

A polynomial analogue of Landau's theorem and related problems

Ofir Gorodetsky

Abstract

Recently, an analogue over $\mathbb{F}_q[T]$ of Landau's theorem on sums of two squares was considered by Bary-Soroker, Smilansky and Wolf. They counted the number of monic polynomials in $\mathbb{F}_q[T]$ of degree n of the form $A^2 + TB^2$, which we denote by $B(n, q)$. They studied $B(n, q)$ in two limits: fixed n and large q ; and fixed q and large n . We generalize their result to the most general limit $q^n \rightarrow \infty$. More precisely, we prove

$$B(n, q) \sim K_q \cdot \binom{n - \frac{1}{2}}{n} \cdot q^n, \quad q^n \rightarrow \infty,$$

for an explicit constant $K_q = 1 + O(1/q)$. Our methods are different and are based on giving explicit bounds on the coefficients of generating functions. These methods also apply to other problems, related to polynomials with prime factors of even degree.

1 Introduction

Let $b(n)$ be the characteristic function of integers that are representable as a sum of two squares and let

$$B(x) = \sum_{n \leq x} b(n) \tag{1.1}$$

be the number of such integers up to x . Landau's theorem [Lan08] gives an asymptotic formula for $B(x)$:

$$B(x) = K \frac{x}{\sqrt{\ln x}} + O\left(\frac{x}{\ln^{3/2} x}\right), \quad x \rightarrow \infty, \tag{1.2}$$

where

$$K = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} (1 - p^{-2})^{-1/2} \approx 0.764 \tag{1.3}$$

is the Landau-Ramanujan constant.

A polynomial analogue of the function $B(x)$, which we describe below, was studied by Bary-Soroker, Smilansky and Wolf [BSSW16]. Let q be an odd prime power, and \mathbb{F}_q denote the field of q elements. Denote by $\mathcal{M}_{n,q}$ the set of monic polynomials in $\mathbb{F}_q[T]$ of degree n , by $\mathcal{M}_q = \cup_{n \geq 0} \mathcal{M}_{n,q}$ the set of all monic polynomials in $\mathbb{F}_q[T]$ and by \mathcal{P}_q the set of monic irreducible polynomials in $\mathbb{F}_q[T]$.

For a polynomial $f \in \mathcal{M}_{n,q}$ we define the characteristic function

$$b_q(f) = \begin{cases} 1, & f = A^2 + TB^2 \text{ for } A, B \in \mathbb{F}_q[T], \\ 0 & \text{otherwise,} \end{cases} \tag{1.4}$$

and the counting function

$$B(n, q) = \sum_{f \in \mathcal{M}_{n,q}} b_q(f). \tag{1.5}$$

In [BSSW16, Thms. 1.2 and 1.3], the asymptotic behaviour of $B(n, q)$ was studied in two limits, fixed n and large q and fixed q and large n ,

$$B(n, q) = \frac{\binom{2n}{n}}{4^n} \cdot q^n + O_n(q^{n-1}), \quad q \rightarrow \infty, \tag{1.6}$$

$$B(n, q) = \frac{K_q}{\sqrt{\pi}} \cdot \frac{q^n}{\sqrt{n}} + O_q\left(\frac{q^n}{n^{3/2}}\right), \quad n \rightarrow \infty, \tag{1.7}$$

where

$$K_q = (1 - q^{-1})^{-\frac{1}{2}} \prod_{P \in \mathcal{P}_q: (P/T)=-1} (1 - q^{-2 \deg P})^{-\frac{1}{2}} = 1 + O\left(\frac{1}{q}\right). \quad (1.8)$$

The asymptotic formula (1.6) is proved using elementary combinatorial considerations, while (1.7) is proved using complex analysis. In a recent preprint, Matei [Mat17] extended (1.6) by writing $B(n, q)$ as a polynomial in q and proving that the coefficients have a certain structure and a cohomological interpretation.

The authors of [BSSW16] write “We do not know of an asymptotic formula for $B(n, q)$ in any more general sub-limits of $q^n \rightarrow \infty$ ”. We prove an asymptotic formula in the most general limit $q^n \rightarrow \infty$.

Theorem 1.1.

$$B(n, q) = K_q \cdot \binom{n - \frac{1}{2}}{n} \cdot q^n + O\left(\frac{q^{n-1}}{n^{3/2}}\right), \quad q^n \rightarrow \infty, \quad (1.9)$$

and the implied constant is absolute.

We also investigate the constant K_q , which turns out to be an analytic function of q^{-1} .

Remark 1.2. To see that Theorem 1.1 is consistent with (1.6) and (1.7), note that

$$\binom{n - \frac{1}{2}}{n} = \frac{\binom{2n}{n}}{4^n} \sim \frac{1}{\sqrt{\pi n}}, \quad n \rightarrow \infty, \quad (1.10)$$

and that by (1.8), $K_q = 1 + O(1/q)$.

Our methods differ from those used in [BSSW16], and are based on explicit estimates for the coefficients of a certain class of generating functions. Another advantage of our methods, is that they apply to other problems, see §2.

2 Further applications

2.1 Prime factors of even degree

Suppose we want to count “ordinary” sums of two squares in $\mathbb{F}_q[T]$, i.e. elements of the form $A^2 + B^2$. If $q \equiv 1 \pmod{4}$, then $\sqrt{-1} \in \mathbb{F}_q$. Given $f \in \mathbb{F}_q[T]$, we have $f = ((f-1)/(2\sqrt{-1}))^2 + ((f+1)/2)^2$, and so every polynomial is of the form $A^2 + B^2$. If $q \equiv 3 \pmod{4}$, Leahey [Lea67] has shown that the polynomials of the form $A^2 + B^2$ are those whose prime factors of odd degree appear only with even multiplicity. Imitating Leahey’s proof, one sees that if q is an odd prime power and

$$\alpha \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2, \quad (2.1)$$

then the monic polynomials of the form $A^2 - \alpha B^2$ ($A, B \in \mathbb{F}_q[T]$) are also characterised by the property that their prime factors of odd degree appear with even multiplicity. This raises the problem of estimating the number of monic polynomials of a given degree in the following set, which makes sense for any prime power q :

$$S_1(q) = \{f \in \mathcal{M}_q : P \mid f \text{ and } 2 \nmid \deg P \implies 2 \mid v_P(f)\}, \quad (2.2)$$

where $v_P(f)$ is the multiplicity of P in f . Let

$$B_1(2n, q) = \#\{f \in S_1(q) : \deg f = 2n\}. \quad (2.3)$$

Chuang, Kuan and Yu [CKY15] considered two natural variations on $S_1(q)$. The first is the subset of $S_1(q)$ of polynomials with no odd-degree prime factors:

$$S_2(q) = \{f \in \mathcal{M}_q : P \mid f \implies 2 \mid \deg P\}, \quad (2.4)$$

$$B_2(2n, q) = \#\{f \in S_2(q) : \deg f = 2n\}.$$

The second is the subset of squarefree polynomials in $S_2(q)$:

$$\begin{aligned} S_3(q) &= \{f \in \mathcal{M}_q : P \mid f \implies 2 \mid \deg P \text{ and } P^2 \nmid f\}, \\ B_3(2n, q) &= \#\{f \in S_3(q) : \deg f = 2n\}. \end{aligned} \quad (2.5)$$

The motivation for studying $S_2(q)$, $S_3(q)$ is the following. Assume that q is odd. As observed by Artin [Art24] in his study of quadratic extensions of $\mathbb{F}_q(T)$, the analogue over $\mathbb{F}_q[T]$ of a fundamental discriminant is a squarefree monic polynomial D . The negative Pell equation asks for the solubility of

$$X^2 - DY^2 = \gamma_q \text{ with } X, Y \in \mathbb{F}_q[T], \quad (2.6)$$

where γ_q is a generator of \mathbb{F}_q^\times . By considering (2.6) modulo a prime factor P of D , we find

$$\left(\frac{\gamma_q}{P}\right) = 1, \quad (2.7)$$

where $\left(\frac{\bullet}{P}\right)$ is the Legendre symbol modulo P . By quadratic reciprocity, equation (2.7) implies that P has even degree. Thus, the negative Pell equation has no solution for a given fundamental discriminant D of degree $2N$ unless D is among those $B_3(2N, q)$ polynomials counted in (2.5).

