An Analytic Approach to Smooth Polynomials over Finite Fields

Daniel Panario[1], Xavier Gourdon[2], and Philippe Flajolet[2]

[1] Department of Computer Science, University of Toronto,
M5S 3G4, Toronto, Canada
E-mail: daniel@cs.toronto.edu
[2] Algorithms Project, INRIA Rocquencourt,
F-78153 Le Chesnay, France
E-mail: Philippe.Flajolet@inria.fr, Xavier.Gourdon@inria.fr

Abstract. We consider the largest degrees that occur in the decomposition of polynomials over finite fields into irreducible factors. We expand the range of applicability of the Dickman function as an approximation for the number of smooth polynomials, which provides precise estimates for the discrete logarithm problem. In addition, we characterize the distribution of the two largest degrees of irreducible factors, a problem relevant to polynomial factorization. As opposed to most earlier treatments, our methods are based on a combination of exact descriptions by generating functions and a specific complex asymptotic method.

1 Introduction

The security of many applications in public-key cryptography relies on the computational intractability of finding discrete logarithms in finite fields. Examples are the Diffie-Hellman key exchange scheme [7], El Gamal's cryptosystem [8], and pseudorandom bit generators [3, 10]. On the other hand, algorithms for computing discrete logarithms in finite fields depend on finding polynomials with all of their irreducible factors with degree not greater than certain bound m — such polynomials that are the analogue of highly composite numbers are called *smooth* polynomials. Thus quantitative characterizations of smoothness in random polynomials over finite field are of relevance to cryptographic attacks; see [14–16].

In different contexts, like computer algebra and error-correcting codes, knowledge of the distribution of the largest irreducible factor of a random polynomial over a finite field permits us a fine tuning of the stopping conditions in polynomial factorization algorithms.

In this paper, we give a unified treatment of the asymptotic enumeration of smooth polynomials over finite fields and quantify precisely the distribution of largest irreducible factors. The results are expressed in terms of a familiar number-theoretic function, the Dickman function, that is already known to underlie the study of numbers with no primes larger than m; see [5, 6]. Our approach starts with an exact representation of enumeration problems by means

of combinatorial generating functions. From there, we develop dedicated contour integration methods that are in the spirit of analytic number theory but have quite a different technical flavour since power series are used instead of Dirichlet series. Such an approach is of general applicability and Gourdon [11] introduced it in order to study the size of the largest cycle in random permutations (where nonconstructive Tauberian methods had been previously used), as well as largest components in several decomposable combinatorial structures, like random mappings.

The results on smooth polynomials are presented in Section 2. The number of m-smooth polynomials of degree n over $\mathbb{F}_q$ has already been considered in the literature. Odlyzko [15] provides an asymptotic estimate when $n \to \infty$ for the case $q = 2$ and $n^{1/100} \leq m \leq n^{99/100}$ using the saddle point method. This generalizes to any prime power q; see [13]. Car [4] has given an asymptotic expression for this number in terms of the Dickman function, but Car's estimates only hold for m large with respect to n, typically $m > cn \log\log n / \log n$. Finally, Soundararajan [17] completes the full range $1 \leq m \leq n$ by giving more precise boundaries. He uses the saddle point method for, $\log n / \log\log n \leq m \leq 3n \log\log n / \log n$ while the cases of very small and very large m with respect to n are covered through the use of recurrences As a consequence of a large intermediate range and due to the intricate saddle point expressions, some of the quantitative estimates obtained earlier fail to be transparent. In addition, Soundararajan shows that the Dickman function approaches the number of smooth polynomials when $m \geq \sqrt{n} \log n$. We extend this range to $m \geq (1+\varepsilon)(\log n)^{1/k}$, for a positive integer constant k.

The methods we introduce here follow a clear thread that enables us to expand the range where the Dickman function approximates the number of smooth polynomials. For instance, it can be applied to the enumeration of "semismooth" polynomials over finite fields that are defined by constraints on the degrees of *several* of their largest irreducible factors. (These are the equivalent for polynomials of the semismooth integers defined by Bach and Peralta [2].) We illustrate this fact by treating in some detail the joint distribution of the largest two irreducible factors, a problem that is again of relevance for polynomial factorization algorithms.

