DISCRETE ANALYSIS, 20XX:XX, 32 pp.
www.discreteanalysisjournal.com

Uniform Estimates for Friable Polynomials over Finite Fields

Ofir Gorodetsky*

Received XX Month 20XX; *Revised* XX Month 20XX; *Published* XX Month 20XX

Abstract: We establish new estimates for the number of m-friable polynomials of degree n over a finite field $\mathbb{F}_q$, where the main term involves the number of m-friable permutations on n elements. The range of m in our results is $n \geq m \geq (1+\varepsilon)\log_q n$ and is optimal as these numbers are not comparable for smaller m. For $m \geq 4\log_q n$ the error term in our estimates decays faster than in all previous works.

Our estimates imply that the probability that a random polynomial f_n is m-friable is asymptotic to the probability that a random permutation π_n is m-friable, uniformly for $m \geq (2+\varepsilon)\log_q n$ as $q^n \to \infty$. This should be viewed as an unconditional analogue of a result of Hildebrand (1984), saying that under the Riemann Hypothesis, the probability that a positive integer $\leq x$ is y-friable is of the order of magnitude of the Dickman ρ function at $\log x/\log y$, uniformly for $\log y \geq (2+\varepsilon)\log\log x$. As opposed to Hildebrand's result, we actually obtain an asymptotic result.

As an application of our estimates, we determine the rate of decay in the asymptotic formula for the expected degree of the largest prime factor of a random polynomial. This improves a previous estimate of Knopfmacher and Manstavičius (1997).

Key words and phrases: smooth polynomials, friable polynomials, Dickman function, smooth permutations, friable permutations, largest prime factor, saddle point analysis

1 Introduction

Given a positive integer n, we let π_n be a permutation chosen uniformly at random from S_n. Given a prime power q, we let $f_n = f_{n,q} \in \mathbb{F}_q[T]$ be a polynomial chosen uniformly at random from $\mathcal{M}_{n,q} \subseteq \mathbb{F}_q[T]$, the set of monic polynomials of degree n over the finite field $\mathbb{F}_q$.

*Supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreements Nos. 786758 and 851318)

 DOI: 10.19086/daXXX

We say that a permutation is m-friable (or -smooth) if all its cycles are of length at most m. Similarly, we say that a polynomial is m-friable if all its prime factors are of degree at most m. We define

$$\psi_\pi(n,m) := \#\{\pi \in S_n : \pi \text{ is } m\text{-friable}\}, \qquad \psi_q(n,m) := \#\{f \in \mathcal{M}_{n,q} : f \text{ is } m\text{-friable}\},$$

so that $\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \psi_\pi(n,m)/n!$ and $\mathbb{P}(f_n \text{ is } m\text{-friable}) = \psi_q(n,m)/q^n$.

Throughout the paper, $n \geq 2$, $1 \leq m \leq n$ and

$$u := \frac{n}{m}.$$

Friability (or smoothness) probabilities in S_n were studied extensively in the literature, dating back to Goncharov [Gon44], who studied $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ in the bounded u regime; see [SL66, ABT03] for generalizations. The bounded m regime received significant attention as well, see [CHM51, MW55, WZ85, Wil06, Sac07, Tim08, AM15]. Asymptotic results covering the entire range of m were established by Manstavičius and Petuchovas [MP16]. See also the recent work of Ford [For22].

Friability probabilities in $\mathcal{M}_{n,q}$ were studied extensively in the literature as well, starting with the work of Odlyzko [Odl85], which was motivated by cryptography. Several cryptographic system are based on the difficulty of computing discrete logarithms in finite fields. Index-Calculus algorithms, invented in the late seventies, compute discrete algorithms in subexponential time. The complexity analysis of their running time, as well as the choice of parameters within the algorithm, are highly non-trivial. When the finite field is an extension of $\mathbb{F}_q$, the analysis requires the asymptotics of $\psi_q(n,m)$ in the range $n^\varepsilon \leq m \leq n^{1-\varepsilon}$. This is addressed, for $q = 2$, in [Odl85, App. 1]. Subsequent works on ψ_q include [War91, Lov92, Man92a, Man92b, PGF98, BP98, Sou, ABT03, JL06, Ha14] and are expanded upon later.

Here we estimate friability probabilities in $\mathcal{M}_{n,q}$ by comparing them to the corresponding probabilities in S_n, uniformly in the parameters n and q. Unless stated otherwise, constants, both implicit and explicit, are absolute. For recent results where new function field estimates are obtained by comparing to a permutation quantity, see [Gor17, EG22].

Theorem 1.1. *If $m \geq 6\log n$, then*

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = 1 + O\left(\frac{u\log(u+1)}{mq^{\lceil \frac{m+1}{2}\rceil}}\right). \tag{1.1}$$

The previous asymptotic results for $\mathbb{P}(f_n \text{ is } m\text{-friable})$ in this range of m achieved only the weaker error terms $u\log(u+1)/m$ (see (1.14) and (1.17)) or $1/u$ (see §1.3.2), but with perhaps simpler main terms. For smaller m, we prove

Theorem 1.2. *Fix $\varepsilon > 0$. If $8\log n \geq m \geq (2+\varepsilon)\log_q n$, then*

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = 1 + O_\varepsilon\left(\frac{un^{\frac{1+a}{m}}}{q^{\lceil \frac{m+1}{2}\rceil}}\right) \tag{1.2}$$

where $a = \mathbf{1}_{2|m}$.

Here and throughout, $\log_q$ is the base-q logarithm. Once $m \geq 4\log_q n$, the error term in (1.2) decays faster than $O(1/u)$, the existing error term in the asymptotic result for $\mathbb{P}(f_n \text{ is } m\text{-friable})$ in this range of m (see §1.3.2). In Theorem 1.3 below, the error term in both theorems is improved, at least if m is not too close to n, by modifying the main term 1 in the right-hand side of (1.2).

Theorems 1.1 and 1.2 cover the entire range $n \geq m \geq (2+\varepsilon)\log_q n$, and in particular show that

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) \sim \mathbb{P}(\pi_n \text{ is } m\text{-friable}) \tag{1.3}$$

holds as $q^n \to \infty$, uniformly in that range (a short computation shows that the relative error term in (1.3) is $\ll_\varepsilon 1/(nq)^{c_\varepsilon}$). When $n \to \infty$ and $m \leq (1-\varepsilon)\log_q n$, the probabilities are no longer of the same order of magnitude. Concretely, for n tending to ∞ and fixed q, we have

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = q^{-n+o_{q,\varepsilon}(n)}$$

for $m \sim (1-\varepsilon)\log_q n$ by [Sou, Thm. 1.4], while, in the same limit,

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = q^{-\frac{n}{1-\varepsilon}+o_{q,\varepsilon}(n)}$$

by Proposition 1.8. For $m = o(\log n)$ the situation is even worse: $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ decays superexponentially in n by Proposition 1.8, while $\mathbb{P}(f_n \text{ is } m\text{-friable}) \geq q^{-n}$ can never decay superexponentially.

We prove a comparative result where m can be as small as $(1+\varepsilon)\log_q n$. It requires the introduction of some notation. Define $x = x_{n,m} > 0$ by

$$\sum_{j=1}^{m} x^j = n. \tag{1.4}$$

Observe that $1 \leq x \leq n^{1/m}$. In fact, from Lemma 5.2 it follows that $x = \Theta(n^{1/m})$. Let

$$G_q(z) := \prod_{\substack{P\in\mathcal{P}\\ \deg(P)\leq m}} \left(1-\left(\frac{z}{q}\right)^{\deg(P)}\right)^{-1} \exp\left(-\sum_{i=1}^{m}\frac{z^i}{i}\right),$$

where $\mathcal{P} = \mathcal{P}_q$ is the set of monic irreducible polynomials over $\mathbb{F}_q$. By (5.3), $G_q(x) \geq 1$.

Theorem 1.3. *Fix $\varepsilon > 0$. If $(2+\varepsilon)\log_q n \geq m \geq (1+\varepsilon)\log_q n$, then*

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = G_q(x)\left(1+O_\varepsilon\left(m\left(\frac{1}{q^{m/2}}+\frac{n^3}{q^{2m}}\right)\right)\right) \tag{1.5}$$

where x is defined in (1.4). If $n/(\log n \log^3\log(n+1)) \geq m \geq (2+\varepsilon)\log_q n$, then $1 \leq G_q(x) \leq C_\varepsilon$ and

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = G_q(x) + O_\varepsilon\left(\frac{n^{\frac{1+a}{m}}\min\{m,\log u\}}{mq^{\lceil\frac{m+1}{2}\rceil}}\right) \tag{1.6}$$

where $a = \mathbf{1}_{2|m}$.

Estimate (1.5) gives an asymptotic result as $n \to \infty$ if $m \geq (3/2+\varepsilon)\log_q n \to \infty$, and in any case gives a non-trivial upper bound. We believe a different asymptotic result should hold for $m \leq (3/2-\varepsilon)\log_q n$.

Estimate (1.6) gives an asymptotic result as $q^n \to \infty$. Previous asymptotic results for the range of (1.6) achieved only the weaker error terms $u\log(u+1)/m$ (see (1.14) and (1.17)) or $1/u$ (see §1.3.2). We believe (1.6) should hold in the wider range $n \geq m \geq (2+\varepsilon)\log_q n$ but do not know how to show it.

It is natural to ask when is the function $G_q(x)$ asymptotic to 1. This is answered in the following theorem.

Theorem 1.4. *If $(m-2\log_q n)\log q \to \infty$ then $G_q(x)$ tends to 1, and so in particular (1.3) holds in this limit. If $m = 2\log_q n + O(1)$ then $G_q(x) - 1 \gg_q 1$. If we let $m/\log_q n$ tend to $2-\varepsilon$ ($\varepsilon \in (0,1)$) then $\log G_q(x) = \Theta_q(n^{\varepsilon+o(1)})$.*

We conclude with the following uniform result, holding in the entire range, but most useful when u is bounded.

Proposition 1.5. *For $n \geq m \geq 1$,*

$$0 \leq \mathbb{P}(f_n \textit{ is } m\textit{-friable}) - \mathbb{P}(\pi_n \textit{ is } m\textit{-friable}) \leq \frac{C}{mq^{\lceil \frac{m+1}{2} \rceil}}.$$

We stress that our proofs of all of our estimates are direct, in the sense that we do not make use of existing asymptotics of $\mathbb{P}(f_n \text{ is } m\text{-friable})$. Rather, we bound the differences $|\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable})|$ and $|\mathbb{P}(f_n \text{ is } m\text{-friable}) - G_q(x)\mathbb{P}(\pi_n \text{ is } m\text{-friable})|$ themselves. In the very last step of each proof we plug existing lower bounds on $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ to convert our bounds to relative bounds. We explain the proof strategy in more detail in §2.1. It borrows some ideas from the modern treatments of $\Psi(x,y)$ [Hil84, Hil86, HT86].

1.1 Optimality

Theorems 1.1 and 1.2 combined state

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = 1 + O_\varepsilon\left(\frac{un^{\frac{1+a}{m}}\min\{m, \log(u+1)\}}{mq^{\lceil \frac{m+1}{2} \rceil}}\right) \tag{1.7}$$

for $m \geq (2+\varepsilon)\log_q n$. This is essentially optimal in both the error term and the range. Indeed, from (1.6) and the lower bound for $G_q(x)$ given in (5.3), we have a matching lower bound as long as $(2+\varepsilon)\log_q n \leq m \leq n/(\log n \log^3 \log(n+1))$ and $n \gg 1$.

We observe that for $m = n-1$, (1.7) recovers the Prime Polynomial Theorem with squareroot error term. Indeed,

$$\mathbb{P}(f_n \text{ is } (n-1)\text{-friable}) = 1 - \mathbb{P}(f_n \text{ is irreducible}),$$
$$\mathbb{P}(\pi_n \text{ is } (n-1)\text{-friable}) = 1 - \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1 - \frac{1}{n},$$

and so from (1.7)

$$\#\{f \in \mathcal{M}_{n,q} : f \text{ is irreducible}\} = \frac{q^n}{n} + O\left(\frac{q^{\lfloor n/2 \rfloor}}{n}\right). \tag{1.8}$$

In view of Theorem 1.4, the range of Theorem 1.2 cannot be extended to $m \geq 2\log_q n$. (We can extend it to $m - 2\log_q n \to \infty$ but with a worse error term.)

1.2 Expected largest prime factor

Let $L_q(f)$ be the largest degree of a prime polynomial dividing $f \in \mathbb{F}_q[T]$. Similarly, let $L(\pi)$ be the size of the longest cycle in the cycle decomposition of π.

