check{\varpi}_n$ and their limit $\check{\varpi}$ are nondecreasing functions. Then, the convergence of the sequence $(\check{\varpi}_n)$ to the limit $\check{\varpi}$ is always uniform, and the sequence (ε_n) defined as

$$\varepsilon_n := \sup_{x\in\mathbb{R}} |\check{\varpi}_n(x) - \check{\varpi}(x)|$$

tends to zero and provides the speed of convergence.

2.4. Examples of limit laws.

Figure 3 illustrates the limit laws that arise in the context of this paper. Each graph corresponds to experiments that were done on integer inputs [3] and represents the empirical probability density of the number of steps performed by the plain algorithm during a given phase.

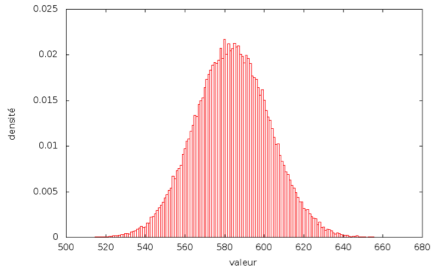
The top of Figure 3 is devoted to the case of two entries ($\ell = 2$), and we consider two different input sizes. On the left, the size of a pair (u, v) is the maximum of the (binary) sizes of u and v (the *sup-size*): this is the usual size in all the previous analyses performed for Euclidean algorithms on two inputs. On the right, the size of the pair (u, v) is the sum of the (binary) sizes of u and v (the *sum-size*). The limit distribution is clearly different in both probabilistic models. With the usual sup-size, the limit law is Gaussian, as it was proved in Hensley (1994). Gaussian limit laws are classical in analysis of algorithms, and, in particular, in the analysis of Euclidean algorithms. However, with the sum-size, the limit law is the uniform law. We recall the expressions of the density f for each of the two laws,

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} \quad \text{[Gaussian law]}, \qquad f(x) = \mathbf{1}_{[0,1]}(x) \quad \text{[Uniform law on } [0,1]\text{]}.$$

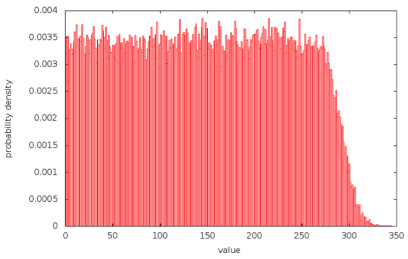
The bottom of Figure 3 describes the case of four entries ($\ell = 4$). The graphs represent the empirical probability density of the number of steps during a given phase, on the left for the first phase ($k = 1$), and on on the right, during the second phase ($k = 2$). The limit law for the first phase is clearly a continuous law, but it is no longer the uniform law. We will prove that it is a beta law with convenient parameters (see Section 2.5 for

[3] These data are obtained with 10^5 executions of the plain algorithm on integer inputs with a total binary size equal to 1000.

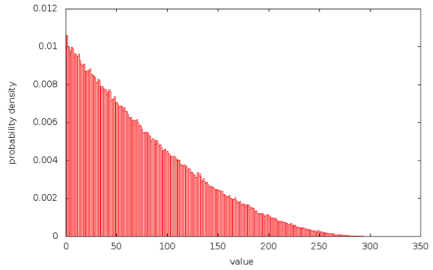
x-axis: possible values of the cost $L(\omega)$ y-axis: probability density $x \mapsto f(x)$
$f(x)dx := \Pr[\omega;\ L(\omega) \in [x, x+dx]]$



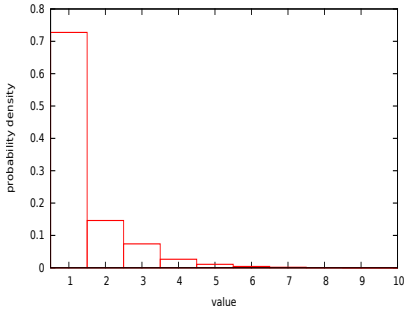
Gaussian law



Uniform law



Beta law



Geometric law

Fig. 3. Examples of limit laws with their densities.

more on beta laws). On the right, the limit law is discrete and we will prove that it is a geometric law, i.e., a "true" geometric law for polynomials, and a quasi-geometric law for integers. We recall that a random variable X follows a *geometric law* of parameter y if the distribution of X satisfies

$$\mathbb{P}[X = m] = y(1-y)^{m-1} \text{ for } m \geq 1.$$

2.5. The beta law inside analysis of algorithms.

We now focus on the beta law which plays an important role in the present study. The beta law of parameters (a, b) has a density on the unit interval given by

$$\beta_{a,b}(x) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1}\mathbf{1}_{[0,1]}(x).$$

The a-th order statistics of a sequence of p variables i.i.d in the unit interval $[0, 1]$ follows a beta law of parameters $(a, p-a+1)$. In the case when $a = 1$ and $p = \ell - 1$, this is the minimum Y of $\ell - 1$ variables i.i.d on the unit interval which follows the beta law of parameters $(1, \ell - 1)$ with a density and a distribution respectively equal to

$$f(x) = (\ell-1)(1-x)^{\ell-2}\mathbf{1}_{[0,1]}(x), \qquad \Pr[Y \geq x] = (1-x)^{\ell-1}.$$

Except this "direct" occurrence of the beta law, there are very few "indirect" instances of the beta law, and we are only aware of the occurrence of the beta law in the Gram-

Schmidt orthogonalization process (see e.g. Akhavi et al. (2009)). Moreover, the book Flajolet and Sedgewick (2009) that contains numerous examples of various types of limit laws does not provide any probabilistic analysis which leads to a beta law (and it contains only very few instances which lead to uniform laws).

2.6. Generating functions.

In the polynomial case, principles of analytic combinatorics directly apply, with power generating functions. In the study of a cost X (here $X \in \{L_k, D_k\}$), the main tool is the bivariate generating function $X(z,u)$: this is a power series, where the variable z marks the size whereas the variable u marks the cost. Two (univariate) generating functions are derived from $X(z,u)$; as their coefficients are expressed as sums of coefficients of $X(z,u)$, they are called *cumulative* generating functions. The first one, $\widehat{X}(z)$, is used for the expectation $\mathbb{E}_n[X_n]$, while the second one, $\widehat{X}^{[m]}(z)$, is well-adapted for the probabilities of events $\mathbb{P}_n[X_n \geq m]$ (see Figure 4 for their description). They are defined and used in Section 4. In the integer case, and, as it is usual in number theory, Dirichlet series replace power series, but the principles are the same. In the study of a cost X, we use as generating functions the bivariate Dirichlet series $X(s,u)$ and two cumulative Dirichlet series $\widehat{X}(s)$ and $\widehat{X}^{[m]}(s)$. Figure 4 describes these Dirichlet series that are defined and used in Section 7.

In both cases, we are interested in the asymptotic behavior of the coefficients of the generating functions, which is closely related to the nature and the position of their dominant singularities. There exist classical theorems that transfer the analytical properties of the generating functions to the asymptotics of their coefficients, and this transfer is often more involved for Dirichlet series than for power series. In this paper, we give two precise transfer results (Propositions 11 and 22). The strong parallelism between these two transfers explains the similarity of our results.

$S(z)$	$S(s)$	plain generating function for Ω
$X(z,u)$	$X(s,u)$	bivariate generating function for parameter $X \in \{L_k, D_k\}$
$\widehat{X}(z)$	$\widehat{X}(s)$	cumulative generating function for parameter $X \in \{L_k, D_k\}$
$\widehat{X}^{[m]}(z)$	$\widehat{X}^{[m]}(s)$	generating function of the event $[X \geq m]$ for $X \in \{L_k, D_k\}$

Fig. 4. The main generating functions used in the paper for the two types of inputs, namely polynomials and integers.

3. Main results for polynomials.

3.1. Set of inputs and size.

We consider the ring $\mathbb{F}_q[X]$ of polynomials over the finite field $\mathbb{F}_q$ with q elements, and the size of a nonzero polynomial x is its degree denoted by $\mathrm{d}(x)$.

The possible inputs are all the sequences $\underline{x}$ formed of ℓ nonzero polynomials, and, without loss of generality, we limit ourselves to monic polynomials. Then, the set of inputs is

$$\Omega = \mathcal{U}^\ell \qquad \text{where } \mathcal{U} \text{ is the set of monic polynomials.}$$

The *size* of the input $\underline{x} = (x_1, x_2, \ldots, x_\ell)$ is defined as the *total degree* of the sequence, and we let

$$\mathrm{d}(\underline{x}) := \mathrm{d}(x_1\, x_2 \ldots, x_\ell) = \mathrm{d}(x_1) + \mathrm{d}(x_2) + \ldots + \mathrm{d}(x_\ell).$$

We recall that the subset Ω_n is formed with the inputs of size n. It is a finite set, endowed with the uniform probability $\mathbb{P}_n$.

We will consider cost functions on the sets Ω_n (corresponding to the parameters D_k, L_k, Π, L), and we will study the probabilistic behavior of these costs (mean, variance, distribution) in an asymptotic way, when n tends to infinity.

With the analytic combinatorics methodology, we prove (in Sections 4 and 5) the results described in Section 3.2, 3.3 and 3.4 below. The first one (Theorem 2) deals with the expected values, whereas the second one (Theorem 3) describes asymptotic limit laws, and lastly, the results of Section 3.4 are devoted to the global parameters.

3.2. Average-case analysis.

Theorem 2 below exhibits a strong difference between the first phase and the subsequent ones. We will find again this difference when considering limit laws in Section 3.3. Theorem 2 shows that, on average, the first phase performs a linear number of iterations which involves the entropy $2q/(q-1)$ of the Gauss map (see Sections 6.2 and 10 for more details). Moreover, whereas the mean degree of the first gcd is linear with respect to the input size, the mean degree of the gcd is proven to be of constant order after the first phase. Then, the mean number of divisions L_k which will be performed in the following phases, together with the mean degrees D_k of the following gcd's, will be of constant order.

Theorem 2. [Expectations.] *Let the set Ω_n of sequences of ℓ monic polynomials with size n (i.e., total degree n) be endowed with the uniform distribution. The following holds.*

(*a*) *The expectation of the number of iterations L_1 during the first phase is linear with respect to the size n and satisfies*

$$\mathbb{E}_n[L_1] = \frac{q-1}{2q}\frac{n}{\ell} + \frac{3q+1}{4q} + O\left(\frac{1}{n}\right).$$

(*b*) *For any $k \in [2..\ell-1]$, the expectation of the number of iterations L_k during the k-th phase is asymptotic to a constant, and satisfies*

$$\mathbb{E}_n[L_k] = \frac{q^k-1}{q^k-q} + O\left(\frac{1}{n}\right) = 1 + \frac{q-1}{q}\frac{1}{q^{k-1}-1} + O\left(\frac{1}{n}\right).$$

(*c*) *The expectation of the degree of the first polynomial x_1 is linear with respect to the size n and satisfies*

$$\mathbb{E}_n[D_1] = \frac{n}{\ell}.$$

(*d*) *For any $k \in [2..\ell-1]$, the expectation of the degree D_k of $y_k = \gcd(x_1, x_2, \ldots, x_k)$ at the beginning of the k-th phase is asymptotic to a constant, and satisfies*

$$\mathbb{E}_n[D_k] = \frac{1}{q^{k-1}-1} + O\left(\frac{1}{n}\right).$$

3.3. Limit laws.

The following result refines Theorem 2, and explains more deeply the difference between the first phase ($k = 1$) and the following phases. For $k = 1$, the expected degrees of the first two polynomials x_1 and x_2 are linear, and the number of divisions L_1 is closely related to $\min(\mathrm{d}(x_1), \mathrm{d}(x_2))$. Then, it is natural to expect beta laws for the first phase, more precisely a beta law of parameter $(1, \ell - 1)$, since it is the law of the minimum of $\ell - 1$ random variables i.i.d. on the unit interval (see Section 2.5). For $\ell = 2$, this is the uniform law. For the subsequent phases, as the expected degrees of the gcd's are of constant order, according to Theorem 2, we may expect geometric laws.

Theorem 3. [Limit laws.] *Let the set Ω_n be endowed with the uniform distribution. The following holds.*

(*a*) *The number of iterations L_1 during the first phase asymptotically follows a beta law of parameter $(1, \ell - 1)$ on the interval $[0, (q-1)/(2q)]$, whereas the number of iterations L_k during each following phase asymptotically follows a geometric law with ratio $p_k = (q-1)/(q^k - 1)$.*

(*i*) *One has $\mathbb{P}_n\left[L_k > n/(k+1)\right] = 0, \quad$ for any k.*

(*ii*) *For $k = 1$, the probability $\mathbb{P}_n[L_1 > m]$ of the event $[L_1 > m]$ satisfies when $n \to \infty$ and $m/n \in [0, (q-1)/(2q)]$*

$$\mathbb{P}_n[L_1 > m] = \left(1 - \frac{2q}{q-1}\frac{m}{n}\right)^{\ell-1} + O\left(\frac{1}{n^\alpha}\right), \qquad \text{with} \quad \alpha = \min\left(1, \frac{(\ell-1)^2}{2\ell-1}\right),$$

where the constant in the O–term is uniform on the interval $[0, (1/2)(q-1)/q]$.

(*iii*) *For $k \geq 2$, the probability $\mathbb{P}_n[L_k > m]$ of the event $[L_k > m]$ satisfies when $n \to \infty$ and $m/n \in [0, 1/(k+1) \cdot (q^k - 1)/q^k]$*

$$\mathbb{P}_n[L_k > m] = \left(\frac{q-1}{q^k - 1}\right)^m + O\left(\frac{\log n}{n}\right),$$

where the constant in the O–term is uniform on the interval $[0, 1/(k+1) \cdot (q^k - 1)/q^k]$.

(*b*) *The degree D_1 of the first polynomial x_1 asymptotically follows a beta law of parameter $(1, \ell - 1)$ on the interval $[0, 1]$, whereas the degree D_k of the gcd y_k at the beginning of each following phase asymptotically follows a geometric law with ratio $r_k = q^{1-k}$.*

(*i*) *One has $\quad \mathbb{P}_n\left[D_k > n/k\right] = 0$ for any k.*

(*ii*) *For $k = 1$, the probability $\mathbb{P}_n[D_1 \geq m]$ of the event $[D_1 \geq m]$ satisfies when $n \to \infty$ and $m/n \in [0, 1]$*

$$\mathbb{P}_n[D_k \geq m] = \left(1 - \frac{m}{n}\right)^{\ell-1} + O\left(\frac{1}{n^\alpha}\right) \qquad \text{with} \quad \alpha = \min\left(1, \frac{(\ell-1)^2}{2\ell-1}\right),$$

where the constant in the O–term is uniform on the interval $[0, 1]$.

(*iii*) *For any* $k \geq 2$, *the probability* $\mathbb{P}_n[D_k \geq m]$ *of the event* $[D_k \geq m]$ *satisfies when* $n \to \infty$ *and* $m/n \in [0, 1/k]$,

$$\mathbb{P}_n[D_k \geq m] = q^{(1-k)m} + O\left(\frac{\log n}{n}\right),$$

where the constant in the O*–term is uniform on the interval* $[0, 1/k]$.

Remark 4. The exponent α of Assertions $(a)(ii)$ and $(b)(ii)$ satisfies the following: $\alpha = 1/3$ for $\ell = 2$, $\alpha = 4/5$ for $\ell = 3$, and $\alpha = 1$ for $\ell \geq 4$.

3.4. Global parameters.

The interrupted algorithm stops as soon as the gcd y_k is of degree 0. Let $\Pi(x_1, \ldots, x_\ell)$ be the number of useful phases. The event $[\Pi \geq k]$ coincides with the event $[D_k \geq 1]$ for $k \in [1..\ell - 1]$, which is estimated in Theorem 3. Then, it is possible to consider the total number $\tilde{L}$ of divisions performed by the interrupted version: we provide an estimate of its mean value, and prove that it itself asymptotically follows a beta law, the same as the number L_1 of the first phase.

Theorem 5. [Global parameters.] *When the set* Ω_n *is endowed with the uniform distribution, the following holds.*

(*a*) *The distribution of the number* Π *of useful phases satisfies* $\mathbb{P}_n[\Pi \geq 0] = 1$, $\mathbb{P}_n[\Pi \geq \ell] = 0$, *and*

$$\mathbb{P}_n[\Pi \geq k] = q^{1-k} + O\left(\frac{1}{n}\right) \quad \textit{for } k \in [1..\ell - 1].$$

(*b*) *The total number of divisions* $\tilde{L}$ *performed by the interrupted version of the* ℓ*-Euclid algorithm has an expected value* $\mathbb{E}_n[\tilde{L}]$ *equal to*

$$\frac{q-1}{2q}\frac{n}{\ell} + \frac{3q+1}{4q} + \sum_{k=2}^{\ell-1}\left(\frac{q}{q^k} + \frac{q-1}{q^k - 1}\right) + O\left(\frac{\ell}{n}\right).$$

(*c*) *The total number* L *of iterations, and the total number* $\tilde{L}$ *of iterations of the interrupted algorithm both asymptotically follow a beta distribution of parameter* $(1, \ell-1)$ *on the interval* $[0, (q-1)/(2q)]$ *with a speed of convergence* $O(\log n/n)$.

4. Generating functions in the polynomial case.

4.1. General setting.

We use the analytic combinatorics methodology, such as described in (Flajolet and Sedgewick, 2009), and deal with its main tool, namely generating functions. We use a variable z_i to mark the degree $\mathrm{d}(x_i)$ of the i–th polynomial x_i, and the generating function $F(z_1, z_2, \ldots, z_\ell)$ of the set $\Omega = \mathcal{U}^\ell$, relative to the total size d, is defined as

$$F(z_1, z_2, \ldots, z_\ell) := \sum_{\underline{x} \in \mathcal{U}^\ell} z_1^{\mathrm{d}(x_1)}\, z_2^{\mathrm{d}(x_2)} \ldots z_\ell^{\mathrm{d}(x_\ell)}.$$

It is equal to the product $U(z_1)\,U(z_2)\ldots U(z_\ell)$, where $U(z)$ is the generating function of the set $\mathcal{U}$ of the monic polynomials relative to the size d, namely

$$U(z) = \sum_{x\in\mathcal{U}} z^{\mathrm{d}(x)} = \sum_{n\geq 0} q^n z^n = \frac{1}{1-qz}.$$

Most of the time, we limit ourselves to the case when all the variables z_i are equal, and we write $F(z)$ instead of $F(z,\cdots,z)$. One has

$$F(z) = \sum_{\underline{x}\in\mathcal{U}^\ell} z^{\mathrm{d}(\underline{x})} = U(z)^\ell = \frac{1}{(1-qz)^\ell}.$$

For studying a parameter (or a cost C) on $\Omega = \mathcal{U}^\ell$ (here, the costs L_k and D_k), a main tool is the *bivariate generating function relative to the cost* C, obtained by introducing a further variable u to mark the cost C, and defined as

$$C(z,u) := \sum_{\underline{x}\in\mathcal{U}^\ell} z^{\mathrm{d}(\underline{x})} u^{C(\underline{x})}.$$

The probability distribution of the cost C can be studied with the generating function $C(z,u)$, via the relation

$$\mathbb{P}_n[C=i] = \frac{[z^n\,u^i]C(z,u)}{[z^n]F(z)}.$$

We are first interested in the mean value of parameter C, and we deal with the (univariate) *cumulative generating function*

$$\widehat{C}(z) := \frac{\partial C}{\partial u}(z,u)\Big|_{u=1}, \quad \text{which yields} \quad \mathbb{E}_n[C] = \frac{[z^n]\widehat{C}(z)}{[z^n]F(z)}. \tag{1}$$

When we are interested in the probability of the event $[C\geq m]$, we deal with the (univariate) *generating function of the event* $[C\geq m]$, which is another cumulative generating function, defined as

$$\widehat{C}^{[m]}(z) := \sum_{i\geq m} [u^i]C(z,u), \quad \text{which yields} \quad \mathbb{P}_n[C\geq m] = \frac{[z^n]\widehat{C}^{[m]}(z)}{[z^n]F(z)}. \tag{2}$$

By definition, the cumulative function $\widehat{C}(z)$ is the sum of all the cumulative functions $\widehat{C}^{[m]}(z)$ of the event $[C\geq m]$.

Note that Example IX.15 in (Flajolet and Sedgewick, 2009) describes the analysis of Euclid Algorithm over polynomials with generating functions. The context is simpler and may help the reader to understand the role of each generating series.

4.2. Algorithmic expression for the generating functions.

In order to perform an analysis of the plain ℓ-Euclid algorithm, we first derive an alternative expression for the generating function $F(z)$, which describes the algorithm as a sequence of phases. This new expression will be a product of $\ell-1$ factors, each of them describing a phase of the algorithm.