Throughout this paper, we take a field $\mathbb{F}_q$ of fixed cardinality q; it seems possible to obtain similar results uniformly on q. Asymptotic estimates are expressed as functions of the degree n of the polynomials considered.

2 Smooth polynomials

The Dickman function plays a central rôle in our results on smooth polynomials. This classical number-theoretic function describes the distribution of the largest prime divisor of a random integer [5, 6]. A survey on this topic is due to Hildebrand and Tenenbaum [12]. Our general reference for this paper is Tenenbaum's book [18].

Definition 1. The *Dickman function*, $\rho(u)$, is the unique continuous solution of the difference-differential equation

$$\begin{aligned} \rho(u) &= 1 && 0 \le u \le 1, \\ u\rho'(u) &= -\rho(u-1) && u > 1. \end{aligned}$$

In order to prove our main result we need the following lemma that deals with the crucial technicality of approximating the required generating functions. An essential rôle is played by the exponential integral function E that is defined as

$$E(a) = \int_a^{+\infty} \frac{e^{-s}}{s}\, ds.$$

Lemma 1. *The remainders of the logarithm series,*

$$r_m(z) = \sum_{k>m} \frac{z^k}{k},$$

are approximable in terms of the exponential integral as

$$r_m(e^{-h}) = E(mh) + O\left(\frac{1}{m}\right),$$

where the big-Oh error term is uniform with respect to h, for $\Re(h) > 0$ and $|\Im(h)| \le \pi$.

PROOF. When $\Re(h) > 0$, we have

$$r_m(e^{-h}) = \int_h^{+\infty} \left(\sum_{k>m} e^{-ku} \right) du = \int_h^{+\infty} \frac{e^{-(m+1)u}}{1-e^{-u}}\, du = \int_{mh}^{+\infty} e^{-s} \frac{1/m}{e^{s/m}-1}\, ds.$$

This can be written in terms of the function $\psi(z) = \frac{1}{e^z-1} - \frac{1}{z}$ and the exponential integral as

$$r_m(e^{-h}) = E(mh) + R_m(mh), \qquad R_m(u) = \frac{1}{m} \int_u^{+\infty} e^{-s} \psi\left(\frac{s}{m}\right) ds, \qquad (1)$$

where we only need to observe that

$$\frac{1}{m(e^{s/m}-1)} = \frac{1}{m}\left(\psi\left(\frac{s}{m}\right) + \frac{1}{s/m}\right) = \frac{1}{m}\psi\left(\frac{s}{m}\right) + \frac{1}{s}.$$

Finally, the analyticity of $\psi(z)$ in $|z| < 2\pi$ implies that $R_m(u) = O(1/m)$ uniformly for $\Re(u) \ge 0$ and $|\Im(u)| \le m\pi$. □

Theorem 1. *The number of m-smooth polynomials of degree n over $\mathbb{F}_q$ satisfies*

$$N_q(n,m) = q^n \rho\left(\frac{n}{m}\right)\left(1 + O\left(\frac{\log n}{m}\right)\right),$$

where ρ is the Dickman function.

PROOF. Let $\mathcal{I}$ be the collection of all monic irreducible polynomials in $\mathbb{F}_q$, and $|\omega|$ the degree of $\omega \in \mathcal{I}$. The collection of monic polynomials with all irreducible factors with degree smaller than or equal to m can be symbolically written as

$$S_m = \prod_{\omega \in \mathcal{I},\ |\omega| \le m} (1 + \omega + \omega^2 + \cdots) = \prod_{\omega \in \mathcal{I},\ |\omega| \le m} (1 - \omega)^{-1}.$$

Let z be a formal variable. The substitution $\omega \mapsto z^{|\omega|}$ gives rise to the generating function $S_m(z)$ of m-smooth polynomials

$$S_m(z) = \prod_{\omega \in \mathcal{I},\ |\omega| \le m} \left(1 - z^{|\omega|}\right)^{-1} = \prod_{k=1}^{m} \left(\frac{1}{1 - z^k}\right)^{I_k}.$$