Golomb [GG97] proved that $\mathbb{E}L(\pi_n)/n$ tends to a limit, known as the Golomb-Dickman constant, and approximated it as $0.624329\ldots$. Knopfmacher and Manstavičius [KM97] proved that

$$\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) = O\left(\sqrt{\frac{n}{q\log n}}\right)$$

holds uniformly in n and q. We prove the following estimate, which uncovers a transition around $\log q \asymp n\log n$.

Theorem 1.6. *We have*

$$c\exp(-C\max\{\sqrt{n\log n\log q}, \log q\}) \leq \mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) \leq C\exp(-c\max\{\sqrt{n\log n\log q}, \log q\}).$$

To relate L_q and L with friable polynomials and permutations, observe that $\mathbb{P}(L_q(f_n) \leq m)$ is equal to $\mathbb{P}(f_n \text{ is } m\text{-friable})$ and $\mathbb{P}(L(\pi_n) \leq m)$ is equal to $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$. The identity $\mathbb{E}X = 1 + \sum_{i\geq 1}(1 - \mathbb{P}(X \leq i))$ for $\mathbb{N}$-valued random variables shows that

$$\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) = \sum_{m=1}^{n}\left(\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable})\right). \tag{1.9}$$

By definition, the total variation distance between $L_q(f_n)$ and $L(\pi_n)$ is

$$d_{TV}(L_q(f_n), L(\pi_n)) = \sum_{m=1}^{n} |\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable}) \\ - (\mathbb{P}(f_n \text{ is } (m-1)\text{-friable}) - \mathbb{P}(\pi_n \text{ is } (m-1)\text{-friable}))|.$$

The fact that $\mathbb{P}(f_n \text{ is } m\text{-friable}) \geq \mathbb{P}(\pi_n \text{ is } m\text{-friable})$ (see Proposition 1.5) implies that

$$\frac{1}{2}d_{TV}(L_q(f_n), L(\pi_n)) \leq \mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n),$$

so Theorem 1.6 yields an upper bound for $d_{TV}(L_q(f_n), L(\pi_n))$:

Corollary 1.7. *We have*

$$d_{TV}(L_q(f_n), L(\pi_n)) \leq C\exp(-c\max\{\sqrt{n\log n\log q}, \log q\}).$$

1.3 Previous works

1.3.1 Dickman function and friability

To discuss previous results, we introduce the Dickman function $\rho\colon [0,\infty) \to (0,1]$. It is defined as $\rho(t) = 1$ for $t \in [0,1]$, and for the rest of its range it is defined through the differential delay equation

$$t\rho'(t) + \rho(t-1) = 0.$$

It is a weakly-decreasing function, that decays superexponentially: $\rho(t) = t^{-t+o(t)}$ [Ten15, p. 374]. It was introduced by Dickman [Dic30] in his study of friable integers. We say that a positive integer is y-friable if its prime factors are no larger than y. Dickman proved that, for any fixed $a > 0$,

$$\#\{1 \le n \le x : n \text{ is } x^{1/a}\text{-friable}\} \sim x\rho(a) \tag{1.10}$$

as $x \to \infty$. Goncharov [Gon44] proved that

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \rho(u) + o(1) \tag{1.11}$$

as $u = n/m$ tends to a positive constant; this is a permutation analogue of (1.10). From Proposition 1.5 and Goncharov's result, we immediately obtain a polynomial analogue of his result:

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u) + o(1) + O\left(\frac{1}{mq^{\lceil \frac{m+1}{2} \rceil}}\right) = \rho(u) + o(1)$$

as n/m tends to a positive constant. This polynomial analogue was first established by Car [Car87], without making use of Goncharov's work. She established the quantitative version

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u) + O\left(\frac{2^u}{m}\right).$$

This was later improved by Warlimont [War91] to

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u) + O\left(\frac{1}{m}\right). \tag{1.12}$$

A slightly weaker version of (1.12) was proved independently by Panario, Gourdon and Flajolet [PGF98].

We explain how (1.12) easily follows from our work. We first state a quantitative version of (1.11), proved in [MP16]:

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \rho(u)\left(1 + O\left(\frac{u\log(u+1)}{m}\right)\right) \tag{1.13}$$

for $m \ge \sqrt{n\log n}$. For $m \ge \sqrt{n\log n}$, (1.12) follows at once from Proposition 1.5 and (1.13), with an improved error term. For $m < \sqrt{n\log n}$, $1/m$ is greater than $c\rho(u)$, so (1.12) amounts to $\mathbb{P}(f_n \text{ is } m\text{-friable}) = O(1/m)$, which follows from Proposition 1.5 and (1.13).

For $m \gg \sqrt{n\log n}$, Manstavičius proved [Man92a, Thm. 2]

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u)\left(1 + O\left(\frac{u\log(u+1)}{m}\right)\right). \tag{1.14}$$

This follows at once from (1.7) and (1.13).

Under the Riemann Hypothesis, Hildebrand [Hil84] (cf. [Gra08, Thm.]) proved that

$$\#\{n \le x : n \text{ is } y\text{-friable}\} = x\rho\left(\frac{\log x}{\log y}\right)\exp\left(O_\varepsilon\left(\frac{\log\left(\frac{\log x}{\log y}+1\right)}{\log y}\right)\right)$$

uniformly for $\log y \ge (2+\varepsilon)\log\log x$. In fact, this result also implies the Riemann Hypothesis. We find (1.7) akin to Hildebrand's result, where in the polynomial setting, ρ is replaced with $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$. Note that our result is stronger: our error term goes to zero when $m \sim (2+\varepsilon)\log_q n$, while the error of term of Hildebrand does not if $\log y \sim (2+\varepsilon)\log\log x$.

Remark 1.1. *By combining a conditional result of Saias [Sai89, p. 81] (given without proof) with estimates of de Bruijn's approximation* $\Lambda(x,y)$ *implicit in [FT91], it follows that (conditionally)* $\#\{n \le x : n \text{ is } y\text{-friable}\}$ *is not asymptotic to* $x\rho(\log x/\log y)$ *in the regime* $\log y \asymp \log\log x$*. Comparing with [Sai89], it seems that our main term* $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ *is analogous to* $\Lambda(x,y)$*.*

It is natural to ask whether the approximation $\mathbb{P}(\pi_n \text{ is } m\text{-friable}) \sim \rho(u)$ holds beyond the range $m/\sqrt{n\log n} \to \infty$ implied by (1.13). In the appendix we show that ρ is not an asymptotic approximation once $m/\sqrt{n\log n}$ is bounded from above. A related result was proved in [MP16, Cor. 3] by a different method.

1.3.2 Saddle point analysis

Odlyzko [Odl85] used saddle point analysis to estimate $\mathbb{P}(f_n \text{ is } m\text{-friable})$ for $q=2$ and $n^{1/100} \le m \le n^{99/100}$. Lovorn [Lov92] extended this to general q in his thesis. Note that the range $n^{1/100} \le m \le n^{99/100}$ is captured in full by Theorem 1.1.

Manstavičius [Man92a, Man92b] extended the range of these results to $n \ge m\log m(\log\log m)^3$ with $m \to \infty$, and proved a relative error term of order $u^{-1} + mq^{-m}$. This result is an analogue of the work of Hildebrand and Tenenbaum [HT86], who estimated $\#\{1 \le n \le x : n \text{ is } y\text{-friable}\}$ uniformly in the range $2 \le y \le x$, with a relative error term of $\log y/\log x + \log y/y$. We do not give the full statements of these asymptotics for polynomials as they are somewhat complicated and are not needed here. For permutations, Manstavičius and Petuchovas obtained [MP16, Thm. 2, Cor. 5]

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{D(x)}{\sqrt{2\pi\lambda}}\left(1+O\left(u^{-1}\right)\right) \tag{1.15}$$

uniformly in the range $1 \le m \le n$, where

$$D(x) = \exp\left(\sum_{j=1}^{m}\frac{x^j}{j}\right)x^{-n} \tag{1.16}$$

and $\lambda = \lambda(x) = \sum_{j=1}^{m} jx^j$. Here x is as defined in (1.4). This result provides an asymptotic as long as $u \to \infty$.

1.3.3 Inequalities

Warlimont [War91] proved the upper bound $\mathbb{P}(f_n \text{ is } m\text{-friable}) \le C\exp(-cu)$ in $1 \le m \le n$. Several lower bounds have been proved. Bender and Pomerance [BP98, Thm. 2.1] proved that $\mathbb{P}(f_n \text{ is } m\text{-friable}) \ge n^{-u}$ for $m \le \sqrt{n}$. In [JL06, App. A], Joux and Lercier prove $\log \mathbb{P}(f_n \text{ is } m\text{-friable}) \ge -(1+o_m(1))u\log u$ for fixed m and growing q and n. Granville, Harper and Soundararajan [GHS15, Ex. 6] show that $\mathbb{P}(f_n \text{ is } m\text{-friable}) \ge \rho(n/m)$ and state, without proof, $\mathbb{P}(f_n \text{ is } m\text{-friable}) \ge \rho(n/m)\exp(cn/m^2)$. This implies the Dickman function is not a good approximation once $m/\sqrt{n}$ is bounded from above. In the appendix we make this optimal and show that the Dickman function is not an asymptotic approximation if $m/\sqrt{n\log n}$ is bounded.

1.3.4 Soundararajan's polynomial results and Ford's permutation results

In an unpublished manuscript[1] Soundararajan [Sou, Thm. 1.1], building on Manstavičius [Man92a, Man92b], proved that

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u)\exp\left(O\left(\frac{n\log n}{m^2}\right)\right) \tag{1.17}$$

uniformly for $n \ge m \ge \log(n\log^2 n)/\log q$. For $m \le \log_q n$ he gives lower and upper bounds which are of different nature from (1.17), and are analogous to Ennola's work in the integer case [Enn69]. It would be interesting to adapt the work of La Bretèche and Tenenbaum [dlBT17], improving Ennola's results, to the polynomial and permutation settings as well.

Additionally, Soundararajan obtains an asymptotic formula for $\log \psi_q(n,m)$ uniformly in the full range $1 \le m \le n$, with a relative error term $1/m + 1/\log n$.

Very recently, Ford proved for $n \ge m \ge 1$ the upper bound $\mathbb{P}(\pi_n \text{ is } m\text{-friable}) \le e^{-u\log u + u}$ [For22, Thm. 1.16] by elementary means. Additionally, he gave a short proof for for the following estimate [For22, Thm. 1.17]

$$\rho\left(\frac{n}{m}\right) \le \mathbb{P}(\pi_n \text{ is } m\text{-friable}) \le \rho\left(\frac{n+1}{m+1}\right), \tag{1.18}$$

holding for $n \ge m \ge 1$. It implies $\mathbb{P}(\pi_n \text{ is } m\text{-friable}) \sim \rho(u)$ for $m/\sqrt{n\log n} \to \infty$ [For22, Cor. 1.18].

In §7 we give a quick proof that Ford's (1.18) implies the following.[2]

Proposition 1.8. *For $n \ge m \ge 1$ we have*

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \rho(u)\exp\left(O\left(\frac{u\log(u+1)}{m}\right)\right).$$

This extends (1.13) to the full range $n \ge m \ge 1$. Although Proposition 1.8 does not give an asymptotic result for $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ itself if m is relatively small, it does show that $\log \mathbb{P}(\pi_n \text{ is } m\text{-friable}) \sim \log\rho(u)$ as $n,m \to \infty$. This behavior also holds for bounded m by [MP16, Thm. 1]. We record this as

Corollary 1.9. *As $n \to \infty$ we have $\log \mathbb{P}(\pi_n \text{ is } m\text{-friable}) \sim \log\rho(u)$, uniformly in $1 \le m \le n$.*

[1] Soundararajan's work is surveyed in [Odl94, Gra08]. In [Odl00, Sch02] it is explained that Soundararajan's work remained unpublished in view of the stronger result published in [PGF98]; however, as shown in §1.3.5, that work is flawed.

[2] A slightly weaker version of Proposition 1.8 can be derived by plugging (1.17) in Proposition 1.5 and letting $q \to \infty$.

Our methods allow us to deduce (1.17) from Proposition 1.8. Namely, we prove

Theorem 1.10. *Suppose $n \geq m \geq \log(n\log n)/\log q$. Then*

$$\mathbb{P}(f_n \textit{ is } m\textit{-friable}) = \mathbb{P}(\pi_n \textit{ is } m\textit{-friable})\exp\left(O\left(\frac{u\log(u+1)}{m}\right)\right).$$

From Theorem 1.10 and Proposition 1.8 we immediately obtain (1.17).