The problem of estimating, in the limit $n \rightarrow \infty$, the proportion in $B_3(2n, q)$ of the discriminants D for which (2.6) is soluble, is an open problem studied by Bae and Jung [BJ12, Thm. 1.5]. Their work is motivated by the number field setting, studied by Steinhagen [Ste93, Conj. 1.2] and Fouvry and Klüners [FK10, Thm. 1].

The asymptotics of $B_2(2n, q)$, $B_3(2n, q)$ in the limit $n \rightarrow \infty$ are given in [CKY15, Thms. 1 and 2]:

$$\begin{aligned} B_2(2n, q) &= C_{q,2} \frac{q^{2n}}{\sqrt{\pi n}} + O_q \left(\frac{q^{2n}}{n^{3/2}} \right), \quad n \rightarrow \infty, \\ B_3(2n, q) &= C_{q,3} \frac{q^{2n}}{\sqrt{\pi n}} + O_q \left(\frac{q^{2n}}{n^{3/2}} \right), \quad n \rightarrow \infty, \end{aligned} \quad (2.8)$$

where $C_{q,2}$ and $C_{q,3}$ are positive constants, given explicitly in [CKY15, Thms. 1 and 2] as infinite products.

We modify the main term of (2.8) to obtain an asymptotic formula in the general limit $q^n \rightarrow \infty$.

Theorem 2.1. *For any positive integer n ,*

$$B_1(2n, q) = C_{q,1} \cdot \binom{n - \frac{1}{2}}{n} \cdot q^{2n} + O \left(\frac{q^{2n-1}}{n^{3/2}} \right), \quad q^n \rightarrow \infty, \quad (2.9)$$

$$B_2(2n, q) = C_{q,2} \cdot \binom{n - \frac{1}{2}}{n} \cdot q^{2n} + O \left(\frac{q^{2n-1}}{n^{3/2}} \right), \quad q^n \rightarrow \infty, \quad (2.10)$$

$$B_3(2n, q) = C_{q,3} \cdot \binom{n - \frac{1}{2}}{n} \cdot q^{2n} + O \left(\frac{q^{2n-1}}{n^{3/2}} \right), \quad q^n \rightarrow \infty, \quad (2.11)$$

where the implied constants are absolute. Moreover, $C_{q,i} = 1 + O(1/q)$.

2.2 Higher genus

We consider a higher genus analogue of the sets $S_1(q)$, $S_2(q)$ and $S_3(q)$. Consider a function field K with finite constant field \mathbb{F}_q , i.e. K is a finitely generated field extension of transcendence degree one over \mathbb{F}_q and \mathbb{F}_q is algebraically closed in K . Let \mathfrak{Q} be a fixed place of K . Let \mathbb{P}_K be the set of places of K .

For each place \mathfrak{P} of K , the corresponding valuation $K \rightarrow \mathbb{Z} \cup \{\infty\}$ is denoted by $v_{\mathfrak{P}}$. The residue field at \mathfrak{P} is denoted by $\mathbb{F}_{\mathfrak{P}}$. The degree $\deg_K \mathfrak{P}$ of \mathfrak{P} is $[\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_q]$. Let $\text{Div}(K)$ be the divisor group of K . Every element D in $\text{Div}(K)$ may be written uniquely as

$$D = \sum_{\mathfrak{P} \in \mathbb{P}_K} v_{\mathfrak{P}}(D) \cdot \mathfrak{P}. \quad (2.12)$$

Given $D \in \text{Div}(K)$, we define the degree of D as

$$\deg D = \sum_{\mathfrak{P} \in \mathbb{P}_K} v_{\mathfrak{P}}(D) \cdot \deg_K \mathfrak{P}. \quad (2.13)$$

The set

$$\text{Div}_{0,\Omega}(K) = \{D \in \text{Div}(K) : \deg D = 0, \quad v_{\mathfrak{P}}(D) < 0 \implies \mathfrak{P} = \Omega\} \quad (2.14)$$

is an higher genus analogue of the set $\mathcal{M}_q \subseteq \mathbb{F}_q[T]$: If $K = \mathbb{F}_q(T)$ and Ω is the prime at $1/T$, then the map $\mathcal{M}_q \rightarrow \text{Div}_{0,\Omega}(K)$ given by $f \mapsto \text{div}(f)$ is a bijection. Similarly, the function $\deg_{\Omega} : \text{Div}_{0,\Omega}(K) \rightarrow \mathbb{Z}$ given by

$$\deg_{\Omega} \left(\sum_{\mathfrak{P}} n_{\mathfrak{P}} \cdot \mathfrak{P} \right) = \sum_{\mathfrak{P} : n_{\mathfrak{P}} < 0} (-n_{\mathfrak{P}}) \cdot \deg \mathfrak{P} = -n_{\Omega} \cdot \deg \Omega \quad (2.15)$$

is an higher genus analogue of a degree of a polynomial.

Given positive integers $n \geq 1$, $\ell \geq 1$, $r \geq 2$, we consider the following sets of divisors, which are analogues of $S_1(q)$, $S_2(q)$ and $S_3(q)$:

$$S_1(r, K) = \{D \in \text{Div}_{0,\Omega}(K) : v_{\mathfrak{P}}(D) > 0 \implies \frac{r}{\gcd(r, \deg_K \mathfrak{P})} \mid v_{\mathfrak{P}}(D)\}, \quad (2.16)$$

$$S_2(r, K) = \{D \in \text{Div}_{0,\Omega}(K) : v_{\mathfrak{P}}(D) > 0 \implies r \mid \deg_K \mathfrak{P}\}, \quad (2.17)$$

$$S_3(r, \ell, K) = \{D \in \text{Div}_{0,\Omega}(K) : v_{\mathfrak{P}}(D) > 0 \implies r \mid \deg_K \mathfrak{P} \text{ and } v_{\mathfrak{P}}(D) \leq \ell\}. \quad (2.18)$$

We elaborate on the algebraic meaning of the sets S_1 , S_2 , S_3 . Let K_r be the fixed constant field extension over K of degree r . We have the following relation between primes of K_r and K .

Proposition 2.2. *[Ros02, Prop. 8.13] Let \mathfrak{P} be a prime of K . Then \mathfrak{P} splits into $\gcd(r, \deg_K \mathfrak{P})$ primes in K_r . Let \mathfrak{P}_r be a prime of K_r lying over \mathfrak{P} . Denote by $f(\mathfrak{P}_r/\mathfrak{P})$ the relative degree of \mathfrak{P}_r over \mathfrak{P} . Then*

$$\deg_{K_r} \mathfrak{P}_r = \frac{\deg_K \mathfrak{P}}{\gcd(r, \deg_K \mathfrak{P})}, \quad f(\mathfrak{P}_r/\mathfrak{P}) = \frac{r}{\gcd(r, \deg_K \mathfrak{P})}. \quad (2.19)$$

In particular, primes of K of degree divisible by r are exactly those that split completely in K_r , which gives an algebraic meaning to S_2 and S_3 . We may define the (linear) norm map [Che51, Chap. IV.7]

$$N_{K_r/K} : \text{Div}(K_r) \rightarrow \text{Div}(K) \quad (2.20)$$

by

$$\mathfrak{P}_r \mapsto f(\mathfrak{P}_r/\mathfrak{P}) \cdot \mathfrak{P}, \quad (2.21)$$

where \mathfrak{P}_r is a prime of K_r lying over \mathfrak{P} , a prime of K . By Proposition 2.2, the image of $N_{K_r/K}$ is spanned by

$$\left\{ \frac{r}{\gcd(r, \deg_K \mathfrak{P})} \mathfrak{P} : \mathfrak{P} \in \mathbb{P}_K \right\}. \quad (2.22)$$

Intersecting the image $N_{K_r/K}(K_r)$ with $\text{Div}_{0,\Omega}(K)$, we recover the set $S_1(r, K)$. When $r = 2$, $K = \mathbb{F}_q(T)$ and Ω is the prime at $1/T$, we obtain $S_1(r, K) = S_1(q)$. Hence, counting divisors of $S_1(r, K)$ is a generalization of Landau's problem over $\mathbb{F}_q[T]$. The asymptotics of

$$B_i(rn, r, K) = \#\{D \in S_i(r, K) : \deg_{\Omega}(D) = rn\} \quad (i = 1, 2) \quad (2.23)$$

and

$$B_3(rn, r, \ell, K) = \#\{D \in S_3(r, \ell, K) : \deg_{\Omega}(D) = rn\} \quad (2.24)$$

in a very general range of parameters are given in the following theorem.