In this context, the generating function of polynomials over $\mathbb{F}_q$ is

$$P(z) = \prod_{k=1}^{\infty} \left(\frac{1}{1 - z^k}\right)^{I_k} = \frac{1}{1 - qz}.$$

The number of m-smooth polynomial of degree n over $\mathbb{F}_q$ is given by Cauchy's coefficient formula

$$N_q(n, m) = [z^n] S_m(z) = \frac{1}{2\pi i} \int_{\mathcal{C}} S_m(z) \frac{dz}{z^{n+1}},$$

where the contour $\mathcal{C}$ is chosen to be $z = e^{-1/n + i\theta}$, $-\pi \le \theta \le \pi$. The change of variable $z = e^{-h/n}$ within the integral provides $z^n = e^{-1 + in\theta}$. Thus, $h = 1 - in\theta$, and the limits of integration are $(1 + ni\pi, 1 - ni\pi)$. Therefore,

$$N_q(n, m) = \frac{1}{2\pi i} \int_{1+ni\pi}^{1-ni\pi} S_m(e^{-h/n}) \left(-\frac{1}{n}\right) \frac{dh}{e^{-h}}. \tag{2}$$

An equivalent expression for $S_m(z)$ that makes explicit the singularity at $z = 1/q$ can be obtained by taking the logarithm and inverting summations. Indeed, considering $r_m^{[j]}(z) = \sum_{k>m} I_k z^{kj}$, we have

$$S_m(z) = P(z) \prod_{k>m} (1 - z^k)^{I_k} = \frac{1}{1 - qz} \exp\left(-r_m^{[1]}(z) - \frac{r_m^{[2]}(z)}{2} - \frac{r_m^{[3]}(z)}{3} \cdots\right).$$

The last equality holds since

$$\begin{aligned}
\prod_{k>m} (1 - z^k)^{I_k} &= \exp\left(\sum_{k>m} I_k \log\left(1 - z^k\right)\right) \\
&= \exp\left(-\sum_{k>m} I_k \left(z^k + \frac{z^{2k}}{2} + \frac{z^{3k}}{3} + \cdots\right)\right) \\
&= \exp\left(-\sum_{j=1}^{\infty} \frac{1}{j} \left(\sum_{k>m} I_k z^{kj}\right)\right) \\
&= \exp\left(-r_m^{[1]}(z) - \frac{r_m^{[2]}(z)}{2} - \frac{r_m^{[3]}(z)}{3} \cdots\right).
\end{aligned}$$

Now, the estimate $kI_k = q^k + O(q^{k/2})$ gives

$$r_m^{[1]}\left(\frac{z}{q}\right) = \sum_{k>m} \frac{z^k}{k} + O(q^{-m/2}) \qquad \text{for } |z| < \frac{1}{q},$$

and,

$$\sup_{|z|\le 1/q} r_m^{[j]}\left(\frac{z}{q}\right) = O\left(\frac{1}{q^{m(j-1)}}\right) \qquad \text{for } j \ge 2.$$

The estimate of the remainders r_m of the logarithm given in Lemma 1 applied to $S_m(z)$ entails

$$S_m\left(\frac{e^{-h}}{q}\right) = \frac{e^{-E(mh)+O(1/m)}}{1-e^{-h}}, \tag{3}$$

where we may disregard the error term in the exponent since it is of smaller order than the one in the statement of the theorem.

Substituting this estimate in (2) yields, for $\mu = \frac{m}{n}$,

$$N_q(n,m) = q^n \frac{1}{2\pi i} \int_{1-ni\pi}^{1+ni\pi} \frac{e^{-E(\mu h)+O(1/m)}}{n(1-e^{-h/n})} e^h \, dh.$$

Set $\psi(z) = \frac{1}{1-e^{-z}} - \frac{1}{z}$, that is an analytic function in $|z| < 2\pi$. We can express the above number in terms of ψ as follows. First,

$$\frac{1}{n(1-e^{-h/n})} = \frac{1}{n}\left(\psi\left(\frac{h}{n}\right) + \frac{1}{h/n}\right) = \frac{1}{n}\psi\left(\frac{h}{n}\right) + \frac{1}{h}.$$

Second,

$$\frac{e^{O(1/m)}}{n(1-e^{-h/n})} = \frac{1}{h} + \frac{1}{n}\psi\left(\frac{h}{n}\right) + O\left(\frac{1}{hm}\right).$$