1.3.5 Some inaccuracies

Let $\psi(x,y) := \#\{1 \leq n \leq x : n \text{ is } y\text{-friable}\}$. The Buchstab-de Bruijn identity states [Gra08, Eq. (3.10)]

$$\psi(x,y) = 1 + \sum_{p \leq y} \psi\left(\frac{x}{p}, p\right), \tag{1.19}$$

where the sum is over primes up to y. De Bruijn used it to prove that [dB51]

$$\psi(x,y) = x\rho(u)\left(1 + O_{\varepsilon}\left(\frac{\log(\frac{\log x}{\log y}+1)}{\log y}\right)\right)$$

holds in the range $x \geq y \geq \exp((\log x)^{5/8+\varepsilon})$. We are not aware of a polynomial analogue of this identity. In the survey [Gra08], the identity

$$\psi_q(n,m) - \psi_q(n,m-1) = \pi_q(m)\psi_q(n-m,m)$$

is suggested as an analogue of (1.19), where $\pi_q(m)$ is the number of monic irreducibles of degree m. However, this identity is false already for $n=4$, $m=2$ and $q=3$.

In [Hil86], Hildebrand extended de Bruijn's result to the range $x \geq y \geq \exp((\log\log x)^{5/3+\varepsilon})$, by using the following identity:

$$\psi(x,y)\log x = \int_1^x \frac{\psi(t,y)}{t}dt + \sum_{\substack{p^m \leq x \\ p \leq y}} \psi\left(\frac{x}{p^m}, y\right)\log p,$$

where the sum is over y-friable prime powers up to x. Hildebrand's identity does have a simple polynomial analogue, namely

$$\psi_q(n,m)n = \sum_{\substack{\deg(P^k) \leq n \\ \deg(P) \leq m}} \psi_q\left(n - \deg(P^k), m\right)\deg P.$$

It is proved in complete analogy with Hildebrand's original identity.

In [Man92a, Thm. 2] (cf. [KM97, Thm. A]) it is claimed that

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \mathbb{P}(\pi_n \text{ is } m\text{-friable})\left(1 + O_{\varepsilon}(q^{-m(1/2-\varepsilon)})\right) \tag{1.20}$$

holds uniformly in m and q. This cannot hold as stated for small m, per the discussion in the introduction. In particular, a short computation shows that for $m=1$, $\mathbb{P}(f_n \text{ is 1-friable})/\mathbb{P}(\pi_n \text{ is 1-friable}) \geq cn^2/q$, which contradicts (1.20) if, say, $n \geq q$.

In [PGF98] an estimate similar to Warlimont's estimate (1.12) is proved, but with an additional factor of $\log n$ in the numerator[3]. Moreover, a proof is sketched of the following estimate, for every integer $k \geq 2$:

$$\mathbb{P}\left(f_n \text{ is } m\text{-friable}\right) = \rho(u) + O_k\left(\frac{\log n}{m^k}\right)$$

for $m < n/k$, as long as $m^k/\log n \to \infty$. However, this cannot hold as stated, even for bounded u and $k=2$. Indeed, this violates the lower bound $\mathbb{P}(f_n \text{ is } m\text{-friable}) \geq \rho(u) + c\rho(u)u\log u/m$ (valid for $n/2 \geq m$) proven in the appendix.

Acknowledgements

The author thanks Dor Elboim for useful discussions, Kevin Ford, Brad Rodgers, Gérald Tenenbaum for helpful comments on an earlier version of the manuscript and Kannan Soundararajan for kindly sharing his unpublished manuscript. The author would also like to thank the referee for their thorough and careful reading of the manuscript and useful comments which improved the presentation of the results and proofs. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreements Nos. 786758 and 851318).

2 Strategy and preliminaries

Throughout the paper, the letters C and c will stand for positive absolute constants that may change from one occurrence to the next.

2.1 Strategy

In the integer setting, $\Psi(x,y)$ is studied by applying Perron's formula to the partial zeta function

$$\zeta_y(s) = \prod_{p \leq y} (1-p^{-s})^{-1}$$

and reducing the problem to the study of a complex integral

$$\frac{1}{2\pi i}\int_{(2)} \zeta(s,y)x^s \frac{ds}{s}.$$

If y is not 'too small', we have the relation [Ten15, Lem. III.5.16]

$$\zeta_y(s) \sim (s-1)\zeta(s)\hat{\rho}((s-1)\log y)\log y$$

[3]The result is stated as $\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u)(1+O(\frac{\log n}{m}))$, but – as observed in Tenenbaum's review [Ten01] – this should read $\mathbb{P}(f_n \text{ is } m\text{-friable}) = \rho(u) + O(\frac{\log n}{m})$.

in some range of s, where $\hat{\rho}$ is the Laplace transform of ρ. This allows us to relate the above integral to $\rho(\log x/\log y)$ in some range. In the permutation and polynomial setting, the same approach can be used to relate $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ and $\mathbb{P}(f_n \text{ is } m\text{-friable})$ to $\rho(n/m)$. One first introduces the generating functions

$$\begin{aligned} F(z) &:= 1 + \sum_{n\geq 1} \mathbb{P}(\pi_n \text{ is } m\text{-friable}) z^n = 1 + \sum_{n\geq 1} \frac{\psi_\pi(n,m)}{n!} z^n, \\ F_q(z) &:= 1 + \sum_{n\geq 1} \mathbb{P}(f_n \text{ is } m\text{-friable}) z^n = 1 + \sum_{n\geq 1} \frac{\psi_q(n,m)}{q^n} z^n \end{aligned} \tag{2.1}$$

whose analytic properties are explored in §2.3 below. One then applies Cauchy's formula to F and F_q, instead of Perron:

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=r} \frac{F(z)}{z^{n+1}} dz, \qquad \mathbb{P}(f_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=r} \frac{F_q(z)}{z^{n+1}} dz.$$

One can relate the integrands to $\hat{\rho}$ as well, obtaining $\mathbb{P}(f_n \text{ is } m\text{-friable})$ and $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ are asymptotic to $\rho(n/m)$ in some range, see [Man92a, Man92b, MP16]. We modify this strategy: instead of studying the polynomial and permutations probabilities individually, we study the difference

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=r} \frac{F_q(z) - F(z)}{z^{n+1}} dz.$$

Our aim is to upper bound this and in particular to see when this is $o(\mathbb{P}(\pi_n \text{ is } m\text{-friable}))$. It is easier than studying the probabilities individually, because we just aim to upper bound an integral. This can be done rather conveniently as the ratio $G_q := F_q/F$ is close to 1 in a wide range.

For y which is not 'too large', $\Psi(x,y)$ is studied using a saddle point approach. One still applies Perron's formula, and integrates along a line $\Re s = \alpha$ where α is the saddle point which is defined as the real solution to $-(\log\zeta(s,y))' = \log x$. On part of the line $\Re s = \alpha$, the integrand $\zeta(s,y)x^s/s$ is asymptotic to the constant $\zeta(\alpha,y)x^\alpha/\alpha$ times a gaussian in $\Im s$, see [HT86]. Similarly, in the permutation and polynomial setting we can approximate the integrands $F_q(z)/z^{n+1}$ and $F(z)/z^{n+1}$ as gaussians by choosing the radii r to be $x_q = x_{q,n,m}$ and $x = x_{n,m}$, respectively, where x is the saddle point with respect to $F(z)/z^{n+1}$ (defined as the real positive solution to $-z(\log F(z))' = n$) and similarly x_q is defined as the real solution to $-z(\log F_q(z))' = n$ [Man92a, Man92b, MP16]. The saddle point x coincides with x defined in (1.4). Again, we modify this approach: we study both $F_q(z)/z^{n+1}$ and $F(z)/z^{n+1}$ near the saddle point x associated with $F(z)/z^{n+1}$. We consider the difference

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) - G_q(x)\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=x} \frac{F(z)(G_q(z) - G_q(x))}{z^{n+1}} dz.$$

We want to bound this and in particular see when this is $o(\mathbb{P}(\pi_n \text{ is } m\text{-friable}))$. This can be done as $G_q(z) - G_q(x)$ is small in a wide range.

Our strategy has some similarities with the work of Saias [Sai89], who studied $\Psi(x,y)$ by comparing it to de Bruijn's approximation $\Lambda(x,y)$.

2.2 Primes

We denote by $\pi_q(n) := |\mathcal{P} \cap \mathcal{M}_{n,q}|$ the number of prime polynomials of degree n. From Gauss's identity [ABT93, Eq. (1.3)]

$$\sum_{d|n} d\pi_q(d) = q^n, \tag{2.2}$$

we obtain the estimate

$$\frac{q^n}{2n} \le \pi_q(n) \le \frac{q^n}{n} \tag{2.3}$$

(cf. [Pol13, Lem. 4]) as well as (1.8).

2.3 Generating functions

Since $\mathbb{P}(\pi_n \text{ is } m\text{-friable})$ and $\mathbb{P}(f_n \text{ is } m\text{-friable})$ are between 0 and 1, the generating series F and F_q defined in (2.1) converge absolutely in $|z| < 1$ and define analytic function in the open disc. We shall show that they can be analytically continued to a larger region. The logarithm function will always be used with its principal branch.

Lemma 2.1. *We have*

$$F(z) = \exp\left(\sum_{i=1}^{m} \frac{z^i}{i}\right), \tag{2.4}$$

while for every prime power q we have

$$G_q(z) = \frac{F_q(z)}{F(z)} = \exp\left(\sum_{i>m} \frac{a_i}{i} z^i\right), \qquad a_i = a_{i,m,q} := q^{-i} \sum_{d|i,\, d\le m} d\pi_q(d). \tag{2.5}$$

The coefficients a_i satisfy, for all $i > m$,

$$\frac{1}{2} q^{\max\{d\le m:\, d \text{ divides } i\}-i} \le a_i \le 2q^{\max\{d\le m:\, d \text{ divides } i\}-i} \le 2q^{\min\{m,\lfloor i/2\rfloor\}-i}. \tag{2.6}$$

In particular, the functions F_q and G_q are analytic in $|z| < q$, and $a_i = \Theta(q^{-i/2})$ for even $i \in [m+1, 2m]$.

Proof. The exponential formula for permutations [Sta99, Cor. 5.1.9] states the following. Given a function $g\colon \mathbb{N} \to \mathbb{C}$, we construct a corresponding function on permutations (on an arbitrary number of elements) as follows:

$$G(\pi) = \prod_{C\in\pi} g(|C|),$$

where the product is over the disjoint cycles of π. We then have the following identity of formal power series:

$$1 + \sum_{i\ge 1} \mathbb{E}_{\pi\in S_i} G(\pi) z^i = \exp\left(\sum_{j\ge 1} \frac{g(j)}{j} z^j\right).$$

Applying the identity with $g(j) = \mathbf{1}_{j\leq m}$, we obtain (2.4). For F_q we have, by unique factorization in $\mathbb{F}_q[T]$,

$$F_q(z) = \prod_{\substack{P\in\mathcal{P}\\ \deg(P)\leq m}} \left(\sum_{i\geq 0}\left(\frac{z}{q}\right)^{\deg(P^i)}\right) = \prod_{\substack{P\in\mathcal{P}\\ \deg(P)\leq m}} \left(1-\left(\frac{z}{q}\right)^{\deg(P)}\right)^{-1} = G_q(z)F(z)$$

and

$$\log G_q(u) = \sum_{j\geq 1}\sum_{\deg(P)\leq m}\frac{1}{j}\left(\frac{z}{q}\right)^{\deg(P)j} - \sum_{i=1}^{m}\frac{z^i}{i}$$
$$= \sum_{i\leq m}\frac{z^i}{i}\left(q^{-i}\sum_{\substack{\deg(P)\leq m\\ \deg(P)|i}}\deg(P)-1\right)+\sum_{i>m}\frac{z^i}{i}q^{-i}\sum_{\substack{\deg(P)\leq m\\ \deg(P)|i}}\deg(P).$$

For $i\leq m$ we have $\sum_{\deg(P)\leq m,\deg(P)|i}\deg(P)/q^i = \sum_{d|i} d\pi_q(d)/q^i = 1$ by (2.2), proving (2.5). The bound (2.6) now follows from (2.3). □

3 Proof of Proposition 1.5

We write $[z^n]H(z)$ the for the nth coefficient in a power series H. By definition, $\mathbb{P}(f_n \text{ is } m\text{-friable}) = [z^n]F(z)$ and $\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = [z^n]F_q(z)$, where F and F_q are defined in §2.3. We are set out to prove

$$0 \leq [z^n](F_q - F) \leq \frac{C}{mq^{\lceil\frac{m+1}{2}\rceil}}.$$

By Lemma 2.1,

$$F_q - F = F(G_q - 1),$$

and both F and $G_q - 1$ have non-negative coefficients. This proves $[u^n](F_q - F) \geq 0$. For the upper bound we also use the non-negativity, which implies that

$$[z^n](F_q - F) \leq (\max_{0\leq i\leq n}[z^i]F)(G_q(1)-1).$$

We have

$$[z^i]F = \mathbb{P}(\pi_i \text{ is } m\text{-friable}) \leq 1,$$

and so $[z^n](F_q - F) \leq G_q(1) - 1$. By (2.6),

$$0 \leq \sum_{i>m}\frac{a_i}{i} \leq \frac{2}{m}\sum_{i>m}\frac{1}{q^{\lceil\frac{i}{2}\rceil}} \leq \frac{C}{q^{\lceil\frac{m+1}{2}\rceil}m} \leq C,$$

so that

$$G_q(1) \leq \exp\left(\frac{C}{mq^{\lceil\frac{m+1}{2}\rceil}}\right) = 1 + O\left(\frac{1}{mq^{\lceil\frac{m+1}{2}\rceil}}\right)$$

and the required bound follows. □

4 Analysis via Laplace transform

Here we shall use properties of the Laplace transform of ρ to deduce Theorem 1.1 in a limited range.