Theorem 2.3. Let K be a function field with constant field \mathbb{F}_q . Fix a prime \mathfrak{Q} of K . Let g_K be the genus of K , and define

$$M_{K,\mathfrak{Q}} = \max\{g_K, \deg \mathfrak{Q}\}. \quad (2.25)$$

Let $n \geq 1$, $\ell \geq 1$, $r \geq 2$ be given integers. If $\deg_K \mathfrak{Q} \nmid rn$, we have

$$B_1(rn, r, K) = B_2(rn, r, K) = B_3(rn, r, \ell, K) = 0. \quad (2.26)$$

Otherwise, we have

$$B_1(rn, r, K) = \left(n + \frac{1}{r} - 1\right) \cdot q^{rn} \cdot \left(C_{1,r,K} + O\left(\frac{\exp(150 \frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}) \frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}}{n}\right)\right), \quad (2.27)$$

$$B_2(rn, r, K) = \left(n + \frac{1}{r} - 1\right) \cdot q^{rn} \cdot \left(C_{2,r,K} + O\left(\frac{\exp(150 \frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}) \frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}}{n}\right)\right), \quad (2.28)$$

$$B_3(rn, r, \ell, K) = \left(n + \frac{1}{r} - 1\right) \cdot q^{rn} \cdot \left(C_{r,\ell,K} + O\left(\frac{\exp(150 \frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}) \frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}}{n}\right)\right), \quad (2.29)$$

as long as

$$n \gg 1 + \frac{M_{K,\mathfrak{Q}}}{r^2 \ln(q)} \ln\left(\frac{M_{K,\mathfrak{Q}}}{r^2 \ln(q)} + 1\right). \quad (2.30)$$

In addition, the constants $C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K}$ may be estimated by

$$C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K} = \exp\left(O\left(\frac{M_{K,\mathfrak{Q}}}{rq^{r/2}}\right)\right). \quad (2.31)$$

A variant of the functions $B_2(rn, r, K)$, $B_3(rn, r, \ell, K)$, where a prime \mathfrak{Q} was not included in the definition, was studied in [CKY15, Thm. 4]. The results obtained there are meaningful only in the limit $n \rightarrow \infty$.

We also investigate the constants $C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K}$ and provide an expression for them, involving an infinite product over primes of \mathbb{P}_K .

Remark 2.4. In the limit $n \rightarrow \infty$, the expression $(n + \frac{1}{r} - 1)$ appearing in Theorem 2.3 may be replaced with $\frac{n^{\frac{1}{r}-1}}{\Gamma(\frac{1}{r})} (1 + O(\frac{1}{rn}))$: by [Jam13, Eq. 14],

$$\begin{aligned} \left(n + \frac{1}{r} - 1\right) &\leq \frac{n^{\frac{1}{r}-1}}{\Gamma(\frac{1}{r})}, \quad \text{and} \\ \left(n + \frac{1}{r} - 1\right) &\geq \frac{(n + \frac{1}{r})^{\frac{1}{r}-1}}{\Gamma(\frac{1}{r})} = \frac{n^{\frac{1}{r}-1}}{\Gamma(\frac{1}{r})} \left(1 + \frac{1}{rn}\right)^{\frac{1}{r}-1} \\ &\geq \frac{n^{\frac{1}{r}-1}}{\Gamma(\frac{1}{r})} \left(1 + \frac{1}{rn}\right)^{-1} \geq \frac{n^{\frac{1}{r}-1}}{\Gamma(\frac{1}{r})} \left(1 - \frac{1}{rn}\right). \end{aligned} \quad (2.32)$$

2.3 Prime factors in an arithmetic progression

Let $a, m \in \mathbb{F}_q[T]$ be a pair of coprime polynomials with m monic of positive degree. Let $G_{a,m} \subseteq \mathbb{F}_q[T]$ be the set of monic polynomials whose monic prime factors are in the arithmetic progression $a(T) \bmod m(T)$. Let

$$S(n; a, m) = \#\{f \in G_{a,m} : \deg(f) = n\}, \quad (2.33)$$

be the number of polynomials of degree n in the semigroup $G_{a,m}$. What bounds are satisfied by $S(n; a, m)$?

Although studying $S(n; a, m)$ is interesting for its own sake, the case $a = 1$ is an important ingredient in the proof of the following theorem of Thorne [Tho08, Thm. 1.2], which is a function field analogue of a theorem of Shiu [Shi00, Thm. 1].

Theorem 2.5 (Thorne). *Let $a, m \in \mathbb{F}_q[T]$ with $\gcd(a, m) = 1$ and $\deg m > 0$, m monic. There exists a constant D' (depending on q and m) such that for any $D > D'$ there exists a string of consecutive monic primes*

$$p_{r+1} \equiv p_{r+2} \cdots \equiv p_{r+k} \equiv a \pmod{m} \quad (2.34)$$

of degree at most D , where k satisfies

$$k \gg_q \frac{1}{\phi(m)} \left(\frac{\log D}{(\log \log D)^2} \right)^{1/\phi(m)}. \quad (2.35)$$

Here “consecutive” is to be understood with respect to lexicographic order. Thorne’s proof uses the following asymptotic formula, corollary of a result of Manstavicius and Skrabutėnas [MS93, Thm. 1]:

$$S(n; 1, m) \sim C_{1,m} \cdot \frac{n^{-1+\frac{1}{\phi(m)}}}{\Gamma(1/\phi(m))} \cdot q^n, \quad n \rightarrow \infty, \quad (2.36)$$

where

$$C_{a,m} = \lim_{u \rightarrow \frac{1}{q}^-} (1 - qu)^{1/\phi(m)} \prod_{P \in \mathcal{P}_q: P \equiv a \pmod{m}} (1 - u^{\deg P})^{-1}. \quad (2.37)$$

As remarked after [Tho08, Lem. 3.5], making (2.36) effective allows one to determine the constant D' appearing in Theorem 2.5. We establish the following version of (2.36).

Theorem 2.6. *Let $a, m \in \mathbb{F}_q[T]$ be a pair of coprime polynomials with $\deg m > 0$ and m monic. For*

$$n \geq 1 + 5(6 \deg m + 30) \ln(6 \deg m + 30), \quad (2.38)$$

we have

$$S(n; a, m) = \left(n + \frac{1}{\phi(m)} - 1 \right) \cdot q^n \left(C_{a,m} + O \left(\frac{\exp(\frac{3(\deg m + 3)}{\sqrt{q}}) \frac{(\deg m + 3)}{\sqrt{q}}}{n} \right) \right), \quad (2.39)$$

where the implied constant is (at most) 48.

3 Methods

Let q be a prime power, and let $\mathbb{F}_q[T]$ be the polynomial ring over the finite field \mathbb{F}_q . Denote by $\pi_q(n)$ the number of irreducible monic polynomials in $\mathbb{F}_q[T]$ of degree n .