Proposition 6. [Phase-function.] *The generating function $F(z)$ of the set $\Omega = \mathcal{U}^\ell$ with the size equal to the total degree decomposes as*

$$F(z) = U(z)^\ell = U(z^\ell) \cdot \prod_{k=1}^{\ell-1} T(z, z^k) \tag{3}$$

and involves the phase-function T defined as

$$T(z,t) = \frac{U(z) + U(t) - 1}{1 - G(zt)}, \tag{4}$$

the generating function $U(z)$ of monic polynomials, and the generating function $G(z)$ of general polynomials with positive degree, i.e.,

$$U(z) = \frac{1}{1-qz}, \qquad G(z) = \frac{(q-1)qz}{1-qz} = (q-1)\left(\frac{1}{1-qz} - 1\right). \tag{5}$$

Proof. We first focus on the first phase; it only involves x_1 and x_2 and consists in applying Euclid algorithm on the pair (x_1, x_2). The Euclid algorithm first compares the degrees of x_1 and x_2. There are three cases:

$$\mathrm{d}(x_1) = \mathrm{d}(x_2), \qquad \mathrm{d}(x_1) > \mathrm{d}(x_2), \qquad \mathrm{d}(x_1) < \mathrm{d}(x_2).$$

In the first case, the first step is a subtraction, which can be viewed as a division with a quotient equal to 1.

In all the cases, the gcd $y_2 := \gcd(x_1, x_2)$ together with the sequence of quotients $(m_1, m_2, \ldots, m_r)$ completely determines the input pair (x_1, x_2). More precisely, one writes $(x_1, x_2) = (y_2\,\widehat{x}_1, y_2\,\widehat{x}_2)$ with a coprime pair $(\widehat{x}_1, \widehat{x}_2)$ and the execution of the Euclid algorithm on the pair $(\widehat{x}_1, \widehat{x}_2)$ produces the same sequence $(m_1, m_2, \ldots, m_r)$ as the pair (x_1, x_2). The first quotient m_1 is monic (this is due to the fact that x_1 and x_2 are monic) and the remainder of the sequence $\Sigma = (m_2, \ldots, m_r)$ is formed with general polynomials m_i (no longer monic) with $\mathrm{d}(m_i) \geq 1$. As previously, the total degree of the sequence Σ is $\mathrm{d}(\Sigma) = \mathrm{d}(m_2) + \ldots + \mathrm{d}(m_r)$.

We now focus on the first quotient m_1, and we consider the three possible cases.

(i) If $\mathrm{d}(x_1) = \mathrm{d}(x_2)$, then $m_1 = 1$.

(ii) If $\mathrm{d}(x_1) > \mathrm{d}(x_2)$, then $\mathrm{d}(m_1) \geq 1$, $\mathrm{d}(\widehat{x}_2) = \mathrm{d}(\Sigma)$, $\mathrm{d}(\widehat{x}_1) = \mathrm{d}(m_1) + \mathrm{d}(\Sigma)$.

(iii) If $\mathrm{d}(x_1) < \mathrm{d}(x_2)$, then $\mathrm{d}(m_1) \geq 1$, $\mathrm{d}(\widehat{x}_1) = \mathrm{d}(\Sigma)$, $\mathrm{d}(\widehat{x}_2) = \mathrm{d}(m_1) + \mathrm{d}(\Sigma)$.

All these remarks provide an alternative expression of the product $U(z_1)\,U(z_2)$. Indeed, the relation

$$z_1^{\mathrm{d}(x_1)} z_2^{\mathrm{d}(x_2)} = (z_1 z_2)^{\mathrm{d}(y_2)} \cdot z_1^{\mathrm{d}(\widehat{x}_1)} z_2^{\mathrm{d}(\widehat{x}_2)}$$

yields the factorisation

$$U(z_1)\,U(z_2) = U(z_1 z_2) \cdot \sum_{\widehat{x}_1, \widehat{x}_2} z_1^{\mathrm{d}(\widehat{x}_1)} z_2^{\mathrm{d}(\widehat{x}_2)},$$

together with the equality

$$\sum_{\widehat{x}_1, \widehat{x}_2} z_1^{\mathrm{d}(\widehat{x}_1)} z_2^{\mathrm{d}(\widehat{x}_2)} = \left[1 + \sum_{m_1} z_1^{\mathrm{d}(m_1)} + z_2^{\mathrm{d}(m_1)}\right]\left[\sum_{\Sigma} (z_1 z_2)^{\mathrm{d}(\Sigma)}\right], \tag{6}$$

with the conditions previously described on the first quotient m_1, the sequence Σ and the gcd y_2. The first factor in (6) involves the generating function $U(z)$ of monic polynomials,

$$1 + \sum_{m_1} z_1^{\mathrm{d}(m_1)} + z_2^{\mathrm{d}(m_1)} = 1 + (U(z_1) - 1) + (U(z_2) - 1) = U(z_1) + U(z_2) - 1.$$

The second factor is the generating function (with respect to the variable $z_1 z_2$) of the sequences of general polynomials with a positive degree, that is,

$$\sum_{\Sigma} (z_1 z_2)^{\mathrm{d}(\Sigma)} = \frac{1}{1 - G(z_1 z_2)}.$$

We have thus obtained the following alternative form for the product

$$U(z_1)\, U(z_2) = U(z_1 z_2) \cdot T(z_1, z_2), \qquad \text{with} \quad T(z,t) = \frac{U(z) + U(t) - 1}{1 - G(zt)}.$$

When we replace this expression into the total product

$$U(z_1)\, U(z_2) \dots U(z_\ell) = F(z_1, z_2, \dots, z_\ell)$$

and iterate the transformation, we obtain an alternative expression for the generating function $F(z_1, z_2, \dots, z_\ell)$ with a product of $\ell - 1$ factors, each of them involving the phase-function T at points z_k and $t_k = z_1 \dots z_k$, i.e.,

$$F(z_1, z_2, \dots, z_\ell) = U(t_\ell) \cdot \prod_{k=1}^{\ell-1} T(t_k, z_{k+1}).$$

It can be useful in some studies to keep all the variables z_i, but here, we let $z_1 = z_2 = \dots = z_\ell = z$, and we obtain an expression of the generating function $F(z)$. □

4.3. Generating functions for parameters.

We will now deal with bivariate generating functions. The two parameters of interest L_k (number of steps in the k-th phase) and D_k (degree of the gcd y_k at the beginning of the k-th phase) are only related to the k-th phase. Then we isolate, in the total generating function $F(z)$, the generating function which describes the k-th phase, and replace it by its associated bivariate generating function: this means that we mark this part of the generating function with the variable u. Then, instead of

$$F(z) = U(z^\ell) \cdot \prod_{k=1}^{\ell-1} T(z, z^k),$$

we consider the two generating functions

$$L_k(z,u) = U(z)^\ell \cdot \frac{T(z, z^k, u)}{T(z, z^k)}, \qquad D_k(z,u) = U(z)^\ell \cdot \frac{U(z^k, u)}{U(z^k)}. \tag{7}$$

We now explain how to define the two generating functions $T(z,t,u)$ and $D(t,u)$.

When studying the parameter L_k (number of steps in the k-th phase), the extra variable u marks each step of the k-th iteration, and we deal with the generating function

$$T(z,t,u) = u \cdot \frac{U(z) + U(t) - 1}{1 - u \cdot G(zt)} \qquad \text{with } t = z^k. \tag{8}$$

When studying the parameter D_k (degree of the gcd y_k at the beginning of the k-th phase), the extra variable u marks the degree of the gcd y_k, and we deal with the generating function

$$U(t,u) = \frac{1}{1-qut} \qquad \text{with } t = z^k. \tag{9}$$

Finally, the following result provides explicit expressions for the cumulative generating functions and the cumulative bivariate generating functions.

Proposition 7. [Generating functions.] *The following holds, for any $k \in [1..\ell-1]$.*

(*i*) *The bivariate generating function $L_k(z,u)$, as well as the cumulative generating functions $\widehat{L}_k(z)$ and $\widehat{L}_k^{[m]}(z)$ relative to the number of divisions during the k-th phase satisfy*

$$\frac{L_k(z,u)}{U(z)^\ell} = u\,\frac{1-G(z^{k+1})}{1-uG(z^{k+1})}, \qquad \frac{\widehat{L}_k(z)}{U(z)^\ell} = \frac{1}{1-G(z^{k+1})}, \qquad \frac{\widehat{L}_k^{[m]}(z)}{U(z)^\ell} = G(z^{k+1})^{m-1},$$

and involve the generating functions G, U defined in (5).

(*ii*) *The bivariate generating function $D_k(z,u)$, as well as the cumulative generating functions $\widehat{D}_k(z)$ and $\widehat{D}_k^{[m]}(z)$ relative to the degree D_k of the gcd at the beginning of the k-th phase satisfy*

$$\frac{D_k(z,u)}{U(z)^\ell} = \frac{1-qz^k}{1-uqz^k}, \qquad \frac{\widehat{D}_k(z)}{U(z)^\ell} = \frac{qz^k}{1-qz^k}, \qquad \frac{\widehat{D}_k^{[m]}(z)}{U(z)^\ell} = (qz^k)^m.$$

Proof. Equalities (7) and (8) (in the L-case) and equalities (7) and (9) (in the D-case) lead to exact expressions of the bivariate generating functions $L_k(z,u)$ and $D_k(z,u)$. Taking the derivative with respect to u (at $u=1$), we obtain the cumulative generating functions

$$\frac{\widehat{L}_k(z)}{U(z)^\ell} = \frac{1}{1-G(z^{k+1})} = \frac{1-qz^{k+1}}{1-q^2z^{k+1}}, \qquad \frac{\widehat{D}_k(z)}{U(z)^\ell} = \frac{qz^k}{1-qz^k}. \tag{10}$$

Extracting the coefficient of $[u^i]$ in the bivariate generating functions and taking the sum over $i \geq m$ gives

$$\frac{\widehat{L}_k^{[m]}(z)}{U(z)^\ell} = G(z^{k+1})^{m-1}, \qquad \frac{\widehat{D}_k^{[m]}(z)}{U(z)^\ell} = (qz^k)^m. \tag{11}$$

□

Remark 8. According to Remark 1, we are interested in the cost $L_k - 1$ in order to compare it in a more efficient way to D_k. With Proposition 7 (i), the two bivariate generating functions related, respectively, to the number of iterations $L_k - 1$ and to the degree D_k of the gcd y_k share the same common form

$$U(z)^\ell\,\frac{1-\underline{A}_k(z)}{1-u\underline{A}_k(z)},$$

$$\text{with} \quad \underline{A}_k(z) = G(z^{k+1}) \quad [(L_k-1)\text{-case}], \qquad \text{or} \quad \underline{A}_k(z) = qz^k \quad [D_k\text{-case}]. \tag{12}$$

5. Analytic study in the polynomial case.

We have obtained in Proposition 7 the expressions of the cumulative generating functions

$$\widehat{D}_k, \quad \widehat{D}_k^{[m]}, \quad \widehat{L}_k, \quad \widehat{L}_k^{[m]}.$$

As they are fractional functions, it is thus possible to directly compute their coefficients, and use (1) and (2) to obtain an exact expression of the expectation and the probability distribution of the parameters D_k and L_k. However, this is not the general viewpoint developed here, as we are mainly interested in the asymptotic probabilistic behavior (as $n \to \infty$) of these random variables. Singularity analysis relates the analytic properties of a generating function and the asymptotic behavior of its coefficients. More precisely, it views the generating function as a function of the complex variable, determines the position and the nature of its dominant singularity (the singularity closest to 0), and transfers this knowledge to the asymptotic behavior of its coefficients. Such an approach is completely described in the book Flajolet and Sedgewick (2009) where general hypotheses are given on the bivariate generating functions to obtain Gaussian limit laws (see Theorem IX.9 for instance). However, the general framework is here different, as will be discussed later, in particular in the conclusion.

5.1. A general framework for expectations.

Here, the main series used in the proof of Theorem 2 (which is the object of the present section) are the cumulative generating functions $\widehat{D}_k$ and $\widehat{L}_k$ whose expression is provided by (10). These expressions exhibit a dominant pole at $z = 1/q$, with an order which is varying according to the phase. For the first phase ($k = 1$), this pole is of order $\ell + 1$, whereas this pole remains of order ℓ for the other phases ($k \geq 2$). This explains the differences between the first phase and subsequent phases.

We first design a general scheme for the analysis of expectations.

Proposition 9. [Expectations.] *Consider a combinatorial structure, with a cost C, whose bivariate generating function $C(z, u)$ is of the form*

$$C(z, u) = \frac{1}{(1-z)^\ell} \cdot \frac{1 - A(z)}{1 - uA(z)}, \qquad (\ell \geq 2)\,. \tag{13}$$

(i) Then, the expectation of the cost C satisfies

$$\mathbb{E}_n[C] = \frac{[z^n]\widehat{C}(z)}{[z^n](1-z)^{-\ell}} \qquad \text{with} \quad \widehat{C}(z) = \frac{\partial C}{\partial u}(z, u)\Big|_{u=1} = \frac{1}{(1-z)^\ell} \cdot \frac{A(z)}{1 - A(z)}.$$

(ii) Assume now the following:

(a) $A(z)$ is analytic in a disk $|z| \leq \rho$, with $\rho > 1$;

(b) $a := A(1) \neq 0$, $b := A'(1) > 0$;

(c) The derivative $A'(z)$ never takes zero values on the circle $|z| = 1$.

Then, the following estimates hold for the expectations $\mathbb{E}_n[C]$, with $e := A''(1)$:

$$\text{in the case } a = 1, \qquad \mathbb{E}_n[C] = \frac{1}{b}\frac{n}{\ell} + \left(\frac{1}{b} - 1 + \frac{e}{2b^2}\right) + O\left(\frac{1}{n}\right),$$

$$\text{in the case } a < 1, \qquad \mathbb{E}_n[C] = \frac{a}{1-a} + O\left(\frac{1}{n}\right).$$

5.2. Average-case analysis.

Before proving Proposition 9, we explain how it leads to Theorem 2.

Proof of Theorem 2. We begin with the formula of the expectation in (1), the expressions of $F(z)$ and of the cumulative generating functions $D_k(z)$ and $L_k(z)-1$ given in (12). All these generating series have a dominant pole which is located at $1/q$. We then perform the change of variable $z \mapsto z/q$. Note that these generating functions are of the form described in (13), up to this change of variable $z \mapsto z/q$. Moreover, in the L-case, we deal with the generating functions relative to the parameter $L_k - 1$, and we will add 1 to the asymptotic estimates to recover the expectations of parameter L_k. Proposition 9 now applies with $A_k(z) := \underline{A}_k(z/q)$, where $\underline{A}_k$ is defined in (12), namely,

$$A_k(z) = G\left((z/q)^{k+1}\right) \quad (\text{case } L_k - 1), \qquad A_k(z) = q\,(z/q)^k \quad (\text{case } D_k). \tag{14}$$

There are two main cases according to the phase index k, as the value $a_k := A_k(1)$ equals 1 for $k = 1$, whereas the value a_k is strictly less than 1 for $k \geq 2$.
In the case $k \geq 2$, Proposition 9 applies (case $a < 1$), and this gives rise to the constants

$$\frac{a_k}{1-a_k} = \frac{q-1}{q^k-1} \quad (\text{case } L_k - 1), \qquad \frac{a_k}{1-a_k} = \frac{1}{q^{k-1}-1} \quad (\text{case } D_k).$$

Consider now the case $k = 1$. In the D_1-case, one has $A_1(z) = z$ and one gets an exact expression for $\mathbb{E}_n[D_1]$ as $\mathbb{E}_n[D_1] = n/\ell$. In the $(L_1 - 1)$-case, one has

$$A_1(z) = (q-1)\left(\frac{q}{q-z^2} - 1\right), \quad b_1 = A_1'(1) = \frac{2q}{q-1}, \quad e_1 = A_1''(1) = \frac{2q(q+3)}{(q-1)^2}.$$

We now add the constant 1 to the constant term, and this ends the proof of Theorem 2. □

5.3. Proof of Proposition 9.

The proof of Proposition 9 is mainly based on the following lemma which provides asymptotic expressions for the numerator and the denominator of $\mathbb{E}_n[C]$.

Lemma 10. [Coefficients extraction.] *Consider a function*

$$C(z) = B(z) \cdot (1-z)^{-j} \quad (j \geq 2)$$

where $B(z)$ is analytic in the disk $|z| \leq \rho$ with $\rho > 1$. Let $\underline{a} := B(1) \neq 0$ and $\underline{b} := B'(1)$. Then, the following estimates hold for the coefficients $[z^n]C(z)$:

$$\begin{aligned}
[z^n]C(z) &= \underline{a}\binom{n+j-1}{j-1} - \underline{b}\binom{n+j-2}{j-2} + O(n^{j-3}) \\
&= \left(\underline{a}\frac{n}{j-1} + \underline{a} - \underline{b}\right)\binom{n+j-2}{j-2} + O(n^{j-3}) \\
&= \underline{a}\binom{n+j-1}{j-1} + O(n^{j-2}).
\end{aligned}$$

When $B(z)$ admits simple poles on the punctured circle $\{|z| = 1 \mid z \neq 1\}$, the third estimate remains valid, and the second estimate remains also valid as soon as $j \geq 3$.

Proof of Lemma 10. The coefficient $[z^n]C(z)$ is the residue at $z = 0$ of the function $C(z)/z^{n+1}$. This function has two poles inside the disk $|z| \leq \rho$, the pole $z = 0$ and the pole $z = 1$. Then, the residue theorem entails the equality

$$[z^n]C(z) = -\mathrm{Res}\left(\frac{C(z)}{z^{n+1}}, z = 1\right) + \frac{1}{2i\pi}\int_{\Gamma_r} \frac{C(z)}{z^{n+1}}dz \tag{15}$$

where Γ_r is a circle (with a positive orientation) of center 0 and radius r with $1 < r \leq \rho$. The integral term in (15) gives rise to a remainder term in $O(\rho^{-n})$. The equality

$$\mathrm{Res}\left(\frac{1}{(z-1)^j}\frac{1}{z^{n+1}}, z = 1\right) = \binom{n+j-1}{j-1}$$

together with the singular expression of $C(z)$ at $z = 1$, namely

$$C(z) = \frac{\underline{a}}{(z-1)^j} + \frac{\underline{b}}{(z-1)^{j-1}} + O\left(\frac{1}{(z-1)^{j-2}}\right),$$

provide the expression for the residue. The possible isolated poles $B(z)$ on the punctured circle $\{|z| = 1 \mid z \neq 1\}$ give rise to terms of asymptotically constant order and are thus remainder terms as soon as $j \geq 3$. □

We now prove Proposition 9.

Proof of Proposition 9. First, Lemma 10 applies to the asymptotic behaviour of the denominator with $B(z) = 1$ and $j = \ell$. (Recall that $\ell \geq 2$.)
Second, Lemma 10 also applies to the asymptotic behaviour of the numerator, with two main cases. In the case when $a < 1$, we choose

$$j = \ell, \quad B(z) := \frac{A(z)}{1 - A(z)}, \qquad B(1) = \underline{a} = \frac{a}{1-a}.$$

In the case when $a = 1$, we choose

$$j = \ell{+}1, \quad B(z) = A(z){\cdot}\frac{1-z}{1-A(z)} \quad \text{with} \quad B(z) = \frac{1}{b}{+}(1{-}z)\left(1 - \frac{e}{2b^2}\right){+}O(1) \quad (z \to 1).$$

In both cases, Hypothesis (c) entails that $B(z)$ admits only possibly simple isolated poles on the punctured circle $\{|z| = 1 \mid z \neq 1\}$. □

5.4. A general framework for limit laws.

In the same vein as for expectations, we design a general framework for distributions described by the following proposition. In all the cases, the cumulative generating function of the event $[C \geq m]$ is expressed as a product of the function $U(z)^\ell$ which has a pole of order ℓ at $z = 1/q$, with a "large power" of a function $A(z)$. The term "large power" is used since the exponent m may depend on the size n. The following proposition deals with this case.

Proposition 11. [Coefficients extraction and distribution.] *Consider a combinatorial structure, with a cost C, whose bivariate generating function $C(z, u)$ is of the form*

$$C(z, u) = \frac{1}{(1-z)^\ell} \cdot \frac{1 - A(z)}{1 - uA(z)}, \qquad (\ell \geq 2)\,. \tag{16}$$

(*i*) *Then the distribution of the cost C is expressed as*

$$\mathbb{P}_n[C \geq m] = \frac{[z^n]\widehat{C}^{[m]}(z)}{[z^n](1-z)^{-\ell}}, \qquad \text{with} \quad \widehat{C}^{[m]}(z) = \frac{1}{(1-z)^\ell} \cdot A(z)^m.$$

(*ii*) *Assume now the following:*

(*a*) *$A(z)$ is analytic in a disk $|z| \leq \rho$, with $\rho > 1$;*

(*b*) *$a := A(1) \neq 0$, $b := A'(1) \geq 0$;*

(*c*) *for $|z|$ close enough to 1, $|A(z)| \leq A(|z|)$.*

Then, for any pair (m, n) whose ratio m/n belongs to the interval $[0, c]$, with $c = a/b$, the following estimates hold for the probabilities $\mathbb{P}_n[C \geq m]$.

In the case $a = 1$, one has

$$\mathbb{P}_n[C \geq m] = \left[\left(1 - \frac{b}{a}\frac{m}{n}\right)^{\ell-1} + O\left(\frac{1}{n^\alpha}\right)\right], \qquad \alpha = \min\left(1, \frac{(\ell-1)^2}{2\ell-1}\right).$$

In the case $a < 1$, one has

$$\mathbb{P}_n[C \geq m] = a^m + O\left(\frac{\log n}{n}\right).$$

In both cases, the hidden constant in the O–term is uniform with respect to m, when m/n belongs to the interval $[0, c]$.