Theorem 4.1. *If $n \geq m \geq C\sqrt{n\log n}$, then*

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = 1 + O\left(\frac{u\log(u+1)}{mq^{\lceil \frac{m+1}{2} \rceil}}\right).$$

4.1 Asymptotics of parameters

We define $\xi\colon (1,\infty) \to (0,\infty)$, a function of variable $u > 1$, by

$$e^{\xi} = 1 + u\xi. \tag{4.1}$$

Lemma 4.2. *[Hil84, Lem. 1] We have $\xi \sim \log u$ as $u \to \infty$, and $\xi' = u^{-1}(1+O(1/\log u))$.*

Recall we have

$$H_n := \sum_{i=1}^{n} \frac{1}{i} = \log n + \gamma + O\left(\frac{1}{n}\right)$$

for the Euler-Mascheroni constant γ. Define the entire function $I(s)$ by

$$I(s) = \int_0^s \frac{e^v - 1}{v}\, dv, \qquad s \in \mathbb{C}. \tag{4.2}$$

Note that $I(\xi)$ grows faster than any polynomial in ξ.

Lemma 4.3. *[Ten15, Ch. III.5, Thms. 7, 8] We have*

$$\hat{\rho}(s) := \int_0^{\infty} e^{-sv}\rho(v)\, dv = \exp\left(\gamma + I(-s)\right) \tag{4.3}$$

for all $s \in \mathbb{C}$. Also,

$$\exp\left(\gamma - u\xi + I(\xi)\right) = \rho(u)\sqrt{\frac{2\pi}{\xi'}}\left(1 + O\left(\frac{1}{u}\right)\right). \tag{4.4}$$

Lemma 4.4. *[Ten15, Lem. III.5.12] The following bounds hold for $s = -\xi(u) + i\tau$, $\tau \in \mathbb{R}$:*

$$\hat{\rho}(s) = \begin{cases} O\left(\exp\left(I(\xi) - \frac{\tau^2 u}{2\pi^2}\right)\right) & \text{if } |\tau| \leq \pi, \\ O\left(\exp\left(I(\xi) - \frac{u}{\pi^2+\xi^2}\right)\right) & \text{if } |\tau| \geq \pi, \\ \frac{1}{s} + O\left(\frac{1+u\xi}{s^2}\right) & \text{if } |\tau| \geq 1 + u\xi. \end{cases}$$

We define a function $T(s)$ which arises in (4.7) when relating the generating function $F(z)$ (at $z = e^{-s/m}$) to $\hat{\rho}(s)$:

$$T(s) = \int_0^s \frac{e^v - 1}{v}\left(\frac{v}{m}\frac{e^{v/m}}{e^{v/m}-1} - 1\right) dv.$$

It is analytic in the strip $|\Im s| < 2\pi m$.

Lemma 4.5. *[MP16, Lem. 11] Let $s = \eta + i\tau$, $0 \le \eta \le \pi m$ and $-\pi m \le \tau \le \pi m$. We have*

$$\left|T(s) + \frac{s}{2m}\right| \ll \frac{e^{\eta}}{m} + \frac{\tau^2}{m^2}.$$

Lemma 4.6. *Suppose $n \ge m \ge \sqrt{n \log n}$. If n is sufficiently large we have*

$$0 \le G_q(e^{\xi/m}) - 1 \le \frac{Cu\log(u+1)}{mq^{\lceil \frac{m+1}{2} \rceil}}.$$

Proof. By Lemma 4.2 we have $e^{\xi} = 1 + u\xi \le 1 + Cu\log u \le 1 + Cn\log n \le 1 + Cm^2 \le q^{m/3}$ if n is sufficiently large, and so $e^{\xi/m}/\sqrt{q} \le q^{-1/6} \le 2^{-1/6}$. We have

$$0 \le \sum_{i>m} \frac{a_i}{i}(e^{\xi/m})^i \ll \frac{1}{m}\sum_{i>m}(e^{\xi/m})^i q^{-\lceil i/2 \rceil} \ll \frac{1}{m}\left(\frac{e^{\xi(m+1)/m}}{q^{\lceil \frac{m+1}{2} \rceil}} + \frac{e^{\xi(m+2)/m}}{q^{\lceil \frac{m+2}{2} \rceil}}\right) \ll \frac{u\log(u+1)}{mq^{\lceil \frac{m+1}{2} \rceil}} \ll 1.$$

Since $0 \le e^y - 1 \ll y$ for bounded non-negative y, the inequality follows. □

Lemma 4.7. *Let $A > 0$. Suppose $m\pi \ge 1 + u\xi$ and $u \ge \max\{A+1, 3\}$. Let $\Delta_2 = \{-\xi + i\tau : \tau \in [-m\pi, -(1+u\xi)] \cup [1+u\xi, m\pi]\}$. Then*

$$\int_{\Delta_2} e^{(u-A)s}\hat{\rho}(s)\,ds \ll \exp(\xi A)\rho(u).$$

Proof. Without loss of generality, we restrict our attention to $\Delta_2' = \{-\xi + i\tau : \tau \in [1+u\xi, m\pi]\} \subset \Delta_2$, and the other part is bounded in the same way. We integrate by parts, differentiating $\hat{\rho}(s)$ using (4.3) and (4.2):

$$\int_{\Delta_2'} e^{(u-A)s}\hat{\rho}(s)\,ds = \frac{e^{(u-A)s}}{u-A}\hat{\rho}(s)\Bigg|_{-\xi+i(1+u\xi)}^{-\xi+im\pi} - \frac{1}{u-A}\int_{\Delta_2'} e^{(u-A)s}\hat{\rho}(s)\frac{e^{-s}-1}{s}\,ds.$$

Since $|\exp((u-A)s)| \le \exp(-\xi(u-A))$ and $\int_{\Delta_2'} |ds|/|s|^2 = O(1)$, the result follows by Lemmas 4.3–4.4 and the triangle inequality. We exploit the fact that $\exp(-u\xi) \ll_C \rho(u)/u^C$ for any $C > 0$, due to the factor $\exp(I(\xi))$ in (4.4). □

4.2 Proof of Theorem 4.1

Suppose $u \le M$. By (1.13) (or Theorem A.1) and Proposition 1.5, $\mathbb{P}(f_n \text{ is } m\text{-friable}) \ge c_M > 0$. Proposition 1.5 now implies that

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \mathbb{P}(\pi_n \text{ is } m\text{-friable})\left(1 + O_M\left(\frac{1}{mq^{\lceil \frac{m+1}{2} \rceil}}\right)\right),$$

which establishes the theorem in the case of bounded u. Hence, we may assume $u \gg 1$ in our argument.

Let $y := e^{\xi/m}$, where ξ is defined in (4.1). By Proposition 1.5,

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = 1 + O_n\left(\frac{1}{q^{\lceil \frac{m+1}{2} \rceil}}\right) \tag{4.5}$$

and so we may assume that n is sufficiently large. In particular, by Lemma 4.2, $|y| \le e^{C\log u/m} \le e^{C\log n/\sqrt{n\log n}} \le 3/2 < q$ for sufficiently large n. Since F and F_q are analytic in $|z| < q$ by Lemma 2.1, we have, by Cauchy's integral formula,

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=y} \frac{F(z)}{z^{n+1}}\,dz, \qquad \mathbb{P}(f_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=y} \frac{F_q(z)}{z^{n+1}}\,dz.$$

Using the parametrization $z = e^{-s/m}$ with $s = -\xi - i\tau$, $-m\pi \le \tau \le m\pi$, we obtain

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i m}\int_{\Delta} e^{us} F(e^{-s/m})\,ds, \qquad \mathbb{P}(f_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i m}\int_{\Delta} e^{us} F_q(e^{-s/m})\,ds$$

where $\Delta := \{-\xi + i\tau : -m\pi \le \tau \le m\pi\}$. By Lemma 2.1, as in the proof of [MP16, Cor. 3],

$$\begin{aligned}\log F(z) - H_m = \sum_{i=1}^{m} \frac{z^i - 1}{i} = \int_1^z \sum_{i=1}^{m} t^{i-1}\,dt = \int_1^z \frac{t^m - 1}{t-1}\,dt \\ = \int_0^{m\log z} \frac{e^v - 1}{v}\frac{v}{m}\frac{dv}{1 - e^{-v/m}} = I(m\log z) + T(m\log z)\end{aligned}$$

where I, T are defined in §4.1 and $z \ge 1$. Hence

$$F(e^{-s/m}) = \exp\big(H_m + I(-s) + T(-s)\big), \tag{4.6}$$

which holds for all $s \in \Delta$ (not only $s \le 0$) by the uniqueness principle. By (4.3) and (4.6),

$$F(e^{-s/m}) = \exp\big(H_m - \gamma + T(-s)\big)\hat{\rho}(s). \tag{4.7}$$

Hence,

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{\exp\big(H_m - \gamma\big)}{2\pi i m}\int_{\Delta} e^{us}\hat{\rho}(s)\exp(T(-s))(G_q(e^{-s/m}) - 1)\,ds. \tag{4.8}$$

We have $|\exp(H_m - \gamma)/m| = O(1)$, and we turn to bound the integral in the right-hand side of (4.8). We partition Δ as $\Delta_0 \cup \Delta_1 \cup \Delta_2$, where $\Delta_0 = \{-\xi + i\tau : -\pi \le \tau \le \pi\}$, $\Delta_1 = \{-\xi + i\tau : \tau \in [-(1 + u\xi), -\pi] \cup [\pi, 1 + u\xi]\}$ and $\Delta_2 = \{-\xi + i\tau : \tau \in [-m\pi, -(1+u\xi)] \cup [1 + u\xi, m\pi]\}$. We may assume that $m\pi > 1 + u\xi > \pi$ since we can take $n \gg 1$ and $u \gg 1$. By Lemma 4.5, $T(-s)$ is bounded in Δ, and so

$$\begin{aligned}\Big|\int_{\Delta_i} e^{us}\hat{\rho}(s)\exp(T(-s))(G_q(e^{-s/m}) - 1)\,ds\Big| \le \int_{\Delta_i} \big|e^{us}\hat{\rho}(s)\exp(T(-s))(G_q(e^{-s/m}) - 1)\,ds\big| \\ \ll \exp(-u\xi)(G_q(e^{\xi/m}) - 1)\int_{\Delta_i} |\hat{\rho}(s)|\,|ds|\end{aligned}$$

for $i = 0, 1$. For $i = 0$ we have by the first part of Lemma 4.4

$$\int_{\Delta_0} |\hat{\rho}(s)|\,|ds| \ll \exp\big(I(\xi)\big) \int_{-\pi}^{\pi} \exp(-\tau^2 u/2\pi^2)\,d\tau \ll \frac{\exp\big(I(\xi)\big)}{\sqrt{u}},$$

and so, by Lemmas 4.2 and 4.3,

$$\Big|\int_{\Delta_0} e^{us}\hat{\rho}(s)\exp(T(-s))(G_q(e^{-s/m})-1)\,ds\Big| \ll \rho(u)(G_q(e^{\xi/m})-1).$$

