On the distribution of polynomials having a given number of irreducible factors over finite fields

Arghya Datta

Abstract

Let $q \geq 2$ be a fixed prime power. We prove an asymptotic formula for counting the number of monic polynomials that are of degree $n$ and have exactly $k$ irreducible factors over the finite field $\mathbb{F}_q$. We also compare our results with the analogous existing ones in the integer case, where one studies all the natural numbers up to $x$ with exactly $k$ prime factors. In particular, we show that the number of monic polynomials grows at a surprisingly higher rate when $k$ is a little larger than $\log n$ than what one would speculate from looking at the integer case.

Keywords: Polynomials over finite field, Fixed number of irreducible factors, Selberg–Delange method, Multiplicative functions, Saddle point approximation

Mathematics Subject Classification: 11T06, 11N37, 11T55, 11N56

1 Introduction

How many integers are there up to 1000 billion (or any large number) with exactly 2022 (or any given integer) prime factors? This exciting question fascinated mathematicians for ages. Gauss initially started the investigation and the question was later pursued by several eminent mathematicians, including Landau, Hardy and Ramanujan, Sathe and Selberg. Thanks to their compound effort, we entirely understand these answers in the integer setting. The main goal of this work is to study the analogous question for polynomials over finite fields. We begin our discussion with a brief historical interlude and then state our main results.

Let $m \leq x$ be positive integers and $\Omega(m)$ denotes the number of prime factors counted with multiplicity that divide $m$. In 1900, Landau [6] showed using the prime number theorem that for $k \in \mathbb{N}$ fixed we have

$$\Pi(x, k) \sim \frac{x}{\log x} \frac{\left(\log \log x\right)^{k-1}}{(k-1)!},$$

where

$$\Pi(x, k) := \# \left\{ m \leq x : \Omega(m) = k \right\}.$$
The above result was predicted by Gauss [4] long ago. However, understanding the asymptotic behaviour of \( \Pi(x, k) \) for growing \( k \) uniformly with \( x \) remained an open problem for a long time.

In 1953, Sathe [10] ingeniously showed that if \( \epsilon \in (0, 2) \) is given, then uniformly for \( 1 \leq k \leq (2 - \epsilon) \log \log x \) we have

\[
\Pi(x, k) \sim F \left( \frac{k}{\log \log x} \right) \frac{(\log \log x)^{k-1}}{(k-1)!} \frac{x}{\log x},
\]

where

\[
F(z) = \frac{1}{\Gamma(z + 1)} \prod_p \left( 1 - \frac{1}{p} \right)^z \left( 1 - \frac{z}{p} \right)^{-1} (|z| < 2).
\]

This beautiful result was further extended by Selberg [11] when \( k \) is a little larger and varies uniformly in a slightly wider range \((2 + \epsilon) \log \log x \leq k \leq B^* \log \log x\), where \( B^* > 2 \) is a real constant. In his paper Selberg only discussed the main ideas behind the proof. He observed a significant change in the asymptotic behaviour of \( \Pi(x, k) \). He showed for this range we have

\[
\Pi(x, k) \sim Cx \log \left( \frac{x}{2^k} \right),
\]

where \( C \) is an absolute constant. Finally Nicolas [7] settled this question for the entire range \((2 + \epsilon) \log \log x \leq k < \log x / \log 2 \) by proving the same asymptotic result holds as (2) in this range. Unlike the previous attempts his main idea behind the proof was less analytic and more of combinatorial nature.

As mentioned earlier, we will be working in the polynomial ring \( \mathbb{F}_q[t] \). Henceforth \( q \) is assumed to be fixed and all the implied constants are allowed to depend on \( q \). For an easy reference later on, we employ some standard notation that will be used throughout the paper.

### 1.1 Notation

We set

\[
\mathcal{M} := \{ \text{set of all monics in } \mathbb{F}_q[t] \},
\]

\[
\mathcal{M}_n := \{ \text{set of all monics in } \mathbb{F}_q[t] \text{ having no root in } \mathbb{F}_q \},
\]

\[
\mathcal{P} := \{ \text{set of all monic irreducibles in } \mathbb{F}_q[t] \}.
\]

Let \( \mathcal{M}_n \) consist of only those monics that have degree \( n \) and similarly we define \( \mathcal{M}_n, \mathcal{P}_n \).

Let \( \mathcal{P}_{\geq j} \) denote the set of all monic irreducibles whose degree is at least \( j \).

Given \( f \in \mathbb{F}_q[t] \), let \( \Omega(f) \) denote the number of irreducible polynomials counted with multiplicity that divide \( f \). We also set

\[
N(n, k) := \# \{ f \in \mathcal{M}_n : \Omega(f) = k \},
\]

\[
N'(n, k) := \# \{ f \in \mathcal{M}_n : \Omega(f) = k \}.
\]

As discussed initially, we are interested in understanding the object \( N(n, k) \) for different ranges of \( k \). Surprisingly one of our main results reveals that the situation in \( \mathbb{F}_q[t] \) is quite
different than what one could naively guess from the knowledge in the integer case. This is remarkable since these two worlds are significantly different in only a few instances.

We first give a proof of (1) in the context of polynomials. The result was first proved in Warlimont [13] and Carr [2], and it was generalized in a recent work [3], which is uniform in both parameters $n$ and $q$. However, $q$ remains fixed for our purposes and we sketch a proof of Warlimont’s result for completeness and the techniques we discuss are tailored in a way that will naturally extend to our main result which is Theorem 1.2.

**Theorem 1.1** Given $\epsilon \in (0, q)$, then uniformly for $1 \leq k \leq (q - \epsilon) \log n$ we have

$$N(n, k) \sim \frac{q^n}{n} H \left( \frac{k}{\log n} \right) \left( \frac{\log n}{k - 1} \right)^{k-1},$$

where

$$H(z) = \frac{1}{\Gamma(z + 1)} \prod_{p \in \mathbb{P}} \left( 1 - \frac{1}{q^{\deg(p)}} \right)^z \left( 1 - \frac{z}{q^{\deg(p)}} \right)^{-1}$$

for $|z| < q$.

We may notice that the expression for the function $H$ is quite similar to $F$ in the integer case. The appearance of $q^n/n$ is also no surprise as letting $q^n/n \approx x$ yields $q^n/n \approx x/\log x$ up to constant factors. While the above result is more or less an application of the Selberg–Delange method developed in [8], the following surprising outcome of our work is where a substantial amount of new techniques goes in.

We would like to mention that Hwang [5] considered the object $N(n, k)$ for the entire range $1 \leq k \leq n$. We reproduce similar results but using a completely different approach. We consider a mild restriction on the range of uniformity of $k$ but this assumption allows us to obtain a result that has a considerably simpler shape (only in terms of elementary functions) compared to Hwang. Hwang considered the following decomposition $\Omega(f) = \Omega^{(1)}(f) + \Omega^{(2)}(f)$, where $\Omega^{(1)}(f)$ and $\Omega^{(2)}(f)$ denote the number of monic irreducible factors of $f$ of degree $\geq 2$ and $= 1$. Roughly speaking, Hwang showed that if $f \in \mathbb{M}_n$ is chosen uniformly at random then the object $\Omega^{(1)}$ is Poisson distributed while $\Omega^{(2)}$ follows a negative binomial distribution. Hwang then looks at the sum of these two random objects and studies their convolution law for different ranges of $k$. He showed that if $k$ is small, i.e. $1 \leq k \leq (q - \epsilon) \log n$, then the behaviour of $\Omega = \Omega^{(1)} + \Omega^{(2)}$ is dominated by the $\Omega^{(1)}$ component and thus resulting an approximate Poisson distribution (as obtained by Warlimont earlier)

$$\mathbb{P}(\Omega = k) \sim H \left( \frac{k}{\log n} \right) \left( \frac{\log n}{k - 1} \right)^{k-1} \frac{1}{n}.$$

On the other hand, if $k$ is “largish” and in particular $k/\log n \to \infty$, then the sum $\Omega$ is considerably inflated by the component $\Omega^{(2)}$ resulting a significant change in the final asymptotic. Contrary to Hwang’s probabilistic approach, our line of attack uses a crucial combinatorial decomposition identity from [7] in the context of polynomials.

It is worthwhile to mention that similar studies concerning the function $\omega(f)$ instead of $\Omega(f)$ can be found in [1].

**Theorem 1.2** Let $B \geq 2$ be a real constant and $q > 2$ be a prime power. Let $\xi : \mathbb{N} \to \mathbb{R}$ be a function such that $\xi(n) \to \infty$ however slowly as $n \to \infty$. Then uniformly for $\xi(n) \log n \leq$
Given $k \leq n/B$, we have
\[ N(n, k) \sim C(q) q^{n_k q^{-1}(n - k)^{q^{-1}}}, \]
where
\[ C(q) = \frac{1}{((q - 1)q)^2} \left(1 - \frac{1}{q}\right)^q \prod_{p \in \mathcal{P} \geq 2} \left(1 - \frac{1}{q^{\deg(p)-1}}\right)^{-1} \left(1 - \frac{1}{q^{\deg(p)}}\right)^q, \]
a constant that depends only on $q$.

Here “however slowly” means that $\xi(n)$ could be any function that grows to infinity with an additional constraint that $\xi$ is sufficiently small so that the interval $[\lfloor \xi(n) \log n, n/B \rfloor]$ contains at least one integer for $n$ sufficiently large. We remind the reader that $x/2^k$ is replaced by $q^n/q^k$ as was expected. The appearance of $(n - k)$ is not also surprising in light of the main theorem proved in [7] and (2) where a factor of $\log (x/2^k)$ is present in the statement. However, the extra factor $k^{q-1}$ and also the presence of higher powers of $(n - k)$ are what seem surprising at the moment, which shows $N(n, k)$ grows at a much larger rate than what we would predict from (2).