Thus,

$$N_q(n,m) = q^n \frac{1}{2\pi i} \int_{1-in\pi}^{1+in\pi} e^{-E(\mu h)} \left(\frac{1}{h} + \frac{1}{n}\psi\left(\frac{h}{n}\right) + O\left(\frac{1}{hm}\right)\right) e^h \, dh.$$

We treat separatedly the three integrals. The fact that $e^{-E(z)}$ is bounded in the domain $\Re(z) \ge 0$ (see [1], § 5.1) entails that the contribution of the big-Oh term in the integral is $O(\log n/m)$. Then, an integration by parts gives also a small contribution of order $O(\log n/n)$ for the term containing $\psi(h/n)$. Finally, we have

$$N_q(n,m) = q^n \left(\frac{1}{2\pi i} \int_{1-in\pi}^{1+in\pi} \frac{e^{-E(\mu h)}}{h} e^h \, dh + O\left(\frac{\log n}{m}\right)\right).$$

We write

$$\frac{1}{2\pi i} \int_{1-in\pi}^{1+in\pi} \frac{e^{-E(\mu h)}}{h} e^h \, dh = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h)}}{h} e^h \, dh - \int_{\mathcal{L}} \frac{e^{-E(\mu h)}}{h} e^h \, dh,$$

where the integration domain $\mathcal{L}$ is the union of the two semi-vertical lines defined by $\Re(h) = 1$, $|\Im(h)| \geq n\pi$. The last integral is $O(1/n)$ as can be checked by partial integration. Therefore,

$$N_q(n,m) = q^n \left(\frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h)}}{h} e^h \, dh + O\left(\frac{\log n}{m}\right)\right). \tag{4}$$

To conclude the proof, it remains to show that the above integral is $\rho(n/m)$. The Laplace transform $\widehat{\rho}(s)$ of the Dickman function satisfies (see [18], §5.4, p. 373) $s\,\widehat{\rho}(s) = e^{-E(s)}$. Thus,

$$\rho(u) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \left(\frac{e^{-E(v)}}{v}\right) e^{uv} \, dv. \tag{5}$$

We now relate Equations (4) and (5). The change of variable $\mu h = v$ in (4) implies

$$\begin{aligned} \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h)}}{h} e^h \, dh &= \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \left(\frac{e^{-E(v)}}{v/\mu}\right) e^{v/\mu} \frac{dv}{\mu} \\ &= \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \left(\frac{e^{-E(v)}}{v}\right) e^{vn/m} \, dv = \rho\left(\frac{n}{m}\right). \end{aligned}$$

The theorem follows since $\rho(u) \leq 1/\Gamma(u+1)$ for all $u \geq 0$ ([18], §5.3, p. 366). □

The previous theorem shows that when $m/\log n \to \infty$, the number of smooth polynomials is given asymptotically by the Dickman function. In the sequel, we extend the range of applicability of Theorem 1 to sublogarithmic values of m with respect to n.

Note that we can restrict our attention to $m < n$ since the case $m = n$ corresponds to the well-known enumeration of irreducible polynomials.

Theorem 2. *Let $m < n$, and k a positive integer such that $km < n$ and $m^k/\log n \to \infty$. Then, the number of m-smooth polynomials of degree n over $\mathbb{F}_q$ satisfies*

$$N_q(n,m) = q^n \, \rho\left(\frac{n}{m}\right)\left(1 + O\left(\frac{\log n}{m^k}\right)\right),$$

where ρ is the Dickman function.

PROOF. We use the same notation of Theorem 1, and only show the case $k = 2$.