Similarly, for $i = 1$ we have by the second part of Lemma 4.4

$$\int_{\Delta_1} |\hat{\rho}(s)|\,|ds| \ll \exp\big(I(\xi)\big)\exp(-u/(\pi^2+\xi^2))(1+u\xi),$$

and so, by Lemmas 4.2 and 4.3,

$$\begin{aligned}\Big|\int_{\Delta_1} e^{us}\hat{\rho}(s)\exp(T(-s))(G_q(e^{-s/m})-1)\,ds\Big| &\ll \rho(u)\sqrt{u}\exp(-u/(\pi^2+\xi^2))(1+u\xi)(G_q(e^{\xi/m})-1)\\ &\ll \rho(u)(G_q(e^{\xi/m})-1).\end{aligned}$$

As $G_q(e^{\xi/m})-1 = O(u\log(u+1)/(mq^{\lceil (m+1)/2\rceil}))$ by Lemma 4.6, the integrals over Δ_0 and Δ_1 contribute at most

$$\ll \frac{\rho(u)u\log(u+1)}{mq^{\lceil (m+1)/2\rceil}}. \tag{4.9}$$

We wish to bound the integral over Δ_2 by the same quantity. However, using the triangle inequality as before we will incur an extra factor of $\log m$ coming from the integral of $|\hat{\rho}(s)| = O(1/|s|)$ on Δ_2. To remove this factor, we first replace $\exp(T(-s))$ by 1 – the error obtained is acceptable, since by Lemma 4.5

$$\begin{aligned}&\int_{\Delta_2} e^{us}\hat{\rho}(s)(e^{T(-s)}-1)(G_q(e^{-s/m})-1)ds\\ &\qquad \ll \int_{\Delta_2} |e^{us}\hat{\rho}(s)T(-s)||(G_q(e^{-s/m})-1)||ds|\\ &\qquad \ll e^{-u\xi}(G_q(e^{\xi/m})-1)\int_{\Delta_2} |s|^{-1}\left(\left|\frac{s}{m}\right| + \left|\frac{s}{m}\right|^2 + \frac{u\log(u+1)}{m}\right)|ds|\end{aligned}$$

and this is $\ll \rho(u)((G_q(e^{\xi/m})-1))$ which we saw is at most (4.9). It remains to bound

$$\int_{\Delta_2} e^{us}\hat{\rho}(s)(G_q(e^{-s/m})-1)\,ds. \tag{4.10}$$

Lemma 2.1 shows we may write

$$G_q(e^{-s/m})-1 = \sum_{i=m+1}^{4m} \frac{a_i\left(e^{-s/m}\right)^i}{i} + O\left(\frac{e^{2\xi}}{q^m}\right)$$

with $a_i = O(q^{-\lceil i/2 \rceil})$. The integral $\int_{\Delta_2} |e^{us}\hat{\rho}(s)e^{2\xi}/q^m| ds$ is sufficiently small (smaller than (4.9)). The term corresponding to i is bounded as follows by Lemma 4.7:

$$\int_{\Delta_2} e^{us}\hat{\rho}(s)\frac{a_i\left(e^{-s/m}\right)^i}{i}\,ds \ll \exp\left(\xi i/m\right)\frac{\rho(u)}{mq^{\lceil \frac{i}{2} \rceil}}.$$

Summing over $m+1 \le i \le 4m$, we see that (4.10) is smaller than (4.9). All in all,

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable}) = O\left(\rho(u)\frac{u\log(u+1)}{q^{\lceil \frac{m+1}{2} \rceil}m}\right).$$

By (1.13) (or Theorem A.1), $\rho(u) \ll \mathbb{P}(\pi_n \text{ is } m\text{-friable})$, which gives the desired result. □

5 Saddle point analysis

We shall deduce Theorems 1.2 and 1.3 from the following

Theorem 5.1. *If* $\min\{n/(\log n \log^3 \log(n+1)), n/3\} \ge m > \log_q n$ *then*

$$\frac{\mathbb{P}(f_n \textit{ is } m\textit{-friable})}{\mathbb{P}(\pi_n \textit{ is } m\textit{-friable})} = G_q(x)\left(1 + O\left(\frac{G_q''(x)x^2 + G_q'(x)xm}{nmG_q(x)}\right)\right). \tag{5.1}$$

5.1 Asymptotics of parameters

Recall that x is the positive constant defined by $\sum_{j=1}^m x^j = n$, and that $\lambda = \sum_{j=1}^m jx^j$.

Lemma 5.2. *[MP16, Lem. 9] For* $u > 1$ *we have* $|\lambda - mn| \le mn/\log u$. *For* $u \ge 3$ *we have*

$$x^m = \Theta\left(n \min\left\{1, \frac{\log u}{m}\right\}\right). \tag{5.2}$$

Lemma 5.3. *Suppose* $n/3 \ge m \ge (2+\varepsilon)\log_q n$ *for some* $\varepsilon > 0$. *Let* $a = \mathbf{1}_{2|m}$. *Then*

$$1 + \frac{cux^{1+a}}{q^{\lceil \frac{m+1}{2} \rceil}} \min\left\{1, \frac{\log u}{m}\right\} \le G_q(x) \le 1 + \frac{C_\varepsilon ux^{1+a}}{q^{\lceil \frac{m+1}{2} \rceil}} \min\left\{1, \frac{\log u}{m}\right\}, \tag{5.3}$$

and in particular,

$$G_q(x) = 1 + \Theta_{n,\varepsilon}\left(\frac{1}{q^{\lceil \frac{m+1}{2} \rceil}}\right). \tag{5.4}$$

Moreover,

$$|G_q'(x)| \le C_\varepsilon \frac{nx^a}{q^{\lceil \frac{m+1}{2} \rceil}} \min\left\{1, \frac{\log u}{m}\right\}, \qquad |G_q''(x)| \le C_\varepsilon \frac{nmx^{a-1}}{q^{\lceil \frac{m+1}{2} \rceil}} \min\left\{1, \frac{\log u}{m}\right\}.$$

Proof. By (2.6),

$$\sum_{i>m} \frac{a_i}{i} x^i \leq \sum_{i>m} \frac{2x^i}{mq^{\lceil \frac{i}{2} \rceil}}. \tag{5.5}$$

Since $a_i \gg q^{-i/2}$ if $i \in [m+1, 2m]$ is even, we also have

$$G_q(x) - 1 \geq \sum_{i>m} \frac{a_i}{i} x^i \geq \frac{cx^m}{m}(a_{m+1}x + a_{m+2}x^2) \geq \frac{cx^m x^{1+a}}{mq^{\lceil \frac{m+1}{2} \rceil}}. \tag{5.6}$$

As $1 \leq x \leq n^{1/m} \leq q^{1/(2+\varepsilon)}$, the right-hand side of (5.5) is at most $C_\varepsilon (x^m/m) x^{1+a} q^{-\lceil (m+1)/2 \rceil}$ (consider even and odd i separately). As $x \leq q^{1/2}$, this is $O_\varepsilon(1)$, which also proves the upper bound for $G_q(x)$ in (5.3). For the lower bound, (5.2) guarantees that the right-hand side of (5.6) is at least as stated.

As $C_\varepsilon u x^{1+a} = O_{n,\varepsilon}(1)$, we obtain (5.4). Similarly, as $x^m \leq n$,

$$\sum_{i>m} a_i x^{i-1} \leq C_\varepsilon \left(\frac{x^m}{q^{\lceil \frac{m+1}{2} \rceil}} + \frac{x^{m+1}}{q^{\lceil \frac{m+2}{2} \rceil}} \right) \leq C_\varepsilon \frac{nx^a}{q^{\lceil \frac{m+1}{2} \rceil}} \min\left\{1, \frac{\log u}{m}\right\} \leq \frac{C_\varepsilon}{x},$$

yielding the bound on $G_q'(x)$ since we have the identity $G_q'(x) = G_q(x) \sum_{i>m} a_i x^{i-1}$ and the above shows $G_q(x) = O_\varepsilon(1)$. Considering separately $m < i \leq 2m+1$ and $i \geq 2m+2$,

$$\sum_{i>m} (i-1) a_i x^{i-2} \leq C_\varepsilon m \left(\frac{x^{m-1}}{q^{\lceil \frac{m+1}{2} \rceil}} + \frac{x^m}{q^{\lceil \frac{m+2}{2} \rceil}} + \frac{x^{2m}}{q^{m+2}} \right) \leq C_\varepsilon \frac{nmx^{a-1}}{q^{\lceil \frac{m+1}{2} \rceil}} \min\left\{1, \frac{\log u}{m}\right\},$$

which yields the desired bound on $G_q''(x)$ as $G_q''(x) = G_q(x)((\sum_{i>m} a_i x^{i-1})^2 + \sum_{i>m}(i-1) a_i x^{i-2})$. □

Lemma 5.4. *Fix $\varepsilon > 0$. Suppose $(2+\varepsilon)\log_q n \geq m \geq (1+\varepsilon)\log_q n$. Letting*

$$S = \frac{n}{q^{m/2}} \left(\frac{n^{1/m}}{\sqrt{q}} \right)^{1+a} \sum_{j=0}^{\lceil \frac{m-2}{2} \rceil} \left(\frac{n^{2/m}}{q} \right)^j$$

where $a = \mathbf{1}_{2|m}$, we have

$$\frac{G_q'(x)x}{G_q(x)} = \Theta_\varepsilon\left(S + \frac{n^2}{q^m}\right), \qquad \frac{G_q''(x)x^2}{G_q(x)} = \Theta_\varepsilon\left(\left(S + \frac{n^2}{q^m}\right)\left(S + \frac{n^2}{q^m} + m\right)\right),$$

$$\log G_q(x) = \Theta_\varepsilon\left(\frac{S}{m} + \frac{n^2}{mq^m}\right).$$

Moreover,

$$S \asymp \begin{cases} m & \text{if } |m - 2\log_q n| \leq 1/\log q, \\ \left(1 - \frac{n^{2/m}}{q}\right)^{-1} \left(\frac{n}{q^{m/2}}\right)^{1+\frac{1+a}{m}} & \text{if } m - 2\log_q n \geq 1/\log q, \\ \left(1 - \frac{q}{n^{2/m}}\right)^{-1} \frac{n^2}{q^m} & \text{if } m - 2\log_q n \leq -1/\log q. \end{cases}$$

Proof. Letting

$$S' = \sum_{i=m+1}^{2m} a_i x^i$$

where a_i are defined in (2.5), we have

$$S' = \Theta(S)$$

by (2.6) and (5.2). To prove the estimate for $G_q'(x)x/G_q(x)$ we use (2.6) and argue as follows:

$$\frac{G_q'(x)x}{G_q(x)} = \sum_{i>m} a_i x^i = \Theta(S' + \sum_{i\geq 2m} a_i x^i) = \Theta_\varepsilon\left(S' + \frac{n^2}{q^m}\right).$$

The estimate for $G_q''(x)x^2/G_q(x)$ follows similarly from

$$\frac{G_q''(x)x^2}{G_q(x)} = \left(\sum_{i>m} a_i x^i\right)^2 + \sum_{i>m} a_i x^i (i-1) = \Theta_\varepsilon\left(\left(\frac{G_q'(x)x}{G_q(x)}\right)^2 + mS' + \frac{mn^2}{q^m}\right).$$

In the same way, the estimate for $\log G_q(x)$ follows from

$$\log G_q(x) = \sum_{i=m+1}^{2m-1} \frac{a_i x^i}{i} + \sum_{i\geq 2m} \frac{a_i x^i}{i} = \Theta_\varepsilon\left(\frac{S'}{m} + \frac{n^2}{mq^m}\right).$$

We estimate S by the following general estimate for geometric sums: for $a>0$ we have that $\sum_{i=0}^{d-1} a^i$ is $\Theta(d)$ if $|a-1| \leq c/d$, is $\Theta(a^d/(a-1))$ if $a-1 \geq c/d$ and is $\Theta(1/(1-a))$ if $a-1 \leq -c/d$. □

5.2 Proof of Theorem 5.1

Since F is entire, we have, by Cauchy's integral formula,

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=x} \frac{F(z)}{z^{n+1}}\,dz.$$

The parametrization $z = xe^{it}$, $t \in [-\pi, \pi]$ shows, by Lemma 2.1, that

$$\begin{aligned}\mathbb{P}(\pi_n \text{ is } m\text{-friable}) &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \exp\left(\sum_{j=1}^{m} \frac{x^j e^{itj}}{j} - n(it + \log x)\right) dt \\ &= \frac{D(x)}{2\pi}\int_{-\pi}^{\pi} \exp\left(\sum_{j=1}^{m} \frac{x^j(e^{itj}-1)}{j} - int\right) dt,\end{aligned}$$

where $D(x)$ is defined in (1.16). As F_q is analytic in $|z| < q$, and $x < q$, we similarly have, by Lemma 2.1, that