We note Theorem 1.2 is valid for $q \neq 2$. However, the result is still true (see [5, Corollary 3]) for $q = 2$, but our methods do not cover this particular instance for technical reasons. We will discuss this technical restriction in the proof of Proposition 4.7. (see Remark 4.8)

Also, there is a slight gap between the upper bound of $k$ in Theorem 1.1 and the lower bound of $k$ in Theorem 1.2. While it is fairly easy to prove an upper bound of the shape $N(n, k) \ll q^{n-k}q^{k-1}(n - k)^{q-1}$ in the intermediate range $q \log n \leq k \ll \log n$ using the ideas in Proposition 4.7, it seems difficult to obtain any meaningful and “simple to state” lower bound for that range, which is expected in light of the complicated transitional behaviour of $N(n, k)$ sketched in [5, Corollary 2]. The proofs of the above theorems are discussed in detail in the following sections. The main ingredients are the following two key propositions.

**Proposition 1.3** For all $\epsilon \in (0, q)$ and uniformly for $|z| \leq q - \epsilon$ we have
\[ M_z(n) := \sum_{f \in \mathcal{M}_n} z^{\Omega(f)} = q^n n^{q - 1} \left\{ zH(z) + O_\epsilon \left(\frac{1}{n}\right) \right\}, \]
with $H(z)$ as described in Theorem 1.1.

**Proposition 1.4** For all $\delta \in (0, 1)$ and uniformly for $|z| \leq q^2 - \delta$ we have
\[ \tilde{M}_z(n) := \sum_{f \in \tilde{\mathcal{M}}_n} z^{\Omega(f)} = q^n n^{q - 1} \left\{ z h(z) + O_\delta \left(\frac{1}{n}\right) \right\}, \]
where $h(z) = \frac{1}{\Gamma(z + 1)} \left(1 - \frac{1}{q}\right)^{qz} \prod_{p \in \mathcal{P} \geq 2} \left(1 - \frac{z}{q^{\deg(p)}}\right)^{-1} \left(1 - \frac{1}{q^{\deg(p)}}\right)^z$, an analytic function for $|z| < q^2$.

The connection between Theorem 1.1 and Proposition 1.3 becomes clear once we notice $N(n, k)$ is precisely given by the coefficient of $z^k$ in $M_z(n)$. In other words, if we could extract the information about $N(n, k)$ from $M_z(n)$, we would have our result. Furthermore, we
note that $M_z(n)$ is a polynomial in $z$ of degree at most $n$ and therefore, we could hope to study the coefficients using Cauchy's integral formula. This is going to be our main strategy to attack Theorem 1.1. The connection between $\tilde{M}_z(n)$ and Theorem 1.2 is not as immediate as the previous case since the coefficient of $z^k$ in $\tilde{M}_z(n)$ is $N'(n, k)$ and not $N(n, k)$. As we shall see, in Sect. 4 the two objects $N(n, k)$ and $N'(n, k)$ are intimately entangled, and information about one could be transferred into another. Also, one can check the relation $C(q) = qh(q)/(q - 1)!$ holds.

2 Set-up and the proof of Proposition 1.3

2.1 Preparatory results for Proposition 1.3

In this subsection we aim to develop the framework for a Selberg–Delange type argument that will be used to establish Proposition 1.3. As already discussed we are interested in the quantity

$$M_z(n) := \sum_{f \in \mathcal{M}_n} z^\Omega(f) = \sum_{k \geq 0} z^k N(n, k).$$

We also want to introduce an auxiliary quantity

$$G_z(u) = \sum_{f \in \mathcal{M}} z^\Omega(f) u^{\deg(f)} = \prod_{p \in \mathcal{P}} \left(1 - zu^{\deg(p)}\right)^{-1}. \quad (3)$$

The function $G_z(u)$ defines an analytic function since the Euler product converges uniformly on the compact subsets of the region defined by $|u| < \min \{|z|^{-1}, q^{-1}\}$ which we argue now.

We recall a key result from complex analysis (see [9, Theorem 15.4]) that says if a sequence of bounded complex functions $\{f_n(z)\}$ on a set $S$ is such that $\sum_{n \geq 1} |f_n(z)|$ converges uniformly on $S$, then the product $P(z) = \prod_{n \geq 1} (1 + f_n(z))$ converges uniformly and consequently defines a holomorphic function on $S$, and $P(z_0) = 0$ at some point $z_0 \in S$ if and only if $f_n(z_0) = -1$ for some $n$. The same result also applies to a sequence of bounded complex functions of two complex variables $\{f_n(z, u)\}$ where holomorphicity simply means holomorphic in each variable.

Using the above result we see the product in (3) converges uniformly on the compact subsets of the region $0 < |u| < q^{-1}$. Indeed we have

$$\sum_{p \in \mathcal{P}} |zu^{\deg(p)}| \leq \sum_{p \in \mathcal{P}} |u|^{\deg(p) - 1} \quad (|uz| < 1).$$

$$\leq q + \sum_{p \in \mathcal{P}, p \geq 2} |u|^{\deg(p) - 1}$$

$$\leq q + \sum_{n=2}^{\infty} q^n |u|^{n-1} \quad \text{(since \#P_n \leq q^n)}$$

$$\leq q + \frac{1}{|u|} \sum_{n=2}^{\infty} |qu|^n < \infty \quad (|qu| < 1), \quad (4)$$

where the finite quantity $\sum_{n=2}^{\infty} q^n |u|^{n-1}$ depends only on the chosen compact subset of the region $0 < |u| < q^{-1}$, but not on the point $(u, z)$. Finally we check that

$|1 - zu^{\deg(p)}| \geq 1 - |zu^{\deg(p)}| \geq 1 - |zu| > 0,$

showing there is no pole in the concerned region.
Our job is to understand $M_z(n)$, which is precisely given by the coefficient of $u^n$ in the power series of $G_z(u)$. Hence information about $M_z(n)$ can be obtained from $G_z(u)$ by applying Cauchy’s integral formula. We took this leap from $M_z(n)$ to $G_z$ because it seems to have a nicer arithmetic structure (i.e. an Euler product expansion), making it more amenable from the analytic point of view. Therefore it is natural to seek to meromorphically extend $G_z(u)$ beyond the region of absolute convergence discussed above to collect the contribution coming from the singularity of $G_z$ in the extended domain. We do this job by introducing another function $F_z(u)$ via the Euler product

$$F_z(u) = \prod_{p \in \mathcal{P}} \left(1 - zu^{\deg(p)}\right)^{-1} \left(1 - u^{\deg(p)}\right)^z.$$  

(5)

We intend to analyze the above Euler product in the following open region and show it is holomorphic.

$$\mathcal{R} := \left\{(u, z) \in \mathbb{C}^2 : |z| < q, |u| < |z|^{-1}, |u| < q^{-1/2}\right\} \subset \mathbb{C}^2.$$  

The following lemma shows $F_z(u)$ does converge uniformly on the compact subsets of $\mathcal{R}$ which is what we wanted to establish.

**Lemma 2.1** We have that $F_z(u)$ defined in (5) converges uniformly on the compact subsets of $\mathcal{R}$ and hence defines a holomorphic function in the sense of two complex variables.

**Proof** We take the standard branch of complex logarithm defined over $\mathbb{C} \setminus (-\infty, 0]$. Since $|u|^n, |zu^n| < 1$ we could make use of their Taylor series and write

$$z \log(1 - u^n) - \log(1 - zu^n) = -zu^n + O\left(|zu^{2n}|\right) + zu^n + O\left(|z^2u^{2n}|\right)$$

$$= O\left(|q^2u^{2n}|\right) \ (|z| < q)$$  

(6)

and hence using $\exp(O(x)) = 1 + O(x)$ for $x = O(1)$ we get

$$(1 - u^n)^z(1 - zu^n)^{-1} = 1 + O\left(|q^2u^{2n}|\right).$$

We now observe the product in (5) converges uniformly in the compact subsets of $\mathcal{R}$. Since $\#\mathcal{P}_n \leq q^n$, we have that

$$\sum_{p \in \mathcal{P}} |u|^{2n} \leq \sum_{n \geq 1} |qu^2|^n < \infty,$$

where the finite quantity $\sum_{n \geq 1} |qu^2|^n$ depends on the chosen compact subset of $\mathcal{R}$, but is independent of the point $(u, z)$.  