Using (1) as the estimate of the remainders of the logarithm, Equation (3) can be written as

$$S_m\left(\frac{e^{-h/n}}{q}\right) = \frac{e^{-E(\mu h) - R_m(\mu h)}}{1 - e^{-h}}. \tag{6}$$

Integrating $R_m(\mu h)$ by parts yields

$$R_m(\mu h) = \frac{1}{m} \int_{\mu h}^{+\infty} e^{-s} \psi\left(\frac{s}{m}\right) ds$$

$$= \frac{1}{m}\left(-\psi\left(\frac{s}{m}\right)e^{-s}\Big|_{\mu h}^{\infty} + \frac{1}{m}\int_{\mu h}^{+\infty}\psi'\left(\frac{s}{m}\right)e^{-s}\,ds\right)$$
$$= \frac{1}{m}e^{-\mu h}\psi\left(\frac{h}{n}\right) + \frac{1}{m^2}e^{-\mu h}\psi'\left(\frac{h}{n}\right) + O\left(e^{-\mu h}/m^3\right).$$

Thus,

$$R_m^2(\mu h) = \frac{1}{m^2}e^{-2\mu h}\psi^2\left(\frac{h}{n}\right) + O\left(e^{-2\mu h}/m^3\right).$$

Expanding $e^{-R_m(\mu h)}$ in (6), we have

$$\frac{e^{-R_m(\mu h)}}{n(1-e^{-h/n})} = \frac{1}{h} + \frac{1}{n}\psi\left(\frac{h}{n}\right) - \frac{1}{h}\frac{e^{-\mu h}}{m}\psi\left(\frac{h}{n}\right) - \frac{1}{n}\frac{e^{-\mu h}}{m}\psi^2\left(\frac{h}{n}\right) + O\left(\frac{1}{hm^2}\right).$$

Arguments similar to the ones employed in the previous theorem lead to the conclusion that

$$N_q(n,m) = q^n\,\rho\left(\frac{n}{m}\right)\left(1 + O\left(\frac{\log n}{m^2}\right)\right).$$

(In order to improve on the error estimate, it would suffice to consider successive terms in the expansion of $e^{-R_m(\mu h)}$.) □

3 Distribution of largest degrees of factors

The distribution of the largest degree among the irreducible factors of a random polynomial over $\mathbb{F}_q$ underlies many problems dealing with polynomials over finite fields. An instance is in the factorization problem. The joint distribution of the two largest degrees $D_n^{[1]}$, $D_n^{[2]}$ of the distinct factors of a random polynomial of degree n in $\mathbb{F}_q$ provides the halting condition for the distinct-degree factorization stage; see [9].

We first investigate the distribution of the largest degree $D_n^{[1]}$ which is of independent interest. The same analysis techniques are then applied in order to produce the joint distribution of $D_n^{[1]}$, $D_n^{[2]}$.

3.1 Largest degree of factors

The following theorem gives a local distribution for the largest degree $D_n^{[1]}$ of a random polynomial of degree n. We only sketch the proof since it is similar to that of Theorem 1.

Theorem 3. *The largest degree $D_n^{[1]}$ among the irreducible factors of a random polynomial of degree n over $\mathbb{F}_q$ satisfies*

$$\Pr(D_n^{[1]} = m) = \frac{1}{m}f\left(\frac{m}{n}\right) + O\left(\frac{\log n}{m^2}\right),$$

where $f(\mu) = \rho(1/\mu - 1)$ is a variant of the Dickman function; alternatively

$$f(\mu) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h)}}{h} e^{(1-\mu)h}\, dh. \tag{7}$$

PROOF. The generating function of the class of m-smooth polynomials is

$$S_m(z) = \prod_{k=1}^{m} \left(\frac{1}{1-z^k}\right)^{I_k}.$$

Thus, the generating function of polynomials for which $D_n^{[1]} = m$ is

$$L_m(z) = S_m(z) - S_{m-1}(z) = S_m(z)\left(1 - (1-z^m)^{I_m}\right). \tag{8}$$

The probability we are interested in is then given by the Cauchy formula

$$\Pr(D_n^{[1]} = m) = \frac{[z^n]L_m(z)}{q^n} = \frac{1}{2\pi i} \int_{\mathcal{C}} L_m\left(\frac{z}{q}\right) \frac{dz}{z^{n+1}},$$

where the contour $\mathcal{C}$ is chosen to be $z = e^{-1/n+i\theta}$, $-\pi \le \theta \le \pi$. As in Theorem 1, the change of variable $z = e^{-h/n}$ within the integral gives

$$\Pr(D_n^{[1]} = m) = \frac{1}{2\pi i} \int_{1-ni\pi}^{1+ni\pi} L_m\left(\frac{e^{-h/n}}{q}\right) \frac{e^h}{n} dh.$$