Let $G \subseteq \mathbb{F}_q[T]$ be a multiplicative semigroup generated by (possibly infinitely many) mutually coprime monic polynomials. Let $g(n)$ be the number of generators of degree n . The coefficients of the generating function

$$\begin{aligned} F_G(x) &:= \prod_{n \geq 1} (1 + x^n + x^{2n} + \cdots)^{g(n)} \\ &= \prod_{n \geq 1} (1 - x^n)^{-g(n)} \end{aligned} \quad (3.1)$$

count how many polynomials in G are of a specified degree. By writing $F_G(x) = \exp(\ln F_G(x))$, we may express $F_G(x)$ as the formal power series

$$\exp \left(\sum_{n \geq 1} \frac{\psi_G(n) x^n}{n} \right), \quad (3.2)$$

where

$$\psi_G(n) := \sum_{d|n} d \cdot g(d). \quad (3.3)$$

For instance, when $G = \mathcal{M}_q \subseteq \mathbb{F}_q[T]$ is the semigroup of monic polynomials, generated by monic irreducible polynomials, the corresponding function $\psi_{\mathcal{M}_q}$ is the weighted prime-counting function $\psi_{\mathcal{M}_q}(n) = \sum_{d|n} d \cdot \pi_q(d)$, which satisfies [Ros02, Prop. 2.1]

$$\psi_{\mathcal{M}_q}(n) = \sum_{d|n} d \cdot \pi_q(d) = q^n. \quad (3.4)$$

It turns out that for many semigroups that occur in counting problems, ψ_G satisfies the following bound, where α, β, c_1, c_2 are some real numbers satisfying $\alpha > \beta > 0$:

$$|\psi_G(n) - c_1 \beta^{-n}| \leq c_2 \alpha^{-n}. \quad (3.5)$$

The bound (3.5) insures that we can write F_G as a product of two analytic functions, with radii of convergence at most α and exactly β , respectively:

$$\begin{aligned} F_G(x) &= \exp \left(\sum_{n \geq 1} \frac{e_n x^n}{n} \right) \cdot \exp \left(\sum_{n \geq 1} \frac{c_1 \beta^{-n} x^n}{n} \right) \\ &= \exp \left(\sum_{n \geq 1} \frac{e_n x^n}{n} \right) \cdot \left(1 - \frac{x}{\beta} \right)^{-c_1}, \end{aligned} \quad (3.6)$$

where

$$e_n = \psi_G(n) - c_1 \beta^{-n}. \quad (3.7)$$

In particular, the radii of convergence are distinct.

The problem of estimating the coefficients of a product of two functions with different radii of convergence has been studied previously. First, we introduce a useful piece of notation. For a power series $f(x) = \sum_{i \geq 0} f_i x^i$, $[x^n]f(x)$ denotes the coefficient of x^n in f , i.e. f_n .

We mention two classical results. The first is [FS09, Thm. VI.12].

Theorem 3.1. *Let $a(x) = \sum a_n x^n$ and $b(x) = \sum b_n x^n$ be two power series with radii of convergence $\alpha > \beta \geq 0$, respectively. Assume that $b_{n-1}/b_n \rightarrow \beta$ as n tends to ∞ , and that $a(\beta) \neq 0$. Then the coefficients of the product $f(x) = a(x) \cdot b(x)$ satisfy the following, as n tends to ∞ :*

$$[x^n]f(x) \sim a(\beta) \cdot b_n. \quad (3.8)$$

Theorem 3.1 is proved using calculus. Applying Theorem 3.1, we solve the problem of estimating $[x^n]F_G(x)$ as n tends to ∞ and q is fixed, under assumption (3.5):

$$\begin{aligned} [x^n]F_G(x) &\sim \exp \left(\sum_{n \geq 1} \frac{e_n \beta^n}{n} \right) \cdot \binom{-c_1}{n} \cdot \left(-\frac{1}{\beta} \right)^n \\ &= \exp \left(\sum_{n \geq 1} \frac{e_n \beta^n}{n} \right) \cdot \binom{n + c_1 - 1}{n} \cdot \beta^{-n}. \end{aligned} \quad (3.9)$$

Theorem 3.1 does not give information on the rate of convergence. A method, due to Darboux, gives a more informative estimate for certain b [Hen77, Thm. 11.10b].

Theorem 3.2. *Let $a(x) = \sum a_n x^n$ and $b(x) = (1 - \frac{x}{\beta})^{-c_1} = \sum b_n x^n$ ($c_1 \in \mathbb{C} \setminus \mathbb{Z}$) be two power series with radii of convergence $\alpha > \beta \geq 0$, respectively. Fix an integer $m \geq 0$. Then the coefficients of the product $f(x) = a(x) \cdot b(x)$ satisfy the following, as n tends to ∞ :*

$$[x^n]f(x) = b_n \cdot \left(a(\beta) + \sum_{k=1}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta) + O_{a,b,m} \left(\frac{1}{n^{m+1}} \right) \right). \quad (3.10)$$

Most proofs of Theorem 3.2 use contour integration, although an elementary proof was found by Knuth and Wilf [KW89]. Using (3.6), Theorem 3.2 gives an asymptotic expansion of $[x^n]F_G(x)$, as n tends to ∞ , in all of this paper's applications.

Methods similar to Theorem 3.2 were used to study semigroup counting problems related to finite fields in the limit $n \rightarrow \infty$ and q fixed, see the papers [War92, MS93] and the monographs [Kno90, KZ01].

Our objective is to establish results on the magnitude of $[x^n]F_G(x)$ in the limit $q^n \rightarrow \infty$, for which Theorem 3.2 is not suitable. To do so, we need to work out the dependency of the error term in (3.10) on the parameters a, b . This is done in the following theorem, under additional restrictions influenced by (3.5).

Theorem 3.3. *Let $a(x) = \exp\left(\sum_{n \geq 1} \frac{\widetilde{a}_n x^n}{n}\right) = \sum a_n x^n$ and $b(x) = (1 - \frac{x}{\beta})^{-c_1} = \sum b_n x^n$ ($c_1 \in (0, 1)$) be two power series, with radii of convergence at least α and exactly β , respectively. Assume that $\alpha > \beta > 0$. Assume that*

$$r = \frac{\beta}{\alpha} \leq \frac{1}{\sqrt{2}}. \quad (3.11)$$

Further assume that there is a positive number c_2 such that

$$|\widetilde{a}_n| \leq \frac{c_2}{\alpha^n}. \quad (3.12)$$

Fix an integer $m \geq 0$. For an integer $n > m$, write the n th coefficient f_n of $f(x) = a(x) \cdot b(x)$ as

$$[x^n]f(x) = b_n \cdot \left(a(\beta) + \sum_{k=1}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta) + E \right). \quad (3.13)$$

Then

$$|E| \ll_m \exp(3c_2 r) \left(\left(\frac{r}{n} \right)^{m+1} (c_2 + m)_{m+1} + \binom{n+c_2-1}{n} \frac{4n^2}{c_1} r^n \right) \quad (3.14)$$

$$\ll_{m, c_1, c_2} \left(\frac{r}{n} \right)^{m+1}, \quad (3.15)$$

where $(x)_n := x(x-1) \cdots (x-(n-1))$ is the falling factorial. For $m = 0$, the implicit constant in (3.14) is (at most) 24.

We also establish the following effective corollary.

Corollary 3.4. *Let a, b, α, β be as in Theorem 3.3, and assume that they satisfy (3.11) and (3.12). Let $f(x) = a(x) \cdot b(x)$. For n large enough, specifically*

$$n \geq \max\left\{ 5 \left(\frac{2c_2 + 4}{\ln(1/r)} + 1 \right) \ln \left(\frac{2c_2 + 4}{\ln(1/r)} + 1 \right) + 1, 2 \frac{\ln(c_1^{-1})}{\ln(1/r)} + 1 \right\}, \quad (3.16)$$

we have

$$[x^n]f(x) = b_n \cdot \left(a(\beta) + O \left(\frac{\exp(3c_2 r) c_2 r}{n} \right) \right), \quad (3.17)$$

where the implied constant is (at most) 48.