5.5. Distributional analysis.

Before proving Proposition 11, we explain how it leads to Theorem 3.

Proof of Theorem 3. As previously, we deal with the costs $L_k - 1$ and D_k, and we will shift the distributions for $L_k - 1$ in order to return to L_k. In each case, the functions $A_k(z)$ of interest are provided by Equation (14). In both cases, (case D_k or case $L_k - 1$), the function $A_k(z)$ is a multiple of z^k and this entails the equalities

$$\mathbb{P}_n\left[D_k > n/k\right] = 0, \qquad \mathbb{P}_n\left[L_k > n/(k+1)\right] = 0.$$

The hypotheses of Proposition 11 are fulfilled for the functions A_k, with

$$a_k = q^{1-k}, \qquad \frac{b_k}{a_k} = k \qquad \text{(case } D_k\text{)},$$

$$a_k = \frac{q-1}{q^k-1}, \qquad \frac{b_k}{a_k} = (k+1)\frac{q^k}{q^k-1}. \qquad \text{(case } L_k - 1\text{)}.$$

For $k = 1$, the constants a_k are equal to 1, whereas they are strictly less than 1 for $k \geq 2$. This ends the proof of Theorem 3. □

5.6. Proof of Proposition 11.

Proof. The coefficient $[z^n]\widehat{C}^{[m]}(z)$ is the residue at $z = 0$ of the function $\widehat{C}^{[m]}(z)/z^{n+1}$. This function has two poles inside the disk $|z| \leq \rho$, the pole $z = 0$ and the pole $z = 1$. Then, the residue theorem entails the equality

$$[z^n]C^{[m]}(z) = -\text{Res}\left(\frac{\widehat{C}^{[m]}(z)}{z^{n+1}}, z = 1\right) + \frac{1}{2i\pi}\int_{\Gamma_r} \frac{\widehat{C}^{[m]}(z)}{z^{n+1}} dz \tag{17}$$

where Γ_r is a circle (with a positive orientation) centered at the origin of radius r with $1 < r \leq \rho$. We study the two terms in (17). In both studies, the functions

$$R_{n,m}(z) := \frac{A^m(z)}{z^n} \tag{18}$$

will play an important role in the proof.

Study of the residue. The residue at $z = 1$ equals

$$\operatorname{Res}\left(\frac{\widehat{C}^{(m]}(z)}{z^{n+1}}; z = 1\right) = \frac{(-1)^{\ell-1}}{(\ell-1)!}\frac{d^{\ell-1}}{dz^{\ell-1}}\left[\frac{A(z)^m}{z^{n+1}}\right]_{z=1}.$$

We write

$$R_{n+1,m}(z) = \frac{A(z)^m}{z^{n+1}} = \exp[-ng(z)], \qquad \text{with} \quad g(z) = \frac{1}{n}\Big(-m\log A(z) + (n+1)\log z\Big).$$

The derivative of g at $z = 1$ is positive provided that the ratio m/n is at most equal to $c = a/b$ with $a = A(1)$ and $b = A'(1)$. The k-th derivative of $R_{n+1,m}(z)$ at $z = 1$ is of the form

$$(-1)^k a^m \cdot P_k(m, n)$$

where $P_k(m, n)$ is a polynomial of degree at most k (with respect to n) which has a unique term of degree k equal to $n^k g'(1)^k$. Finally, provided that m/n is at most equal to $c = a/b$, one has

$$\frac{d^{\ell-1}}{dz^{\ell-1}}\left[\frac{A(z)^m}{z^{n+1}}\right]_{z=1} = (-1)^{\ell-1}a^m\left[n^{\ell-1}g'(1)^{\ell-1} + O\left(n^{\ell-2}\right)\right],$$

and, with $a := A(1),\ b := A'(1)$,

$$\operatorname{Res}\left(\frac{\widehat{C}^{(m]}(z)}{z^{n+1}}; z = 1\right) = a^m\frac{n^{\ell-1}}{(\ell-1)!}\left[\left(1 - \frac{m}{n}\frac{b}{a}\right)^{\ell-1} + O\left(\frac{1}{n}\right)\right],$$

where the constant in the O-term is uniform when the ratio m/n belongs to $[0, c]$.

Study of the integral. With Hypothesis (c), the following upper bound holds

$$\left|\frac{1}{2i\pi}\int_{\Gamma_r}\frac{\widehat{C}^{[m]}(z)}{z^{n+1}}dz\right| \leq \frac{A(r)^m}{r^n}\frac{1}{(r-1)^\ell}.$$

Consider the function $R = R_{n,m}$ defined as in (18). Using the definition of a and b, and letting $d := 2\sup\{|(\log A(r))''|\ ;\ r \in [1, \rho]\}$, one has

$$\frac{1}{n}\log R_{n,m}(r) \leq \frac{1}{n}\log R_{n,m}(1) + (r-1)\left[-\left(1 - \frac{m}{n}\frac{b}{a}\right) + (r-1)\frac{m}{n}d\right].$$

Condider any pair (m, n) whose ratio m/n is at most equal to c_0 with $c_0 < c$, and $c = a/b$. There are two cases according to d: the case $d = 0$, which occurs when the function $\log A(z)$ is linear (this will occur in our D–case), and the case $d > 0$. In the first case, the second term of the right member is negative, and in the second case, this is also true as soon as $r - 1$ is small enough. More precisely, let

$$r - 1 = A\left(1 - \frac{c_0}{c}\right), \qquad \text{with} \quad A := \frac{1}{2c_0 d}.$$

Then, in both cases, for any pair (m,n) with $m/n \le c_0$, one has

$$\frac{R_{n,m}(r)}{R_{n,m}(1)} \le \exp\left[-\frac{n}{2}\left(1-\frac{c_0}{c}\right)^2\right] \quad \text{and thus} \quad \left|\frac{1}{2i\pi}\int_{\Gamma_r}\frac{\widehat{C}^{[m]}(z)}{z^{n+1}}dz\right| = a^m\, O\left(1-\frac{c_0}{c}\right)^{-\ell},$$

where the constant in the O–term does not depend on c_0.

Study of probabilities. Now, with the normalisation provided by the denominator, described in Proposition 10, and for any pair (m,n) whose ratio belongs to the interval $[0,c_0]$ with $c_0 < c$, the following estimate holds

$$\mathbb{P}_n[C \ge m] = a^m\left[1+O\left(\frac{1}{n}\right)\right]\left[\left(1-\frac{m}{n}\frac{b}{a}\right)^{\ell-1}+O\left(\frac{1}{n}\right)+O\left(\frac{1}{n^{\ell-1}}\right)\left(1-\frac{c_0}{c}\right)^{-\ell}\right],$$

where the constants of the O-term are uniform. We let now $c_0 \to c$ as a function of n, and study in a separate way the cases $a=1$ and $a<1$.

Case a = 1. We consider $(1-c_0/c) = n^{-\alpha}$ so that one has $n^{\ell-1}\,(1-c_0/c)^{\ell} = n^{\ell-1-\alpha\ell}$. Then, one has

$$\begin{aligned}
&\text{for } m/n \le c_0, \quad \mathbb{P}_n[C\ge m] = \left(1-\frac{m}{n}\frac{b}{a}\right)^{\ell-1} + O(n^{-(\ell-1)+\alpha\ell}) + O(n^{-1}),\\
&\text{for } m/n \ge c_0, \quad \mathbb{P}_n[C\ge m] = O(n^{-\alpha(\ell-1)}) \quad + O(n^{-(\ell-1)+\alpha\ell}) + O(n^{-1}).
\end{aligned}$$

The best choice is $\alpha = (\ell-1)/(2\ell-1)$, which gives the result.

Case a < 1. We let $m_0 := \log_{1/a} n$. Then, one has

$$\begin{aligned}
&\text{for } m/n \le m_0, \quad \mathbb{P}_n[C\ge m] = a^m + O\left(\frac{\log n}{n}\right),\\
&\text{for } m/n \ge m_0, \quad \mathbb{P}_n[C\ge m] = a^m + O\left(\frac{1}{n}\right).
\end{aligned}$$

This ends the proof of Proposition 11. □

5.7. Study of global parameters.

Let us now prove Theorem 5.

Assertion (a). It is a direct consequence of Theorem 3 together with the fact that the events $[\Pi \ge k]$ and $[D_k \ge 1]$ coincide, by definition of the variable Π.

Assertion (b). The total number of divisions $\tilde{L}$ of the interrupted algorithm can be written as a sum of variables $\tilde{L}_k$:

$$\left(\tilde{L} = \sum_{k=1}^{\Pi} L_k \text{ if } \Pi \ge 1\right) \quad \Longrightarrow \quad L = \sum_{k=1}^{\ell-1}\tilde{L}_k \qquad \text{with} \quad \tilde{L}_k := L_k \cdot \mathbf{1}_{[k\le\Pi]}.$$

One has $L_k - \tilde{L}_k = L_k \cdot \mathbf{1}_{[k>\Pi]}$. The inclusion $[D_k = 0] \subset [L_k = 1]$, together with the fact that the events $[\Pi < k]$ and $[D_k = 0]$ coincide, entails the equality $L_k \cdot \mathbf{1}_{[\Pi<k]} = \mathbf{1}_{[\Pi<k]}$, and thus,

$$\mathbb{E}_n[L_k] - \mathbb{E}_n[\tilde{L}_k] = \mathbb{E}_n[\mathbf{1}_{[\Pi<k]}] = \mathbb{P}_n[\Pi < k] = 1 - \mathbb{P}_n[k \le \Pi].$$

Then Theorems 2 and 3 apply, and we obtain

$$\mathbb{E}_n[\tilde{L}_k] = \frac{q-1}{q^k-q} + \frac{q}{q^k} + O\left(\frac{1}{n}\right) \quad (\text{for } k \geq 2), \qquad \mathbb{E}_n[\tilde{L}_1] = \mathbb{E}_n[L_1] + O\left(\frac{1}{n}\right) \quad (\text{for } k = 1)\,.$$

We conclude with the linearity of the mean.

Assertion (c). We now prove that L asymptotically follows a beta law, the same as L_1. We split the random variable L into two random variables, namely

(i) the *main* random variable L_1, which admits a beta limit law (Theorem 3),

(ii) the *remainder* random variable $R = L - L_1$, which is a sum of random variables, each of them admitting an asymptotic geometric law.

The next proposition shows that, in this situation, the sum $L = L_1 + R$ asymptotically follows the same beta law as L_1. This provides an extension of the result obtained in (Lhote and Vallée, 2008) for Gaussian laws.

Proposition 12. *Consider a sequence of probabilistic spaces $(\Omega_n, \mathbb{P}_n)_n$ and two sequences of random variables X_n and Y_n defined on Ω_n with integer values. Assume the following.*

(i) *There exists a sequence $\gamma_n \to \infty$ for which the random variable X_n/γ_n asymptotically follows a law whose distribution function is a function $f : [0, c] \to [0, 1]$, increasing, Lipschitz, with $f(0) = 0$ and $f(c) = 1$. For any $c_0 < c$, there exists a sequence $(\varepsilon_n)_n$, with $\varepsilon_n \to 0$, for which, for any n, and for any $d \in [0, c_0]$, one has*

$$\mathbb{P}_n[X_n < d\gamma_n] = f(d) + O(\varepsilon_n).$$

(ii) *The random variable Y_n is a sum of $(\ell - 2)$ variables $Y_{k,n}$, each of them admitting an asymptotic geometric law of ratio $1/a_k$, with $a_k > 1$.*

Then, the random variable $X_n + Y_n$ asymptotically follows the same law as X_n. More precisely, let $a := (\min a_k)^{1/(\ell-2)}$. Then, for any $c_0 < c$, for any n, and for any $d \in [0, c_0]$, one has

$$\mathbb{P}_n[X_n + Y_n < d\gamma_n] = f(d) + O\left(\varepsilon_n + \frac{1}{\gamma_n} |\log_a \varepsilon_n|\right).$$

Proof. Consider a sequence $(\delta_n)_n$ which will be made precise later, and define the two events E_n and F_n as

$$E_n = [X_n + Y_n < d\gamma_n], \qquad F_n = [Y_n \leq \delta_n].$$

The asymptotic geometric law of each $Y_{k,n}$ yields

$$\mathbb{P}_n[E_n \cap F_n^c] \leq \mathbb{P}_n[F_n^c] = O(a^{-\delta_n})\,. \tag{19}$$

Indeed, this bound is due to the following inclusion between the events

$$[Y_n > \delta_n] \subset \bigcup_{k=2}^{\ell-1} \left[Y_{k,n} > \frac{\delta_n}{\ell - 2}\right]$$

which entails (recall that $a = (\min a_k)^{1/(\ell-2)}$), the following upper bound

$$\mathbb{P}_n[Y_n \geq \delta_n] = O(a^{-\delta_n}).$$

On the other hand, the following inclusions hold:

$$[X_n \leq d\gamma_n - \delta_n] \cap F_n \subset E_n \cap F_n \subset [X_n \leq d\gamma_n + \delta_n]. \tag{20}$$

The rightmost inclusion in (20) and the Lipschitz condition on f entail the upper bound

$$\mathbb{P}_n[E_n \cap F_n] \leq f\left(d + \frac{\delta_n}{\gamma_n}\right) + O(\varepsilon_n) = f(d) + O\left(\varepsilon_n + \frac{\delta_n}{\gamma_n}\right). \tag{21}$$

The leftmost inclusion in (20) together with (19) and the Lipschitz condition entail the lower bound

$$\mathbb{P}_n[E_n \cap F_n] \geq f(d) + O\left(\varepsilon_n + a^{-\delta_n} + \frac{\delta_n}{\gamma_n}\right). \tag{22}$$

With relations (19), (21) and (22), we obtain

$$\mathbb{P}_n[E_n] = f(d) + O\left(\varepsilon_n + a^{-\delta_n} + \frac{\delta_n}{\gamma_n}\right).$$

Then the optimal choice $\delta_n = |\log_a \varepsilon_n|$ concludes the proof. □

To derive the proof of Theorem 5, we apply the previous proposition to the variables L_1 and $(L - L_1)$ with

$$\gamma_n = n, \qquad \varepsilon_n = O\left(\frac{1}{n}\right), \quad \delta_n = \log_a n, \quad c = \frac{q-1}{2q}, \quad f(d) = 1 - \left(1 - \frac{d}{c}\right)^{\ell-1}.$$

6. Main results in the number case.

We now consider the analysis of the plain algorithm in the case of integers, and conduct a study that will appear to be very close to the previous one, dedicated to the polynomial inputs. As usual (see, e.g., (Lhote and Vallée, 2008; Vallée, 2006)), the polynomial study shows the road, and similar results are expected in the integer study, even if they are often more difficult to obtain and sometimes less precise.

In the integer case, the ℓ–plain Euclid algorithm has exactly the same structure as in the polynomial case. It is composed of $\ell - 1$ phases, each of them being the Euclid algorithm which performs the gcd computation between two integers.

We first define below the notion of size in Section 6.1. We then introduce further concepts specific to the number case, namely transfer operators in Section 6.2, and variations around the zeta function in Section 6.3. We then can formulate the main results in Section 6.5 (average case) and Section 6.6 (limit laws).

6.1. Set of inputs and notion of size.

The possible inputs are all the sequences $\underline{x}$ formed of ℓ integers, and we limit ourselves to positive integers, without loss of generality. The set of inputs is thus $\Omega = \mathbb{N}_+^\ell$, where $\mathbb{N}_+$ is the set of positive integers.

In the integer framework, the size is usually the binary length ν, defined as the number of digits in the binary expansion, namely $\nu(x) = 1 + \lfloor \log_2 x \rfloor$. Here, it is more convenient [4] to define the *size* d of an integer x as

$$\mathrm{d}(x) := \lfloor \log x \rfloor .$$

[4] The choice of the base 2 would introduce the factor $\log 2$ in many places in the asymptotic analysis. And we eliminate the additive factor $+1$, as we wish to have the equality $\mathrm{d}(1) = 0$, as in the polynomial case.

The size $\mathrm{d}(\underline{x})$ of the input $\underline{x} = (x_1, x_2, \ldots, x_\ell)$ is then defined as

$$\mathrm{d}(\underline{x}) := \mathrm{d}(x_1 x_2 \ldots x_\ell) = \lfloor \log(x_1 x_2 \ldots x_\ell) \rfloor.$$

Observe that the difference between $\mathrm{d}(\underline{x})$ and the total binary size occupied by the ℓ-uple $\underline{x}$ is bounded. Here again, the subset Ω_n of inputs with size n is

$$\Omega_n := \{\underline{x} \in \mathbb{N}^\ell \mid \mathrm{d}(x_1 x_2 \ldots x_\ell) = n\} = \{\underline{x} \in \mathbb{N}^\ell \mid \lfloor \log(x_1 x_2 \ldots x_\ell) \rfloor = n\}.$$

Then, we also deal with the notion of *product length*. The product length of a sequence $\underline{x} = (x_1, x_2, \ldots, x_\ell)$ is defined as the product

$$\pi(\underline{x}) := x_1 x_2 \ldots x_\ell$$

of its components. With this notation, the set of the inputs of size n

$$\Omega_n = \{\underline{x} \mid e^n \leq \pi(\underline{x}) < e^{n+1}\}$$

gathers the inputs whose product length belongs to the interval $[e^n, e^{n+1}[$. This is a finite set, and it is endowed with the uniform probability.

6.2. The underlying dynamical system and the transfer operator.

In the integer case, the 2-Euclid algorithm is described with the underlying dynamical system $([0,1], S)$, namely the Gauss map S defined on the unit interval $[0,1]$ by

$$S(x) := 1/x - \lfloor 1/x \rfloor, \text{ if } x \neq 0, \text{ and } S(0) = 0.$$

We use in particular the transfer operator of the dynamical system, introduced in a general setting in Ruelle (2004) and deeply studied in the case of the Gauss map in Mayer (1990). This operator deals here with the Gauss map S and the set $\mathcal{G}$ of its inverse branches, namely

$$\mathcal{G} := \left\{ h_m(x) : x \mapsto \frac{1}{m+x} \mid m \geq 1 \right\}.$$

It extends the Perron-Frobenius operator, it now involves a complex parameter s, and acts for $\Re s > 1$ on functions f defined on the unit interval as [5]

$$\mathbf{G}_s[f](x) = \sum_{h \in \mathcal{G}} |h'(x)|^{s/2} \cdot f \circ h(x) = \sum_{m \geq 1} \frac{1}{(m+x)^s} \cdot f\left(\frac{1}{m+x}\right). \tag{23}$$

In particular, the relation

$$\mathbf{G}_s[1](0) = \sum_{h \in \mathcal{G}} |h'(0)|^{s/2} = \sum_{n \geq 1} \frac{1}{n^s} = \zeta(s) \tag{24}$$

relates the transfer operator to the Riemann ζ function $\zeta(s)$. There is also a nice formula [6] which relates the quasi-inverse of the transfer operator and the Riemann ζ function, namely

$$(I - \mathbf{G}_s)^{-1}[1](0) = 2\,\frac{\zeta(s-1)}{\zeta(s)}. \tag{25}$$

[5] The usual definition of $\mathbf{G}_s$ is with the exponent s and not $s/2$ as here. But the present choice is more convenient here.

[6] See a proof of this relation, e.g., in (Flajolet and Vallée, 1998), where unfortunately the expression and the proof are not completely exact, there is indeed an extra factor -1.

It will be extended in Equation (31) of Proposition 16 into

$$(I - \mathbf{G}_{s+t})^{-1} \circ (\mathbf{G}_s + \mathbf{G}_t)[1](0) = 2\,\frac{\zeta(s)\zeta(t)}{\zeta(s+t)}.$$

In particular, the function $\varphi_{s,t}$ defined for $\Re s > 1$ and $\Re t > 1$ as

$$\varphi_{s,t}(x) := \frac{1}{2}\,\frac{\zeta(s+t)}{\zeta(s)\zeta(t)}(I - \mathbf{G}_{s+t})^{-1} \circ (\mathbf{G}_s + \mathbf{G}_t)[1](x) \tag{26}$$

is equal to 1 at $x = 0$. It can be extended (it will be proved and used later) when the parameter t is equal to 1, or when the pair (s, t) is equal to $(1, 1)$ as

$$\varphi_{s,1}(x) = \frac{1}{2}\,\frac{\zeta(s+1)}{\zeta(s)}(I - \mathbf{G}_{s+1})^{-1}[1](x), \qquad \varphi_{1,1}(x) = \frac{1}{1+x}, \tag{27}$$

and it plays an important rôle (see Assertion (b) of Theorem 13 and 14).

Here, the operator $\mathbf{G}_s$ is viewed as a generating operator for continued fractions, and it will play exactly the same role as the generating functions $G(z)$ for polynomials. (We will return to this point in Section 6.4.) We will describe more deeply the functional properties of the operator $\mathbf{G}_s$ in Section 8.4, but we now mention an essential property of this operator.