Using the estimate in (3) for $S_m(z)$ and (8), we obtain

$$L_m\left(\frac{e^{-h}}{q}\right) = \frac{e^{-E(mh)+O(1/m)}}{1-e^{-h}} \frac{e^{-mh}}{m}. \tag{9}$$

The estimate of L_m in (9) yields, for $\mu = \frac{m}{n}$,

$$\Pr(D_n^{[1]} = m) = \frac{1}{m} \frac{1}{2\pi i} \int_{1-ni\pi}^{1+ni\pi} \frac{e^{-E(\mu h)+O(1/m)}}{n(1-e^{-h/n})} e^{(1-\mu)h}\, dh.$$

A similar argument to the one employed in Theorem 1 completes the proof. □

3.2 Joint distribution of the two largest degrees of factors

The method used to prove the previous theorem generalizes to the joint distribution of the two largest degrees $D_n^{[1]}$, $D_n^{[2]}$ of *distinct* irreducible factors of a random polynomial of degree n in $\mathbb{F}_q[x]$. In the context of the general factorization algorithm, this study appears naturally when analyzing the early-abort stopping rule during the distinct-degree factorization stage; see [9].

The joint distribution of the largest two irreducible factors is also related to *semismooth polynomials*. Bach and Peralta [2] define and study the asymptotics of *semismooth integers*. An integer n is semismooth with respect to y and z

if $n_1 \leq y$ and $n_2 \leq z$ for n_i the ith largest prime factor of n. Analogously, a polynomial f of degree n over $\mathbb{F}_q$ is a semismooth polynomial with respect to m_1 and m_2, $m_1 \geq m_2$, if $D_n^{[1]} \leq m_1$ and $D_n^{[2]} \leq m_2$.

The next theorem provides the asymptotics for the joint distribution of the two largest degrees among the distinct irreducible factors of a random polynomial over $\mathbb{F}_q$. (A similar result holds for the case when repetitions of factors are allowed.)

Theorem 4. *The two largest degrees $D_n^{[1]}$ and $D_n^{[2]}$ of the distinct factors of a random polynomial of degree n in $\mathbb{F}_q$ satisfy*

(i) for $0 \leq m \leq n$,

$$\Pr(D_n^{[1]} = m, D_n^{[2]} \leq m/2) = \frac{1}{m} g_1\left(\frac{m}{n}\right) + O\left(\frac{\log n}{m^2}\right),$$

where $g_1(\mu)$ is expressed in terms of the exponential integral E as

$$g_1(\mu) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu h/2)}}{h} e^{(1-\mu)h}\, dh;$$

(ii) for $0 \leq m_2 < m_1 \leq n$,

$$\Pr(D_n^{[1]} = m_1, D_n^{[2]} = m_2) = \frac{1}{m_1 m_2} g_2\left(\frac{m_1}{n}, \frac{m_2}{n}\right) + O\left(\frac{\log n}{m_1 m_2^2}\right),$$

where $g_2(\mu_1, \mu_2)$ is

$$g_2(\mu_1, \mu_2) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{e^{-E(\mu_2 h)}}{h} e^{(1-\mu_1-\mu_2)h}\, dh.$$

PROOF. We only sketch the proof. With the same notations as in the proof of the previous theorem, the generating function of polynomials for which $D_n^{[1]} = m$ and $D_n^{[2]} \leq m/2$ is

$$\widetilde{L}_m(z) = S_{\lfloor m/2 \rfloor}(z) \frac{I_m z^m}{1 - z^m}. \tag{10}$$

The generating function of polynomials with $D_1^{[n]} = m_1$ and $D_2^{[n]} = m_2$, $m_2 < m_1$ is

$$\widetilde{L}_{m_1,m_2}(z) = L_{m_2}(z) \frac{I_{m_1} z^{m_1}}{1 - z^{m_1}}. \tag{11}$$

The behavior of the nth coefficient of the generating functions in (10) and (11) is then extracted like in Theorem 3. We briefly demonstrate the process for the generating function of (11).