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) = \frac{1}{2\pi i}\int_{|z|=x} \frac{F_q(z)}{z^{n+1}}\,dz = \frac{D(x)}{2\pi}\int_{-\pi}^{\pi} \exp\left(\sum_{j=1}^{m} \frac{x^j(e^{itj}-1)}{j} - int\right) G_q(xe^{it})\,dt.$$

Hence,

$$\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable})G_q(x) = \frac{D(x)}{2\pi}\int_{-\pi}^{\pi}\exp\left(\sum_{j=1}^{m}\frac{x^j(e^{itj}-1)}{j} - int\right)(G_q(xe^{it})-G_q(x))\,dt. \quad (5.7)$$

By assumption, $u \geq 3$. Let $t_0 = n^{-1/3}m^{-2/3}$ and $t_1 = 1/m$. We shall bound separately the contribution of $|t| \leq t_0$, $t_0 \leq |t| \leq t_1$ and $t_1 \leq |t| \leq \pi$ to the right-hand side of (5.7). For $k = 1,2,3$, let

$$I_k = \int_{A_k}\exp\left(\sum_{j=1}^{m}\frac{x^j(e^{itj}-1)}{j} - int\right)\left(G_q(xe^{it})-G_q(x)\right)dt,$$

where $A_1 = [-t_0,t_0]$, $A_2 = [-t_1,t_1]\setminus A_1$ and $A_3 = [-\pi,\pi]\setminus A_2$. A second-order Taylor approximation shows that for $|t| \leq \pi$,

$$\begin{aligned} G_q(xe^{it}) - G_q(x) &= G_q'(x)(xe^{it}-x) + O\left(G_q''(x)\left|xe^{it}-x\right|^2\right) \\ &= iG_q'(x)xt + O\left(\left(G_q''(x)x^2 + G_q'(x)x\right)t^2\right). \end{aligned} \quad (5.8)$$

For $|t| = O(1/m)$ and $1 \leq j \leq m$ we have $e^{itj} - 1 = itj - (tj)^2/2 + O(|t|^3 j^3)$, so that

$$\sum_{j=1}^{m}\frac{x^j(e^{itj}-1)}{j} - int = it\left(\sum_{j=1}^{m}x^j - n\right) - \frac{t^2}{2}\sum_{j=1}^{m}x^j j + O\left(|t|^3\sum_{j=1}^{m}x^j j^2\right) = -\frac{\lambda t^2}{2} + O\left(|t|^3\lambda_2\right) \quad (5.9)$$

where

$$\lambda_2 := \sum_{j=1}^{m}x^j j^2 \leq m\sum_{j=1}^{m}x^j j = m\lambda.$$

In A_1 we have $|t|^3\lambda_2 = O(n^{-1}m^{-2}m\lambda) = O(1)$ by Lemma 5.2. By (5.8) and (5.9),

$$I_1 = \int_{-t_0}^{t_0}\exp\left(-\frac{\lambda t^2}{2}\right)\left(iG_q'(x)xt + O\left(|t|^2 a + |t|^4 b\lambda_2 + |t|^5 a\lambda_2\right)\right)dt$$

for $a = G_q''(x)x^2 + G_q'(x)x$, $b = G_q'(x)x$. We have $\int_{-t_0}^{t_0}\exp(-\lambda t^2/2)t\,dt = 0$ and $\int_{\mathbb{R}}\exp(-\lambda t^2/2)|t|^k\,dt \ll \lambda^{-(k+1)/2}$ for $k = 2,4,5$. Hence

$$|I_1| \ll \lambda^{-3/2}a + \lambda^{-5/2}b\lambda_2 + \lambda^{-3}a\lambda_2 \ll \frac{1}{\lambda^{3/2}}\left(a + bm + \frac{am}{\sqrt{\lambda}}\right).$$

As $n \geq 3m$, we have $\lambda \geq cnm$ by Lemma 5.2. Thus

$$|I_1| \ll \frac{1}{\sqrt{\lambda}}\frac{a+bm}{nm}.$$

We turn our attention to I_2. We have $1-\cos s \ge cs^2$ in $|s| \le \pi$, and so

$$\left|\exp\left(\sum_{j=1}^{m} \frac{x^j(e^{itj}-1)}{j} - int\right)\right| \le \exp\left(-c\lambda t^2\right)$$

for $t \in A_2$. Moreover, $|G(x)-G(xe^{it})| \ll b|t|$, yielding

$$|I_2| \ll b\int_{A_2} |t|\exp\left(-c\lambda t^2\right)dt \ll b\exp\left(-c\lambda t_0^2\right)\int_{A_2}|t|\,dt \ll \frac{b}{m^2}\exp\left(-c\lambda t_0^2\right) \ll \frac{1}{\sqrt{\lambda}}\frac{b}{n}.$$

We turn our attention to I_3. We first treat the case $m \ge 4$. We have $|G_q(xe^{it})-G_q(x)| \ll b$ for $|t| \le \pi$. By [MP16, Lem. 12],

$$\max_{1/m \le |t| \le \pi} \Re \sum_{j=1}^{m} \frac{x^j(e^{itj}-1)}{j} \le -\frac{1}{4\pi^2}\frac{u^{1-\frac{4}{m+1}}}{\log^2 u} + \frac{2}{m} + \frac{2}{\log u}$$

for $n/m \ge 3$. Hence

$$\begin{aligned} |I_3| &\ll b \max_{1/m \le |t| \le \pi}\left|\exp\left(\sum_{j=1}^{m}\frac{x^j(e^{itj}-1)}{j} - int\right)\right| \\ &\ll b\exp\left(-\frac{1}{4\pi^2}\frac{u^{1-\frac{4}{m+1}}}{\log^2 u} + \frac{2}{m} + \frac{2}{\log u}\right) \\ &= \frac{b}{n\sqrt{\lambda}}\exp\left(\frac{\log\lambda}{2} + \log n - \frac{1}{4\pi^2}\frac{u^{1-\frac{4}{m+1}}}{\log^2 u} + \frac{2}{m} + \frac{2}{\log u}\right). \end{aligned}$$

We want to show that the expression in the exponent is bounded by a constant from above, and then the upper bound for $|I_3|$ will match that of $|I_1|$. The terms $2/m$ and $2/\log u$ are already bounded. The term $\log\lambda/2$ is bounded by $C+(\log mn)/2$ by Lemma 5.2, so it suffices to bound

$$S(m,u) := 2\log m + \frac{3\log u}{2} - \frac{1}{4\pi^2}\frac{u^{1-\frac{4}{m+1}}}{\log^2 u}.$$

We may also assume $n \gg 1$, since otherwise $S(m,u)$ is trivially bounded. As $m \ge 4$, if $4\log u > m+1$ we have

$$S(m,u) \le 2\log m + \frac{3\log u}{2} - \frac{1}{4\pi^2}\frac{u^{1-\frac{4}{5}}}{\log^2 u} \le 2\log(4\log u - 1) + \frac{3\log u}{2} - \frac{1}{4\pi^2}\frac{u^{\frac{1}{5}}}{\log^2 u},$$

which is bounded for $u \ge 3$. If $4\log u \le m+1$ and n is sufficiently large,

$$\frac{1}{4\pi^2}\frac{u^{1-\frac{4}{m+1}}}{\log^2 u} \ge \frac{cu}{\log^2 u} \ge \frac{c\log n\log^3\log(n+1)}{\log^2\log(n+1)} \ge \frac{7\log n}{2} \ge 2\log m + \frac{3\log u}{2}$$

using the condition $m \le n/(\log n\log^3\log(n+1))$, and so $S(m,u) \le 0$. All in all, $S(m,u)$ is bounded. If $1 \le m \le 3$, we run the same argument but with the naive bound $\Re\sum_{j=1}^{m} x^j(e^{itj}-1)/j \le -cn^{1/m}/m$ for $1/m \le |t| \le \pi$ coming from considering only the first term in the sum. In summary,

$$|I_3| \ll \frac{b}{n\sqrt{\lambda}}.$$

By (5.7) and our bounds on I_i, we find that

$$\left|\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable})G_q(x)\right| \ll \frac{D(x)}{\sqrt{\lambda}}\frac{a+bm}{nm}.$$

By (1.15), $D(x)/\sqrt{\lambda} \ll \mathbb{P}(\pi_n \text{ is } m\text{-friable})$, which yields (5.1). □

5.3 Proof of Theorem 1.1

For $m \geq C\sqrt{n\log n}$ this is Theorem 4.1, so it is left to deal with $C\sqrt{n\log n} \geq m \geq 6\log n$. We may assume that $n \gg 1$ due to Proposition 1.5. The condition $C\sqrt{n\log n} \geq m$ implies $n/(\log n \log^2 \log(n+1)), n/3 \geq m$ (for $n \gg 1$), while the condition $m \geq 6\log n$ implies $x = \Theta(1)$ and $m \gg \log u$. Lemma 5.3 now says that $G_q(x) = \Theta(1)$ and also gives upper bounds on $|G_q'(x)|$ and $|G_q''(x)|$. Plugging these in Theorem 5.1, we obtain

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = G_q(x)\left(1+O\left(\frac{\log u}{mq^{\lceil \frac{m+1}{2}\rceil}}\right)\right). \tag{5.10}$$

By (5.3), $G_q(x) = 1+O(u\log u/(mq^{\lceil (m+1)/2\rceil}))$, which yields (1.1). □

5.4 Proof of Theorem 1.2

The condition $8\log n \geq m$ implies $n/(\log n \log^2 \log(n+1)), n/3 \geq m$ as long as n is sufficiently large. In this case, we have by Lemma 5.3 that $1 \leq G_q(x) \leq C_\varepsilon$ and also upper bounds on $|G_q'(x)|$ and $|G_q''(x)|$. Plugging these in Theorem 5.1, we obtain

$$\frac{\mathbb{P}(f_n \text{ is } m\text{-friable})}{\mathbb{P}(\pi_n \text{ is } m\text{-friable})} = G_q(x)\left(1+O_\varepsilon\left(\frac{x^{1+a}}{q^{\lceil \frac{m+1}{2}\rceil}}\right)\right). \tag{5.11}$$

By (5.3), $G_q(x) = 1+O_\varepsilon(ux^{1+a}/q^{\lceil (m+1)/2\rceil})$, which gives (1.2). For bounded n, the required result is immediate from (4.5) and (5.4). □

5.5 Proof of Theorem 1.3

The estimate (1.6) is (5.11) if $m \leq 8\log n$ and is (5.10) otherwise. Estimate (1.5) follows from Theorem 5.1 and Lemma 5.4. It is useful to note that if $m - 2\log_q n \geq 1/\log q$ then $1 - n^{2/m}/q \leq C/m$ and if $m - 2\log_q n \leq -1/\log q$ then $1 - q/n^{2/m} \geq c/m$. □

5.6 Proof of Theorem 1.4

This follows directly from the estimates for $\log G_q(x)$ given in Lemma 5.4. □

6 Proof of Theorem 1.6

We shall utilize identity (1.9). We shall also use the fact that $\mathbb{P}(f_n \text{ is } m\text{-friable}) \geq \mathbb{P}(\pi_n \text{ is } m\text{-friable})$, see Proposition 1.5. For $m = 1$ we have strict inequality.

We first assume $n\log n \leq \log q$. In this range we must prove $c/q^C \leq \mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) \leq C/q^c$. Since $L_q(f_n)$ and $L(\pi_n)$ are bounded from above by n, we can bound the difference $\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n)$ by n times the total variation distance of the two random variables, which is known to be $O(1/q)$ [ABT93, Thm. 6.1] (cf. [BSG18]), so we have

$$\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) = O\left(\frac{n}{q}\right).$$

This shows $\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) \leq \log q/q$. To produce a lower bound, we consider the contribution of 1-friable polynomials and permutations to (1.9):

$$\begin{aligned}\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) \geq \mathbb{P}(f_n \text{ is 1-friable}) - \mathbb{P}(\pi_n \text{ is 1-friable}) &= \frac{\binom{q+n-1}{n}}{q^n} - \frac{1}{n!}\\ &= \frac{1}{n!}\left(\prod_{i=1}^{n}\left(1+\frac{i-1}{q}\right)-1\right) \geq cn^{-n}\frac{n^2}{q} \geq \frac{1}{q^2}.\end{aligned}$$

We turn to the case $n\log n \geq \log q$; we may assume $n \gg 1$. To prove an upper bound, we use Theorems 1.1 and 1.2, and the monotonicity of $\mathbb{P}(f_n \text{ is } m\text{-friable})$ in m to obtain

$$\begin{aligned}\sum_{m=1}^{n}\left(\mathbb{P}(f_n \text{ is } m\text{-friable}) - \mathbb{P}(\pi_n \text{ is } m\text{-friable})\right) &\leq M\mathbb{P}(f_n \text{ is } M\text{-friable}) + \sum_{n\geq m>M}\frac{n\mathbb{P}(\pi_n \text{ is } m\text{-friable})}{mq^{m/2}}\\ &\ll M\mathbb{P}(\pi_n \text{ is } M\text{-friable}) + \frac{n}{q^{M/2}}\end{aligned}$$

for any $M \geq 3\log_q n$. We take $M = \lceil A\sqrt{n\log n/\log q}\rceil$ for large A (admissible if $n \gg 1$). The term $n/q^{M/2}$ is $\leq C\exp(-c\sqrt{n\log n\log q})$. By Proposition 1.8, so is $M\mathbb{P}(\pi_n \text{ is } M\text{-friable})$.