Remark 3.5. In all of our applications, the Riemann hypothesis for function fields shows that β^{-1} is a of the form q^c for some positive integer c depending on the application and α^{-1} is the square root of β^{-1} . Thus, $r = \beta/\alpha = q^{-c/2}$, which has two implications. First, equation (3.11) is satisfied. Second,

$$\lim_{q \rightarrow \infty} \frac{r}{n} = 0, \quad (3.18)$$

which by (3.15) shows that as q tends to ∞ , the relative error term E tends to zero.

Remark 3.6. Assumption (3.12) implies that

$$\begin{aligned} |a(\beta)| &\geq \exp\left(\sum_{n \geq 1} \frac{-|\widetilde{a_n}| \beta^n}{n}\right) \geq \exp\left(\sum_{n \geq 1} \frac{-c_2 r^n}{n}\right) = (1-r)^{c_2}, \\ |a(\beta)| &\leq \exp\left(\sum_{n \geq 1} \frac{|\widetilde{a_n}| \beta^n}{n}\right) \leq \exp\left(\sum_{n \geq 1} \frac{c_2 r^n}{n}\right) = (1-r)^{-c_2}. \end{aligned} \quad (3.19)$$

In particular, we obtain the bound $a(\beta) = \exp(O(c_2 r))$.

4 Landau's theorem over $\mathbb{F}_q[T]$, for $A^2 + TB^2$

We begin with an overlook of the proof of Theorem 1.1, leaving the more technical details to §4.1. Let $G_q \subseteq \mathbb{F}_q[T]$ be the set of monic polynomials of the form $A^2 + TB^2$. By [BSSW16, Thm. 2.5], a monic polynomial f is in G_q if and only if the multiplicity of any monic irreducible polynomial P of the form $\left(\frac{P}{T}\right) = -1$ in the factorization of f is even. In other words, G_q is the semigroup generated by the following set of mutually coprime polynomials:

$$\begin{aligned} &\{P \in \mathbb{F}_q[T] : P \text{ is monic irreducible satisfying } \left(\frac{P}{T}\right) = 1\} \\ &\bigcup \{P^2 : P \in \mathbb{F}_q[T] \text{ is monic irreducible satisfying } \left(\frac{P}{T}\right) = -1\} \bigcup \{T\}. \end{aligned} \quad (4.1)$$

Let $\chi_2 : \mathbb{F}_q[T] \rightarrow \mathbb{C}$ denote the quadratic character modulo T :

$$\chi_2(f) = \left(\frac{f}{T}\right). \quad (4.2)$$

For any subset $S \subseteq \{-1, 0, 1\}$, let $\pi_q(n; \chi_2, S)$ count the monic irreducible polynomials P of degree n in $\mathbb{F}_q[T]$ such that $\chi_2(f) \in S$. For $s \in \{-1, 0, 1\}$, we write $\pi_q(n; \chi_2, s)$ for $\pi_q(n; \chi_2, \{s\})$. It follows that the generating function F_{G_q} of $B(n, q)$ is

$$\begin{aligned} F_{G_q}(x) &= \sum_{n \geq 0} B(n, q) x^n \\ &= \prod_{n \geq 1} (1 - x^n)^{-\pi_q(n; \chi_2, \{0, 1\})} (1 - x^{2n})^{-\pi_q(n; \chi_2, -1)}. \end{aligned} \quad (4.3)$$

If we set

$$g(n) = \begin{cases} \pi_q(n; \chi_2, \{0, 1\}) & 2 \nmid n, \\ \pi_q(n; \chi_2, \{0, 1\}) + \pi_q(\frac{n}{2}; \chi_2, -1) & 2 \mid n, \end{cases} \quad (4.4)$$

then F_{G_q} assumes the form

$$F_{G_q}(x) = \prod_{n \geq 1} (1 - x^n)^{-g(n)}. \quad (4.5)$$

As before, one sees that

$$F_{G_q}(x) = \exp\left(\sum_{n \geq 1} \frac{\psi_{G_q}(n) x^n}{n}\right), \quad (4.6)$$

where

$$\psi_{G_q}(n) = \sum_{d \mid n} d \cdot g(d). \quad (4.7)$$

In §4.1 we obtain a closed-form expression for $\psi_{G_q}(n)$. In particular, we find that

$$e_n = \psi_{G_q}(n) - \frac{q^n}{2} \quad (4.8)$$

satisfies

$$e_n = O(q^{\lfloor n/2 \rfloor}), \quad (4.9)$$

and, as we saw in (3.6), we may write F_{G_q} as a product of two power series with distinct radii of convergence:

$$F_{G_q}(x) = \exp \left(\sum_{n \geq 1} \frac{e_n x^n}{n} \right) \cdot (1 - qx)^{-\frac{1}{2}}. \quad (4.10)$$

Theorem 3.3 with

$$a(x) = \exp \left(\sum_{n \geq 1} \frac{e_n x^n}{n} \right), \quad b(x) = (1 - qx)^{-\frac{1}{2}} \quad (4.11)$$

gives the asymptotics of $B(n, q)$.

4.1 Proof of Theorem 1.1

First, we obtain an explicit formula for e_n . We write the (formal) zeta function of $\mathbb{F}_q[T]$ and its Euler product:

$$\begin{aligned} \mathcal{Z}_{\mathbb{F}_q[T]}(u) &= \sum_{f \in \mathcal{M}_q} u^{\deg f} = (1 - qu)^{-1} \\ &= \prod_{P \in \mathcal{P}_q} (1 - u^{\deg P})^{-1} = \prod_{n \geq 1} (1 - u^n)^{-\pi_q(n)}. \end{aligned} \quad (4.12)$$

We have $\pi_q(n) = \pi_q(n; \chi_2, \{0, 1\}) + \pi_q(n; \chi_2, -1)$, and so logarithmic differentiation of (4.12) gives

$$q^n = \sum_{d|n} d \cdot (\pi_q(d; \chi_2, \{0, 1\}) + \pi_q(d; \chi_2, -1)). \quad (4.13)$$

We consider the (formal) L-function of the quadratic character χ_2 :

$$\mathcal{L}_{\mathbb{F}_q[T]}(u, \chi_2) = \sum_{f \in \mathcal{M}_q} \chi_2(f) u^{\deg f}. \quad (4.14)$$

On the one hand, $\mathcal{L}_{\mathbb{F}_q[T]}(u, \chi_2)$ is actually the constant polynomial 1, as half of the elements of \mathbb{F}_q^\times are squares and half are non-squares (cf. [Ros02, Prop. 4.3]):

$$\mathcal{L}_{\mathbb{F}_q[T]}(u, \chi_2) = 1. \quad (4.15)$$

On the other hand, since χ_2 is completely multiplicative, $\mathcal{L}_{\mathbb{F}_q[T]}(u, \chi_2)$ admits the following Euler product:

$$\begin{aligned} \mathcal{L}_{\mathbb{F}_q[T]}(u, \chi_2) &= \prod_{P \in \mathcal{P}_q: \chi_2(P)=1} (1 - u^{\deg P})^{-1} \prod_{P \in \mathcal{P}_q: \chi_2(P)=-1} (1 + u^{\deg P})^{-1} \\ &= \prod_{n \geq 1} (1 - u^n)^{-\pi_q(n; \chi_2, 1)} \prod_{n \geq 1} (1 + u^n)^{-\pi_q(n; \chi_2, -1)} \\ &= \prod_{n \geq 1} (1 - u^n)^{-\pi_q(n; \chi_2, \{0, 1\})} \prod_{n \geq 1} (1 + u^n)^{-\pi_q(n; \chi_2, -1)} \cdot (1 - u). \end{aligned} \quad (4.16)$$

Comparing (4.15) and (4.16), we have the following identity:

$$\frac{1}{1 - u} = \prod_{n \geq 1} (1 - u^n)^{-\pi_q(n; \chi_2, \{0, 1\})} \prod_{n \geq 1} (1 + u^n)^{-\pi_q(n; \chi_2, -1)}. \quad (4.17)$$