We recall the Riemann zeta function in the context of polynomials over finite field, defined for $|u| < q^{-1}$

$$\zeta(u) = \frac{1}{1 - qu} = \prod_{p \in \mathcal{P}} \left(1 - u^{\deg(p)}\right)^{-1}.$$  

As we can see $\zeta(u)$ can be continued meromorphically on $\mathbb{C}$ with a simple pole at $u = 1/q$. Furthermore considering the Euler products in (3) and (5) we can connect $G_z(u)$ and $F_z(u)$ in the following way whenever $|u| < \min \left\{|z|^{-1}, q^{-\frac{1}{2}}\right\}$

$$G_z(u) = \zeta(u)^z F_z(u).$$  

(7)

We are now in a position to prove our first Proposition. However, first, we want to record the following estimate [8, Lemma 1], which is going to be helpful in the further calculation of the contribution that comes from the singularity of $G_z(u)$ at $u = 1/q$ (Fig. 1).
Lemma 2.2 Let $A, \delta > 0$. Let $\mathcal{H}$ be the Hankel contour of radius 1 around 0 going in clockwise direction along the negative real axis to $-n\delta$. Then uniformly for $|z| \leq A$ we have that

\[
\frac{1}{2\pi i} \int_{\mathcal{H}} w^z \left(1 - \frac{w}{n}\right)^{-1} = -\frac{1}{\Gamma(-z)} + O_{\delta, A} \left(\frac{1}{n}\right).
\]
2.2 Deduction of Proposition 1.3

Proof of Proposition 1.3 Let $|u| = r < q^{-1}$ (small green circle in Fig. 2). Using Cauchy’s integral formula on (3) we get for each fixed $z$ satisfying the hypothesis $|z| \leq q - \epsilon$,

$$M_z(n) = \frac{1}{2\pi i} \int_{|u|=r} G_z(u) \frac{du}{u^{n+1}} = \frac{1}{2\pi i} \int_{|u|=r} \zeta(u)^{2} F_z(u) \frac{du}{u^{n+1}}. \quad (8)$$

We wish to get past the point $u = 1/q$ so that we could collect the contribution coming from the singularity of $\zeta(u)$ there. To be specified shortly, we shift the smaller (green) circle $|u| = r$ to a bigger circle (black) $|u| = q^{-1} + \eta$ and a portion of a Hankel contour (red) around the point $q^{-1}$ (Fig. 2). Let $\mathcal{H}'$ be the contour that consists of a circle of radius $(qn)^{-1}$ traversed clockwise around $q^{-1}$ and the two line segments on the ray 0 to $q^{-1}$ joining this small circle to the bigger circle $|u| = q^{-1} + \eta$ where $\eta > 0$ is a fixed number. However we must have $q^{-1} + \eta < q^{-\frac{1}{2}}$ as we cannot go beyond the region $\mathcal{R}$ in (7) where $G_z(u)$ makes sense. We recall that $|z| \leq (q - \epsilon)$ inside $\mathcal{R}$ while performing the above integral. Keeping this in mind we get another constraint on $\eta$, $|uz| \leq ((q^{-1} + \eta)(q - \epsilon)) \leq 1$. This shows taking any $0 < \eta < \min\{1/(q - \epsilon) - 1/q, 1/\sqrt{q} - 1/q\}$ suffices. We then plan to use Lemma 2.2 to evaluate the integral in (8) with $\eta = \min\{1/(q - \epsilon) - 1/q, 1/\sqrt{q} - 1/q\}/2$ for $|z| \leq q - \epsilon$. We observe that for $z$ fixed, $F_z(u)$ and $\zeta(u)$ are both analytic in an open neighbourhood containing the circle $|u| = q^{-1} + \eta$ which is compact. This implies $F_z(u)$, $\zeta(u)$ and hence $G_z(u)$ are uniformly bounded (bound depends on $q, \eta$) on this circle. Thus we obtain

$$M_z(n) = \frac{1}{2\pi i} \int_{\mathcal{H}'} G_z(u) \frac{du}{u^{n+1}} + O\left(\int_{|u|=\frac{1}{q} + \eta} |G_z(u) \frac{du}{u^{n+1}}|\right) := I + O_q, \epsilon\left(\frac{q^n}{(1 + q\eta)^n}\right),$$

where at the last step we used the fact that, $\int_{|u|=R} |du/u^{n+1}| = \frac{1}{R^{n+1}} \int_{|u|=R} |du| = 2\pi/R^n$ and the big-O-uniform bound here depends only on $q$ and $\eta$ while $\eta$ according our choice depends only on $q$ and $\epsilon$. Now we focus on the integral $I$.

Analyticity of $F_z$ near $q^{-1}$ allows us to consider the Taylor series around $q^{-1}$ and write

$$F_z(u) = F_z(1/q) + a_1 (u - 1/q) + a_2 (u - 1/q)^2 + \cdots$$

Hence we have that

$$I = F_z\left(\frac{1}{q}\right) \frac{1}{2\pi i} \int_{\mathcal{H}'} \zeta(u)^{2} \frac{du}{u^{n+1}} + O\left(\int_{\mathcal{H}'} \left|\zeta(u)^{2} \frac{du}{u^{n+1}}\right|\right).$$

We use a change of variable so that our contour $\mathcal{H}'$ transforms to $\mathcal{H}$ and we could then use our Lemma 2.2. The change of variable is given by, $w = n(1 - uq) \implies u = 1/q (1 - w/n)$. We can quickly check the transformation is indeed a valid one. If $u$ is parameterized by $u = 1/q + (1/qn)e^{-t}$, $t \in [\epsilon', 2\pi - \epsilon']$ for some small enough $\epsilon' > 0$ near the tiny circle around $1/q$ then $w = -e^{-u}$ is a circle revolving around 0 of radius 1 in the clockwise direction and similarly, the horizontal ray part also gets reflected, transforming $\mathcal{H}'$ into $\mathcal{H}$. Since $|u|$ goes up to $1/q + \eta$, we have $w$ going up to $-n\delta$ with $\delta = nq$. We note for this change of variable $du = -dw/nq$. First we show the alleged error term is small. The $O$-term is
\[ \ll q \int_{H'} \left| \frac{(1 - qu) du}{u^{n+1}(1 - qu)^2} \right| = \int_{H} \left| \frac{1}{\left( \frac{w}{n} \right)^{z-1} \frac{1}{q^{n+1}} (1 - \frac{w}{n})} \right| \frac{-dw}{nq} \]

\[ = \frac{q^n}{n} \int_{H} \left| \frac{1}{\left( \frac{w}{n} \right)^{z-1} (1 - \frac{w}{n})^{n+1}} \right| \quad \text{(using Lemma 2.2)} \]

\[ \ll q^n n^{R(z) - 2}. \quad (9) \]

Now, we evaluate the main term using Lemma 2.2

\[ F_z \left( \frac{1}{q} \right) \frac{1}{2\pi i} \int_{H'} \zeta(u) \frac{du}{u^{n+1}} = F_z \left( \frac{1}{q} \right) \frac{1}{2\pi i} \int_{H'} \frac{1}{(1 - qu)^2} \frac{du}{u^{n+1}} \]

\[ = F_z \left( \frac{1}{q} \right) q^n \frac{1}{2\pi i} \int_{H} \frac{1}{\left( \frac{w}{n} \right)^{z-1}} \left( 1 - \frac{w}{n} \right)^{-n+1} \frac{-dw}{nq} \]

\[ = F_z \left( \frac{1}{q} \right) q^n n^{z-1} \left( \frac{1}{\Gamma(z)} + O \left( \frac{1}{n} \right) \right). \quad (10) \]

Hence we have that

\[ M_z(n) = F_z \left( \frac{1}{q} \right) \frac{q^n n^{z-1}}{\Gamma(z)} + O \left( q^n n^{R(z) - 2} \right) = q^n n^{z-1} \left\{ zH(z) + O \left( \frac{1}{n} \right) \right\}, \quad (11) \]

where \( H(z) = \frac{1}{\Gamma(z+1)} F_z \left( \frac{1}{q} \right) \) is an analytic function for \(|z| < q\). \hfill \square

3 Deduction of Theorem 1.1

With Proposition 1.3 at our disposal, we are now ready to prove Theorem 1.1. We also note three other straightforward results which will help us do so. We will verify the following claims in the “Appendix A”.

**Lemma 3.1** For \( t \in [-\pi, \pi] \) we have \( \cos t - 1 \leq -\frac{t^2}{2} \) and \( |1 - e^{it}|^2 \leq t^2 \).

**Lemma 3.2** We have the following upper bound

\[ \int_{|z|=r} |n^{z-t}| |dz| \ll \frac{r}{\sqrt{j}}, \]

where \( j = r \log n \).

**Lemma 3.3** We have the following estimate

\[ \int_{-\infty}^{\infty} \theta^2 \exp \left( -\frac{k\theta^2}{5} \right) d\theta \ll k^{-\frac{3}{2}}. \]

**Proof** Deduction of Theorem 1.1 We plan to recover \( N(n, k) \) with another application of Cauchy’s integral formula

\[ N(n, k) = \frac{1}{2\pi i} \int_{|z|=\frac{k}{\log n}} M_z(n) \frac{dz}{z^{k+1}}. \quad (12) \]
Given $\epsilon \in (0, q)$ by the hypothesis of Theorem 1.1, from (11) we see the main term of $M_z(n)$ which is $F_z \left( \frac{1}{q} \right) q^n n^{r-1}/z^k$ is analytic in the disk $|z| = r = k/\log n \leq (q - \epsilon)$ since $F_z \left( \frac{1}{q} \right)$ is analytic for $|z| < q$ and $n^2, 1/\Gamma$ are entire functions. Now writing $M_z(n)/q^n = n^{r-1} (f(z) + O(1/n))$ where $f(z) = zH(z) = F_z(1/q) \frac{1}{\Gamma(z)}$ and considering the Taylor expansion of $f(z)$ near $z = r, f(z) = f(r) + f'(r)(z - r) + O(|z - r|^2)$ we get

$$\frac{1}{q^n} \eta(n,k) = \frac{1}{2\pi i} \int_{|z|=r} n^{z-1}f(z) \frac{dz}{z^{k+1}} + O(E), \quad \text{(13)}$$

where $E$ is given by $\frac{1}{n} \int_{|z|=r} n^{z-1} \frac{dz}{z^{k+1}} |dz|$. We see that

$$\frac{1}{2\pi i} \int_{|z|=r} (z - r)n^{z-1} \frac{dz}{z^{k+1}} = \frac{1}{n} \left\{ (\log n)^{k-1} - r \frac{(\log n)^k}{k} \right\} = 0.$$