The estimate in (9) for $L_{m_2}(z)$ and (11) entails

$$\widetilde{L}_{m_1,m_2}\left(\frac{e^{-h}}{q}\right) = \frac{e^{-E(m_2 h)+O(1/m_2)}}{1 - e^{-h}} \frac{e^{-m_2 h}}{m_2} \frac{e^{-m_1 h}}{m_1}.$$

Plugging this estimate in the Cauchy integral yields, for $\mu_1 = \frac{m_1}{n}, \mu_2 = \frac{m_2}{n}$,

$$m_1 m_2 \Pr(D_n^{[1]} = m_1, D_n^{[2]} = m_2) = \frac{1}{2\pi i} \int_{1-ni\pi}^{1+ni\pi} \frac{e^{-E(\mu_2 h)+O(1/m_2)}}{n(1-e^{-h/n})} e^{(1-\mu_1-\mu_2)h}\, dh.$$

An argument once more similar to the one in Theorem 1 completes the proof. □

We note that it is possible to generalize the above theorem to the joint distribution of the jth largest distinct irreducible factors.

Acknowledgements. This work was supported in part by the Long Term Research Project *Alcom-IT* (# 20244) of the European Union.

References

1. Abramowitz, M., and Stegun, I. *Handbook of mathematical functions.* Dover, New York, 1970.
2. Bach, E., and Peralta, R. Asymptotic semismoothness probabilities. *Math. Comp. 65* (1996), 1701–1715.
3. Blum, M., and Micali, S. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput. 13* (1984), 850–864.
4. Car, M. Théorèmes de densité dans $\mathbb{F}_q[x]$. *Acta Arith. 48* (1987), 145–165.
5. de Bruijn, N. On the number of positive integers $\leq x$ and free of prime factors $> y$. *Indag. Math. 13* (1951), 2–12.
6. Dickman, K. On the frequency of numbers containing prime factors of a certain relative magnitude. *Ark. Mat. Astr.Fys. 22* (1930), 1–14.
7. Diffie, W., and Hellman, M. New directions in cryptography. *IEEE Trans. Inform. Theory 22* (1976), 644–654.
8. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Info. Theory 31* (1985), 469–472.
9. Flajolet, P., Gourdon, X., and Panario, D. The complete analysis of a polynomial factorization algorithm over finite fields. Submitted March 1998. [Extended abstract in *Proc. 23rd ICALP Symp.*, Lecture Notes in Computer Science, vol. 1099, p. 232–243, 1996.] Full version in technical report 3370, INRIA, March 1998.
10. Gao, S., von zur Gathen, J., and Panario, D. Gauss periods: orders and cryptographical applications. *Math. Comp. 67* (1998), 343–352.
11. Gourdon, X. *Combinatoire, algorithmique et géométrie des polynômes.* Thèse, École Polytechnique, 1996.
12. Hildebrand, A., and Tenenbaum, G. Integers without large prime factors. *J. Théorie des Nombres de Bordeaux 5* (1993), 411–484.
13. Lovorn, R. *Rigourous, subexponential algorithms for discrete logarithm algorithms in* $\mathbb{F}_{p^2}$. PhD thesis, University of Georgia, 1992.
14. Lovorn Bender, R., and Pomerance, C. Rigourous discrete logarithm computations in finite fields via smooth polynomials. In *Computational Perspectives on Number Theory Proc. of a Conference in Honor of A.O.L. Atkin* (Providence, 1998), vol. 7 of *AMS/International Press Studies in Advanced Mathematics.*

15. ODLYZKO, A. Discrete logarithms and their cryptographic significance. In *Advances in Cryptology, Proceedings of Eurocrypt 1984* (1985), vol. 209 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 224–314.
16. ODLYZKO, A. Discrete logarithms and smooth polynomials. In *Finite fields: theory, applications and algorithms*, G. Mullen and P. J.-S. Shiue, Eds. Contemporary Mathematics 168, Amer. Math. Soc., 1994, pp. 269–278.
17. SOUNDARARAJAN, K. Asymptotic formulae for the counting function of smooth polynomials. To appear in J. London Math. Soc.
18. TENENBAUM, G. *Introduction to analytic and probabilistic number theory.* Cambridge University Press, 1995.