We now prove a lower bound for $\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n)$. Considering only the term $m = M$ in (1.9), and using Theorem 1.3, we obtain

$$\mathbb{E}L_q(f_n) - \mathbb{E}L(\pi_n) \geq \mathbb{P}(\pi_n \text{ is } M\text{-friable})\left(G_q(x) - 1 + O\left(\frac{x^{1+a}\min\{1, \frac{\log u}{M}\}}{q^{\lceil\frac{M+1}{2}\rceil}}\right)\right). \tag{6.1}$$

The term $\mathbb{P}(\pi_n \text{ is } M\text{-friable})$ is $\geq c\exp(-C\sqrt{n\log n\log q})$ by Proposition 1.8. By (5.3),

$$G_q(x) - 1 \geq c\frac{ux^{1+a}\min\{1, \frac{\log u}{M}\}}{q^{\lceil\frac{M+1}{2}\rceil}}. \tag{6.2}$$

As the right-hand side of (6.2) dominates the error term in (6.1) (if $n \gg 1$) and $1/q^{\lceil(M+1)/2\rceil}$ is bounded from below by $c\exp(-C\sqrt{n\log n\log q})$, we conclude the proof. □

7 Deriving Soundararajan's result from Ford's result

7.1 Proof of Proposition 1.8

We will use two results of Hildebrand on ratios of ρ values. By [Hil84, Lem. 1] we have

$$\frac{\rho(u-t)}{\rho(u)} = e^{t\xi}(1+O(u^{-1})) \tag{7.1}$$

uniformly for $0 \le t \le 1$ and $u \ge 1$, where $\xi > 0$ is as in (4.1) and it satisfies $\xi \sim \log u$ by Lemma 4.2. The second result, given in [Hil86, Lem. 1(vi)], states that

$$\frac{\rho(u-t)}{\rho(u)} \ll (u\log^2(u+1))^t \tag{7.2}$$

uniformly for $u \ge 1$ and $0 \le t \le u$. By (1.18), it suffices to show that

$$\rho\left(\frac{n+1}{m+1}\right) - \rho\left(\frac{n}{m}\right) \ll \rho\left(\frac{n}{m}\right)\left(\exp\left(C\frac{u\log(u+1)}{m}\right)-1\right).$$

We express the left-hand side as

$$\int_{\frac{n}{m}}^{\frac{n+1}{m+1}} \rho'(t)dt.$$

As $\rho'(u) = -\rho(u-1)/u$, this is

$$\ll \frac{\rho\left(\frac{n}{m}\right)}{\frac{n}{m}} \int_{\frac{n+1}{m+1}}^{\frac{n}{m}} \frac{\rho(t-1)}{\rho\left(\frac{n}{m}\right)} dt.$$

If u is bounded we are done, because the integral is $\ll_u n/m-(n+1)/(m+1) \ll_u 1/n$. We assume $u \ge 2$. Applying (7.2) with $(u,t) = (u-1,u-t)$, and also invoking (7.1), we see that the last expression is

$$\ll \frac{\rho\left(\frac{n}{m}\right)}{\frac{n}{m}} \int_{\frac{n+1}{m+1}}^{\frac{n}{m}} (u\log^2 u)^{u-t} \frac{\rho(u-1)}{\rho(u)} dt \ll \rho(u)\log u \int_0^{\frac{n-m}{m(m+1)}} (u\log^2 u)^s ds \ll \rho(u)\left((u\log^2 u)^{\frac{u-1}{m}}-1\right),$$

which is $\ll \rho(u)(\exp(Cu\log u/m)-1)$ as needed. □

7.2 Proof of Theorem 1.10

By Theorems 1.1 and 1.2, the required estimate already holds in the range $n \ge m \ge (2+\varepsilon)\log_q n$ (with a better error term). Moreover, for bounded n this is trivial, so we may assume $n \gg 1$. It remains to prove a result in the range $3\log_q n \ge m \ge \log_q(n\log n)$, $n \gg 1$. From this point on we shall assume m lies in the (slightly) wider range $\log_q n < m \le 3\log_q n$, $n \gg 1$, and we shall work out what lower bound on m is needed for our result to hold.

By Theorem 5.1, it suffices to prove the following 3 bounds:

$$\log G_q(x) = \sum_{i>m} \frac{a_i x^i}{i} \ll \frac{u \log u}{m},$$
$$\frac{G_q'(x)x}{nG_q(x)} = \sum_{i>m} \frac{a_i x^i}{n} \ll \exp\left(\frac{Cu\log u}{m}\right),$$
$$\frac{G_q''(x)x^2}{nmG_q(x)} = \frac{1}{nm}\left(\sum_{i>m} a_i x^i\right)^2 + \frac{1}{nm}\sum_{i>m}(i-1)a_i x^i \ll \exp\left(\frac{Cu\log u}{m}\right).$$

In the range $\log_q n < m \le 3\log_q n$ we have $u\log u/m \asymp (n/\log n)\log^2 q$. In particular, $\exp(Cu\log u/m)$ can absorb any power of n, m and q. This allows us to reduce the last 3 inequalities to the following:

$$\begin{aligned} \sum_{2m\ge i>m} a_i x^i &\ll n\log q, \\ \sum_{i>2m} \frac{a_i x^i}{i} &\ll \frac{n\log^2 q}{\log n}, \\ \sum_{i>2m} i a_i x^i &\ll \exp\left(\frac{Cn\log^2 q}{\log n}\right). \end{aligned} \tag{7.3}$$

We will now use freely the bounds $a_i \ll q^{-i/2}, q^{m-i}$, given in (2.6), as well as the estimate $x \le n^{1/m} < q$. To prove the first inequality in (7.3) it suffices to show

$$\sum_{2m\ge i>m}\left(\frac{x}{\sqrt{q}}\right)^i \ll n\log q.$$

If $x \le \sqrt{q}$, this is trivial because the left-hand side is $\le m$. If $x/\sqrt{q}$ is greater then 1.1 then the left-hand side is $\ll x^{2m}/q^m \ll n^2/q^m \le n$. In the remaining case $1 \le x/\sqrt{q} \le 1.1$ the left-hand side is $\ll m(1.1)^{2m} \ll \log n (1.1)^{6\log_q n} \ll n$. Here we used $6\log_q 1.1 < 0.9 < 1$.

We turn our attention to the second inequality in (7.3). It suffices to show

$$\sum_{i>2m} \frac{\left(\frac{x}{q}\right)^i}{i} \ll q^{-m}\frac{n\log^2 q}{\log n}.$$

The left-hand side is $\ll (1-x/q)^{-1}(x/q)^{2m+1}/m \ll (1-x/q)^{-1}n^2/(q^{2m}\log_q n)$, so it suffices to show

$$\left(1-\frac{x}{q}\right)^{-1} \ll \frac{q^m \log q}{n}. \tag{7.4}$$

We write m as $m = \log(nf)/\log q$ for $f \ge 1$. As $x \le n^{1/m}$, it suffices to show

$$1-\exp\left(-\frac{\log q \log f}{\log(nf)}\right) \gg \frac{1}{f\log q}$$

which evidently holds if $f \geq \log n$. We turn our attention to the last inequality in (7.3), which will follow from

$$\sum_{i>2m} \left(\frac{x}{q}\right)^i i \ll \exp\left(\frac{Cn\log^2 q}{\log n}\right).$$

Writing $i = j+2m+1$, the left-hand side is

$$\ll \left(\frac{x}{q}\right)^{2m+1} \sum_{j=0}^{\infty} \left(\frac{x}{q}\right)^j (j+2m+1) \ll \frac{n^2}{q^m}\left(2m\left(1-\frac{x}{q}\right)^{-1} + \left(1-\frac{x}{q}\right)^{-2}\right) \ll n^2\left(1-\frac{x}{q}\right)^{-2}.$$

The required inequality now follows from (7.4), which holds if $m \geq \log(n\log n)/\log q$. □

Appendix

A Limitation to approximation via the Dickman function

We define a quantity $\Delta(n,m)$ by

$$\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \rho(u)(1+\Delta(n,m)).$$

By (1.13), $\Delta(n,m) = O(u\log(u+1)/m)$ if $n\log n \leq m^2$. We prove a matching lower bound.

Theorem A.1. *For $n > m$, $\Delta(n,m) > 0$. If furthermore $m \leq n/2$, then $\Delta(n,m) \gg u\log(u)/m$.*

The inequality $\Delta > 0$ is not new, see [GHS15, Ex. 6]. We expect a similar phenomenon to hold for friable integers, see [Gra08, p. 274]. In the integer setting, an *asymptotic* version of the integer analogue of $\Delta > 0$ is known to hold. De Bruijn [dB51] (cf. Levin and Fainleib [LF67] and Saias [Sai89]) gave an asymptotic series for $\#\{1 \leq n \leq x : n \text{ is } y\text{-friable}\}/x$, whose first term is $\rho(\log x/\log y)$ while the second term is *positive*, namely $(1-\gamma)\rho(\log x/\log y - 1)/\log x$.

Note that if m is close to n, we really do not expect the lower bound in Theorem A.1 to hold, e.g. $\Delta(n,n-1) = O(1/n^2) = o(u\log(u+1)/m)$.

An asymptotic result for Δ was proved by Manstavičius and Petuchovas in [MP16, Cor. 3] in some range. They essentially show that $1+\Delta(n,m) \sim \exp(u\xi/2m)$ for $n^{1/3+\varepsilon} \leq m \leq n^{1-\varepsilon}$, where ξ is as in (4.1). Their proof method is different and is based on expressing the main term $D(x)/\sqrt{2\pi\lambda}$ appearing in (1.15) in terms of ρ.

Our proof is inspired by [Hil84], where Hildebrand was concerned with *upper bounds* on Δ in the integer setting. Ford's inequality (1.18) gives an upper bound on Δ, and we find its proof similar in spirit to [Hil84] as well.

A.1 Preparatory lemmas

Let

$$S_1(n,m) := \frac{1}{u\rho(u)}\left(\frac{1}{m}\sum_{i=1}^{m}\rho\left(u-\frac{i}{m}\right) - \int_0^1 \rho(u-t)dt\right) = \frac{1}{n}\sum_{i=1}^{m}\frac{\rho(u-\frac{i}{m})}{\rho(u)} - 1,$$

where the second equality follows from the identity $\int_0^1 \rho(u-t)dt = u\rho(u)$. Let

$$S_2(n,m) := \frac{1}{n}\sum_{i=1}^{m} \frac{\rho(u-\frac{i}{m})\Delta(n-i,m)}{\rho(u)}.$$

Lemma A.2. *For $n \geq m \geq 1$ we have the relation $\Delta(n,m) = S_1(n,m) + S_2(n,m)$.*

Proof. By differentiating (2.4) and equating coefficients we have, for $n \geq m$,

$$n\mathbb{P}(\pi_n \text{ is } m\text{-friable}) = \sum_{i=1}^{m} \mathbb{P}(\pi_{n-i} \text{ is } m\text{-friable}).$$

Rewriting this in terms of $\Delta(n,m)$ yields the result. □

Lemma A.3. *If $n \geq m \geq 1$ we have $S_1(n,m) \geq 0$ with equality if and only if $n = m$.*

Proof. Since ρ is strictly decreasing for $u \geq 1$, for each $1 \leq i \leq m$ we have

$$\frac{1}{m}\rho\left(u-\frac{i}{m}\right) \geq \int_{(i-1)/m}^{i/m} \rho(u-t)\,dt$$

with equality if and only if $u \leq (i-1)/m+1$. The result follows by summing over $i = 1,\dots,m$. □

Lemma A.4. *For positive x let $F(x) = (1-e^{-x})^{-1} - x^{-1} \geq 1/2$. For $m \leq n/2$ we have*

$$S_1(n,m) = (1+o_{u\to\infty}(1))\frac{\log u}{m}F\left(\frac{\log(u\log u)}{m}\right).$$

Moreover, the $1+o_{u\to\infty}(1)$ term is bounded away from 0 (that is, there is a uniform lower bound).