Hence

$$\frac{1}{q^n} \eta(n,k) = f(r) \frac{1}{2\pi i} \int_{|z|=r} n^{z-1} \frac{dz}{z^{k+1}} + O \left( r^{-k-1} \int_{|z|=r} n^{z-1} |z - r|^2 |dz| + E \right)$$

$$= f(r) \frac{(\log n)^k}{k! n} + \text{Error term.} \quad \text{(14)}$$

By using Lemmas 3.1 and 3.3, we see the integral in the Error term is bounded by

$$\frac{r^3}{n} \int_{-\pi}^{\pi} \left| 1 - e^{i\theta} \right|^2 e^{i\theta} e^{\theta} d\theta \ll \frac{r^3}{n} \int_{-\infty}^{\infty} \theta^2 e^{\theta(1 - r^2/\pi)} d\theta \ll \frac{r^3}{n} e^{r^2 k - \frac{3}{2}}.$$

Since there is a factor of $r^{-k-1}$ outside, we have the above expression (final step by Stirling’s formula)

$$\ll \frac{1}{n} e^{-k} e^{k - \frac{3}{2}} \ll (\log n)^{k-2} \frac{e\sqrt{k}}{nk^k} \ll \frac{1}{n} \frac{(\log n)^{k-2}}{k(k-1)!}.$$

Noting $e^k = n^r \iff k = r \log n$ and using Lemma 3.2, we also see the term $E$ is bounded by

$$\ll \frac{r^{-k-1} e^k}{n^2} \int_{|z|=r} |n^{z-r}| |dz| \ll \frac{r^{-k-1} e^k}{n^2} \left( \frac{r}{\sqrt{k}} \right) \ll \frac{1}{n^2} \frac{(e \log n)^k}{k^{k+\frac{1}{2}}} \ll \frac{1}{n^2} \frac{(\log n)^k}{k!},$$

where in the last step we have used Stirling. Thus we finally obtain

$$\eta(n,k) \sim q^n f(r) \frac{(\log n)^k}{k! n} = \frac{q^n}{n} \frac{F_z(1/q)}{\Gamma(r+1)} \frac{1}{(k-1)!} (\log n)^{k-1}$$

and the proof follows once we note $F_z(1/q)$ is bounded by some positive constant (which does not depend on $n$ or $k$) from below since $F_z(u)$ has an absolutely convergent Euler product representation in the region $\mathcal{R}$ given by (5). In particular, one can choose a compact set $\mathcal{K}$ (which depends on $\epsilon$ but is independent of the parameters $n$ and $k$) such that $(1/q, r) \in \mathcal{K} \subset \mathcal{R}$ and since $F_z(u)$ is analytic and hence $|F_z(u)|$ is continuous on $\mathcal{K}$, it must be bounded from below and the lower bound must be positive as $F_z(u)$ has an Euler product in the concerned region. We also substituted $r = k/\log n$. The derived expression is identical to the integer case for $k \leq (2 - \epsilon) \log \log x$ as mentioned in [7] on the first page, a result due to Sathe [10].

\[\Box\]

We now begin to discuss the main contribution of this work. For the convenience of the reader, we provide the following outline.
3.1 Organization of the following sections

The proof of Theorem 1.2 rests on a technique developed by Sathe and Selberg along with a combination of an observation made by Nicolas [7] in his work and an analogue of the Selberg–Delange style argument for function fields developed in Porrit [8, Sect. 2]. We will also use ideas from Tenenbaum [12, Chap. II.6], where the author outlines an application of the Selberg–Delange method to integers with a given number of prime factors. In the earlier sections, we gave detailed proofs of Theorem 1.1 and Proposition 1.3 as a direct application of the Selberg–Delange method discussed in [8]. The flow of the argument and preliminary lemmas leading to Theorem 1.2 are fairly delicate. The proof of Proposition 1.4 will be fundamentally the same as that of Proposition 1.3 apart from some technical modifications. We will begin Sect. 4 by establishing Lemma 4.1, an odd–even decomposition for polynomials. We will then discuss the role of the auxiliary results Lemmas 4.2, 4.5, 4.6, 4.4 behind the main proof of the Theorem 1.2. Next, we establish two important results, Propositions 4.3 and 4.7 which will finally lead us to Theorem 1.2. Detailed proofs of the technical lemmas and Proposition 1.4 will be presented in the "Appendix". The graphical dependency between the results in Sect. 4 is described below:

4 Preparatory results and an odd–even decomposition

4.1 An odd–even decomposition for polynomials

We begin this subsection by introducing a decomposition for $\Pi(x, k)$ into $k$ smaller parts used by Nicolas [7] to prove (2). We first note that any integer $n \leq x$ can be uniquely written as $n = 2^j \ell$ with $\ell$ odd. We note the following identity

$$
\Pi(x, k) = \sum_{0 \leq j \leq k} \Pi(x/2^j, j), \tag{15}
$$

where

$$
\Pi'(x, k) := \# \left\{ m \leq x : m \text{ odd and } \Omega(m) = k \right\}
$$

holds. If $2 \log \log x < k < \log x/\log 2$, then the key idea proposed in [7] says the major contribution in (15) comes if we restrict $0 \leq j \leq \alpha \log \log (x/2^k)$ for some explicit constant $\alpha > 2$.

Inspired from the idea above we wish to write $f = hg$ for any $f \in \mathcal{M}_n$, where the polynomials $g$ and $h$ are expected to play the role of “odd” and “even” respectively in some appropriate sense. Let us define the set

$$
S(f) := \left\{ h \in \mathcal{M}_j : h \text{ has only degree 1 irreducible factors} \right\}.
$$
Given \( f \in M_n \) with \( \Omega(f) = k \), we can uniquely write \( f = hg \) where \( h \in S(j) \) for some \( 0 \leq j \leq k \) and \( g \) has no degree 1 irreducible factor. Elements of the set \( S(j) \) mimic the even part while the odd part is mimicked by the polynomial \( g \). Using this heuristic we could prove the following decomposition result for \( N(n, k) \).

**Lemma 4.1** We have
\[
N(n, k) = \sum_{1 \leq j \leq k} \binom{k-j+q-1}{q-1} N'(n+j-k,j)
\]
for \( 1 \leq k \leq \frac{n}{2} \).

**Proof** We observe that for any \( h \in S(j) \), one can find non negative integers \( a_1, a_2, \ldots, a_q \) such that \( h(t) = (t - \alpha_1)^{a_1}(t - \alpha_2)^{a_2} \ldots (t - \alpha_q)^{a_q} \) with \( \Omega(h) = a_1 + a_2 + \cdots + a_q = j \). Here \( \{a_i\}_{1 \leq i \leq q} \) are the \( q \)-elements in \( \mathbb{F}_q \). Counting the number of non negative integral solutions we readily see that, \( \#S(j) = \binom{j+q-1}{q-1} \). If we consider the unique decomposition \( f = hg \) for some \( f \in M_n \) with \( \Omega(f) = k \), then we note that \( j \neq k \). For if \( j = k \) then \( f = hg \) will imply \( f = h \) and hence they both have the same degree, a contradiction since \( k \leq \frac{n}{2} \) by the hypothesis. Therefore we obtain
\[
N(n, k) = \sum_{0 \leq j \leq k-1} \sum_{h \in S(j)} N'(n-j,k-j) = \sum_{0 \leq j \leq k-1} \binom{j+q-1}{q-1} N'(n-j,k-j).
\]
The statement of the lemma follows after we make the change of variable \( j \mapsto k-j \). \( \square \)

The rough sketch of our strategy to prove the Theorem 1.2 is: (a) in light of the approach discussed in (15) in the integer setting, we start by splitting the whole sum in the above decomposition up to \( j \ll \log(n-k) \) and hence we end up with two parts so that we can write, \( T_1 = \sum_{1 \leq j \leq \log(n-k)} \binom{k-j+q-1}{q-1} N'(n+j-k,j) \) and \( T_2 = \sum_{\log(n-k) \leq j \leq k} \binom{k-j+q-1}{q-1} N'(n+j-k,j) \).

(b) We then show the main contribution comes from \( T_1 \) and is of order \( q^{n-k-kq^{-1}}(n-k)^{q^{-1}} \) while the term \( T_2 \) is significantly smaller and is of order \( q^{n-k}(n-k)^{q^{-2}} \). Unlike the ideas discussed in the integer case, which is very combinatorial, our proof will be more analytical. The central idea to use a Selberg–Delange type argument followed by an application of Cauchy’s integral formula shall remain the same. The situation over \( \mathbb{F}_q[t] \) is quite different due to the presence of many degree 1 irreducibles which is why an extra binomial term and other technical difficulties arise.

We begin our preparation with the easier task, a non-trivial upper bound on \( T_2 \). To do so, we would like an upper bound on each summand of \( T_2 \). The following result accomplishes this job.

**Lemma 4.2** Let \( 0 < \delta < 1, 0 < \eta \leq q^2 - q - \delta \) be given. We have the following upper bound
\[
N'(n,j) \ll \delta \ q^n \eta^{n+1} \left( \frac{1}{q + \eta} \right)^j.
\]
Throughout our discussion, the implied constants are allowed to depend on \( q, \delta \) and the value of \( \delta \) is soon to be fixed in the following result. It is possible to show the above result as a direct application Proposition 1.4. The proof of Proposition 1.4 will roughly be in the same spirit as that of Proposition 1.3. We will present this proof followed by an argument
leading to Lemma 4.2 in the “Appendix B.1, B.2”. We now shift our attention to check that the term \( T_2 \) is small as claimed.