On a convenient functional space, and when s is close to the real axis, the operator $\mathbf{G}_{2s}$ admits a unique dominant eigenvalue denoted by $\lambda(s)$. For $s = 1$, the eigenvalue $\lambda(s)$ equals 1 and the eigenfunction is equal to $1/(1+x)$. The derivative of $s \mapsto \lambda(s)$ at $s = 1$ equals $-h/2$ where[7] *h is the entropy of the dynamical system provided by the Gauss map, equal to $\pi^2/(6\log 2)$.*

6.3. Various zeta functions.

There are also further close connections between the operator $\mathbf{G}_s$ and the Riemann ζ function, as we now see. The Riemann ζ function and the Hurwitz ζ functions are

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s}, \qquad \zeta(s, 1+x) := \sum_{n\geq 1} \frac{1}{(n+x)^s}.$$

The relation

$$\mathbf{G}_s[1](x) = \sum_{h\in\mathcal{G}} |h'(x)|^{s/2} = \sum_{n\geq 1} \frac{1}{(n+x)^s} = \zeta(s, 1+x)$$

holds, and explains the role of the Hurwitz ζ function here. We will be led to consider two variations of the ζ function, namely the *truncated ζ function* for indices n at least equal to M

$$\zeta_M(s) := \sum_{n\geq M} \frac{1}{n^s}, \tag{28}$$

that intervenes in Assertion (d) of Theorem 14, and the *bivariate ζ function*, with the variable u marking the size d,

$$Z(s, u) := \sum_{n\geq 1} \frac{u^{\mathrm{d}(n)}}{n^s}\,, \tag{29}$$

[7] The occurrence of the factor 1/2 is due to the change of variable $s \mapsto s/2$ already mentioned.

together with its cumulative generating function,

$$\widehat{\zeta}'(s) := \frac{d}{du} Z(s,u)\big|_{u=1} = \sum_{n\geq 1} \frac{\mathrm{d}(n)}{n^s}, \tag{30}$$

which resembles the derivative of $\zeta(s)$. We call here the *modified derivative* of the ζ function. It intervenes in Assertion (d) of Theorem 13.

6.4. From the polynomial to the number setting.

Let us now discuss the analogy between the analyses in the two settings (polynomials and integers). In the polynomial setting, the analysis was based on classical analytic combinatorics, with power generating functions, whereas in the number case, it will be based on dynamical combinatorics and Dirichlet generating functions. In both cases, the ℓ-Euclid algorithm translates as a product of generating functions (of power type for polynomials, and of Dirichlet type for integers), with each factor being associated with a given phase. Each phase is a sequence of divisions, which is expressed with the power generating function $G(z)$ in the polynomial setting, and, in the integer setting, with the functional operator $\mathbf{G}_s$ that generates the quotients. The coefficient extraction is provided in the polynomial case by the Cauchy formula on circles and in the number case, by the Perron formula on vertical lines. The dominant singularity is located at the complex z for which $G(z^{k+1}) = 1$ (polynomial case), and at the complex s for which $\lambda((k+1)s) = 1$ (number case). The following notation table stresses the parallelism between the generating functions that will be introduced for the number case in Section 7 and those which have been already introduced in Section 4, even though they are of power type in the polynomial setting, and of Dirichlet type in the integer setting.

6.5. Average-case analysis.

The following result is an exact analog of Theorem 2. In particular, in Assertion (a), the entropy $\pi^2/(6\log 2)$ of the integer Euclidean system (that is, of the Gauss map) replaces its polynomial analog $(2q)/(q-1)$ on $\mathbb{F}_q[X]$.

Theorem 13. [Expectations.] *When the set Ω_n is endowed with the uniform distribution, the following holds.*

(a) *The expectation of the number of iterations L_1 during the first phase is linear with respect to the size n and satisfies*

$$\mathbb{E}_n[L_1] = \frac{6\log 2}{\pi^2} \cdot \frac{n}{\ell} + K + O\left(\frac{1}{n}\right)$$

where the constant K depends on the dominant spectral objects of the operator $\mathbf{G_2}$ and is given in Equation (51) in Section 9.

(b) *For any $k \in [2..\ell-1]$, the expectation of the number of iterations L_k during the k-th phase is asymptotic to a constant which is expressed in terms of the operator $\mathbf{G}_s$ defined in* (23)*, taken at $s = k+1$, and of the function $\varphi_{k,1}$ defined in* (27)*, that is,*

$$\mathbb{E}_n[L_k] = (I - \mathbf{G}_{k+1})^{-1}[\varphi_{k,1}](0) + O\left(\frac{1}{n}\right).$$

$U(z)$	$\dfrac{1}{1-qz}$	$\zeta(s)$	$\displaystyle\sum_{n\geq 1}\frac{1}{n^s}$
$T(z,t)$	$\dfrac{U(z)+U(t)-1}{1-G(zt)}$	$2T(s,t)$	$(I-\mathbf{G}_{s+t})^{-1}\circ(\mathbf{G}_s+\mathbf{G}_t)[1](0)$
$T(z,t,u)$	$u\cdot\dfrac{U(z)+U(t)-1}{1-u\cdot G(zt)}$	$2T(s,t,u)$	$u\cdot(1-u\cdot\mathbf{G}_{s+t})^{-1}\circ(\mathbf{G}_s+\mathbf{G}_t)[1](0)$
$L_k(z,u)$	$U(z)^\ell\cdot\dfrac{T(z,z^k,u)}{T(z,z^k)}$	$L_k(s,u)$	$\zeta(s)^\ell\cdot\dfrac{T(s,ks,u)}{T(s,ks)}$
$U(t,u)$	$\dfrac{1}{1-qut}$	$Z(s,u)$	$\displaystyle\sum_{n\geq 1}\frac{u^{\mathrm{d}(n)}}{n^s}$
$D_k(z,u)$	$U(z)^\ell\cdot\dfrac{U(z^k,u)}{U(z^k)}$	$D_k(s,u)$	$\zeta(s)^\ell\cdot\dfrac{Z(ks,u)}{\zeta(ks)}$
$\widehat{L}_k(z)$	$U(z)^\ell\cdot\dfrac{1-qz^{k+1}}{1-q^2z^{k+1}}$	$\widehat{L}_k(s)$	$\zeta(s)^\ell\cdot(I-\mathbf{G}_{(k+1)s})^{-1}[\varphi_{ks,s}](0)$
$\widehat{L}_k^{[m]}(z)$	$U(z)^\ell\cdot G(z^{k+1})^{m-1}$	$\widehat{L}_k^{[m]}(s)$	$\zeta(s)^\ell\cdot\mathbf{G}_{(k+1)s}^{m-1}[\varphi_{ks,s}](0)$
$\widehat{D}_k(z)$	$U(z)^\ell\cdot\dfrac{qz^k}{1-qz^k}$	$\widehat{D}_k(s)$	$\zeta(s)^\ell\cdot\dfrac{\widehat{\zeta}'(ks)}{\zeta(ks)}$
$\widehat{D}_k^{[m]}(z)$	$U(z)^\ell\cdot(qz^k)^m$	$\widehat{D}_k^{[m]}(s)$	$\zeta(s)^\ell\cdot\dfrac{\zeta_{e^m}(ks)}{\zeta(ks)}$

Fig. 5. Generating functions (power series on the left for the polynomial case and Dirichlet type series on the right for the number case).

(c) *The expectation of the size of the first integer x_1 is linear with respect to the size n and satisfies*

$$\mathbb{E}_n[D_1]=\frac{n}{\ell}.$$

(d) *For any $k\in[2..\ell-1]$, the expectation of the size D_k of the gcd y_k at the beginning of the k-th phase is asymptotic to a constant which involves both the ζ function and its modified derivative defined in* (30) *at $s=k$, that is,*

$$\mathbb{E}_n[D_k]=\frac{\widehat{\zeta}'(k)}{\zeta(k)}+O\left(\frac{1}{n}\right).$$

The constant K is computed in Section 9.10. It involves explicit constants like the Euler-Mascheroni constant γ or $\zeta'(2)$. But it also involves dominant spectral objects of $\mathbf{G}_{2s}$ around $s=1$ that, as far as we know, do not have explicit closed-form expressions.

6.6. Limit laws.

The following results are analogs of the corresponding theorems in the polynomial case, but they are *not their exact* analogs. For the first phase, there are asymptotic beta laws, exactly as in the same vein as before; in particular, the entropy of the Euclid

dynamical system $\pi^2/(6\log 2)$ replaces its polynomial case analog. However, the results for subsequent phases ($k \geq 2$) are *not* the exact analogs of their polynomial counterparts. In the polynomial case, we have exhibited asymptotic geometric laws: for each k, there exists a ratio a_k for which

$$\mathbb{P}_n[L_k > m] = a_k^m + O\left(\frac{\log n}{n}\right), \qquad \mathbb{P}_n[D_k \geq m] = a_k^m + O\left(\frac{\log n}{n}\right).$$

Now, we obtain asymptotic (quasi)-geometric laws, that is,

$$\mathbb{P}_n[L_k > m] = a_{k,m} + O\left(\frac{\log n}{n}\right), \qquad \mathbb{P}_n[D_k \geq m] = a_{k,m} + O\left(\frac{\log n}{n}\right),$$

where $a_{k,m}$ is not an exact m-th power, but only an asymptotic m-power (when $m \to \infty$): there exist a_k, b_k and $\rho_k > 1$ for which

$$a_{k,m} = b_k a_k^m \left(1 + O(\rho_k^{-m})\right).$$

We will say that it is a *(quasi)-geometric asymptotic law with ratio* a_k.

For instance, in the D–case, the distribution involves the distribution of the Zipf law of order k, namely $x \mapsto \zeta_x(k)/\zeta(k)$, composed with an exponential change of variable $x \mapsto e^x$. This does not give rise to a "true" geometric law, but a (quasi)-geometric law.

Theorem 14. [Limit laws.] *When the set Ω_n is endowed with the uniform distribution, the following holds.*

(*a*) *The number of steps L_1 during the first phase asymptotically follows a beta law with parameters $(1, \ell-1)$ on the interval $[0, (6\log 2)/\pi^2]$: for any pair (m, n) whose ratio m/n belongs to the interval $[0, (6\log 2)/\pi^2]$, the probability of the event $[L_1 > m]$ satisfies*

$$\mathbb{P}_n[L_1 > m] = \left(1 - \frac{m}{n}\frac{\pi^2}{6\log 2}\right)^{\ell-1} + O\left(\frac{1}{n^\alpha}\right),$$

where the constant of the O-term is uniform when m/n belongs to $[0, (6\log 2)/\pi^2]$.

(*b*) *The number of steps L_k during the subsequent phases asymptotically follows a (quasi)-geometric law with ratio $\lambda(k+1)$: for any pair (m, n) for which the ratio m/n belongs to the interval $[0, \lambda(k+1)/|\lambda'(k+1)|]$, the probability of the event $[L_k > m]$ satisfies*

$$\mathbb{P}_n[L_k > m] = \mathbf{G}_{k+1}^m[\varphi_{k,1}](0) + O\left(\frac{\log n}{n}\right),$$

where the constant hidden in the O-term is uniform when m/n belongs to the interval $[0, \lambda(k+1)/|\lambda'(k+1)|]$. Here, the operator $\mathbf{G}_s$ is the transfer operator of the Euclidean dynamical system defined in (23), $\lambda(s)$ is its dominant eigenvalue, and the function $\varphi_{k,1}$ is defined in (27).

(*c*) *The size D_1 of the first gcd x_1 asymptotically follows a beta law of parameter $(1, \ell-1)$ on the interval $[0, 1]$: for any pair (m, n) for which the ratio m/n belongs to the interval $[0, 1]$, the probability of the event $[L_1 \geq m]$ satisfies*

$$\mathbb{P}_n[D_1 \geq m] = \left(1 - \frac{m}{n}\right)^{\ell-1} + O\left(\frac{1}{n^\alpha}\right),$$

where the constant of the O-term is uniform when m/n belongs to $[0,1]$.

(*d*) *The size D_k of the gcd y_k at the beginning of the phase of index $k \in [2..\ell]$ asymptotically follows a (quasi)-geometric law with ratio e^{1-k}: for any pair (m,n) for which the ratio m/n belongs to the interval $[0,1]$, the probability of the event $[D_k \geq m]$ involves both the function $\zeta(s)$ and its truncated version ζ_M defined in (28), both taken at $s=k$, under the form*

$$\mathbb{P}_n[D_k \geq m] = \frac{\zeta_{e^m}(k)}{\zeta(k)} + O\left(\frac{\log n}{n}\right),$$

where the constant hidden in the O-term is uniform when m/n belongs to $[0,1]$.

6.7. Global parameters in the number case.

The following results are the analog of Theorem 5 and the proof follows the same principles.

The interrupted algorithm stops as soon as the gcd y_k is 1. If $\Pi(x_1,\dots,x_\ell)$ is the number of useful phases, the event $[\Pi \geq k]$ coincides with the event $[D_k \geq 1]$ for $k \in [1..\ell-1]$, which is estimated in Theorem 14. Then, it is possible to consider the total number L and $\tilde{L}$ of divisions performed by the naive algorithm and its interrupted version.

Theorem 15. [Global parameters.] *When the set Ω_n is endowed with the uniform distribution, the following holds.*

(*a*) *The distribution of the number Π of useful phases satisfies $\mathbb{P}_n[\Pi \geq 0] = 1$, $\mathbb{P}_n[\Pi \geq \ell] = 0$, $\mathbb{P}_n[\Pi \geq 1] = 1 + O(n^{-\alpha})$ and*

$$\mathbb{P}_n[\Pi \geq k] = \frac{\zeta_e(k)}{\zeta(k)} + O\left(\frac{\log n}{n}\right) \quad \text{for } k \in [2..\ell-1].$$

(*b*) *The total number of divisions $\tilde{L}$ performed by the interrupted version of the ℓ-Euclid algorithm has an expected value $\mathbb{E}_n[\tilde{L}]$ equal to*

$$\frac{6\log 2}{\pi^2}\cdot\frac{n}{\ell} + K + \sum_{k=2}^{\ell-1}\left((I-\mathbf{G}_{k+1})^{-1}[\varphi_{k,1}](0) + \frac{\zeta_e(k)}{\zeta(k)} - 1\right) + O\left(\frac{1}{n^\alpha}\right).$$

(*c*) *The total number L of iterations, and the total number $\tilde{L}$ of iterations of the interrupted algorithm both asymptotically follow a beta distribution of parameter $(1,\ell-1)$ on the interval $[0, 6\log 2/\pi^2]$ with a speed of convergence $O(\log n/n)$.*

7. Generating functions in the number case.

7.1. Dirichlet generating functions.

In the integer case, the study also relies on generating functions, being now of Dirichlet type.

The basic one is the (Dirichlet) generating function of the set $\mathbb{N}_+^\ell$. We deal with ℓ–uples $\underline{x}$ of positive integers $\underline{x} = (x_1, x_2, \dots, x_\ell)$ and consider the generating function

$$F(s_1,s_2,\dots,s_\ell) = \sum_{\underline{x}\in\mathbb{N}_+^\ell} \frac{1}{x_1^{s_1}}\frac{1}{x_2^{s_2}}\cdots\frac{1}{x_\ell^{s_\ell}} = \zeta(s_1)\dots\zeta(s_\ell),$$

where the ζ function is the generating function of $\mathbb{N}_+$, that is,

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s}.$$

In particular, the main case of interest $s_1 = s_2 = \dots s_\ell = s$ gives rise to

$$F(s) := F(s,\dots,s) = \sum_{\underline{x}\in\mathbb{N}^\ell} \frac{1}{\pi(\underline{x})^s} = \zeta(s)^\ell,$$

recalling that $\pi(\underline{x}) = x_1 x_2 \dots x_\ell$.

Consider now the case when the ℓ–uple $s = (s_1,\dots,s_\ell)$ is general. As previously in the polynomial case with Proposition 6, we first provide an alternative "algorithmic" expression for the generating function $\zeta(s_1)\,\zeta(s_2)$ as

$$\zeta(s_1)\,\zeta(s_2) = \zeta(s_1+s_2)\cdot T(s_1,s_2),$$

where the generating function $T(s_1,s_2)$ describes the Euclid algorithm on two integers. The following result is thus an analog of Proposition 6.

Proposition 16. [Phase-function.] *The generating function $F(s)$ of $\Omega = \mathbb{N}_+^\ell$ (with respect to the product length) decomposes as*

$$F(s) = \zeta(s)^\ell = \zeta(\ell s)\cdot \prod_{k=1}^{\ell-1} T(s,ks),$$

where the phase-function T is defined as

$$T(s,t) := \frac{\zeta(s)\zeta(t)}{\zeta(s+t)}.$$

Moreover, it can be expressed in terms of the transfer operator $\mathbf{G}_s$ relative to the Euclid dynamical system, defined in (23)*, as*

$$T(s,t) = \frac{1}{2}(I-\mathbf{G}_{s+t})^{-1}\circ(\mathbf{G}_s+\mathbf{G}_t)[1](0). \tag{31}$$

Proof. We again begin with the first phase. The gcd $y_2 := \gcd(x_1,x_2)$ together with the sequence of quotients $(m_1,m_2,\dots,m_r)$ completely determines the input pair (x_1,x_2). More precisely, one writes $(x_1,x_2) = (y_2\,\widehat{x}_1, y_2\,\widehat{x}_2)$ with a coprime pair $(\widehat{x}_1,\widehat{x}_2)$ and the execution of the Euclid algorithm on the pair $(\widehat{x}_1,\widehat{x}_2)$ produces the same sequence $(m_1,m_2,\dots,m_r)$ as the pair (x_1,x_2), with now remainders $\widehat{x}_i$ satisfying $x_i = y_2\widehat{x}_i$. Then the Dirichlet series decomposes as

$$F(s_1,s_2) = \sum_{x_1,x_2} \frac{1}{x_1^{s_1}}\frac{1}{x_2^{s_2}} = \sum_{y_2\geq 1} \frac{1}{y_2^{s_1+s_2}} \sum_{\widehat{x}_1,\widehat{x}_2} \frac{1}{\widehat{x}_1^{s_1}}\frac{1}{\widehat{x}_2^{s_2}} = \zeta(s_1+s_2)\left(\sum_{\widehat{x}_1,\widehat{x}_2} \frac{1}{\widehat{x}_1^{s_1}}\frac{1}{\widehat{x}_2^{s_2}}\right). \tag{32}$$

We need an alternative form for the last series. The Euclid algorithm first compares the two integers x_1 and x_2 (and then the two integers $\widehat{x}_1$ and $\widehat{x}_2$). There are three cases:

$$\widehat{x}_1 = \widehat{x}_2 = 1, \qquad \widehat{x}_1 > \widehat{x}_2, \qquad \widehat{x}_1 < \widehat{x}_2.$$

The execution of the Euclid algorithm on the pair $(\widehat{x}_1, \widehat{x}_2)$ with $\widehat{x}_1 > \widehat{x}_2$ builds continued fraction expansions for the two rational numbers, namely

$$\frac{\widehat{x}_2}{\widehat{x}_1} = h \circ g(0), \qquad \frac{\widehat{x}_3}{\widehat{x}_2} = g(0).$$

Here, $h := h_{m_1}$ is related to the first quotient and $g =: h_{m_2} \circ h_{m_3} \circ \ldots \circ h_{m_r}$ is related to the sequence $(m_2, m_3, \ldots, m_r)$. Since the two pairs $(\widehat{x}_1, \widehat{x}_2)$ and $(\widehat{x}_2, \widehat{x}_3)$ are coprime, the denominators of the two rational numbers $\widehat{x}_2/\widehat{x}_1$ and $\widehat{x}_3/\widehat{x}_2$ are expressed with derivatives, namely

$$\frac{1}{\widehat{x}_1^2} = |(h \circ g)'(0)| = |h'(g(0))| \cdot |g'(0)|, \qquad \frac{1}{\widehat{x}_2^2} = |g'(0)|.$$

Hence, in the case when $\widehat{x}_1 \geq \widehat{x}_2$ (which covers $\widehat{x}_1 = \widehat{x}_2 = 1$ and $\widehat{x}_1 > \widehat{x}_2$), the sum

$$\sum_{\widehat{x}_1 \geq \widehat{x}_2} \frac{1}{\widehat{x}_1^{s_1}} \frac{1}{\widehat{x}_2^{s_2}} = 1 + \sum_{h,g} |h'(g(0))|^{s_1/2} \cdot |g'(0)|^{(s_1+s_2)/2},$$

can be expressed, using Relation (24), with the transfer operator $\mathbf{G}_s$ as

$$\frac{1}{2}\left(1 + (I - \mathbf{G}_{s_1+s_2})^{-1} \circ \mathbf{G}_{s_1}[1](0)\right).$$

The factor $(1/2)$ is here to take into account the fact that any rational of $]0, 1]$ admits two continued fraction expansions, namely the proper one and the improper one (see (Lhote and Vallée, 2008) for more details).