Proof. We write

$$S_1(n,m) = \frac{1}{u\rho(u)}\sum_{i=1}^{m}\int_{(i-1)/m}^{i/m}\left(\rho\left(u-\frac{i}{m}\right)-\rho(u-t)\right)dt = \frac{-1}{u\rho(u)}\sum_{i=1}^{m}\int_{(i-1)/m}^{i/m}\int_{t}^{i/m}\rho'(u-x)\,dx\,dt.$$

As $\rho'(u) = -\rho(u-1)/u$ and $\rho(u-1) > 0$, this becomes

$$S_1(n,m) = \frac{1+O(u^{-1})}{u^2\rho(u)}\sum_{i=1}^{m}\int_{(i-1)/m}^{i/m}\int_{t}^{i/m}\rho(u-x-1)\,dx\,dt.$$

By applying (7.1) to $\rho(u-x-1)/\rho(u-1)$ and to $\rho(u-1)/\rho(u)$, this is

$$\begin{aligned}
S_1(n,m) &= (1+o_{u\to\infty}(1))\frac{\log u}{u}\sum_{i=1}^{m}\int_{(i-1)/m}^{i/m}\int_{t}^{i/m}(u\log u)^x\,dx\,dt \\
&= \frac{1+o_{u\to\infty}(1)}{\log(u\log u)}\frac{\log u}{u}\sum_{i=1}^{m}\int_{(i-1)/m}^{i/m}((u\log u)^{i/m}-(u\log u)^t)dt \\
&= \frac{1+o_{u\to\infty}(1)}{u}\left(\frac{u\log u-1}{m(1-(u\log u)^{-1/m})}-\frac{u\log u-1}{\log(u\log u)}\right) \\
&= (1+o_{u\to\infty}(1))\frac{\log u}{m}F\left(\frac{\log(u\log u)}{m}\right)
\end{aligned}$$

and the estimate follows. Running the proof when $u \geq 2$ is bounded shows that the term $1+o_{u\to\infty}(1)$ is $\geq c$. □

A.2 Proof of Theorem A.1

Positivity follows by direct induction from Lemmas A.2 and A.3. Suppose $n/2 \geq m$. We introduce

$$a(n) := \frac{\Delta(n,m)}{\log(n/m)/m}$$

which by the recurrence in Lemma A.2 and the estimates (7.1) and Lemma A.4 satisfies the relation

$$a(n) \geq c + \frac{(1+o_{u\to\infty}(1))}{n}\sum_{i=1}^{m} a(n-i)(u\log u)^{i/m}$$

for $n/2 \geq m$. Moreover, $a(n) \gg 1$ by Lemma A.4 and the non-negativity of S_2.

Observe that $\sum_{i=1}^{m}(u\log u)^{i/m} \geq n(1+o_{u\to\infty}(1))$. Hence, if $a(n),\ldots,a(n+m-1) \geq A$ then $a(n+m),\ldots,a(n+2m-1) \geq c + A(1+o_{u\to\infty}(1)) \geq (c/2)+A$ for $u \gg 1$. Iterating this implication yields $a(n) \gg n/m$ for $u \gg 1$, implying $\Delta(n,m) \gg u(\log u)/m$, as needed. □

Acknowledgments

The author thanks Dor Elboim for useful discussions, Kevin Ford, Brad Rodgers, Gérald Tenenbaum for helpful comments on an earlier version of the manuscript and Kannan Soundararajan for kindly sharing his unpublished manuscript. The author would also like to thank the referee for their thorough and careful reading of the manuscript and useful comments which improved the presentation of the results and proofs.

References

[ABT93] Richard Arratia, A. D. Barbour, and Simon Tavaré. On random polynomials over finite fields. *Math. Proc. Cambridge Philos. Soc.*, 114(2):347–368, 1993. 12, 24

[ABT03] Richard Arratia, A. D. Barbour, and Simon Tavaré. *Logarithmic combinatorial structures: a probabilistic approach*. EMS Monographs in Mathematics. European Mathematical Society (EMS), Zürich, 2003. 2

[AM15] Tewodros Amdeberhan and Victor Moll. Involutions and their progenies. *J. Comb.*, 6(4):483–508, 2015. 2

[BP98] Renet Lovorn Bender and Carl Pomerance. Rigorous discrete logarithm computations in finite fields via smooth polynomials. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 221–232. Amer. Math. Soc., Providence, RI, 1998. 2, 8

[BSG18] Lior Bary-Soroker and Ofir Gorodetsky. Roots of polynomials and the derangement problem. *Amer. Math. Monthly*, 125(10):934–938, 2018. 24

[Car87] Mireille Car. Théorèmes de densité dans $\mathbf{F}_q[X]$. *Acta Arith.*, 48(2):145–165, 1987. 6

[CHM51] S. Chowla, I. N. Herstein, and W. K. Moore. On recursions connected with symmetric groups. I. *Canad. J. Math.*, 3:328–334, 1951. 2

[dB51] N. G. de Bruijn. On the number of positive integers $\leq x$ and free of prime factors $> y$. *Nederl. Acad. Wetensch. Proc. Ser. A.*, 54:50–60, 1951. 9, 27

[Dic30] Karl Dickman. On the frequency of numbers containing prime factors of a certain relative magnitude. *Ark. Mat. Astron. Fys.*, 22 A(10):14, 1930. 6

[dlBT17] Régis de la Bretèche and Gérald Tenenbaum. Une nouvelle approche dans la théorie des entiers friables. *Compos. Math.*, 153(3):453–473, 2017. 8

[EG22] Dor Elboim and Ofir Gorodetsky. Uniform estimates for almost primes over finite fields. *Proc. Amer. Math. Soc.*, 150(7):2807–2822, 2022. 2

[Enn69] Veikko Ennola. On numbers with small prime divisors. *Ann. Acad. Sci. Fenn. Ser. A I No.*, 440:16, 1969. 8

[For22] Kevin Ford. Cycle type of random permutations: a toolkit. *Discrete Anal.*, 2022:9, 36 pp. 2, 8

[FT91] É. Fouvry and G. Tenenbaum. Entiers sans grand facteur premier en progressions arithmetiques. *Proc. London Math. Soc. (3)*, 63(3):449–494, 1991. 7

[GG97] S. W. Golomb and P. Gaal. On the number of permutations of n objects with greatest cycle length k. In *Probabilistic methods in discrete mathematics (Petrozavodsk, 1996)*, pages 211–218. VSP, Utrecht, 1997. 5

[GHS15] Andrew Granville, Adam J. Harper, and Kannan Soundararajan. Mean values of multiplicative functions over function fields. *Res. Number Theory*, 1:Paper No. 25, 18, 2015. 8, 27

[Gon44] V. Goncharov. Über das Gebiet der kombinatorischen Analysis. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 8:3–48, 1944. 2, 6

[Gor17] Ofir Gorodetsky. A polynomial analogue of Landau's theorem and related problems. *Mathematika*, 63(2):622–665, 2017. 2

[Gra08] Andrew Granville. Smooth numbers: computational number theory and beyond. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 267–323. Cambridge Univ. Press, Cambridge, 2008. 7, 8, 9, 27

[Ha14] Junsoo Ha. *Some Problems in Multiplicative Number Theory*. ProQuest LLC, Ann Arbor, MI, 2014. Thesis (Ph.D.)–Stanford University. 2

[Hil84] Adolf Hildebrand. Integers free of large prime factors and the Riemann hypothesis. *Mathematika*, 31(2):258–271 (1985), 1984. 4, 7, 14, 25, 27

[Hil86] Adolf Hildebrand. On the number of positive integers $\leq x$ and free of prime factors $> y$. *J. Number Theory*, 22(3):289–307, 1986. 4, 9, 25

[HT86] Adolf Hildebrand and Gérald Tenenbaum. On integers free of large prime factors. *Trans. Amer. Math. Soc.*, 296(1):265–290, 1986. 4, 7, 11

[JL06] Antoine Joux and Reynald Lercier. The function field sieve in the medium prime case. In *Advances in cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, pages 254–270. Springer, Berlin, 2006. 2, 8

[KM97] A. Knopfmacher and E. Manstavičius. On the largest degree of an irreducible factor of a polynomial in $\mathbb{F}_q[X]$. *Lith. Math. J.*, 37(1):38–45, 1997. 5, 9

[LF67] B. V. Levin and A. S. Fainleib. Application of some integral equations to problems of number theory. *Russ. Math. Surv.*, 22(3):119–204, 1967. 27

[Lov92] Renet Lovorn. *Rigorous, subexponential algorithms for discrete logarithms over finite fields*. ProQuest LLC, Ann Arbor, MI, 1992. Thesis (Ph.D.)–University of Georgia. 2, 7

[Man92a] E. Manstavičius. Remarks on elements of semigroups that are free of large prime factors. *Liet. Mat. Rink.*, 32(4):512–525, 1992. 2, 6, 7, 8, 9, 11

[Man92b] E. Manstavičius. Semigroup elements free of large prime factors. In *New trends in probability and statistics, Vol. 2 (Palanga, 1991)*, pages 135–153. VSP, Utrecht, 1992. 2, 7, 8, 11

[MP16] Eugenijus Manstavičius and Robertas Petuchovas. Local probabilities for random permutations without long cycles. *Electron. J. Combin.*, 23(1):Paper 1.58, 25, 2016. 2, 6, 7, 8, 11, 15, 16, 18, 22, 27

[MW55] Leo Moser and Max Wyman. On solutions of $x^d = 1$ in symmetric groups. *Canadian J. Math.*, 7:159–168, 1955. 2

[Odl85] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In *Advances in cryptology (Paris, 1984)*, volume 209 of *Lecture Notes in Comput. Sci.*, pages 224–314. Springer, Berlin, 1985. 2, 7

[Odl94] A. M. Odlyzko. Discrete logarithms and smooth polynomials. In *Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993)*, volume 168 of *Contemp. Math.*, pages 269–278. Amer. Math. Soc., Providence, RI, 1994. 8

[Odl00] Andrew Odlyzko. Discrete logarithms: the past and the future. volume 19, pages 129–145. 2000. Towards a quarter-century of public key cryptography. 8

[PGF98] Daniel Panario, Xavier Gourdon, and Philippe Flajolet. An analytic approach to smooth polynomials over finite fields. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 226–236. Springer, Berlin, 1998. 2, 6, 8, 10

[Pol13] Paul Pollack. Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 22:70–78, 2013. 12

[Sac07] V. N. Sachkov. Asymptotic formulas and limit distributions for combinatorial configurations generated by polynomials. *Diskret. Mat.*, 19(3):3–14, 2007. 2

[Sai89] Eric Saias. Sur le nombre des entiers sans grand facteur premier. *J. Number Theory*, 32(1):78–99, 1989. 7, 11, 27

[Sch02] Oliver Schirokauer. The special function field sieve. *SIAM J. Discrete Math.*, 16(1):81–98, 2002. 8

[SL66] L. A. Shepp and S. P. Lloyd. Ordered cycle lengths in a random permutation. *Trans. Amer. Math. Soc.*, 121:340–357, 1966. 2

[Sou] K. Soundararajan. Smooth polynomials: analogies and asymptotics. Unpublished manuscript. 2, 3, 8

[Sta99] Richard P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin. 12

[Ten01] Gérald Tenenbaum. Review of the article "An analytic approach to smooth polynomials over finite fields" by D. Panario, X. Gourdon and P. Flajolet. *Mathematical Reviews*, MR1726074, 2001. 10

[Ten15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion. 6, 10, 14

[Tim08] A. N. Timashov. Random permutations with cycle lengths in a given finite set. *Diskret. Mat.*, 20(1):25–37, 2008. 2

[War91] R. Warlimont. Arithmetical semigroups. II. Sieving by large and small prime elements. Sets of multiples. *Manuscripta Math.*, 71(2):197–221, 1991. 2, 6, 8

[Wil06] Herbert S. Wilf. *generatingfunctionology*. A K Peters, Ltd., Wellesley, MA, third edition, 2006. 2

[WZ85] Jet Wimp and Doron Zeilberger. Resurrecting the asymptotics of linear recurrences. *J. Math. Anal. Appl.*, 111(1):162–176, 1985. 2

AUTHOR

Ofir Gorodetsky
Mathematical Insitute, University of Oxford
Oxford, OX2 6GG, UK
ofir [dot] goro [at] gmail [dot] com