**Proposition 4.3** Let \( q > 2 \) be an integer and \( Y = \log(n - k) \). We have the following upper bound

\[
T_2 = \sum_{eqY < j \leq k} \left( \frac{q - 1 + k - j}{q - 1} \right) N'(n + j - k, j) \ll_B q^{n-k} (n-k)^{q-2}.
\]

**Proof** We plan to use \( \frac{\alpha}{\beta} \leq \alpha / \beta! \) for positive integers \( \alpha \) and \( \beta \). We apply Lemma 4.2 with \( \eta = (e - 1)q \) and \( \delta = 0.6 \) so that \( (q + \eta) = eq \). First we check this choice satisfies the hypothesis of Lemma 4.2. We see that \((e - 1)q < q^2 - q - 0.6\) is true whenever \( q \geq 3 \). We now have that

\[
T_2 \ll \sum_{j > (q+\eta)Y} (q - 1 + k - j)^{q-1} (n + j - k)^{\eta+q-1} \left( \frac{1}{q+\eta} \right)^j
\]

\[
= q^{n-k} \sum_{j > eqY} (q - 1 + k - j)^{q-1} (n + j - k)^{\eta+q-1} \left( 1 + \frac{j}{q+\eta} \right)^{\eta+q-1} e^{-j},
\]

where we used \( q + \eta = eq \). Since \( k \leq n/B \) we have \((q - 1 + k/n)q-1 \leq (q - 1 + k/n)q-1 \leq (q - 1 + 1/n^2)q-1 \leq 1 \). Also \( k + j \leq 2k \leq n \) gives \((1 + j/n^2)^{\eta+q-1} \ll 1 \). Recalling \( Y = \log(n - k) \) and continuing from the previous step we get

\[
T_2 \ll_B q^{n-k} (n-k)^{eq+q-2} \sum_{j > eqY} e^{-j} \ll_B q^{n-k} (n-k)^{eq+q-2} e^{-eqY} = q^{n-k} (n-k)^{q-2}.
\]

\( \square \)

We are now only left to estimate \( T_1 \) and show it dominates in the asymptotic of \( N(n,k) \). For the ease of exploration, the calculation of \( T_1 \) is broken down into three smaller sub-parts. To have a good estimate for \( T_1 = \sum_{1 \leq j \leq \log(n-k)} \left( \frac{j+q-1}{q-1} \right) N'(n + j - k, j) \), first it is natural to want to understand the terms \( N'(n + j - k, j) \) when the range for \( j \) is restricted to \( \ll \log(n - k) \). With these observations in mind we could show the following result.

**Lemma 4.4** Let \( Y = \log(n-k) \). We have uniformly for \( j \leq eqY \),

\[
N'(n + j - k, j) = \frac{q^{n+j-k}}{n-k} \left\{ \mathcal{Q}_j(Y) + O \left( \frac{(\log(n-k))^{j+1}}{j!(n-k)} \right) \right\}
\]

where

\[
\mathcal{Q}_j(X) := \sum_{m+t=j-1} \frac{1}{m!} h^{(m)}(0) X^t.
\]

If we are given the above result in our toolbox, it is then evident that we are just a few steps away from proving an estimate for \( T_1 \) once we take care of what happens with the sum when the terms \( N'(n + j - k, j) \) are twisted by appropriate binomial coefficients for different \( j \)'s. However, before we proceed to do that, we would like to mention a few words about what goes into the proof of Lemma 4.4. The proof of the above result rests on another two
fairly technical auxiliary lemmas, which we shall state next. Details of these three claims are postponed till the “Appendix B.3, B.4, B.5” and can be skipped at the moment as they do not offer many insights into our actual goal.

**Lemma 4.5** We have uniformly for $j \leq eq \log n$,
\[
N'(n, j) = q^n \frac{Q_j(\log n)}{n} + O\left(\frac{\log n}{j!n}\right).
\]

**Lemma 4.6** Let $m \geq 1$ be an integer. We have the following upper bounds
\[
h^{(m)}(0)/m! \ll \left(\frac{1}{2.9q}\right)^m,
\]
\[
Q_j(X) \ll \frac{X^{j-1}}{(j-1)!} \quad \text{and} \quad Q_j'(X) \ll \frac{X^{j-2}}{(j-2)!},
\]
for $1 \leq j \leq eqX$ uniformly, where $X$ is a parameter that tends to $\infty$ with $n$.

We can now set up the stage for proving Theorem 1.2. As mentioned earlier we need to have a precise estimate for the twisted binomial sum appearing in $T_1$. Therefore the following Proposition plays a key role in establishing Theorem 1.2.

**Proposition 4.7** Let $Y = \log(n-k)$. We have the following estimate
\[
\sum_{j \leq eqY} \left(\frac{q - 1 + k - j}{q - 1}\right)^j \frac{q^j Q_j(Y)}{h(q)} = q^{eqY} h(q) \left(1 + o(1)\right).
\]

**Proof** We start with an observation first. By the hypothesis of Theorem 1.2 we have $k > \xi(n) \log n$ yielding $k - j \geq \xi(n) \log n - eq \log(n - k) \geq (\xi(n) - eq) \log n \to \infty$. Therefore using the standard fact \((\alpha \beta) = (1 + o(1))\frac{\alpha^\beta}{\beta!}\) where $\beta$ is assumed to be fixed and $\alpha \to \infty$ we obtain
\[
\sum_{j \leq eqY} \left(\frac{q - 1 + k - j}{q - 1}\right)^j \frac{q^j Q_j(Y)}{h(q)} = q^{eqY} h(q) \left(1 + o(1)\right),
\]
where we used the the Taylor expansion of $(k + q - j - 1)^{q-1} = k^{q-1}(1 + o(1))$ since $j = o(k)$. We now evaluate the sum
\[
\sum_{j \leq eqY} q^j Q_j(Y) = \left(\sum_{j \geq 1} \left(\sum_{m=0} \frac{h^m(0)}{m!} Y^m\right)\frac{q^j}{j!}\right) - R
\]
\[
= \left(\sum_{j \geq 0} \frac{(qY)^j}{j!} \sum_{m=0} \frac{h^m(0)}{m!} q^{j-m-1}\right) - R \quad \text{(after interchanging the sum)}
\]
\[
= \left(\sum_{j \geq 0} \frac{(qY)^j}{j!} \sum_{m=0} \frac{h^m(0)}{m!} q^{m}\right) - R \quad \text{(since $m = j - \ell - 1$ and $j \geq \ell + 1$)}
\]
\[
= qe^{qY} h(q) - R \quad (h(z) \text{ is analytic for } |z| < q^2),
\]
(18)
where

\[
R = \sum_{j > [eqY]} q^j Q_j(Y) \quad \text{(where } [x] \text{ denotes the greatest integer } \leq x) \\
= \sum_{j > [eqY]+1} q^j \sum_{m > [eqY]-\ell} \frac{h^m(0)}{m!} Y^\ell \\
= q \left( \sum_{0 \leq \ell \leq [eqY]} \frac{(eqY)^\ell}{\ell!} \sum_{m > [eqY]-\ell} \frac{h^m(0)}{m!} q^m \right) + q \left( \sum_{\ell > [eqY]+1} \frac{(eqY)^\ell}{\ell!} \sum_{m \geq 0} \frac{h^m(0)}{m!} q^m \right) \\
\ll q S_1 + S_2 \quad \text{(say).} \quad (19)
\]

We have the following estimates

\[
S_1 \leq \sum_{0 \leq \ell \leq [eqY]} \frac{(eqY)^\ell}{\ell!} \sum_{m \geq [eqY]-\ell} \left( \frac{1}{2} \right)^m \quad \text{(using } h^m(0)/m! < (1/2)^m \text{ from Lemma 4.6)} \\
= \sum_{0 \leq \ell \leq [eqY]} \frac{(eqY)^\ell}{\ell!} \left( \frac{1}{2} \right)^{[eqY]-\ell} \\
= \left( \frac{1}{2} \right)^{[eqY]} \sum_{0 \leq \ell \leq [eqY]} \frac{2(eqY)^\ell}{\ell!} \\
\leq e^{0.12qY} \quad \text{(since } \left( \frac{1}{2} \right)^{[eqY]} = e^{-0.88qY} \text{ and the rest is bounded by the complete sum } e^{2eqY} \text{).} \quad (20)
\]

Similarly

\[
S_2 = h(q) \sum_{\ell \geq [eqY]+1} \frac{(eqY)^\ell}{\ell!} \\
\ll (eqY)^{[eqY]} \sum_{\ell \geq [eqY]+1} \frac{(eqY)^\ell}{\ell!} \quad \text{(dropping } h(q) \text{ and using a change of variable } \ell \mapsto \ell - [eqY]) \\
\ll \frac{(eqY)^{[eqY]}}{[eqY]!} \sum_{\ell \geq 1} \frac{(eqY)^\ell}{\ell!} \quad \text{(since } \left( \frac{\ell + [eqY]}{\ell} \right) \geq 1 \text{ so that } \frac{1}{(\ell + [eqY])!} \leq \frac{1}{\ell!} \) \\
\ll \frac{1}{\sqrt{eqY}} e^{eqY}. \quad (21)
\]

where at the last step we used Stirling. Indeed letting \( p = eqY \), we have

\[
\frac{(eqY)^{[eqY]}}{[eqY]!} \ll \frac{|p|}{\sqrt{|p|}} = \left( \frac{|p|}{|p|} \right)^{\frac{|p|}{|p|}} \frac{1}{\sqrt{|p|}} \leq \left( 1 + \frac{1}{|p|} \right)^{\frac{|p|}{|p|}} \frac{1}{\sqrt{|p|}} \leq e.
\]

\[\square\]

Remark 4.8 In the hypothesis of the above proposition, the factor \( e \) in the parameter \( eqY \) was chosen carefully. The final application of Stirling will not work if we choose a factor strictly smaller than \( e \). This choice induces a restriction in the hypothesis of the Lemma 4.5. The proof of the lemma in “Appendix B.3” crucially uses the technical condition \( q > e \). This is why our methods do not cover the case \( q = 2 \).