The case $\widehat{x}_2 \geq \widehat{x}_1$ can be dealt with exchanging the roles of $\widehat{x}_1$ and $\widehat{x}_2$. Finally, there is an alternative expression for the series

$$\sum_{\widehat{x}_1, \widehat{x}_2} \frac{1}{\widehat{x}_1^{s_1}} \frac{1}{\widehat{x}_2^{s_2}} = \frac{1}{2}(I - \mathbf{G}_{s_1+s_2})^{-1} \circ (\mathbf{G}_{s_1} + \mathbf{G}_{s_2})[1](0).$$

Finally, with (32), the Dirichlet series $F(s_1, s_2)$ decomposes as

$$F(s_1, s_2) = \zeta(s_1)\ \zeta(s_2) = \zeta(s_1 + s_2) \cdot T(s_1, s_2),$$

with

$$T(s, t) = \frac{\zeta(s)\zeta(t)}{\zeta(s+t)} = \frac{1}{2}(I - \mathbf{G}_{s+t})^{-1} \circ (\mathbf{G}_s + \mathbf{G}_t)[1](0), \tag{33}$$

which corresponds to the definition of T provided by (31).

When we replace this expression into the total product

$$\zeta(s_1)\,\zeta(s_2) \ldots \zeta(s_\ell) = F(s_1, s_2, \ldots, s_\ell),$$

and iterate the transformation, we obtain an alternative expression for the generating function $F(s_1, s_2, \ldots, s_\ell)$ with a product of $\ell - 1$ factors, each of them involving the phase-function T at points s_k and $t_k = s_1 + \ldots + s_k$, that is,

$$F(s_1, s_2, \ldots, s_\ell) = \zeta(t_\ell) \cdot \prod_{k=1}^{\ell-1} T(t_k, s_{k+1}).$$

It may be useful in some studies to keep all the variables s_i, but, here again, we let $s_1 = s_2 = \ldots = s_\ell = s$, and we obtain the expression of the generating function $F(s)$. □

7.2. Dirichlet generating functions for parameters.

As in the polynomial case, for studying a cost C on $\Omega = \mathbb{N}_+^\ell$, we consider the *bivariate generating function relative to the cost* C, obtained by introducing a further variable u to mark the cost, and defined as

$$C(s,u) := \sum_{\underline{x}\in\mathbb{N}^\ell} \frac{1}{\pi(\underline{x})^s}\, u^{C(\underline{x})}.$$

When studying the parameter L_k (number of steps in the k-th phase), the extra variable u marks each step of the k-th iteration, and we deal with the generating function

$$T(s,t,u) := \frac{1}{2}\cdot u \cdot (1 - u\cdot \mathbf{G}_{s+t})^{-1} \circ (\mathbf{G}_s + \mathbf{G}_t)[1](0), \qquad \text{with } t = ks \tag{34}$$

which replaces $T(s,ks)$ inside $F(s)$. Then, for any $k \in [1..\ell-1]$, the bivariate generating function $L_k(s,u)$ relative to the number of divisions during the k-th phase is written as

$$L_k(s,u) = \zeta(s)^\ell \cdot \frac{T(s,ks,u)}{T(s,ks)}. \tag{35}$$

When studying the parameter D_k (which is the size of the gcd at the beginning of the k-th phase), we use again the extra variable u which now marks the size of the gcd y_k, and we deal with the generating function $Z(t,u)$ defined in (29) at $t = ks$, which replaces $\zeta(ks)$ inside $F(s)$. Then, for any $k \in [1..\ell-1]$, the bivariate generating function $D_k(z,u)$ relative to the size of the k-th gcd y_k at the beginning of the k-th phase is written as

$$D_k(s,u) = \zeta(s)^\ell \cdot \frac{Z(ks,u)}{\zeta(ks)}. \tag{36}$$

Compare the expressions obtained in (35) and (36) with (7) in the polynomial setting.

Then, for studying the expectation of cost C (see (1)), we deal with the *cumulative generating function* given by

$$\widehat{C}(s) := \frac{\partial C}{\partial u}(s,u)\Big|_{u=1}.$$

For the distribution of C (see (2)), we use the *generating function of the event* $[C \geq m]$ that is also a cumulative generating function which is related to the generating function $C(s,u)$ as

$$\widehat{C}^{[m]}(s) := \sum_{i\geq m} [u^i] C(s,u).$$

As in the polynomial study, the series $\widehat{C}(s)$ is the sum of the series $\widehat{C}^{(m]}(s)$.

Finally, we obtain the following analog of Proposition 7.

Proposition 17. [Generating functions.] *Consider the transfer operator* $\mathbf{G}_s$ *defined in* (23)*, the function* $\varphi_{s,t}$ *defined in* (26)*, the Riemann* ζ *function, the bivariate Riemann series* $Z(s,u)$ *defined in* (29)*, the modified derivative* $\widehat{\zeta}'(s)$ *defined in* (30)*, and its truncated version* $\zeta_M(s)$ *defined in* (28)*.*

(*i*) *The bivariate generating function* $L_k(s,u)$*, as well as the cumulative generating functions* $\widehat{L}_k(s)$ *and* $\widehat{L}_k^{[m]}(s)$ *relative to the number of divisions during the* k*-th phase satisfy*

$$\frac{L_k(s,u)}{\zeta(s)^\ell} = \frac{\zeta((k+1)s)}{\zeta(ks)\zeta(s)}\, u\cdot(1-u\cdot\mathbf{G}_{(k+1)s})^{-1}\circ(\mathbf{G}_{ks}+\mathbf{G}_s)[1](0),$$

$$\frac{\widehat{L}_k(s)}{\zeta(s)^\ell} = (I-\mathbf{G}_{(k+1)s})^{-1}[\varphi_{ks,s}](0)\,, \qquad \frac{\widehat{L}_k^{[m]}(s)}{\zeta(s)^\ell} = \mathbf{G}_{(k+1)s}^{m-1}[\varphi_{ks,s}](0)\,.$$

(*ii*) *The bivariate generating function* $D_k(s,u)$*, as well as the cumulative generating functions* $\widehat{D}_k(s)$ *and* $\widehat{D}_k^{[m]}(s)$ *relative to the degree* D_k *of the gcd at the beginning of the* k*-th phase satisfy*

$$\frac{D_k(s,u)}{\zeta(s)^\ell} = \frac{Z(ks,u)}{\zeta(ks)}, \qquad \frac{\widehat{D}_k(s)}{\zeta(s)^\ell} = \frac{\widehat{\zeta}'(ks)}{\zeta(ks)}, \qquad \frac{\widehat{D}_k^{[m]}(s)}{\zeta(s)^\ell} = \frac{\zeta_{e^m}(ks)}{\zeta(ks)}\,.$$

Remark 18. According to Remark 1, one has $\mathbb{P}_n[D_k \geq 0] = 1$ in the D–case, whereas one has $\mathbb{P}_n[L_k \geq 1] = 1$ in the L-case. Note that $\zeta_{e^m}(s) = \zeta(s)$ for $m = 0$.

Remark 19. The two bivariate generating functions are written as

$$C(s,u) = \zeta(s)^\ell \frac{A(s,u)}{A(s,1)}\,, \tag{37}$$

with $A(s,u) = Z(s,u)$ [D-case], $\quad A(s,u) = u\cdot(1-u\cdot\mathbf{G}_{(k+1)s})^{-1}\circ(\mathbf{G}_{ks}+\mathbf{G}_s)[1](0)$ [L-case].

Proof. We first consider the generating functions $\widehat{L}_k^{[m]}(s)$ and $\widehat{D}_k^{[m]}(s)$.
In the L–case, extracting with respect to u in $L_k(s,u)$, given in (35), only involves the term $T(s,ks,u)$ in the numerator. One has

$$\begin{aligned} 2\sum_{i\geq m}[u^i]T(s,ks,u) &= \sum_{i\geq m}[u^i]\, u\cdot(I-u\cdot\mathbf{G}_{(k+1)s})^{-1}\circ(\mathbf{G}_s+\mathbf{G}_{ks})[1](0) \\ &= \mathbf{G}_{(k+1)s}^{m-1}\circ(I-\mathbf{G}_{(k+1)s})^{-1}\circ(\mathbf{G}_s+\mathbf{G}_{ks})[1](0). \end{aligned}$$

Then, introducing $T(s,t)$ and the functions $\varphi_{s,t}$, one gets

$$2\varphi_{s,t}(x) = \frac{\zeta(s+t)}{\zeta(s)\zeta(t)}(I-\mathbf{G}_{s+t})^{-1}\circ(\mathbf{G}_s+\mathbf{G}_t)[1](x), \quad T(s,t) = \frac{\zeta(s)\zeta(t)}{\zeta(s+t)},$$

which leads to the expression of $\widehat{L}_k^{[m]}(s)$.

In the D-case, with the expression of $D_k(s,u)$ given in (36), one gets

$$\sum_{i\geq m}[u^i]Z(s,u) = \sum_{i\geq m}[u^i]\sum_{n\geq 1}\frac{u^{\mathrm{d}(n)}}{n^s} = \sum_{i\geq m}\sum_{\substack{n\\ \mathrm{d}(n)=i}}\frac{1}{n^s} = \sum_{\substack{n\\ \mathrm{d}(n)\geq m}}\frac{1}{n^s} = \sum_{n\geq e^m}\frac{1}{n^s}\,.$$

which yields to the expression of $\widehat{D}_k^{[m]}(s)$.

Taking the derivative with respect to u, we obtain the following cumulative generating

functions. In the D–case, one gets

$$\widehat{D}_k(s) = \zeta(s)^\ell \, \frac{\widehat{\zeta}'(ks)}{\zeta(ks)}, \qquad \text{where} \quad \widehat{\zeta}'(s) = \frac{\partial Z}{\partial u}(s,u)\Big|_{u=1} = \sum_{n\geq 1} \frac{\mathrm{d}(n)}{n^s}. \tag{38}$$

In the L-case, the equality

$$\widehat{L}_k(s) = \zeta(s)^\ell \, \frac{\widehat{T}(s,ks)}{T(s,ks)} \tag{39}$$

involves the Dirichlet series $\widehat{T}(s,t)$ defined as

$$\begin{aligned} 2\widehat{T}(s,t) := \frac{\partial T}{\partial u}(s,t,u)\Big|_{u=1} &= \big[\mathbf{G}_{s+t} \circ (I-\mathbf{G}_{s+t})^{-1} + I\big] \circ (I-\mathbf{G}_{s+t})^{-1} \circ (\mathbf{G}_s + \mathbf{G}_t)[1](0) \\ &= (I-\mathbf{G}_{s+t})^{-2} \circ (\mathbf{G}_s + \mathbf{G}_t)[1](0). \end{aligned}$$

When we divide by $T(s,t)$, the function $\varphi_{s,t}$ defined in (26) occurs in a natural way. □

7.3. First properties of the cumulative generating functions.

We claim that the integer case is similar to the polynomial case. It is perhaps not completely clear that the functions

$$A_{k,m}(s) := \mathbf{G}^{m-1}_{(k+1)s}[\varphi_{ks,s}](0), \qquad A_{k,m}(s) = \frac{\zeta_{e^m}(ks)}{\zeta(ks)} \tag{40}$$

satisfy the same properties as their polynomial analogs. We prove that this is actually the case in Proposition 25. Let us first describe in an informal way their main properties.

The functions $A_{k,m}(s)$ defined in (40) *satisfy the following, for any phase of index $k \in [1..\ell-1]$.*

(*a*) *They are analytic on a half plane $\Re s > 1-\delta_0$.*

(*b*) *Near the real axis, the function $A_{k,m}(s)$ resembles an m-th power of a function $\lambda_k(s)$; at $s=1$, one has $\lambda_k(1)=1$ for $k=1$ and $\lambda_k(1)<1$ for $k\geq 2$.*

(*c*) *In a vertical strip $|\Re s - 1| < \delta_0$, the function $\zeta(s)^\ell \cdot A_{k,m}(s)$ is of polynomial growth for $|\Im s| \to \infty$.*

This last property, which will be made precise later, is specific to the study of Dirichlet series.

8. Analytic study in the number case.

8.1. Main principles for probabilistic analysis.

We have obtained in Proposition 17 explicit expressions for the cumulative generating functions. We have now to "extract" coefficients of these Dirichlet series for obtaining the proofs of Theorems 13 and 14. However, such an extraction is more difficult for a Dirichlet generating function: it is (very often) only possible to study partial sums of coefficients of the series F, namely

$$\begin{aligned} \Phi(N)[F(s)] &:= \sum_{p<N} [p^{-s}]F(s), \\ \Psi(n)[F(s)] &:= \sum_{e^n \leq p < e^{n+1}} [p^{-s}]F(s) = \Phi[e^{n+1}](F) - \Phi[e^n](F). \end{aligned} \tag{41}$$

We are mainly interested in the second sum $\Psi(n)[F(s)]$, as it deals with integers p for which $\mathrm{d}(p) = n$, which is useful when we deal with the set Ω_n of inputs with size n. Then, the mean value of a cost C on Ω_n is obtained from the cumulative generating function $\widehat{C}$, and its distribution is studied via the generating function $\widehat{C}^{[m]}$, thanks to the relations

$$\mathbb{E}_n[C] = \frac{\Psi(n)[\widehat{C}(s)]}{\Psi(n)[F(s)]}, \qquad \mathbb{P}_n[C \geq m] = \frac{\Psi(n)[\widehat{C}^{[m]}(s)]}{\Psi(n)[F(s)]}. \tag{42}$$

As previously, singularity analysis performs a transfer between the behavior of a Dirichlet generating function, viewed as a function of the complex variable s, near its dominant singularity (here, the singularity with the largest real part), and the asymptotic behavior of its coefficients. The position and the nature of the dominant singularity play here also a fundamental role.

This transfer is more difficult for Dirichlet series. As previously (in Proposition 11), the basic tool is the Cauchy formula, but, here, the circles centered at 0 are replaced by vertical lines, which are not compact. This is why Property (c) of Section 7.3 is essential in this case, to ensure integrals over the vertical lines to be convergent. We need the analog of Proposition 11, and we have now to deal with the Perron formula, as it was already the case for previous distributional analyses performed in the integer case (see (Baladi and Vallée, 2005), for instance). As we will see in the version of the Landau Theorem stated as Theorem 26, the Perron formula provides precise remainder terms as soon as the Dirichlet series of interest possesses a vertical strip on the left of the vertical line $\Re s = 1$, where $s = 1$ is its only pole (possibly of multiple order) and if it is of polynomial growth for $|\Im s| \to \infty$.

We now explain the plan of the remaining of this section. Its goal is to provide a proof of Theorems 13 and 14. We begin by providing two propositions, namely Propositions 20 and 22 which are the analogs of Propositions 9 and 11. These propositions are themselves two particular cases of the Landau Theorem (Theorem 26) proven in Section 9. As in the analysis in the polynomial case, when applied to the generating functions of interest, this will lead to the two main theorems, namely Theorems 13 and 14. In the following sections, we describe the analytical properties that are fulfilled by the main objects which intervene in the analysis: the transfer operator $\mathbf{G}_s$ (in Proposition 23) and the ζ series together with its variants (in Proposition 24). Finally, we explain in Proposition 25 why these properties entail the hypotheses needed for applying Propositions 20 and 22. And, as already said, applying these propositions yields our two main theorems.

8.2. A general framework for average-case analysis.

In our framework, where the bivariate generating functions admit the common form described in (37), the following proposition provides an analog to Proposition 9.

Proposition 20. [Expectations.] *Consider a cost C defined on $\mathbb{N}_+^\ell$, whose bivariate Dirichlet generating function is of the form*

$$C(s,u) = \zeta(s)^\ell \, \frac{A(s,u)}{A(s,1)}.$$

(*a*) *Then, the expectation* $\mathbb{E}_n[C]$ *satisfies*

$$\mathbb{E}_n[C] = \frac{\Psi(n)[\zeta(s)^\ell B(s)]}{\Psi(n)[\zeta(s)^\ell]},$$

where $\Psi(n)$ *is defined in* (41) *and* $B(s) = \widehat{A}(s)/A(s)$ *is the quotient between the cumulative generating function* $\widehat{A}(s)$ *related to* $A(s,u)$*, and* $A(s) = A(s,1)$*.*

(*b*) *Consider three real parameters* $\delta_0 \in]0,1[$*,* $\tau_0 > 0$*,* $\xi \geq 0$*, together with an integer* $\ell \geq 2$*, and a constant* M*, and assume that the following holds for the quotient* $B(s) = \widehat{A}(s)/A(s)$*.*

(*i*) *On the half-plane* $\{\Re s > 1 - \delta_0\}$*, there are two possibilities for this quotient,*

(*ia*) *either* $B(s)$ *is meromorphic with a unique simple pole at* $s = 1$*,*

(*ib*) *or* $B(s)$ *is analytic.*

(*ii*) *In all the cases, and in the part of the vertical strip* $\{s = \sigma + i\tau \mid |\sigma - 1| \leq \delta, |\tau| \geq \tau_0\}$ *with* $\delta < \delta_0$*,* $B(s)$ *satisfies*

$$|\zeta(s)^\ell B(s)| \leq M \cdot |\tau|^\xi.$$

Then, the following estimates hold for the expectation $\mathbb{E}_n[C]$ *of* C*:*

in the case (*ia*)*,* $$\mathbb{E}_n[C] = \operatorname{Res}\left(B(s); s = 1\right) \frac{n}{\ell} + O(1) + O\left(\frac{1}{n}\right);$$

in the case (*ib*)*,* $$\mathbb{E}_n[C] = B(1) + O\left(\frac{1}{n}\right).$$

As in the polynomial study, Proposition 20 will be proven with the help of the following proposition, whose proof is found in Section 9. It is mainly based on a theorem due to Landau (1924), for which we provide in Section 9 a version due to Mathieu Roux in his thesis (Roux, 2011).

Proposition 21. [Coefficients extraction.] *Consider three real parameters* $\delta_0 \in]0,1[$*,* $\tau_0 > 0$*,* $\xi \geq 0$*, together with an integer* $\ell \geq 2$*, and a bound* M*. Consider a Dirichlet series* $C(s)$ *having nonnegative coefficients, and assume the following.*

(*i*) *On the half-plane* $\{\Re s > 1 - \delta_0\}$*,* $C(s)$ *is meromorphic with a unique pole at* $s = 1$ *of order* $j \geq 2$*, and* $C(s)$ *satisfies*

$$\lim_{s \to 1} (s-1)^j C(s) = a_2.$$

(*ii*) *On the part of the vertical strip* $\{s = \sigma + i\tau \mid |\sigma - 1| \leq \delta, |\tau| \geq \tau_0\}$ *with* $\delta < \delta_0$*, one has*

$$|C(s)| \leq M \cdot |\tau|^\xi.$$

Then, the following estimate holds for the sum of coefficients $\Psi(n)[C(s)]$*, defined in* (41)*, for some constant* $\underline{a}$*,*

$$\Psi(n)[C(s)] = \underline{a}(e-1)e^n \frac{n^{\ell-1}}{(\ell-1)!}\left(1 + O\left(\frac{1}{n}\right)\right).$$

8.3. A general framework for distributional analysis.

In our framework, where the bivariate generating functions admit the common form described in (37), the following proposition provides an analog to Proposition 11.

Proposition 22. [Coefficients extraction and distribution.] *Consider a cost C defined on $\mathbb{N}_+^\ell$, whose bivariate Dirichlet generating function is of the form*

$$C(s,u) = \zeta(s)^\ell \frac{A(s,u)}{A(s,1)}.$$

(*a*) *Then, the probability of the event $\mathbb{P}_n[C \geq m]$ satisfies*

$$\mathbb{P}_n[C \geq m] = \frac{\Psi(n)[\zeta(s)^\ell A_m(s)]}{\Psi(n)[\zeta(s)^\ell])} \qquad \text{with} \quad A_m(s) = \frac{1}{A(s,1)} \sum_{i \geq m} [u^i] A(s,u),$$

where $\Psi(n)$ is defined in (41).

(*b*) *Consider three real parameters $\delta_0 \in]0,1[$, $\tau_0 > 0$, and $\xi \geq 0$, together with an integer $\ell \geq 2$, and two bounds M_1 and M_2, and assume that the following for $A(s)$ and the sequence $A_m(s)$.*

(*i*) *On the half-plane $\{\Re s > 1 - \delta_0\}$, for any $m \geq 1$, the series $A_m(s)$ is analytic, and there are two cases for $A(s) := A(s,1)$, namely*

(*ia*) *either $A(s)$ is meromorphic with a unique simple pole at $s = 1$,*

(*ib*) *or $A(s)$ is analytic.*

(*ii*) *On the rectangle $\mathcal{R}_\delta := \{s = \sigma + i\tau \mid |\sigma - 1| \leq \delta, |\tau| \leq \tau_0\}$, with $\delta < \delta_0$, $A_m(s)$ resembles an m–th power function, and admits the following decomposition*

$$A_m(s) = \lambda(s)^m \left[c(s) + R_m(s)\right], \qquad \text{with} \quad c(s) \neq 0, \quad |R_m(s)| \leq M_1 \cdot \theta^m$$

which involves analytic functions $c(s)$, $\lambda(s)$ and $R_m(s)$. Moreover, the restriction of λ to the horizontal segment $[1 - \delta, 1 + \delta]$ is positive, decreasing, and the restriction of $|\lambda|$ to each vertical segment attains its maximum on the real axis. We let

$$a := \lambda(1) > 0, \qquad b = -\lambda'(1) > 0.$$

(*iii*) *On the part of the vertical strip $\{s = \sigma + i\tau \mid |\sigma - 1| \leq \delta, |\tau| \geq \tau_0\}$, one has*

$$|\zeta(s)^\ell \cdot A_m(s)| \leq M_2 \cdot \lambda(1-\delta)^m \cdot |\tau|^\xi.$$

Then, the following estimates hold for $\mathbb{P}_n[C \geq m]$, for any pair (m,n) whose ratio m/n belongs to the interval $[0, a/b]$.