We take the logarithmic derivative of (4.17), and obtain the following by comparing coefficients:

$$1 = \sum_{d|n} d \cdot \left(\pi_q(d; \chi_2, \{0, 1\}) + \pi_q(d; \chi_2, -1)(-1)^{n/d} \right). \quad (4.18)$$

Using (4.13), we simplify (4.18):

$$\sum_{d|n, 2d \nmid n} d \cdot \pi_q(d; \chi_2, -1) = \frac{q^n - 1}{2}. \quad (4.19)$$

Let $v_2(n)$ be the exponent of the greatest power of 2 that divides n . To compute $\sum_{d|n} d \cdot \pi_q(d; \chi_2, -1)$, we plug $n, \frac{n}{2}, \dots, \frac{n}{2^{v_2(n)}}$ for n in (4.19) and sum:

$$\sum_{d|n} d \cdot \pi_q(d; \chi_2, -1) = \sum_{i=0}^{v_2(n)} \frac{q^{n/2^i} - 1}{2}. \quad (4.20)$$

Using (4.13) and (4.20), we find

$$\sum_{d|n} d \cdot \pi_q(d; \chi_2, \{0, 1\}) = \frac{q^n + 1}{2} - \sum_{i=1}^{v_2(n)} \frac{q^{n/2^i} - 1}{2}. \quad (4.21)$$

Now we can calculate $\sum_{d|n} d \cdot g(d)$, using (4.4), (4.20) and (4.21):

$$\begin{aligned} \sum_{d|n} d \cdot g(d) &= \sum_{d|n} d \cdot \pi_q(d; \chi_2, \{0, 1\}) + \sum_{2|d|n} d \cdot \pi_q\left(\frac{d}{2}; \chi_2, -1\right) \\ &= \sum_{d|n} d \cdot \pi_q(d; \chi_2, \{0, 1\}) + 2 \sum_{2d'|n} d' \cdot \pi_q(d'; \chi_2, -1) \\ &= \frac{q^n + 1}{2} - \sum_{i=1}^{v_2(n)} \frac{q^{n/2^i} - 1}{2} + 2 \sum_{i=0}^{v_2(n)/2} \frac{q^{n/2^{i+1}} - 1}{2} \\ &= \frac{q^n + 1}{2} + \sum_{i=1}^{v_2(n)} \frac{q^{n/2^i} - 1}{2}. \end{aligned} \quad (4.22)$$

By (4.22), the exact value of e_n , as defined in (4.8), is

$$e_n = \frac{1}{2} + \sum_{i=1}^{v_2(n)} \frac{q^{n/2^i} - 1}{2}. \quad (4.23)$$

In particular, e_n satisfies

$$\frac{1}{2} \leq e_n \leq q^{\lfloor n/2 \rfloor}. \quad (4.24)$$

We establish Theorem 1.1 with

$$K_q = a(q^{-1}), \quad (4.25)$$

and show that this is the same K_q defined in (1.8). For $n = 1$, Theorem 1.1 is immediate since $B(1, q) = \frac{q+1}{2}$ and, by (4.24),

$$\begin{aligned} K_q &= a(q^{-1}) = \exp \left(\sum_{n \geq 1} \frac{e_n \cdot q^{-n}}{n} \right) \\ &= \exp \left(\sum_{n \geq 1} \frac{O(q^{\lfloor n/2 \rfloor - n})}{n} \right) = \exp \left(O \left(\frac{1}{q} \right) \right) = O(1), \end{aligned} \quad (4.26)$$

and so

$$B(1, q) = K_q \cdot \begin{pmatrix} 1 - \frac{1}{2} \\ 1 \end{pmatrix} \cdot q + O(1), \quad (4.27)$$

as needed. Now assume that $n > 1$. We may use Theorem 3.3 with $m = 1$ and the functions a, b as defined in (4.11), which satisfy $a \cdot b = F_{G_q}$ as we have seen in (4.10). By (4.24), the parameters for Theorem 3.3 are

$$c_1 = \frac{1}{2}, c_2 = 1, \alpha = q^{-\frac{1}{2}}, \beta = q^{-1}. \quad (4.28)$$

We obtain the following estimate for $B(n, q)$:

$$\frac{B(n, q)}{\binom{n-\frac{1}{2}}{n} \cdot q^n} = a(q^{-1}) + \frac{1}{2n-1} \frac{a'(q^{-1})}{q} + O\left(\frac{1}{qn^2}\right). \quad (4.29)$$

Theorem 1.1 follows once we show $a'(q^{-1}) = O(1)$. Note (4.24) implies that

$$\frac{a'(q^{-1})}{a(q^{-1})} = \sum_{n \geq 1} e_n \cdot q^{1-n} = \sum_{n \geq 1} O(q^{1+\lfloor n/2 \rfloor - n}) = O(1). \quad (4.30)$$

By (4.26) and (4.30), $a'(q^{-1}) = O(1)$ is established, as needed. From 4.29 we see that $\lim_{n \rightarrow \infty} \frac{B(n, q)}{\binom{n-\frac{1}{2}}{n} \cdot q^n} = a(q^{-1})$, while (1.7) implies that $\lim_{n \rightarrow \infty} \frac{B(n, q)}{\binom{n-\frac{1}{2}}{n} \cdot q^n}$ equals the constant K_q defined in (1.8). Hence K_q defined in (1.8) coincides with K_q defined in (4.25), as claimed.

Remark 4.1. We show that $B(n, q)$ is a polynomial in q of degree n , and explain how to compute its first d coefficients. From (4.3) and (4.10), we obtain

$$\begin{aligned} B(n, q) &= [x^n] \left((1 - qx)^{-\frac{1}{2}} \cdot \exp \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right) \right) \\ &= \sum_{i=0}^n q^{n-i} \binom{n-i-\frac{1}{2}}{n-i} \cdot [x^i] \exp \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right). \end{aligned} \quad (4.31)$$

From (4.23) we see that e_n is a polynomial in q of degree $\leq \lfloor \frac{n}{2} \rfloor$. Thus, the n th coefficient of

$$\exp \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right) = \sum_{i \geq 0} \frac{1}{i!} \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right)^i \quad (4.32)$$

is also a polynomial in q of degree at most $\lfloor \frac{n}{2} \rfloor$. Hence, for any $i \leq n$,

$$\deg_q \left(q^{n-i} \binom{n-i-\frac{1}{2}}{n-i} \cdot [x^i] \exp \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right) \right) \leq n-i + \lfloor \frac{i}{2} \rfloor = n - \lceil \frac{i}{2} \rceil, \quad (4.33)$$

and if $i = 0$ then equality holds in (4.33). Hence, (4.33) implies that $B(n, q)$ is a polynomial in q of degree n . If one only wants the first d coefficients of $B(n, q)$, then only the first $2d-1$ coefficients of $\exp \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right)$ are needed, as may be seen from the following identity, which follows from (4.31) and (4.33):

$$B(n, q) = \sum_{i=0}^{2d-2} q^{n-i} \binom{n-i-\frac{1}{2}}{n-i} \cdot [x^i] \exp \left(\sum_{j \geq 1} \frac{e_j x^j}{j} \right) + O_n(q^{n-d}). \quad (4.34)$$

4.2 The constant K_q

We study the constant appearing in the main term of Theorem 1.1, K_q . In (1.8), the constant is expressed as the following Euler product:

$$K_q = (1 - q^{-1})^{-\frac{1}{2}} \prod_{P \in \mathcal{P}_q : (\frac{P}{q}) = -1} (1 - q^{-2 \deg P})^{-\frac{1}{2}}. \quad (4.35)$$

We provide another expression, which is the polynomial analogue of the following similar expression obtained in the integer setting independently in [Sha64, FV96]:

$$K = \frac{1}{\sqrt{2}} \prod_{n \geq 1} \left(\left(1 - \frac{1}{2^{2^n}} \right) \frac{\zeta(2^n)}{L(2^n, \chi)} \right)^{1/2^{n+1}}, \quad (4.36)$$

where $\zeta(s) = \sum_{n \geq 1} n^{-s}$, $L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$ and where χ is the principal character modulo 4.