Proof of Theorem 1.2 We have that
Fig. 3 The contour appearing in the proof of Proposition 1.4

\[ N(n, k) = \sum_{1 \leq j \leq \text{eq}Y} \binom{k - j + q - 1}{q - 1} N'(n + j - k, j) + \sum_{j > \text{eq}Y} \binom{k - j + q - 1}{q - 1} N'(n + j - k, j) = T_1 + T_2. \tag{22} \]

Proposition 4.3 shows the tail \( T_2 \) is small and is \( \ll q^{n-k}(n-k)q^{-2} \). Lemma 4.4 and Proposition 4.7 implies

\[
T_1 = \sum_{j \leq \text{eq}Y} \binom{k - j + q - 1}{q - 1} q^{n-k} q^j Q_j(Y) + O \left( \sum_{j \leq \text{eq}Y} \binom{k - j + q - 1}{q - 1} \left( \frac{\log(n-k)}{j(n-k)} \right) q^j Q_j(Y) \right)
\]
\[
= \frac{q^{n-k} k^{q-1} q^{Y(q-1)}}{(q-1)(n-k)} b(q) \left( 1 + o(1) \right) + O \left( \frac{q^{n-k} k^{q-1} q^{Y(q-1)}}{(q-1)(n-k)} \sum_{j=1}^{\infty} \left( \frac{\log(n-k)}{j(n-k)} \right) \right)
\]
\[
= \frac{q^{n-k+1} k^{q-1} q^{Y(q-1)}}{(q-1)(n-k)} b(q) \left( 1 + o(1) \right) + O \left( \frac{k^{q-1} \log(n-k) e^{\log(n-k)}}{n-k} \right)
\]
\[
= \frac{q^{n-k+1} k^{q-1} q^{Y(q-1)}}{(q-1)(n-k)} b(q) \left( 1 + o(1) \right) + O \left( k^{q-1} \log(n-k) \right). \tag{23} \]

Thus we obtain

\[
T_1 \sim \frac{q^{n-k} k^{q-1} q^{Y(q-1)}}{(n-k)} qh(q) \frac{q^{Y(q-1)}}{(q-1)!} \sim C(q) \frac{q^{n-k+1}(n-k)^{q^{-1}}}{q^k},
\]

where we used \( q^{Y(q-1)}/(n-k) = (n-k)^{q^{-1}} \) when \( Y = \log(n-k) \) and

\[
C(q) = \frac{qh(q)}{(q-1)!} = \frac{1}{((q-1)!)^2} \left( 1 - \frac{1}{q} \right)^q \prod_{p \in \mathbb{P}, p > 2} \left( 1 - \frac{1}{q^{\deg(p)-1}} \right)^{-1} \left( 1 - \frac{1}{q^{\deg(p)}} \right)^q,
\]
a constant that only depends on \( q \). \( \square \)
Acknowledgements
The author would like to thank his supervisor, Professor Andrew Granville, for suggesting that he work on this problem and also his co-supervisor, Professor Dimitris Koukoulopoulos, for many helpful conversations and continuous support during this project and for their valuable suggestions and comments on the previous versions of this manuscript. The author would also like to thank the anonymous referee for many useful comments and Ofir Gorodetsky for informing him about the previous works on the same problem, which the author was initially unaware of. The author was financially supported by his supervisors and the Fellowships provided by Faculté des études supérieures et postdoctorales (FESP), Bourse d’exemption de Université de Montréal, Centre interuniversitaire en calcul mathématique algébrique (CICMA) while carrying out this work.

Data availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current work.

Appendix A. Auxiliary results towards Theorem 1.1
We establish the technical Lemmas 3.1, 3.2 and 3.3, used in the proofs of Theorem 1.1 and will again be used in showing Proposition 1.4.

Lemma 3.3 For $t \in [-\pi, \pi]$ we have $\cos t - 1 \leq -\frac{t^2}{5}$ and $|1 - e^{it}|^2 \leq t^2$.

Proof We define the function $f(t) := 1 - \frac{t^2}{5} - \cos t$ for $t \in [0, \pi]$ and observe that $f'(t) = 0 \implies \sin t = \frac{2t}{5}$. A quick graph plot or plugging this equation into a computer reveals that it has only two solutions in the interval $[0, \pi]$, namely $t = 0$ and $t \approx 2.125$. We verify that $f''(0) = -\frac{2}{5} + \cos 0 = \frac{3}{5} > 0$ and hence $t = 0$ is the global minima in the interval $[0, \pi]$ since $0 = f(0) < f(2.125)$, which can also be checked on a computer.

Finally since $\cos t$ and $t^2$ are both even functions, we have for all $t \in [-\pi, \pi]$ the following inequality

$$f(t) \geq 0 \implies 1 - \frac{t^2}{5} - \cos t \geq 0 \implies \cos t - 1 \leq -\frac{t^2}{5}.$$ 

For $0 \leq x, t \leq \pi$ it is well known that,

$$\sin x \leq x \implies \int_0^t \sin xdx \leq \int_0^t xdx \implies 1 - \cos t \leq \frac{t^2}{2}.$$ 

Again the above inequality is true for $-\pi \leq t \leq \pi$ since $\cos$ and $t^2$ are both even functions. Finally we observe $|1 - e^{it}|^2 = (1 - \cos t)^2 + \sin^2 t = 2(1 - \cos t) \leq t^2$ and the claim follows. \hfill \Box

Lemma 3.4 We have the following upper bound

$$\int_{|z| = r} |n^{z-r}| |dz| \ll \frac{r}{\sqrt{j}},$$

where $j = r \log n$.

Proof Let $I_0 = \int_{|z| = r} |n^{z-r}| |dz|$. After substituting $z = re^{2\pi i t}$ where $t \in \left[ -\frac{1}{2}, \frac{1}{2} \right]$ we get

$$I_0 \ll \int_{-\frac{1}{2}}^{\frac{1}{2}} n^{r e^{2\pi i t} - r} |rdt| = r \int_{-\frac{1}{2}}^{\frac{1}{2}} n^{r (\cos 2\pi t - 1)} |dt| \quad (|n^r \sin 2\pi t| = 1)$$

\[ \ll r \int_{-\frac{1}{2}}^{\frac{1}{2}} n^{-\frac{4s^2\pi^2}{5}} \frac{dt}{s} \quad \text{(by Lemma 3.1)} \]

\[ \ll r \int_{-\infty}^{\infty} e^{-t^2} \frac{dt}{\sqrt{r \log n}} \quad \left( t \mapsto 2\pi t \sqrt{\frac{r \log n}{5}} \right) \]

\[ \ll r \frac{1}{\sqrt{r \log n}} = r \frac{1}{\sqrt{j}} \quad (j = r \log n). \quad (24) \]

\[ \square \]

**Lemma 3.5** We have the following estimate

\[ \int_{-\infty}^{\infty} \theta^2 \exp \left( -\frac{k\theta^2}{5} \right) d\theta \ll k^{-\frac{3}{2}}. \]

**Proof**

\[ \int_{-\infty}^{\infty} \theta^2 \exp \left( -\frac{k\theta^2}{5} \right) d\theta = \frac{5\sqrt{5}}{k^2} \int_0^{\infty} \sqrt{ze^{-z}} dz \quad (z = \frac{k\theta^2}{5}) \]

\[ \ll k^{-\frac{3}{2}} \quad \text{(since} \int_0^{\infty} \sqrt{ze^{-z}} dz \text{ is convergent).} \quad (25) \]

\[ \square \]

**Appendix B. Towards Proposition 1.4 and auxiliary results for Theorem 1.2**

**B.1. A Selberg–Delange style argument for \( \widetilde{M}_z(n) \)**

**Proposition 1.4** For all \( \delta \in (0, 1) \) and uniformly for \( |z| \leq q^2 - \delta \) we have

\[ \widetilde{M}_z(n) := \sum_{f \in \widetilde{M}_n} z^{\Omega(f)} = q^nnz^{h(z) + O_{\delta} \left( \frac{1}{n} \right)}, \]

where \( h(z) = \frac{1}{\Gamma(z+1)} \left( 1 - \frac{1}{q} \right)^{qz} \prod_{p \in \mathbb{P}_{\geq 2}} \left( 1 - \frac{z}{q^{\deg(p)}} \right)^{-1} \left( 1 - \frac{1}{q^{\deg(p)}} \right)^z, \) an analytic function for \( |z| < q^2. \)

**Proof** We recall some notations for convenience,

\[ \widetilde{\mathcal{M}} := \left\{ \text{set of all monics in } \mathbb{F}_q[t] \text{ having no root in } \mathbb{F}_q \right\}, \]

\[ \widetilde{\mathcal{M}}_n := \left\{ \text{set of all of degree } n \text{ monics in } \mathbb{F}_q[t] \text{ having no root in } \mathbb{F}_q \right\}, \]

\[ N'(n, k) := \# \left\{ f \in \widetilde{\mathcal{M}}_n : \Omega(f) = k \right\}. \]

We proceed as the proof of Theorem 1.1 by first defining the following quantities,

\[ \widetilde{M}_z(n) = \sum_{f \in \widetilde{\mathcal{M}}_n} z^{\Omega(f)} = \sum_{k \geq 0} z^k N'(n, k) \quad \text{and} \quad \widetilde{G}_z(u) = \sum_{f \in \widetilde{\mathcal{M}}} z^{\Omega(f)} u^{\deg(f)}. \]