In the case (ia), the equalities $A_m(1) = 1$ and $\lambda(1) = 1$ hold, and

$$\mathbb{P}_n[C \geq m] = \left(1 - \frac{a}{b}\frac{m}{n}\right)^{\ell-1} + O\left(\frac{1}{n^\alpha}\right);$$

In the case (ib), the inequality $\lambda(1) < 1$ holds and

$$\mathbb{P}_n[C \geq m] = A_m(1) + O\left(\frac{\log n}{n}\right).$$

Here, in both cases, the hidden constants in the O–terms are uniform when the ratio m/n belongs to $[0, a/b]$, and, as in Proposition 11, the real α satisfies $\alpha = \min(1, (\ell-1)^2/(2\ell-1))$.

The proof of this proposition is based on a theorem due to Landau (1924), the same as for Proposition 20. The proof of this result, due to Mathieu Roux (Roux, 2011), is given in Section 9.

8.4. Analytical properties of the transfer operator $\mathbf{G}_s$.

We now describe the main properties of the transfer operator $\mathbf{G}_s$ and then, in the next section, of various versions of the Riemann ζ function.

The functional space $\mathcal{C}^1([0,1])$ of functions of class $\mathcal{C}^1$ on the interval $[0,1]$ is endowed with the $||\cdot||_{1,1}$ norm defined as

$$||f||_{1,1} = \sup\{|f(x)|\,;\, x \in [0,1]\} + \sup\{|f'(x)|\,;\, x \in [0,1]\}\,,$$

but is proves convenient to consider a family of norms $||\cdot||_{1,\tau}$ defined as

$$||f||_{1,\tau} = \sup\{|f(x)|\,;\, x \in [0,1]\} + \frac{1}{|\tau|}\sup\{|f'(x)|\,;\, x \in [0,1]\}.$$

For $\Re s > 1/2$, the operator $\mathbf{G}_{2s}$ satisfies the following (see (Baladi and Vallée, 2005) for more precisions).

Proposition 23. [Transfer operator.] *For $\Re s > 1/2$, the operator $\mathbf{G}_{2s}$ acts on $\mathcal{C}^1([0,1])$ and defines an analytic functions of s. For $\Re s > \rho_0$, with $\rho_0 < 1/2$, the operator $(I - \mathbf{G}_{2s})^{-1}$ is meromorphic with a unique pole at $s = 1/2$, and the operator $(1/\zeta(s))(I - \mathbf{G}_{2s})^{-1}$ is analytic. For any closed interval $[\sigma_1, \sigma_2] \subset]1/2, +\infty[$, there exist $\tau_0 > 0, K_1 > 0, K_2 > 0, \theta < 1, \xi \geq 0$ (with $\xi = 0$ when $\sigma_1 > 1$ and $\xi = 1/2$ otherwise), such that the following holds.*

(i) On the rectangle $[\sigma_1, \sigma_2] \times \{|\tau| \leq \tau_0\}$, the operator $\mathbf{G}_{2s}$ admits a unique dominant eigenvalue $\lambda(s)$ (positive for real s), with a spectral gap, and there is a spectral decomposition of the form

$$\mathbf{G}_{2s}^m[f] = \lambda(s)^m \mathbf{P}_s[f] + \mathbf{R}_s^m[f] \qquad \text{for } m \geq 1$$

which involves the projector $\mathbf{P}_s$ over the dominant eigenspace and the operator $\mathbf{R}_s$ relative to the remainder of the spectrum. The spectral radius of $\mathbf{R}_s$ is strictly smaller than $|\lambda(s)|$: there exist K_1 and $\theta < 1$ such that $||\mathbf{R}_s^m||_{1,1} \leq K_1\, \theta^m\, |\lambda(s)|^m$. Moreover, the restriction of λ to the horizontal segment $[\sigma_0 - \delta_0, \sigma_0 + \delta_0]$ is positive, log-convex and decreasing, and the restriction of $|\lambda|$ to each vertical segment attains its maximum on the real axis. Finally,

$$\sup\{|\lambda(s)| \mid s \in \mathcal{R}_\delta\} = \lambda(\sigma_1).$$

(ii) On the part of the vertical strip defined by $[\sigma_1, \sigma_2] \times \{|\tau| > \tau_0\}$, the norm $(1, \tau)$ of the operators $\mathbf{G}_s$ and $(I - \mathbf{G}_s)^{-1}$ satisfy

$$||\mathbf{G}_{2s}^m||_{1,\tau} \leq K_2\, |\tau|^\xi \cdot \lambda(\sigma_1)^m, \qquad ||(I - \mathbf{G}_{2s})^{-1}||_{1,\tau} \leq K_2\, |\tau|^\xi.$$

8.5. Analytical properties of the zeta functions.

This study involves several types of functions ζ (introduced in Section 6.3). The next proposition summarizes some important results in our context. See (Edwards, 2001) and (Tenenbaum, 1990) for more precisions.

Proposition 24. [Zeta functions.] *For $\Re s > 1/2$, the Riemann ζ function ζ, the Hurwitz zeta function $\zeta(s, x+1)$ and the truncated ζ function ζ_M define meromorphic functions of s, and the quotients*

$$\frac{\zeta(s, 1+x)}{\zeta(s)}, \qquad \frac{\zeta_M(s)}{\zeta(s)}$$

define analytic functions of s. For any closed interval $[\sigma_1, \sigma_2] \subset]1/2, +\infty[$, there exist $\tau_0 > 0, K_1 > 0, K_2 > 0, \theta < 1, \xi \geq 0$ (with $\xi = 0$ when $\sigma_1 > 1$ and $\xi = 1/2$ otherwise), such that the following holds.

(i) On the rectangle $[\sigma_1, \sigma_2] \times \{|\tau| \leq \tau_0\}$, the function $\zeta_{e^m}(s)/\zeta(s)$ resembles a large m-th power

$$\frac{\zeta_{e^m}(s)}{\zeta(s)} = e^{(1-s)m}\,(1 + R_m(s)) \qquad \text{with } R_m(s) \leq K_1 e^{-m}.$$

(ii) On the part of the vertical strip defined by $[\sigma_1, \sigma_2] \times \{|\tau| > \tau_0\}$, the zeta functions satisfy

$$|\zeta(s| \leq K_2\,|\tau|^{\xi}, \qquad ||\zeta(s, 1+x)||_{1,\tau} \leq K_2\,|\tau|^{\xi}, \qquad |\zeta_M(s)| \leq K_2\,|\tau|^{\xi} \cdot M^{\sigma_1 - 1}.$$

Moreover, for $\sigma_1 > 1$, the function $1/\zeta(s)$ is uniformly bounded there.

8.6. Final step for the probabilistic analysis.

We now prove Theorems 13 and 14. This will conclude the analysis in the integer case.

Proposition 25. *The following holds for the two bivariate generating functions $L_k(s, u)$ and $D_k(s, u)$.*

(a) They satisfy the hypotheses of Proposition 20. When Proposition 20 is applied to these bivariate generating functions, this entails Theorem 13.

(b) They satisfy the hypotheses of Proposition 22. When Proposition 22 is applied to these bivariate generating functions, this entails Theorem 14.

Proof. We first remark that, for any index k, the function $\varphi_{ks,s}$, defined as

$$\zeta((k+1)s) \cdot \frac{(I - \mathbf{G}_{2s})^{-1}}{\zeta(ks)} \left[1 + \frac{\zeta(ks, 1+x)}{\zeta(s)}\right],$$

is always analytic in a vertical strip $|\Re s - 1| \leq \delta_0$, for any value of k. Now, in the proof of each assertion, there are two main cases, according to the index k of the phase. The case $k \geq 2$ is easier to deal with, and we thus begin with it, in the proof of each assertion.

Assertion (a) The cumulative generating functions satisfy

$$\frac{\widehat{L}_k(s)}{\zeta(s)^{\ell}} = (I - \mathbf{G}_{(k+1)s})^{-1}[\varphi_{ks,s}](0)\,, \qquad \frac{\widehat{D}_k(s)}{\zeta(s)^{\ell}} = \frac{\widehat{\zeta}'(ks)}{\zeta(ks)}\,.$$

Case $k \geq 2$. In this case, in a vertical strip $|\Re s - 1| \leq \delta_0$, the two previous quotients define analytic functions of constant growth ($\xi = 0$). Moreover, the function $\zeta(s)^{\ell}$ is meromorphic in this strip, with a unique pole at $s = 1$, of order ℓ, and a polynomial growth with an exponent $\xi \leq \ell/2$. This entails that, in a vertical strip $|\Re s - 1| \leq \delta_0$, the functions $\widehat{L}_k(s)$ and $\widehat{D}_k(s)$ are meromorphic, with a unique pole at $s = 1$ of order ℓ.

Case $k = 1$. We write the two functions $\widehat{L}_k(s)$ and $\widehat{D}_k(s)$ in a different way when we focus on singularities or on polynomial growth.

We first consider *analyticity*. In the decomposition of the quotient function $\widehat{L}_k/\zeta(s)^\ell$ as $(I - \mathbf{G}_{2s})^{-1}[\varphi_{s,s}](0)$, the second factor is analytic in a vertical strip $|\Re s - 1| \leq \delta_0$, whereas the first factor is the quasi-inverse $(I - \mathbf{G}_{2s})^{-1}$ that has a unique pole of order 1 at $s = 1$ there. Then, the series $\widehat{L}_k(s)$ is meromorphic in a vertical strip $|\Re s - 1| \leq \delta_0$, with a unique pole of order $\ell + 1$ at $s = 1$.
The series $\widehat{D}_k(s)$ decomposes as $\zeta(s)^{\ell-1} \cdot \widehat{\zeta}'(s)$ and the series $\widehat{\zeta}'(s)$ is meromorphic in a vertical strip $|\Re s - 1| \leq \delta_0$ with a unique pole of order 2 at $s = 1$. Then, the series $\widehat{L}_k(s)$ is meromorphic in a vertical strip $|\Re s - 1| \leq \delta_0$, with a unique pole of order $\ell + 1$ at $s = 1$.

We now consider *polynomial growth*. The series $\widehat{L}_k(s)$ and $\widehat{D}_k(s)$ decompose as

$$\widehat{D}_k(s) = \zeta(s)^{\ell-1} \cdot \widehat{\zeta}'(s) \qquad \widehat{L}_k(s) = \zeta(s)^{\ell-2} \cdot \zeta(2s) \cdot (I - \mathbf{G}_{2s})^{-2}[\zeta(s, 1 + x)](0),$$

each factor being of polynomial growth in a vertical strip $|\Re s - 1| \leq \delta_0$ (for $|\Im s| \to \infty$).

Assertion (b) The cumulative generating functions satisfy

$$\frac{\widehat{L}_k^{[m]}(s)}{\zeta(s)^\ell} = \mathbf{G}_{(k+1)s}^{m-1}[\varphi_{ks,s}](0), \qquad \frac{\widehat{D}_k^{[m]}(s)}{\zeta(s)^\ell} = \frac{\zeta_{e^m}(ks)}{\zeta(ks)},$$

and these quotients, denoted in a generic way as $A_{k,m}(s)$, are always analytic (for any m and any k) in a vertical strip $|\Re s - 1| \leq \delta_0$. The general function $\lambda_k(s)$ of Proposition 22 satisfies

$$\lambda_k(s) := \lambda\left(\frac{s}{2}(k + 1)\right) \quad [L\text{-case}], \qquad \lambda_k(s) = \exp[1 - ks] \quad [D\text{-case}].$$

Case $k \geq 2$. At $s = 1$, the real numbers $\lambda_k(1)$ are strictly less than 1. Moreover, all the factors in the following decompositions

$$\widehat{L}_k^{[m]}(s) = \zeta(s)^{\ell-1} \cdot \frac{\zeta((k + 1)s)}{\zeta(ks)} \mathbf{G}_{(k+1)s}^{m-1} \circ (I - \mathbf{G}_{(k+1)s})^{-1}[\zeta(s, 1 + x) + \zeta(ks, 1 + x)],$$

$$\widehat{D}_k^{[m]}(s) = \zeta(s)^\ell \cdot \frac{\zeta_{e^m}(ks)}{\zeta(ks)}$$

exhibit polynomial growth (for the first factor) and bounded growth for the other factors.

Case $k = 1$. The real numbers $\lambda_k(1)$ are equal to 1. Moreover the equalities $A_{1,m}(1) = 1$ hold for any integer m. One has indeed in the L–case,

$$A_{1,m}(1) = \mathbf{G}_2^{m-1}[\varphi_{1,1}](0), \qquad \text{with} \quad \varphi_{1,1}(x) = \frac{1}{1 + x}.$$

As $1/(1+x)$ (proportional to the Gauss density) is invariant under the action of $\mathbf{G}_2$, this entails the equalities $A_{1,m}(s) = 1$ in the L-case. In the D-case, the equalities $A_{1,m}(1) = 1$ also hold due to the equality $\zeta(1) = +\infty$.
All the factors in the following decompositions

$$\widehat{L}_k^{[m]}(s) = \zeta(s)^{\ell-2} \cdot \zeta(2s) \cdot \mathbf{G}_{2s}^{m-1} \circ (I - \mathbf{G}_{2s})^{-1}[\zeta(s, 1 + x) + \zeta(ks, 1 + x)],$$

$$\widehat{D}_k^{[m]}(s) = \zeta(s)^{\ell-1} \cdot \zeta_{e^m}(s)$$

exhibit polynomial growth (for the first factor) and bounded growth for the other factors. □

9. A precise version of the Landau Theorem.

9.1. Statement of the Landau Theorem.

The proof we provide here is mainly based on the article (Landau, 1924), with a precise re-writting due to Roux in his thesis (Roux, 2011). We start with this version that we adapt to our context. We wish to apply the Landau Theorem to a sequence of functions that will share the same geometry defined by fixed parameters, namely the parameters $\sigma_0, \delta_0, \tau_0, \xi, \ell$ introduced in the following theorem. Inside this geometry, there is a Dirichlet series (the series $Z(s)$ of the following theorem) that will vary, and that brings its own parameters, namely the functions U and V which define its behavior at the pole $s = \sigma_0$, and the bounds $M(\delta)$ which describe its behavior on vertical lines close to the singulatity.

Theorem 26. *Consider five real parameters $\sigma_0, \delta_0, \tau_0, \rho_0, \xi$ with $\sigma_0 > \delta_0 > 0$, $\rho_0 < \delta_0$, $\tau_0 > 0$ and $\xi \geq 0$ and an integer $\ell \geq 2$. We denote*[8] *by k the integer $\lfloor \xi \rfloor + 2$.*

Consider a Dirichlet series

$$Z(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

with nonnegative coefficients a_n that satisfies the following hypotheses.

- *(i) The series $Z(s)$ is meromorphic on the half-plane $\{\Re s \geq \sigma_0 - \delta_0\}$ and admits a unique pole at $s = \sigma_0$ of order ℓ. We let denote by $U(s)$ the function $U(s) := Z(s)(s-\sigma_0)^\ell$ and by $V(s) := \log(U(s)/s)$. Let $M_0 := \sup\{|V(s)| \text{ s.t. } |s-\sigma_0| \leq \rho_0\}$.*
- *(ii) For any $\delta \in]0, \delta_0[$, there exists a real number $M(\delta)$ such that*
  - *(iia) on the domain $\{s = \sigma + i\tau \mid |\tau| > \tau_0, |\sigma - \sigma_0| \leq \delta\}$, the function $Z(s)$ satisfies $|Z(s)| \leq M(\delta)|\tau|^\xi$;*
  - *(iib) on the segment $\{s = \sigma + i\tau \mid \sigma = \sigma_0 - \delta, |\tau| \leq \tau_0\}$, the function $Z(s)$ satisfies $|(s-\sigma_0)^\ell Z(s)| \leq M(\delta)$.*

Then, for any $\delta \in]0, \delta_0[$ and, for any pair (y, t) with $t, y \to \infty$ and $y/t \to 0$, the following asymptotic estimates hold:

$$\begin{aligned} N_0(t) := \sum_{n \leq t} a_n = \operatorname{Res}\left(\frac{Z(s)}{s} t^s; s = \sigma_0\right) \\ + O\left(\frac{y}{t}\right) t^{\sigma_0} U(\sigma_0) \left(\log t + M_0\right)^{\ell-1} \\ + O(M(\delta))\ t^{\sigma_0 - \delta} \left(\left(\frac{t}{y}\right)^k + \frac{1}{\delta^\ell}\right) \left(1 + O\left(\frac{y}{t}\right)\right), \end{aligned}$$

[8] This notation is only for this section. Outside of Section 9, k stands for the index of a phase in the multiple gcd algorithm.

where the hidden constants in the O-terms only depend on the fixed parameters σ_0, δ_0, τ_0, ξ, and ℓ. They do not depend on the own parameters of $Z(s)$, namely the functions U, V and the bounds $M(\delta)$. They neither depend on the variable parameters (t, y, δ).

9.2. Perron formula of order k.

We are interested in the study of the simple sum $N_0(t)$ (of order 0) of the coefficients a_n for indices $n \leq t$. But, there are other sums which are useful, namely the sums of order k.

Definition 27. For any integer k and a real $t \in \mathbb{R}$, the *sum of order k* of the coefficients of the series $Z(s)$ is defined as

$$N_k(t) := \frac{1}{k!} \sum_{n \leq t} a_n (t-n)^k.$$

For any $k \geq 2$ and any $t \in \mathbb{R}$, the derivative of N_k equals N_{k-1} and the relation remains true for $k = 1$ and $t \in \mathbb{R} \setminus \mathbb{N}$.

We now recall the Perron formula of order k that relates the sum of order k to an integral on a vertical line of the series $Z(s)/(s(s+1)\dots(s+k))$.

Proposition 28. [Perron formula of order k.] *For any integer $k \in \mathbb{N}$, any real $t > 0$ and any $c > \sigma_0$, the sum $N_k(t)$ admits an alternative formula as an integral on a vertical line*

$$N_k(t) = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} \frac{Z(s) t^{s+k}}{s(s+1)\dots(s+k)} ds\,. \tag{43}$$

When $s = \sigma + i\tau$, Hypothesis (iia) of Theorem 26 entails the following estimate, for $|\tau|$ large enough,

$$\frac{Z(s)}{s(s+1)\dots(s+k)} = O(|\tau|^{\xi-k-1}),$$

which shows that the integral in (43) is absolutely convergent as soon as the inequality $k > \xi$ holds.
We wish to obtain an asymptotic estimate for the sum $N_0(t)$ of order 0. The idea is to use the Perron formula of order k, obtain an estimate for $N_k(t)$, and then relate $N_k(t)$ with $N_0(t)$.

9.3. Operators Δ_y and I_y.

This will be done via the operators Δ_y and I_y that we now introduce. The operator Δ_y is a finite-difference operator and I_y is an integral operator.

Definition 29. For $y \in \mathbb{R}$, the operators Δ_y and I_y are defined as

$$\Delta_y[f] : t \to f(t+y) - f(t), \qquad I_y[f] : t \to \int_t^{t+y} f(u)du.$$

We let denote as usual the k–th powers of these operators as Δ_y^k and I_y^k, respectively, and we now describe the main properties of these operators.

Proposition 30. *The following holds.*

(*a*) *The two operators satisfy* $\Delta_y[f](t) = I_y[f'](t)$.

(*b*) *For a Dirichlet series with* nonnegative coefficients*, the following inequality holds for any* $k \geq 1$*:*

$$\frac{1}{y^k}\Delta_y^k[N_k](t-ky) \leq N_0(t) \leq \frac{1}{y^k}\Delta_y^k[N_k](t).$$

(*c*) *Consider* $0 < y \leq t$ *and* $k > \xi$*. Then, there is an integral form for* $\Delta_y^k[N_k](t)$*, namely*

$$\Delta_y^k[N_k](t) = \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} \frac{Z(s)}{s}\, I_y^k[t^s](t)\, ds.$$

(*d*) [Far from the real axis.] *There exists a positive real number* $M_+ = M_+(k)$ *that depends only on* $\tau_0, \sigma_0, \delta_0$ *and* k *such that, for any* $s = \sigma + i\tau$ *in the vertical strip* $\{s = \sigma + i\tau \mid |\sigma - \sigma_0| < \delta_0,\ |\tau| \geq \tau_0\}$ *and any* y, t *with* $0 < y \leq t$*, the function* $I_y^k[t^s](t)$ *satisfies*

$$|I_y^k[t^s](t)| \leq M_+(k)\, t^{\sigma+k}|\tau|^{-k}.$$

(*e*) [Near the real axis.] *There exists a positive real number* $M_- = M_-(k)$ *that depends only on* $\tau_0, \sigma_0, \delta_0$ *and* k*, such that, for any* s *in the rectangle* $\{s = \sigma + i\tau \mid |\sigma - \sigma_0| \leq \delta_0,\ |\tau| \leq \tau_0\}$*, and for any real numbers* y, t *with* $0 < y \leq t$*, the function* $I_y^k[t^s](t)$ *satisfies*

$$I_y^k[t^s](t) = y^k t^s\,(1 + \epsilon(s))\,, \qquad \text{with} \quad |\epsilon(s)| \leq M_-(k)\,\frac{y}{t}.$$

Remark. Nonnegativity of coefficients a_n is only assumed in Assertion (*b*). It is not needed in the other assertions.