Although the method of derivation of (4.36) applies *mutatis mutandis* to the polynomial setting, we do it slightly differently. In the process we obtain a functional equation for $F_{G_q}(x)$.

Lemma 4.2. *Let $A(x) = \exp \left(\sum_{n \geq 1} \frac{a_n x^n}{n} \right)$ be a formal power series. Let*

$$b_n = \begin{cases} a_n - a_{n/2} & 2 \mid n \\ a_n & 2 \nmid n \end{cases} \text{ and } B(x) = \exp \left(\sum_{n \geq 1} \frac{b_n x^n}{n} \right).$$

Then

$$A(x) = \prod_{k \geq 0} B(x^{2^k})^{2^{-k}}, \quad (4.37)$$

where each of the roots $B(x^{2^k})^{2^{-k}}$ is chosen so that the constant term is 1.

In particular,

$$\frac{A^2(x)}{A(x^2)} = B^2(x). \quad (4.38)$$

Proof. Assertion (4.38) follows from (4.37). We have

$$\begin{aligned} \prod_{k \geq 0} B(x^{2^k})^{2^{-k}} &= \prod_{k \geq 0} \exp \left(\sum_{n \geq 1} \frac{b_n x^{2^k n}}{2^k n} \right) \\ &= \exp \left(\sum_{n \geq 1} \frac{\left(\sum_{i=0}^{v_2(n)} b_{n/2^i} \right) x^n}{n} \right), \end{aligned} \quad (4.39)$$

so it suffices to show

$$a_n = \sum_{i=0}^{v_2(n)} b_{\frac{n}{2^i}}, \quad (4.40)$$

which follows from the definition of b_n . □

Applying Lemma 4.2 to $A = F_{G_q}$, we find

$$\frac{F_{G_q}^2(x)}{F_{G_q}(x^2)} = h^2(x), \quad (4.41)$$

where

$$h(x) = \exp \left(\sum_{n \geq 1} \left(\psi_{G_q}(n) - \underbrace{\psi_{G_q}\left(\frac{n}{2}\right)}_{=0 \text{ if } 2 \nmid n} \right) \frac{x^n}{n} \right). \quad (4.42)$$

Using the formula $\psi_{G_q}(n) = \frac{q^n+1}{2} + \sum_{i=1}^{v_2(n)} \frac{q^{n/2^i}-1}{2}$ (see (4.23)) we find

$$\underbrace{\psi_{G_q}(n) - \psi_{G_q}\left(\frac{n}{2}\right)}_{=0 \text{ if } 2 \nmid n} = \frac{q^n - (-1)^n}{2}, \quad (4.43)$$

thus

$$h(x) = \sqrt{\frac{1+x}{1-qx}}, \quad (4.44)$$

and

$$\frac{F_{G_q}^2(x)}{F_{G_q}(x^2)} = \frac{1+x}{1-qx}. \quad (4.45)$$

This functional equation determines $F_{G_q}(x)$ uniquely, assuming F_{G_q} is a power series with $F_{G_q}(0) \neq 0$.

Applying Lemma 4.2 to $A(x) = a(x) = \exp\left(\sum_{n \geq 1} \frac{e_n x^n}{n}\right)$, we find

$$\exp\left(\sum_{n \geq 1} \frac{e_n x^n}{n}\right) = \prod_{k \geq 0} \tilde{h}(x^{2^k})^{2^{-k}}, \quad (4.46)$$

where

$$\tilde{h}(x) = \frac{\sqrt{1+x}}{\sqrt[4]{1-qx^2}}. \quad (4.47)$$

Plugging $x = q^{-1}$ in (4.46) gives the following identity:

$$K_q = \prod_{k \geq 0} \frac{2^{k+1} \sqrt{1+q^{-2^k}}}{2^{k+2} \sqrt{1-q^{1-2^{k+1}}}} = \frac{\sqrt{1+q^{-1}}}{\sqrt[4]{1-q^{-1}}} \frac{\sqrt[4]{1+q^{-2}}}{\sqrt[8]{1-q^{-3}}} \frac{\sqrt[8]{1+q^{-4}}}{\sqrt[16]{1-q^{-7}}} \cdots, \quad (4.48)$$

which shows that K_q is an analytic function of q^{-1} .

Next we discuss the analogy between (4.48) and (4.36). Define $|f| = q^{\deg f}$, and put

$$\begin{aligned} \zeta_{\mathbb{F}_q[T]}(s) &= \sum_{f \in \mathcal{M}_q} |f|^{-s} = \frac{1}{1-q^{1-s}}, \\ L_{\mathbb{F}_q[T]}(s, \chi_2) &= \sum_{f \in \mathcal{M}_q} \chi_2(f) |f|^{-s} = 1. \end{aligned} \quad (4.49)$$

One may rearrange the terms of the product in (4.48) in a way that gives an expression which is analogous to (4.36):

$$K_q = \frac{1}{\sqrt{1-q^{-1}}} \prod_{n \geq 1} \left(\left(1 - \frac{1}{q^{2^n}}\right) \frac{\zeta_{\mathbb{F}_q[T]}(2^n)}{L_{\mathbb{F}_q[T]}(2^n, \chi_2)} \right)^{1/2^{n+1}}. \quad (4.50)$$

4.3 Second-order term for fixed q

In the integer setting, Shanks [Sha64] computed numerically the coefficient c appearing in the following expansion:

$$\sum_{n \leq x} b(n) = K \frac{x}{\sqrt{\ln x}} \left(1 + \frac{c}{\ln x} + O\left(\frac{1}{\ln^2 x}\right) \right), \quad (4.51)$$

and found that $c \approx 0.581948659$. We study a similar problem in the polynomial setting.

Equation (4.29) shows that in the limit $n \rightarrow \infty$, we may expand $B(n, q)$ as follows:

$$B(n, q) = K_q \cdot \binom{n - \frac{1}{2}}{n} \cdot q^n \left(1 + \frac{a'(q^{-1})}{2q \cdot a(q^{-1})} \frac{1}{n} + O\left(\frac{1}{qn^2}\right) \right). \quad (4.52)$$

We give a formula for the constant

$$c_q = \frac{a'(q^{-1})}{2q \cdot a(q^{-1})} = \frac{1}{2} \sum_{i \geq 1} e_i q^{-i}, \quad (4.53)$$

using the exact formula (4.23) for e_n :

$$\begin{aligned} c_q &= \frac{1}{2} \sum_{i \geq 1} e_i q^{-i} = \frac{1}{4} \sum_{i \geq 1} \left(q^{-i} + \sum_{k=1}^{v_2(i)} \left(q^{\frac{i}{2^k} - i} - q^{-i} \right) \right) \\ &= \frac{1}{4} \left(\frac{1}{q-1} + \sum_{j \geq 1} \sum_{i' \geq 1} q^{i'(1-2^j)} - q^{-i'2^j} \right) \\ &= \frac{1}{4} \left(\frac{1}{q-1} + \sum_{j \geq 1} \left(\frac{1}{q^{2^j-1}-1} - \frac{1}{q^{2^j}-1} \right) \right) \end{aligned} \quad (4.54)$$

In particular, (4.54) gives the following estimate for c_q :

$$c_q = \frac{1}{2q} + O\left(\frac{1}{q^2}\right). \quad (4.55)$$

5 Landau's theorem over $\mathbb{F}_q[T]$, for $A^2 - \alpha B^2$

5.1 Proof of Theorem 2.1

We only prove estimate (2.9), as (2.10), (2.11) are proven *mutatis mutandis*.