The Euler product decomposition for \( \widetilde{G}_z(u) \) now becomes

\[ \widetilde{G}_z(u) = \prod_{p \in \mathbb{P}_{\geq 2}} \left( 1 - zu^{\deg(p)} \right)^{-1}. \]
Following the same spirit we now have
\[
\widetilde{G}_z(u) = \zeta(u)^z \widetilde{F}_z(u),
\]
where \( \widetilde{F}_z \) is given by the Euler product below
\[
\widetilde{F}_z(u) = (1 - u)^{\overline{u}} \prod_{p \in \mathcal{P}_{\geq 2}} \left( 1 - zu^{deg(p)} \right)^{-1} \left( 1 - u^{deg(p)} \right)^z.
\]
We first show the above Euler product converges absolutely in the region defined by,
\[
\widetilde{R} := \left\{ (u, z) \in \mathbb{C}^2 : |z| < q^2, |u|^2 < |z|^{-1}, |u| < q^{-1/2} \right\} \subset \mathbb{C}^2.
\]
We take the standard branch of complex logarithm defined over \( \mathbb{C} \setminus (-\infty, 0] \) and get for each integer \( n \geq 2, (\text{since } |u|^n < 1, |zu^n| \leq |zu^2| < 1) \)
\[
z \log(1 - u^n) - \log(1 - zu^n) = -zu^n + O \left( |zu^{2n}| \right) + zu^n + O \left( |z^2u^{2n}| \right)
\]
\[
= O \left( \left| q^4u^{2n} \right| \right) \quad (|z| < q^2)
\]
and hence using \( \exp(O(x)) = 1 + O(x) \) for \( x = O(1) \) we get,
\[
(1 - u^n)\overline{z}(1 - zu^n)^{-1} = 1 + O \left( \left| q^4u^{2n} \right| \right).
\]
We now observe the Euler product for \( \widetilde{F}_z \) converges uniformly on the compact subsets of \( \widetilde{R} \) as
\[
\sum_{p \in \mathcal{P}_{\geq 2}} |u|^{2n} \leq \sum_{n \geq 2} |qu^2|^n < \infty \quad \text{(where we used, } \# \mathcal{P}_n \leq q^n).
\]
We also verify \( (1 - zu^{deg(p)}) \geq 1 - |zu^{deg(p)}| \geq 1 - |zu^2| > 0, \) which shows none of the \( \left( 1 - zu^{deg(p)} \right)^{-1} \) factors contribute to a pole in \( \widetilde{R} \). Also \( (1 - u)^{\overline{u}} \) is holomorphic in \( \widetilde{R} \) and this proves \( \overline{F}_z(u) \) is holomorphic inside \( \widetilde{R} \). We determine the coefficient of \( u^n \) in \( \overline{G}_z(u) \) using Cauchy’s integral formula and recover \( \overline{M}_z(n) \) exactly as in the proof of Theorem 1.1.

We have that, if \( |u| = r < q^{-1} \) (refer to the small green circle in the same Fig. 3), then using Cauchy’s residue formula on (3) gives
\[
\overline{M}_z(n) = \frac{1}{2\pi i} \int_{|u|=r} \overline{G}_z(u) \frac{du}{uw^{n+1}} = \frac{1}{2\pi i} \int_{|u|=r} \zeta(u)^z \overline{F}_z(u) \frac{du}{uw^{n+1}}.
\]

Now we again want to collect the contribution coming from the singularity of \( \zeta(u)^z \) at \( u = 1/q \) to evaluate the above integral. We shift the contour \( |u| = r \) to a bigger circle \( |u| = 1/q + \eta \) with a different choice of \( \eta \) here (not the same choice for \( \eta \) in Proposition 1.3) and with \( |z| \leq q^2 - \delta \). Since the region of absolute convergence for \( \overline{F}_z(u) \) here is \( \widetilde{R} \), we have a different set of constraints on \( \eta \) than before. Here we get for \( \eta, |zu^2| \leq (q^{-1} + \eta^2)(q^2 - \delta) \leq 1 \) and \( |u| = 1/q + \eta < q^{-\frac{3}{2}} \). This shows taking any \( 0 < \eta < \min\{1/\sqrt{q^2 - \delta} - 1/q, 1/\sqrt{q} - 1/q\} \) suffices. We then plan to use Lemma 2.2 to evaluate the integral in (27) with, \( \eta = \min\{1/\sqrt{q^2 - \delta} - 1/q, 1/\sqrt{q} - 1/q\}/2 \) for \( |z| \leq q^2 - \delta \) just as we did in the proof of Proposition 1.3.

**Remark B.1** \( F_z(u) \) was absolutely convergent in \( R \) which gave us the appropriate choice for \( \eta \). All the calculations are identical here with \( \overline{F}_z \) instead of \( F_z \). The main difference is, here we have \( |z| \leq q^2 - \delta \) instead of \( |z| \leq q - \epsilon \). Earlier \( F_z \left( \frac{1}{\eta} \right) \) had a pole at \( z = q, q^2, \ldots \) but we got rid of the \( z = q \) pole here. This is what essentially allows us to take \( |z| \leq q^2 - \delta \).
We therefore get
\[
\tilde{M}_z(n) = \frac{1}{2\pi i} \int_{|u|=\frac{1}{2+\eta}\cup\mathbb{R}'} \zeta(u) \tilde{F}_z(u) \frac{du}{u^{n+1}} \\
= \tilde{F}_z \left( \frac{1}{q} \right) q^n h^{-1} \left( \frac{1}{\Gamma(z)} + O_\delta \left( \frac{1}{n} \right) \right) \\
= q^n h^{-1} \left( zh(z) + O_\delta \left( \frac{1}{n} \right) \right),
\]
(28)

where
\[
h(z) = \frac{1}{z} \tilde{F}_z \left( \frac{1}{q} \right) = \frac{1}{\Gamma(z)} \left( 1 - \frac{1}{q} \right) \prod_{p \neq q \geq 2} \left( 1 - \frac{z}{q^{deg(p)}} \right)^{-1} \left( 1 - \frac{1}{q^{deg(p)}} \right)^z.
\]

Also we have \( h(z) = \frac{1}{\Gamma(z+1)} \tilde{F}_z \left( \frac{1}{q} \right) \). Since \( \tilde{F}_z \left( \frac{1}{q} \right) \) is analytic in \(|z| < q^2\), so is \( h \).

\[\square\]

B.2 An useful upper bound for \( N'(n, j) \)

**Lemma 4.2** Let \( 0 < \delta < 1, 0 < \eta \leq q^2 - q - \delta \) be given. We have the following upper bound
\[
N'(n, j) \ll_{\delta, \eta} q^n n^{d+n-1} \left( \frac{1}{q + \eta} \right)^j.
\]

**Proof** We use Proposition 1.4 with \( z = q + \eta \) and if \( a_j(f) \) denotes the indicator function of polynomials in \( \tilde{M}_n \) with \( \Omega(f) = j \) then, we see that every time \( a_j = 1 \) occurs, it contributes an amount of \( (q + \eta)^j \) on the left hand side of the sum of Proposition 1.4 and all the other terms are positive. We have by the previous lemma \( h(z) \) is analytic in an open set containing the disc \(|z| \leq q^2 - \delta\). Since the disk is compact and \( h \) is continuous there, we have \( h(z) \ll_{q, \delta, 1} 1 \) for every \(|z| \leq q^2 - \delta\). Consequently for every \(|z| \leq q^2 - \delta, |zh(z)| \leq |(q + \eta)h(q + \eta)| \ll_{q, \delta} 1 \). This observation leads to an upper bound
\[
N'(n, j) \ll_{q, \delta} q^n n^{d+n-1} \left( \frac{1}{q + \eta} \right)^j.
\]

\[\square\]

B.3 An uniform estimate for \( N'(n, j) \) when \( j \leq eq \log n \)

**Lemma 4.5** We have uniformly for \( j \leq eq \log n \),
\[
N'(n, j) = \frac{q^n}{n} \left\{ Q_\delta(q \log n) + O \left( \frac{\log n}{jH} \right) \right\}.
\]

**Proof** We use Proposition 1.4. The coefficient of \( z^j \) in \( \tilde{M}_z(n) \) is what we want to evaluate. We have for \( r < q^2 \),
\[
N'(n, j) = \frac{1}{2\pi i} \int_{|z|=r} \tilde{M}_z(n) \frac{dz}{z^{j+1}}
\]

We recall from Proposition 1.4 \( \tilde{M}_z(n) = \frac{q^n}{n} \left\{ zh(z)n^{x} + O(n^{x-1}) \right\} \). Plugging this back in the integral we get that
\[
\frac{n}{q^n} N'(n, j) = \frac{1}{2\pi i} \int_{|z|=r} zh(z)n^x \frac{dz}{z^{j+1}} + O(E_0),
\]

where
where $E_0$ is given by, $\int_{|z|=r} \left| \frac{\nu^z - 1}{z^j + 1} \right| |dz|$. At this point we choose $r = \frac{j}{\log n} \leq eq < q^2$ since by hypothesis $j \leq eq \log n$ and $q \geq 3$. Noting $e^j = n^r \iff j = r \log n$ and using Lemma 3.2, we get the term $E_0$ is bounded by

$$\ll \frac{r^{-j}e^j}{n} \int_{|z|=r} |z|^{-r} |dz| \ll \frac{r^{-j}e^j}{n} \frac{1}{j^2} \ll \frac{1}{n} \frac{(\log n)^j}{j!},$$

where the final step of bounding follows by Stirling. This is the same trick that we used while bounding above $E$ on p. 10 in the proof of Theorem 1.1. We now return to the main term

$$M_0 = \frac{1}{2\pi i} \int_{|z|=r} z h(z) n^z \frac{dz}{z^j + 1} = \frac{1}{2\pi i} \int_{|z|=r} h(z) n^z \frac{dz}{z^j},$$

where $h(z)$ is an analytic function in the region $|z| < q^2$, so the integrand has a pole at $z = 0$ of order $j$. We evaluate this integral using residue theorem and obtain

$$M_0 = \lim_{z \to 0} \frac{1}{(j-1)!} \frac{d^{j-1}}{dz^{j-1}} h(z) n^z.$$

Using binomial theorem for higher order differentiation of products of two complex functions

$$\frac{1}{(j-1)!} \frac{d^{j-1}}{dz^{j-1}} h(z) n^z \bigg|_{z=0} = \frac{1}{(j-1)!} \sum_{m+\ell=j-1} \frac{(j-1)!}{m!\ell!} h^{(m)}(z)(n^z)^{\ell} \bigg|_{z=0}$$

$$= \sum_{m+\ell=j-1} \frac{1}{m!\ell!} h^{(m)}(0)(\log n)^\ell,$$

(29)

where we have taken the limits inside the argument of the higher order derivatives which is allowed because all the functions here are analytic and hence infinitely differentiable. Plugging everything back we obtain the desired result. $\square$

### B.4 A technical upper bound for $h(z)$, $Q_j(X)$ and their derivatives

**Lemma 4.6** Let $m \geq 1$ be an integer. We have the following upper bounds

$$h^{(m)}(0)/m! \ll \left( \frac{1}{2.9q} \right)^m,$$

$$Q_j(X) \ll \frac{X^{j-1}}{(j-1)!} \quad \text{and} \quad Q_j'(X) \ll \frac{X^{j-2}}{(j-2)!}$$

for $1 \leq j \leq eqX$ uniformly, where $X$ is a parameter that tends to $\infty$ with $n$.