Before proving Proposition 30, we explain how it will be applied to get the estimate of $N_0(t)$ stated in Theorem 26. Assertion (*b*) describes how to replace the study of the sum N_0 of order 0 by the function $t \mapsto \Delta_y^k[N_k](t)]$ which involves the sum N_k of order k. Then Assertion (*c*) provides an expression of $\Delta_y^k[N_k](t)$ as an integral "à la Perron" which resembles the classical integral (43) where the function $I_y^k[t^s]$ replaces the function t^s. As we wish to return to the initial function t^s, Assertions (*d*) and (*e*) provide comparisons between both functions, far from the real axis for Assertion (*d*), and near the real axis for Assertion (*e*).

Proof.

(*a*) Clear.

(*b*) Applying (*a*), with an easy induction on the integer k, shows that $\Delta_y^k[N_k](t)$ can be expressed as a linear combination of the points $N_k(t)$, $N_k(t+y)$,..., $N_k(t+ky)$, namely

$$\Delta_y^k[N_k](t) = \int_t^{t+y} dt_1 \int_{t_1}^{t_1+y} dt_2 \ldots \int_{t_{k-1}}^{t_{k-1}+y} N_0(t_k)dt_k.$$

When the coefficients a_n of the Dirichlet series are *nonnegative*, the function $N_0(t)$ is nondecreasing, and the previous integral expression provides an upper bound and a lower bound.

(*c*) [Obtained as Corollary 16.6 in (Roux, 2011).] The expression is obtained when applying the operator Δ_y^k to the two sides of the Perron formula (43), and using the equality

$$(s+1)\ldots(s+k)\cdot I^k[t^s] = \Delta_y^k[t^{s+k}].$$

Statements (d) and (e) are not proven here. They are stated and proven as Lemmas 16.8.1 and 16.8.2 in (Roux, 2011), respectively. □

9.4. Principles of the proof.

We then wish to compute the following integral, with $c > \sigma_0$:

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{Z(s)}{s}\,I_y^k[t^s](t)\,ds\,. \tag{44}$$

Changing the contour. We consider the rectangle formed with the two vertical lines $\Re s = c$ (with $c > \sigma_0$) and $\mathcal{C}_\delta := \{\Re s = \sigma_0 - \delta\}$ (with $\delta \in]0, \delta_0]$) together with the two horizontal lines $\Im s = \pm M$. Denote by $\mathcal{D}_M$ its frontier with a positive orientation. Inside this rectangle, the function $s \mapsto (Z(s)/s)\cdot I_y^k[t^s](t)$ is meromorphic and admits the unique pole $s = \sigma_0$. Then, the Residue Theorem applies and entails the equality

$$\frac{1}{2i\pi}\int_{\mathcal{D}_M}\frac{Z(s)}{s}I_y^k[t^s](t)ds = \mathrm{Res}\left(\frac{Z(s)}{s}I_y^k[t^s](t);\quad s=\sigma_0\right).$$

When now M tends to ∞, the integrals on the two horizontal lines tend to 0, due to Assertion (d) of Proposition 30 and Hypothesis (iia) of Theorem 26. There remain the integrals on the vertical lines, and we then obtain the equality

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{Z(s)}{s}\,I_y^k[t^s](t)\,ds = \mathrm{Res}\left(\frac{Z(s)}{s}I_y^k[t^s](t);\quad s=\sigma_0\right)+\frac{1}{2i\pi}\int_{\mathcal{C}_\delta}\frac{Z(s)}{s}\,I_y^k[t^s](t)\,ds\,.$$

Getting the estimate for $N_0(t)$. We expect that

$$\mathrm{Res}\left(\frac{Z(s)}{s}\;t^s;\quad s=\sigma_0\right)$$

will be the main term in the final estimate. Then, there will be four remainder terms.

- (i) The remainder term $R_1(t,y)$ which is created by the difference between the two residues.
- (ii) Two remainder terms which arise in the estimate of the integral on the vertical line $\Re s = \sigma_0 - \delta$, the first one $R_2(t,y,\delta)$ near the real axis, and the second one $R_3(t,y,\delta)$ far from the real axis.
- (iii) The last remainder term $R_4(t,y)$ which arises when applying Assertion (b) of Proposition 30.

9.5. Difference between residues.

Lemma 31. *Consider a function $Z(s)$ which fulfills Hypothesis (i) of Theorem 26, and a pair (t,y) where $y > 0$ and $t > 0$ tends to ∞, with a ratio $y/t \to 0$.*

- (a) *Consider an analytic function $\epsilon(s)$ defined on a neighborhood of $s = \sigma_0$ which satisfies $\epsilon(s) = O(y/t)$. Then*

$$\left|\mathrm{Res}\left[\frac{Z(s)}{s}t^s[1+\epsilon(s)]\;;s=\sigma_0\right]-\mathrm{Res}\left[\frac{Z(s)}{s}t^s\;;s=\sigma_0\right]\right| \leq K\,\left(\frac{y}{t}\right)\,t^{\sigma_0}U(\sigma_0)\left(\log t + M_0\right)^{\ell-1},$$

where the constant K only depends on the fixed parameters.

(*b*) *In particular, the remainder $R_1(t,y)$ defined as*

$$R_1(t,y) := \frac{1}{y^k}\mathrm{Res}\left[\frac{Z(s)}{s} I_y^k[t^s](t)\ ; s=\sigma_0\right] - \mathrm{Res}\left[\frac{Z(s)}{s} t^s\ ; s=\sigma_0\right]$$

satisfies

$$|R_1(t,y)| \le K\ \left(\frac{y}{t}\right)\ t^{\sigma_0} U(\sigma_0)\left(\log t + M_0\right)^{\ell-1},$$

where the constant K only depends on the fixed parameters.

Proof. (*a*) Let

$$U(s) := (s-\sigma_0)^\ell Z(s), \quad V(s) := \log\left[\frac{U(s)}{s}\right], \quad W(s) = s\log t + V(s)\,.$$

The difference between the two residues is

$$\mathrm{Res}\left[\frac{Z(s)}{s} t^s \epsilon(s)\ ; s=\sigma_0\right] = \frac{(-1)^{\ell-1}}{(\ell-1)!}\frac{d^{\ell-1}}{ds^{\ell-1}}\Big(\exp[W(s)]\cdot\epsilon(s)\Big)_{s=\sigma_0}.$$

With Cauchy's theorem, for $k \le \ell$, all the derivatives $|\epsilon^{(k)}(\sigma_0)|$ are $O(y/t)$, and all the derivatives $|V^{(k)}(\sigma_0)|$ are $O(M_0)$. Then the first derivative of W at σ_0 is $O(\log t + M_0)$, while the other derivatives of W at σ_0 are $O(M_0)$. This shows that the derivative of order k of $\exp[W(s)]$ at $s=\sigma_0$ is $\exp[W(\sigma_0)]\cdot O(\log t + M_0)^k$. Finally, the residue can be bounded as

$$\mathrm{Res}\left[\frac{Z(s)}{s} t^s \epsilon(s)\ ; s=\sigma_0\right] \le K\ \left(\frac{y}{t}\right)\ t^{\sigma_0} U(\sigma_0)\left(\log t + M_0\right)^{\ell-1}.$$

(*b*) With Assertion (*e*) of Proposition 30, there exist an analytic function $s \mapsto \epsilon(s)$ and a constant M_- such that

$$I_y^k[t^s](t) = y^k\, t^s\, [1+\epsilon(s)] \qquad \text{with} \quad |\epsilon(s)| \le M_-\,\frac{y}{t}$$

where M_- is a positive constant that only depends on the fixed parameters. Then (*a*) may be applied. □

9.6. Estimate of the integral.

We now describe the estimates of the integral over the left vertical line $\Re s = \sigma_0 - \delta$. We consider two parts in this integral, the integral "far from the real axis", taken over the union $\mathcal{C}_\delta^+$ defined as $\{s = \sigma + i\tau \mid \Re s = \sigma_0 - \delta, |\tau| \ge \tau_0\}$, and the integral "near the real axis", taken over the segment $\mathcal{C}_\delta^- := \{s + i\tau \mid \Re s = \sigma_0 - \delta, |\tau| \le \tau_0\}$.

Far from the real axis.

Lemma 32. *With the notations of Theorem 26, one has*

$$R_2(t,y,\delta) = \frac{1}{y^k}\left|\int_{\mathcal{C}_\delta^+} \frac{Z(s)}{s}\ I_y^k[t^s](t)ds\right| = O(M(\delta))\ \left(\frac{t}{y}\right)^k\ t^{\sigma_0-\delta},$$

with a O-term that only depends on the fixed parameters.

Proof. Hypothesis (ii) of Theorem 26 together with Assertion (d) of Proposition 30 entail the existence of two constants $M(\delta)$ and M_+ for which the following inequality holds

$$\left| \int_{\mathcal{C}_\delta^+} \frac{Z(s)}{s}\, I_y^k[t^s](t)\, ds \right| \leq 2 \int_{\tau_0}^{+\infty} \frac{M(\delta)}{\tau}\, \tau^\xi\, M_+\, \frac{t^{\sigma_0-\delta+k}}{\tau^k} d\tau.$$

The integral is convergent as soon as the integer k is strictly larger than ξ. We choose $k = \xi + 2$. In this case, one has

$$\frac{1}{y^k} \left| \int_{\mathcal{C}_\delta^+} \frac{Z(s)}{s}\, I_y^k[t^s](t)\, ds \right| \leq K M(\delta) \left(\frac{t}{y}\right)^k t^{\sigma_0-\delta}$$

where the constant K only depends on the fixed parameters. □

Near the real axis.

Lemma 33. *With the notations of Theorem 26, one has*

$$R_3(t,y,\delta) := \frac{1}{y^k} \left| \int_{\mathcal{C}_\delta^-} \frac{Z(s)}{s} I_y^k[t^s](t) ds \right| = O\left(\frac{M(\delta)}{\delta^\ell}\right) t^{\sigma_0-\delta},$$

where the constant hidden in the O–term only depends on the fixed parameters.

Proof. According to Assertion (e) of Proposition 30, there exists a real M_+ that depends only on the fixed parameters such that

$$|I_y^k[t^s](t)| \leq M_+\, y^k\, t^{\sigma_0-\delta} \qquad \text{for } s \in \mathcal{C}_\delta^-.$$

With Hypothesis (ii) of Theorem 26, the following bound holds

$$\left| \int_{\mathcal{C}_\delta^-} \frac{Z(s)}{s}\, I_y^k[t^s](t)\, ds \right| \leq 2\tau_0 \frac{1}{|\sigma_0 - \delta_0|} \frac{M(\delta)}{\delta^\ell}\, M_+\, y^k\, t^{\sigma_0-\delta}$$

and

$$\frac{1}{y^k} \left| \int_{\mathcal{C}_\delta^-} \frac{Z(s)}{s} I_y^k[t^s](t) ds \right| \leq K_1 \frac{M(\delta)}{\delta^\ell} t^{\sigma_0-\delta},$$

where K_1 only depends on the fixed parameters. □

9.7. Return from $N_k(t)$ to $N_k(t-ky)$.

Assertions (b) and (c) of Proposition 30 exhibit an upper bound as well as a lower bound. The upper bound is an integral "à la Perron" which involves $I_y^k[t^s](t)$, and we have studied it. The lower bound is a similar integral "à la Perron" which now involves $I_y^k[(t-ky)^s](t-ky)$ instead of $I_y^k[t^s](t)$. So, we have to study what happens in our previous bounds when we "replace" t by $t-ky$. We consider the case when t and y tend to ∞, with a ratio y/t which tends to 0. We first observe the change which occurs in the bounds given in Assertions (d) and (e). For the bound of Assertion (d)

$$|I_y^k[(t-ky)^s](t-ky)| \leq M_4 (t-ky)^{\sigma+k} |\tau|^{-k} \leq M_4 t^{\sigma+k} |\tau|^{-k} \left(1 - k\frac{y}{t}\right)^{\sigma+k}. \qquad (45)$$

And, for the bound in Assertion (e), one gets

$$I_y^k[(t-ky)^s](t-ky) = y^k (t-ky)^s \left(1 + \epsilon_1(s)\right), \qquad \text{with} \quad |\epsilon_1(s)| \leq M_5 \frac{y}{t-ky}$$

and thus,

$$I_y^k[(t-ky)^s](t-ky) = y^k t^s \left(1-k\frac{y}{t}\right)^s (1+\epsilon_1(s))\,, \tag{46}$$

with

$$|\epsilon_1(s)| \le M_5 \frac{y}{t}\frac{1}{1-k(y/t)}.$$

Then, all the remainder terms R_1, R_2 et R_3 remain of the same order when t is replaced by $t-ky$ and, more precisely, one gets

$$R_1(t-ky,y) = R_1(t,y)\left(1+O\left(\frac{y}{t}\right)\right), (R_j(t-ky,y,\delta) = R_j(t,y,\delta)\left(1+O\left(\frac{y}{t}\right)\right)$$

where the constants in the O term do not depend on δ. There is also a new remainder term which appears in the residue when t is replaced by $t-ky$. The function changes, and the new residue is

$$y^k \mathrm{Res}\left(\frac{Z(s)}{s}(t-y)^s; s=\sigma_0\right) = y^k \mathrm{Res}\left(\frac{Z(s)}{s}t^s\left(1-k\frac{y}{t}\right)^s; s=\sigma_0\right).$$

We apply Lemma 31 to the function $\epsilon_1(s)$ defined by the relation

$$1+\epsilon_1(s) = \left(1-k\frac{y}{t}\right)^s$$

which is indeed $O(y/t)$ when s is close to σ_0. This ends the proof of Theorem 26.

We now have to apply the estimates given by the Landau Theorem to our setting. Using the specificities of our problem, we shall obtain the proofs of Propositions 21 and 22. We first estimate the residue, and prove that the three terms $R_i(t,y,\delta)$ are exponentially decreasing as soon as both parameters y and δ are chosen in a convenient way,

9.8. Application to Proposition 21.

We wish to study two functions, first $\zeta(s)^\ell$, second the function $\zeta(s)^\ell B(s)$, where $B(s) = \widehat{A}(s)/A(s)$ appears in the numerator and the denominator of the expectation $\mathbb{E}_n[C]$ in Proposition 20. We consider a general function $C(s)$ with a unique pole of order ℓ at $s=1$, we first study the residue, and then the remainder terms. There are now three remainder terms. As we are interested in the estimate of the sum $\Psi(n)$, we let $t=e^n$, and write $C(s) = (s-1)^{-j}B(s)$.

Computation of the residue. The estimate

$$\mathrm{Res}\left(\frac{C(s)}{s}e^{ns};\, s=1\right) = e^n \underline{a}\frac{n^{j-1}}{(j-1)!}\left(1+O\left(\frac{1}{n}\right)\right)$$

is clear. Indeed, according to the arguments that have been used several times in this paper, the residue is closely related to the value at $s=1$ of the $(j-1)$-th derivative of the function $\exp[ns+\log B(s)/s]$ at $s=1$, which is a polynomial with respect of n, of degree $j-1$, with a dominant term as above.

Choice for parameters y and δ. We recall that there are three terms which should give rise to actual remainder terms, provided we find a good choice for the free parameters (y, δ) for which these terms are proven to tend to 0. Here, we will fix $\delta := \delta_0/2$ (for instance) and now let $y = e^{n\theta}$, and choose θ. There are two main terms R_1 and R_2 which depend on y, and in fact on the ratio y/t. The condition $R_1(t, y) = R_2(t, y, \delta)$ entails the following equality (where we neglect the logarithmic factors in t), namely

$$\frac{y}{t} = t^{-\delta} \left(\frac{t}{y}\right)^k \qquad \theta - 1 = -\frac{\delta_0}{k+1}. \tag{47}$$

Then $R_1(t, y)$ and $R_2(t, y, \delta_0)$ are exponentially decreasing, namely of order $O\left(e^{n(\theta-1)}\right)$ (with some polynomial factor in n) and the third remainder term $R_3(t, y, \delta_0)$ is also exponentially decreasing.

9.9. Application to Proposition 22.

We wish to study the sequence $S^{[m]}(s) = \zeta(s)^\ell A_m(s)$ which occurs in the numerator of the probability $\mathbb{P}_n[C \geq m]$, and apply the Landau Theorem. As in the proof of Proposition 11, we first compute the residue which will give rise to the main term, and then, the three remainder terms. In the third step, we finally choose the width δ to conclude. As we are interested in the estimate of the sum $\Psi(n)$, we let $t = e^n$.

Computation of the residue.

Lemma 34. *With the hypotheses of Proposition 22, and for any pair (n, m) whose ratio m/n belongs to the interval $[0, c_0]$ with $c_0 < a/b$, one has, when $n \to \infty$*

$$\operatorname{Res}\left(\frac{S^{[m]}(s)}{s} e^{ns};\, s = 1\right) = e^n A_m(1) \frac{n^{\ell-1}}{(\ell-1)!} \left(1 - \frac{m}{n}\frac{b}{a}\right)^{\ell-1} \left(1 + O\left(\frac{1}{n}\right)\right).$$

Proof. The proof is similar to the proof of Proposition 11. The residue is closely related to the value at $s = 1$ of the $(\ell-1)$-th derivative of the function $\exp[W(s)]$, with

$$W(s) = ns + \log A_m(s) + V(s),$$

where $V(s)$ is related to a fixed function which involves the ζ function. As $A_m(s)$ resembles an m-th power, one has

$$\log A_m(s) = m \log \lambda(s) + \log c(s) + \log(1 + R_m(s)),$$

where $c(s)$, $\log(1 + R_m(s))$ and all their derivatives are uniformy bounded, with respect to pairs (m, n). Then $W(s)$ is written as

$$W(s) = n\left(s + \frac{m}{n} \log \lambda(s) + \frac{1}{n} W_1(s)\right), \tag{48}$$

where $W_1(s)$ is an analytic function which remains bounded (with its derivatives) at $s = 1$. Then, with the same arguments already used in the proof of Proposition 11,

$$\frac{d^{\ell-1}}{ds^{\ell-1}} \exp[W(s)]_{s=1} = \exp[W(1)] \left(W'(1)\right)^{\ell-1} \left[1 + O\left(\frac{1}{n}\right)\right]$$

provided that the derivative $W'(1)$ is positive. As this derivative satisfies, with $a := \lambda(1)$, $b := -\lambda'(1)$,

$$\frac{1}{n}W'(1) = \left(1 - \frac{m}{n}\frac{b}{a}\right) + O\left(\frac{1}{n}\right),$$

this arises for any pair (m, n) whose ratio m/n belongs to the interval $[0, c_0]$ with $c_0 < a/b$. In these conditions, one obtains the expected expression of the residue. □

Choice of the parameters y and δ. We now estimate more precisely, for each series $S^{[m]}(s)$, each of the three terms $R_1(t, y)$, $R_2(t, y, \delta)$ and $R_3(t, y, \delta)$, and we prove that there exists a choice of (y, δ) which gives rise to actual remainder terms, with a speed of convergence being uniform with respect to m.

Lemma 35. *For any $c_0 < a/b$, there exists a choice of parameters $\theta \in]0, 1[$, and $\delta < \delta_0$ for which the three terms $R_j(y, t, \delta)$ (for $j = 1, 2, 3$) satisfy, for any pair (n, m) whose ratio m/n belongs to $[0, c_0]$,*

$$[j = 1, 2] \qquad e^{-n} R_j(e^n, e^{n\theta}, \delta) = A_m(1)\ \ O\left(\exp\left[-n\left(1 - \frac{c_0}{c}\right)^2\right]\right)$$

$$[j = 3] \qquad e^{-n} R_3(e^n, e^{n\theta}, \delta) = A_m(1)\ \ O\left(\left(1 - \frac{c_0}{c}\right)^{-\ell} \exp\left[-n\left(1 - \frac{c_0}{c}\right)^2\right]\right),$$

where the constants of the O-terms do not depend on c_0.