**Proof** From Proposition 1.4 we have that $h(z)$ is holomorphic for $|z| < q^2$ which in particular implies $h(z) \ll_q 1$ for $|z| \leq 2.9q$. Therefore we have by Cauchy’s integral formula,

$$h^{(m)}(0)/m! = \frac{1}{2\pi i} \int_{|z|=2.9q} h(z) \frac{dz}{z^{m+1}} \ll \left( \frac{1}{2.9q} \right)^m (2.9q < q^2 \text{ whenever } q \geq 3).$$

We have from Lemma 4.4

$$Q_j(X) = \sum_{m+\ell=j-1} \frac{1}{m!\ell!} h^{(m)}(0) X^\ell \ll \sum_{m+\ell=j-1} \left( \frac{1}{2.9q} \right)^m \frac{X^\ell}{\ell!}.$$
We now take out the top term \( \frac{X^{j-1}}{(j-1)!} \) to bound the sum from above and observe for each \( m \geq 1 \),
\[
\frac{X^{j-1}}{j!} = \frac{X^{j-m-1}}{j-m-1!} \leq (eq)^m \frac{X^{j-1}}{(j-1)!}
\]
which is true after cross multiplying whenever \( j \leq eqX \) since \((j-1)(j-2)\cdots(j-m) \leq j^m \leq (eqX)^m\). Hence we arrive at the following upper bound,
\[
Q(X) \ll \frac{X^{j-1}}{(j-1)!} \sum_{0 \leq m \leq j-1} \left( \frac{eq}{2.9q} \right)^m \ll \frac{X^{j-1}}{(j-1)!}.
\]
Likewise when \( j \leq eqX \),
\[
Q'(X) = \sum_{m+\ell=j-1} \frac{1}{m!(\ell-1)!} h^{(m)}(0) X^{\ell-1}
\]
\[
\ll \sum_{m+\ell=j-1} \left( \frac{1}{2.9q} \right)^m X^{\ell-1} \frac{1}{(\ell-1)!}
\]
\[
\ll \frac{X^{j-2}}{(j-2)!} \sum_{0 \leq m \leq j-1} \left( \frac{eq}{2.9q} \right)^m
\]
\[
\ll \frac{X^{j-2}}{(j-2)!}.
\]

(B.5) One of the main ingredients of Proposition 4.7 and Theorem 1.2

**Lemma 4.4** Let \( Y = \log(n-k) \). We have uniformly for \( j \leq eqY \),
\[
N'(n+j-k, j) = \frac{q^{n+j-k}}{n-k} Q_j(Y) + O \left( \frac{(\log(n-k))^{j+1}}{j!(n-k)} \right),
\]
where
\[
Q_j(X) := \sum_{m+\ell=j-1} \frac{1}{m!(\ell-1)!} h^{(m)}(0) X^{\ell}.
\]

**Proof** By Lemma 4.5 we have that
\[
N'(n+j-k, j) = \frac{q^{n+j-k}}{n-j-k} \left( Q_j(\log(n+j-k)) + O \left( \frac{1}{j!(n-j-k)} \right) \right) \quad \text{for} \quad j \leq eqY.
\]

We observe \( n-k \geq n \left( 1 - \frac{1}{n} \right) \to \infty \text{ as } n \to \infty \). We also note if \( E_1 = \frac{(\log(n-k))^{j+1}}{j!(n-k)} \) then as \( n \to \infty \)
\[
E_2 = \frac{(\log(n+j-k))^j}{j!(n+j-k)^2}
\]
\[
\leq \left( 1 + \frac{j}{n-k} \right)^j \frac{1}{(\log(n-k))} \to 0
\]
\[
\Rightarrow E_2 = o(E_1).
\]

where we have at the second step the term inside the bracket is bounded, because
\[
\frac{j}{n-k} \leq \frac{eq \log(n-k)}{(n-k)} \to 0 \text{ and hence for } n \text{ large enough it is bounded by } (1 + \log 2/ \log(n-}
\(k\) by \(eq \log(n-k) \leq eq \log^2 = 2eq\). Thus from (31) we arrive at

\[
N'(n + j - k_j) = q^{n+j-k} \left\{ \frac{Q_j(\log(n+j-k))}{n+j-k} + O(E_1) \right\}.
\]

(33)

We show at a small cost it is possible to replace \(\frac{Q_j(\log(n+j-k))}{n+j-k}\) by \(\frac{Q_j(\log(n-k))}{n-k}\). We use the mean value theorem to study the error.

Let \(F(x) := \frac{Q_j(\log x)}{x}\) which is a regular function if \(x > 0\). The difference caused by this replacement

\[
D = \frac{Q_j(\log(n+j-k))}{n+j-k} - \frac{Q_j(\log(n-k))}{n-k} = F(n+j-k) - F(n-k).
\]

By the mean value theorem one can pick \(y \in (n-k, n+j-k)\) such that

\[
D = fF'(y) = j \frac{Q_j'(\log y) - Q_j(\log y)}{y^2} = j \frac{Q_j'(\log y)}{y^2} - \frac{j}{y^2} Q_j(\log y) = F_1 + F_2.
\]

Therefore (33) implies

\[
N'(n + j - k_j) = q^{n+j-k} \left\{ \frac{Q_j(\log(n-k))}{n-k} + F_1 + F_2 + O(E_1) \right\}.
\]

(34)

We apply Lemma 4.6 with the choice \(X = \log y\). We note from the hypothesis that \(j \leq eqY \leq eq \log y\) and \(y > n - k\), so that we must have \(X = \log y \rightarrow \infty\) with \(n\). Using this observation, we upper bound the first term of \(F_1\) which gives \(F_1 = \frac{j}{y^2} Q_j'(\log y) \ll \frac{j}{y^2} \frac{\log(n+j-k)^{j-2}}{(j-2)!}\). Thus we obtain

\[
F_1 = \frac{(n-k)^j}{(\log(n-k))^{j+1} y^2} \frac{j}{(j-2)!} \frac{(\log(n+j-k))^{j-2}}{\log(n-k)} \lesssim 1,
\]

since \(j \leq eq \log(n-k)\) and \(y > n - k\). Hence \(F_1 = O(E_1)\) and likewise from Lemma 4.6 one can show \(|F_2| = \frac{j}{y^2} Q_j(\log y) \ll \frac{\log(n+j-k)^{j-1}}{y^2(j-1)!}\).

Thus we infer

\[
\frac{|F_2|}{E_1} = \frac{j}{y^2} \frac{(\log(n+j-k)^{j-1}}{(\log(n-k))^{j+1} y^2(j-1)!} \lesssim 1.
\]

(36)

The proof is now complete once we plug \(F_1 + F_2 = O(E_1)\) in (34).

\[\square\]

Received: 4 May 2022 Accepted: 5 December 2022 Published online: 4 January 2023

References

1. Afshar, A., Porritt, S.: The function field Sathe–Selberg formula in arithmetic progressions ‘short intervals’. Acta Arith. 187(2), 101–124 (2019)
2. Carr, M.: Factorisation dans \(F_q[x]\). C. R. Acad. Sci. Paris 1294(4), 147–150 (1982)
3. Elboim, D., Gorodetsky, O.: Uniform estimates for almost primes over finite fields (2020). arXiv:2008.05778v2
4. Elliot, P.D.T.A.: Probabilistic Number Theory I et II. Grundlehren der mathematischen Wissenschaften, Springer, New York (1980)
5. Hwang, H.K.: A Poisson negative binomial convolution law for random polynomials over finite fields. Random Struct. Algorithms 13(1), 17–47 (1998)
6. Landau, E.: Handbuch der Lehre von der Verteilung der Primzahlen. Chelsea Publishing Company, New York (1953)
7. Nicolas, J.L.: Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers. Acta Arith. 44, 191–200 (1984)
8. Porritt, S.: Character sums over products of prime polynomials (2020). arXiv:2003.12002
9. Rudin, W.: Real and Complex Analysis. McGraw-Hill Book Company, New York (1987)
10. Sathe, L.G.: On a problem of Hardy on the distribution of integers having a given number of prime factors. J. Indian Math. Soc. 17, 63–141 (1953); 18, 27–81 (1954)
11. Selberg, A.: Note on a paper by L.G. Sathe, ibid. J. Indian Math. Soc. 18, 83–87 (1954)
12. Tenenbaum, G.: An Introduction to Analytic and Probabilistic Number Theory. Cambridge University Press, Cambridge (2015)
13. Warlimont, R.: Arithmetical semigroups. IV. Selberg’s analysis. Arch. Math. (Basel) 60(1), 58–72 (1993)

Publisher’s Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

 Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.