Proof. We let $t = e^n, y = e^{\theta n}$. There are two main terms R_1 and R_2 which depend on y, and in fact on the ratio y/t. Up to the polynomial term in n, the remainder terms $R_1(e^n, e^{\theta n})$ and $R_2(e^n, e^{\theta n}, \delta)$ (in short, R_1 and R_2) satisfy

$$\frac{R_1}{A_m(1)e^n} = e^{-n(1-\theta)} \quad \text{and} \quad \frac{R_2}{A_m(1)e^n} = \exp(-nC) \tag{49}$$

with

$$C = \delta + k(\theta - 1) - \frac{1}{n}\log\frac{A_m(1-\delta)}{A_m(1)}. \tag{50}$$

We study the sign of C. Consider again the function

$$\frac{1}{n}\log A_m(s) = \frac{m}{n}\log\lambda(s) + \frac{1}{n}\Big(\log(c(s) + \log(1 + R_m(s))\Big).$$

The second term defines a function whose derivatives of order $k < \ell$ are $O(1/n)$, while the first term depends linearly on the ratio m/n. Then, neglecting this term of order $O(1/n)$, the function $(1/n)\log A_m(s)$ is equal to the function $(m/n)\log\lambda(s)$. Using the properties of the function $\lambda(s)$ (it is decreasing), the notation $a = \lambda(1)$, $b = -\lambda'(1)$, and letting $d := 2\sup\{|(\log\lambda(s))''| \mid [1 - \delta_0, 1]\}$, we obtain a lower and an upper bound, involving in particular the two constants $c = a/b$, and d, i.e.,

$$\frac{1}{n}\log A_m(1) + \frac{m}{n}\frac{1}{c}\delta \le \frac{1}{n}\log A_m(1-\delta) \le \frac{1}{n}\log A_m(1) + \frac{m}{n}\frac{1}{c}\delta + \frac{m}{n}d\delta^2.$$

Inserting the previous bounds in the expression of C entails that $C + k(1 - \theta)$ belongs to the interval $[B, A]$ with

$$A := \delta\left(1 - \frac{m}{n}\frac{1}{c}\right), \qquad B := \delta\left(1 - \frac{m}{n}\frac{1}{c} - \frac{m}{n}d\delta\right).$$

We decide to choose θ as

$$1-\theta=\frac{A+B}{2(k+1)}=\frac{\delta}{k+1}\left(1-\frac{m}{n}\frac{1}{c}-\frac{1}{2}\frac{m}{n}d\delta\right).$$

With this value, we will have $R_1\approx R_2$.

Study of the term R_2. First, we look for conditions on δ for which there exists $\eta_1>0$ such that $C\geq\eta_1\delta$. More precisely,

$$C\geq B-k(1-\theta)=B-\frac{k}{k+1}\frac{A+B}{2}=\frac{(k+2)B-kA}{2(k+1)}.$$

The constant C is larger than $\eta_1\delta$ for any pair (m,n) whose ratio m/n belongs to $[0,c_0]$ as soon as

$$\delta=\frac{1}{2(k+2)}\frac{c-c_0}{dcc_0}\qquad\eta=\eta_1=\frac{1}{k+1}\frac{c-c_0}{c}.$$

Study of the term R_1. Now, we look for conditions on δ for which there exists $\eta_0>0$ such that

$$1-\theta=\frac{1}{2(k+1)}(A+B)\geq\eta_0\delta>0$$

for any pair (m,n) whose ratio m/n belongs to $[0,c_0]$. Since the inequality $(k+2)B-kA\geq A+B$ holds, this second condition is weaker than the first one, we can thus choose the same δ as in case R_2, and $\eta_0=\eta_1$.

These choices define three functions of the ratio $(c-c_0)/c$, and, with these choices, the three remainder terms are exponentially decreasing, with the third one containing an extra factor $O(\delta^{-\ell})$. We now focus on this third one in the last step.

Study of probabilities. Now, with the normalisation given by the denominator, described in Proposition 21, and for any pair (m,n) whose ratio belongs to the interval $[0,c_0]$, with $c_0<c$, the following estimate holds

$$\mathbb{P}_n[C\geq m]=A_m(1)\left[\left(1-\frac{m}{n}\frac{b}{a}\right)^{\ell-1}+O\left(\frac{1}{n}\right)+O\left(\frac{1}{n^{\ell-1}}\left(1-\frac{c_0}{c}\right)^{-\ell}e^{-\eta_1\delta n}\right)\right],$$

where the constants of the O-term are uniform. We let now $c_0\to c$ as a function of n, and study in a separate way the cases $A_m(1)=1$ and $A_m(1)<1$, as in the proof of Proposition 11. This ends the proof of Proposition 22. □

9.10. Computation of the constant term in $\mathbb{E}_n[L_1]$.

The expression

$$\widehat{L}_1(s)=\zeta(s)^{\ell-2}\zeta(2s)(\mathbf{I}-\mathbf{G}_{2s})^{-2}[\zeta(s,1+x)](0)$$

involves the Hurwitz zeta function $\zeta(s,x)$ and the quasi-inverse $(\mathbf{I}-\mathbf{G}_{2s})^{-2}$ of the transfer operator $\mathbf{G}_{2s}$. They admit both singular expressions at $s=1$, namely

$$(\mathbf{I}-\mathbf{G}_{2s})^{-2}=\frac{\lambda(s)^2}{(1-\lambda(s))^2}\mathbf{P}_s+2\frac{\lambda(s)}{1-\lambda(s)}\mathbf{P}_s+(\mathbf{I}-\mathbf{R}_s)^{-2},$$

$$\zeta(s,1+x)=\frac{1}{s-1}-\frac{\Gamma'(1+x)}{\Gamma(1+x)}+(s-1)f(s,x)$$

where f is analytic in $s=1$. Using furthermore the analyticity of the projector $\mathbf{P}_s$ at $s=1$, and its derivative $\mathbf{P}_1'$, we obtain the asymptotic expression of $\widehat{L}_1(s)$ at $s=1$, namely

$$\begin{aligned}\frac{\widehat{L}_1(s)}{\zeta(s)^{\ell-2}} &= \frac{1}{s-1}\frac{\lambda(s)^2}{(1-\lambda(s))^2}\zeta(2s)\mathbf{P}_1[1](0)\\ &+\frac{\lambda(s)^2}{(1-\lambda(s))^2}\zeta(2s)\left[\mathbf{P}_1'[1]-\mathbf{P}_1\left[\frac{\Gamma'(1+x)}{\Gamma(1+x)}\right]\right](0)\\ &+\frac{1}{s-1}\frac{2\lambda(s)}{1-\lambda(s)}\zeta(2s)\mathbf{P}_1[1](0)\\ &+\frac{1}{s-1}g(s)\end{aligned}$$

where $g(s)$ is analytic in a half plane containing $s=1$. The projector $\mathbf{P}_1$ satisfies

$$\mathbf{P}_1[f](x)=\frac{1}{\log 2}\frac{1}{1+x}\int_0^1 f(t)dt$$

and then

$$\mathbf{P}_1[1](0)=\frac{1}{\log 2},\quad \mathbf{P}_1\left[\frac{\Gamma'(1+x)}{\Gamma(1+x)}\right](0)=0.$$

Then, straightforward computations provide the asymptotic expansions at $s=1$, namely

$$\widehat{L}_1(s)=K_0(s-1)^{-(\ell+1)}+K_1(s-1)^{-\ell}+O((s-1)^{-\ell+1})$$

$$\text{with}\quad K_0=\frac{6\log 2}{\pi^2},\qquad K_1=K_0\left[\log 2\,\mathbf{P}_1'[1](0)+\frac{\lambda''(1)}{\pi^2}\right]+(\ell-2)\frac{\gamma}{\pi^2}+12\zeta'(2)$$

where γ is the Euler constant. With Theorem 26, the following asymptotic expansions hold

$$\frac{\Psi(n)[\widehat{L}_1(s)]}{e^n}=c_0n^\ell+c_1n^{\ell-1}+O(n^{\ell-2}),\qquad \frac{\Psi(n)[\zeta(s)^\ell]}{e^n}=c_2n^{\ell-1}+c_3n^{\ell-2}+O(n^{\ell-3}),$$

and involve the following constants

$$c_0=\frac{K_0}{\ell!}(e-1)\quad c_1=\frac{K_1(e-1)+K_0}{(\ell-1)!},\quad c_2=\frac{1}{(\ell-1)!}(e-1)\quad c_3=\frac{1}{(\ell-2)!}(e\ell\gamma-\ell\gamma+1).$$

Then, the asymptotic mean $\mathbb{E}_n[\widehat{L}_1]$ satisfies

$$\mathbb{E}_n[\widehat{L}_1]=K_0\frac{n}{\ell}+\frac{c_1c_2-c_0c_3}{c_2^2}+O\left(\frac{1}{n}\right). \tag{51}$$

Remark that all the constants which appear here admit explicit forms, except the first derivative $\mathbf{P}_1'$ and the second derivative $\lambda''(1)$, for which such explicit forms are not known.

10. Conclusion.

Analogy between analyses in the two settings. The analogy between the polynomial and the integer settings is deeper than it might occur at first sight. It is not only

syntactic as illustrated in Figure 5, but is also "semantic". This is due to the existence of a dynamical system that underlies the polynomial Euclid algorithm, and presents strong (formal) similarities with its analog in the number case. Then, the classical analysis that can be performed for polynomials without references to the underlying dynamical system may be viewed as an instance of a dynamical analysis.

We first recall how to define a dictionary between integers and polynomials, as it is done in (Berthé and Nakada, 2000) or in (Lhote and Vallée, 2008, Section 6.2). When $\mathbb{F}_q[t]$ replaces $\mathbb{Z}$, then $\mathbb{F}_q(t)$ is the analog of $\mathbb{Q}$, and the field of Laurent formal power series $\mathbb{F}_q((1/t))$ is the analog of $\mathbb{R}$. For a Laurent series x, the degree $\mathrm{d}(x)$, the absolute value $||x||$, and the integer part are defined as follows:

$$\text{if } \; x = \sum_{n\geq n_0} \frac{x_n}{t^n} \;\; (\text{with } x_{n_0}\neq 0), \quad \text{then } \; \mathrm{d}(x) := n_0, \;\; ||x|| := q^{\mathrm{d}(x)}, \;\; \lfloor x \rfloor := \sum_{n=n_0}^{0} x_n \frac{1}{t^n}.$$

We now define the analog of the Gauss dynamical system on $\mathbb{F}_q((1/t))$. The analog of the unit interval is

$$\mathcal{X}_q := \{x \in \mathbb{F}_q((1/t)) \mid \quad ||x|| \leq 1\} = \{x \in \mathbb{F}_q((1/t)) \mid \lfloor x \rfloor = 0\},$$

and the Gauss map is

$$S : \mathcal{X}_q \to \mathcal{X}_q \qquad S(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor \quad (x \neq 0), \qquad S(0) = 0.$$

The set of digits is $\mathcal{D} := \{m \in \mathbb{F}_q[t] \mid ||m|| > 1\} = \{m \in \mathbb{F}_q[t] \mid \mathrm{d}(m) > 0\}$, and the set of the inverse branches of S is $\{h_{[m]}(x) = 1/(m+x); \;\; m \in \mathcal{D}\}$. The ultrametricity of the norm implies that the absolute value of the derivative of each $h_{[m]}$ is constant on $\mathcal{X}_q$, and equal to $||m||^{-2}$. Then, the dynamical system is without memory, with affine branches, and the transfer operator $\mathbf{G}_s$ defined as

$$\mathbf{G}_s[f](x) = \sum_{m\in\mathcal{D}} \left\| h'_{[m]}(x) \right\|^{s/2} f \circ h_{[m]}(x) = \sum_{m\in\mathcal{D}} \frac{1}{||m||^s} f \circ h_{[m]}(x),$$

transforms the function $f = 1$ into a constant function $\mathbf{G}_s[1]$,

$$\mathbf{G}_s[1] = \sum_{m\in\mathcal{D}} \frac{1}{||m||^s} = \sum_{m\in\mathcal{D}} \left(\frac{1}{q^{\mathrm{d}(m)}}\right)^s = \sum_{m\in\mathcal{D}} \left(\frac{1}{q^s}\right)^{\mathrm{d}(m)},$$

which is a power series in $z = q^{-s}$, and coincides with the (usual) generating function $G(z)$ of the set $\mathcal{D}$, i.e.,

$$\mathbf{G}_s[1] = G(z) = \sum_{m\in\mathcal{D}} z^{\mathrm{d}(m)} = (q-1)\sum_{n\geq 1} q^n z^n = \frac{q(q-1)z}{1-qz} = \frac{q-1}{q^{s-1}-1}.$$

Note that this also gives an easy way for computing the entropy of the dynamical system, equal to $2q/(q-1)$.

General issues analytic combinatorics. Here, with Propositions 11 and 22, we have described a general setting which possibly leads to beta laws. We now explain on an example how a beta law may replace a Gaussian law. We consider a product of ℓ sequences, namely $\Omega := \mathcal{V}^\ell$, where $\mathcal{V}$ is the combinatorial structure $\mathtt{Seq}(\mathcal{A})$, and $\mathcal{A}$ is itself

a structure. Then, an element ω of Ω is of the form $\omega = (v_1, v_2, \ldots, v_\ell)$, and each v_i is itself a finite sequence of elements of $\mathcal{A}$. We choose an integer $k \in [1..\ell]$, and consider the parameter R defined as $R(\omega) :=$ the number of components of the sequence v_k. If $\ell = 1$, the distribution of R is (under general conditions) asymptotically Gaussian; if $\ell = 2$, it is asymptotically uniform, and for $\ell \geq 3$, it follows asymptotically a beta law of parameters $(1, \ell - 1)$.
In a future work, we wish to better understand in which general settings a beta law may occur, and describe in which cases it may "replace" a Gaussian law.

Comparison with the random strategy. We now wish to compare more precisely the random strategy described in (von zur Gathen and Shparlinski, 2006) with the present analysis. The discussion is not completely clear as the size of the entries is not the same, and we know that changing the size may strongly change the results. We deal here with the sum-size while von zur Gathen and Shparlinski (2006) deal with the sup-size, and more precisely with the height, defined as [9] $h(\underline{x}) := \sup(|x_i|)$. The following is proved in (von zur Gathen and Shparlinski, 2006): the gcd of two linear combinations of *asymptotically the same size* as the inputs coincides with their gcd with probability $6/\pi^2$. More precisely, the following holds.

Consider three integers M, N, ℓ satisfying $M \geq \max(9\ell, \log N)$. Consider a vector $\underline{a} \in \mathbb{N}^\ell$ with a height at most equal to N. Then, the following two gcd's are equal

$$\gcd(\underline{a}) = \gcd(\underline{a}\cdot\underline{x}\,,\, \underline{a}\cdot\underline{y}),$$

with a probability close to $1/\zeta(2)$ when the pair $(\underline{x}, \underline{y})$ is uniformly chosen in the set $\{(\underline{x}, \underline{y}) \in \Omega^2 \mid \sup(h(\underline{x}), h(\underline{y})) \leq M\}$.

We assume that most of entries are balanced, then, with the notation of Section 6.1, $h(\underline{x}) \sim \pi(\underline{x})^{1/\ell} \sim \exp(\mathrm{d}(\underline{x})/\ell)$. The previous result may be thus stated in our setting as follows.

Consider three integers m, n, ℓ satisfying $m \geq \max(\ell\log(9\ell), \ell\log(n/\ell))$. Consider a vector $\underline{a} \in \mathbb{N}_+^\ell$ with a size at most equal to n. Then, the previous equality between the two gcd's still holds with a probability close to $1/\zeta(2)$ when the pair $(\underline{x}, \underline{y})$ is uniformly chosen in the set Ω_m^2.

The size of a scalar product $\mathrm{d}(\underline{a}\cdot\underline{x})$ satisfies

$$\mathrm{d}(\underline{a}\cdot\underline{x}) \sim \log\left(\ell \cdot \exp\left[\frac{1}{\ell}(\mathrm{d}(\underline{a}) + \mathrm{d}(\underline{x}))\right]\right) \sim \log\ell + \frac{1}{\ell}(\mathrm{d}(\underline{a}) + \mathrm{d}(\underline{x})).$$

Then, the number of steps of the gcd computation is

$$[\text{for } \gcd(\underline{a})] \qquad \frac{1}{\ell}\mathrm{d}(\underline{a}) \qquad [\text{for the random computation}] \qquad \log\ell + \frac{1}{\ell}(\mathrm{d}(\underline{a}) + \mathrm{d}(\underline{x})).$$

With the sum-size, the number ℓ of entries plays a more important role, and there are two cases, according to the position of the size n with respect to ℓ^2. In the case $n \leq \ell^2$ (there are many entries with a small size), then we choose $\mathrm{d}(\underline{x}) = \ell\log\ell$, and the extra-cost for the random computation is $O(\log\ell)$. In the other case (there are few entries with a large size), we choose $\mathrm{d}(\underline{x}) = \ell\log(\mathrm{d}(\underline{a})/\ell)$ and the extra-cost is of order $\log(\mathrm{d}(\underline{a})/\ell)$, and it is negligible with respect to the initial cost. Then, with the sum-size, there is a need of a deeper discussion for comparing the deterministic algorithm to the random strategy.

[9] As previously, the notation $\underline{x}$ stands for a vector having ℓ components.

When the number of entries and their size are related. The previous discussion is based on the relative position of the number ℓ of entries and their total size n. Our study is performed when ℓ is fixed. What happens when ℓ and n are related?

Towards the analysis of other gcd algorithms. The Euclid algorithm (more exactly its extension as the continued fraction algorithm) admits many generalizations to higher dimensions, for which there exists an underlying dynamical system. These dynamical systems have been widely studied for their ergodic properties, for instance by Schweiger (2000). After a precise study of their transfer operator, we plan to apply the methods developed here in this multidimensional setting and perform a dynamical analysis of such algorithms, notably the Brun and the Jacobi-Perron algorithms.

Acknowledgements

Section 9 is mainly based on the (unpublished) work that Mathieu Roux has done in the last part of his PhD thesis (see Roux (2011)). We wish to thank him for the inclusion of an adapted version of his proof in our paper and for many valuable discussions. We would like to thank warmly the referees for their careful reading and their valuable suggestions.

References

Akhavi, A., Marckert, J.-F., Rouault, A., 2009. On the reduction of a random basis. ESAIM Probab. Stat. 13, 437–458.
URL `http://dx.doi.org/10.1051/ps:2008012`

Baladi, V., Vallée, B., 2005. Euclidean algorithms are Gaussian. Journal of Number Theory 110, 331–386.

Berthé, V., Creusefond, J., Lhote, L., Vallée, B., 2013. Multiple gcds. probabilistic analysis of the plain algorithm. In: International Symposium on Symbolic and Algebraic Computation, ISSAC'13. ACM, pp. 37–44.

Berthé, V., Nakada, H., 2000. On continued fraction expansions in positive characteristic: Equivalence relations and some metric properties. Expositiones Mathematicae 18, 257–284.

Brent, R. P., 1976. Analysis of the binary Euclidean algorithm. In: Algorithms and complexity (Proc. Sympos., Carnegie-Mellon Univ., Pittsburgh, Pa., 1976). Academic Press, New York, pp. 321–355.

Dixon, J. D., 1970. The number of steps in the Euclidean algorithm. Journal of Number Theory 2, 414–422.

Edwards, H., 2001. Riemann's Zeta Function. Dover Publications.

Flajolet, P., Sedgewick, R., 2009. Analytic Combinatorics. Cambridge University Press.

Flajolet, P., Vallée, B., 1998. Continued fraction algorithms, functional operators, and structure constants. Theor. Comput. Sci. 194 (1-2), 1–34.

Friesen, C., Hensley, D., 1996. The statistics of continued fractions for polynomials over a finite field. Proc. Amer. Math. Soc 124, 2661–2673.

von zur Gathen, J., Gerhard, J., 2003. Modern Computer Algebra. Cambridge University Press.

von zur Gathen, J., Shparlinski, I. E., 2006. GCD of random linear combinations. Algorithmica 46 (1), 137–148.
URL http://dx.doi.org/10.1007/s00453-006-0072-1

Heilbronn, H., 1969. On the average length of a class of continued fractions. In: Turan, P. (Ed.), Number Theory and Analysis. pp. 87–96.

Hensley, D., 1994. The number of steps in the Euclidean algorithm. Journal of Number Theory 2 (49), 149–182.

Knopfmacher, A., Knopfmacher, J., 1988. The exact length of the Euclidean algorithm in $F_q[X]$. Mathematika 35, 297–304.

Knuth, D. E., 1998. Seminumerical Algorithms, 3rd Edition. Vol. 2 of The Art of Computer Programming. Addison-Wesley.

Landau, E., 1924. Über die Anzahl der Gitterpunkte in gewissen Bereichen. IV. Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. 1924, 137–150.

Lhote, L., Vallée, B., 2008. Gaussian laws for the main parameters of the Euclid algorithms. Algorithmica 50 (4), 497–554.

Ma, K., von zur Gathen, J., 1990. Analysis of Euclidean algorithms for polynomials over finite fields. Journal of Symbolic Computation 9 (4), 429 – 455.
URL http://www.sciencedirect.com/science/article/pii/S0747717108800211

Mayer, D. H., 1990. On the thermodynamic formalism for the Gauss map. Comm. Math. Phys. 130 (2), 311–333.
URL http://projecteuclid.org/euclid.cmp/1104200514

Roux, M., 2011. Théorie de l'information, séries de Dirichlet, et analyse d'algorithmes. Ph.D. thesis, Université de Caen.

Ruelle, D., 2004. Thermodynamic Formalism. Cambridge University Press.

Schönhage, A., 1971. Schnelle Berechnung von Kettenbruchentwicklungen. Acta Inf. 1, 139–144.

Schweiger, F., 2000. Multidimensional continued fractions. Oxford Science Publications. Oxford University Press, Oxford.

Stehlé, D., Zimmermann, P., 2004. A binary recursive gcd algorithm. In: Algorithmic number theory. Vol. 3076 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 411–425.
URL http://dx.doi.org/10.1007/978-3-540-24847-7_31

Tenenbaum, G., 1990. Introduction à la théorie analytique des nombres. Vol. 13. Institut Élie Cartan, Nancy, France.

Vallée, B., 2006. Euclidean dynamics. Discrete and Continuous Dynamical Systems 1 (15), 281–352.