Let q be a prime power. As explained in the beginning of §2, given a non-square element $\alpha \in \mathbb{F}_q$, the set $S_1(q)$ defined in (2.2) is the set of monic polynomials of the form $A^2 - \alpha B^2$. By definition, $S_1(q)$ is the multiplicative semigroup of $\mathbb{F}_q[T]$ generated by the following set of mutually coprime polynomials:

$$\begin{aligned} &\{P \in \mathbb{F}_q[T] : P \text{ is monic irreducible of even degree}\} \\ &\bigcup \{P^2 : P \in \mathbb{F}_q[T] \text{ is monic irreducible of odd degree}\}. \end{aligned} \quad (5.1)$$

It follows that the generating function of $B_1(2n, q)$ (counting function of $S_1(q)$, defined in (2.3)) is

$$\begin{aligned} F_{S_1(q)}(x) &= \sum_{n \geq 0} B_1(2n, q) x^n \\ &= \prod_{P \in \mathcal{P}_q : 2 \mid \deg P} (1 - x^{\deg P/2})^{-1} \prod_{P \in \mathcal{P}_q : 2 \nmid \deg P} (1 - x^{\deg P})^{-1} \\ &= \prod_{n \geq 1} (1 - x^n)^{-\pi_q(2n)} (1 - x^{2n-1})^{-\pi_q(2n-1)}. \end{aligned} \quad (5.2)$$

If we set

$$h(n) = \begin{cases} \pi_q(2n) + \pi_q(n) & 2 \nmid n, \\ \pi_q(2n) & 2 \mid n, \end{cases} \quad (5.3)$$

then $F_{S_1(q)}$ assumes the form

$$F_{S_1(q)}(x) = \prod_{n \geq 1} (1 - x^n)^{-h(n)}. \quad (5.4)$$

As before, one sees that

$$F_{S_1(q)}(x) = \exp \left(\sum_{n \geq 1} \frac{\psi_{S_1(q)}(n)x^n}{n} \right), \quad (5.5)$$

where

$$\psi_{S_1(q)}(n) = \sum_{d|n} d \cdot h(d). \quad (5.6)$$

We evaluate $\psi_{S_1(q)}(n)$. Let $v_2(n)$ be the exponent of the greatest power of 2 that divides n . By (5.6), we have

$$\begin{aligned} \psi_{S_1(q)}(n) &= \sum_{d|n} d \cdot \pi_q(2d) + \sum_{d|n, 2 \nmid d} d \cdot \pi_q(d) \\ &= \frac{1}{2} \left(\sum_{d'|2n} d' \cdot \pi_q(d') - \sum_{d'|2n, 2 \nmid d'} d' \cdot \pi_q(d') \right) + \sum_{d|n, 2 \nmid d} d \cdot \pi_q(d) \\ &= \frac{1}{2} \left(\sum_{d'|2n} d' \cdot \pi_q(d') \right) + \frac{1}{2} \left(\sum_{d'|n, 2 \nmid d'} d' \cdot \pi_q(d') \right) \\ &= \frac{1}{2} \left(\sum_{d'|2n} d' \cdot \pi_q(d') \right) + \frac{1}{2} \left(\sum_{d'|\frac{n}{2^{v_2(n)}}} d' \cdot \pi_q(d') \right). \end{aligned} \quad (5.7)$$

By (3.4) and (5.7), we find

$$\psi_{S_1(q)}(n) = \frac{q^{2n}}{2} + \frac{q^{\left(\frac{n}{2^{v_2(n)}}\right)}}{2}. \quad (5.8)$$

If we define

$$f_n = \psi_{S_1(q)}(n) - \frac{q^{2n}}{2}, \quad (5.9)$$

we see by (5.7) that

$$f_n = \frac{q^{\left(\frac{n}{2^{v_2(n)}}\right)}}{2} = O(q^n). \quad (5.10)$$

As we saw in (3.6), we may write $F_{S_1(q)}$ as a product of two power series with distinct radii of convergence:

$$F_{S_1(q)}(x) = \exp \left(\sum_{n \geq 1} \frac{f_n x^n}{n} \right) \cdot (1 - q^2 x)^{-\frac{1}{2}}. \quad (5.11)$$

We may apply Theorem 3.3 with $m = 0$ and

$$a(x) = \exp \left(\sum_{n \geq 1} \frac{f_n x^n}{n} \right), \quad b(x) = (1 - q^2 x)^{-\frac{1}{2}}. \quad (5.12)$$

By (5.10), the parameters for Theorem 3.3 are

$$c_1 = \frac{1}{2}, \quad c_2 = \frac{1}{2}, \quad \alpha = q^{-1}, \quad \beta = q^{-2}. \quad (5.13)$$

By Theorem 3.3 we find

$$B_1(2n, q) = \binom{n - \frac{1}{2}}{n} \cdot q^{2n} \cdot \left(a(q^{-2}) + O\left(\frac{1}{qn}\right) \right). \quad (5.14)$$

This establishes (2.9) with

$$C_{q,1} = a(q^{-2}). \quad (5.15)$$

By Remark 3.6,

$$C_{q,1} = 1 + O\left(\frac{1}{q}\right), \quad (5.16)$$

which concludes the proof.

5.2 The constant $C_{q,1}$

We study the constant appearing in the main term of (2.9), $C_{q,1}$. First, we show how we may express it as a product over primes. By (5.11) (5.12), and (5.13),

$$a(x) = \frac{F_{S_1(q)}(x)}{b(x)} \quad (5.17)$$

for any $|x| < q^{-2}$. Letting $x \rightarrow (q^{-2})^-$ in (5.17) and using (5.15), we obtain

$$C_{q,1} = \lim_{x \rightarrow (q^{-2})^-} \frac{F_{S_1(q)}(x)}{b(x)}. \quad (5.18)$$

For $0 < x < q^{-2}$, b has the following Euler product:

$$\begin{aligned} b(x) &= (1 - q^2 x)^{-\frac{1}{2}} = (1 - q\sqrt{x})^{-\frac{1}{2}} (1 + q\sqrt{x})^{-\frac{1}{2}} \\ &= \mathcal{Z}_{\mathbb{F}_q[T]}^{1/2}(\sqrt{x}) \cdot \mathcal{Z}_{\mathbb{F}_q[T]}^{1/2}(-\sqrt{x}) \\ &= \prod_{P \in \mathcal{P}_q} (1 - x^{\deg P/2})^{-1/2} \cdot \prod_{P \in \mathcal{P}_q} (1 - (-1)^{\deg P} x^{\deg P/2})^{-1/2}, \end{aligned} \quad (5.19)$$

where $\mathcal{Z}_{\mathbb{F}_q[T]}(x)$ is defined in (4.12). By considering odd-degree and even-degree primes separately, equation (5.19) shows

$$b(x) = \prod_{P \in \mathcal{P}_q: 2|\deg P} (1 - x^{\deg P/2})^{-1} \prod_{P \in \mathcal{P}_q: 2 \nmid \deg P} (1 - x^{\deg P})^{-1/2}. \quad (5.20)$$

By (5.18), (5.20) and the Euler product for $F_{S_1(q)}$ given in (5.2), we obtain the following expression for $C_{q,1}$:

$$\begin{aligned} C_{q,1} &= \lim_{x \rightarrow (q^{-2})^-} \frac{\prod_{P \in \mathcal{P}_q: 2|\deg P} (1 - x^{\deg P/2})^{-1} \prod_{P \in \mathcal{P}_q: 2 \nmid \deg P} (1 - x^{\deg P})^{-1}}{\prod_{P \in \mathcal{P}_q: 2|\deg P} (1 - x^{\deg P/2})^{-1} \prod_{P \in \mathcal{P}_q: 2 \nmid \deg P} (1 - x^{\deg P})^{-1/2}} \\ &= \lim_{x \rightarrow (q^{-2})^-} \prod_{P \in \mathcal{P}_q: 2 \nmid \deg P} (1 - x^{\deg P})^{-\frac{1}{2}} \\ &= \prod_{P \in \mathcal{P}_q: 2 \nmid \deg P} (1 - q^{-2 \deg P})^{-\frac{1}{2}}. \end{aligned} \quad (5.21)$$

We provide another expression for $C_{q,1}$. Applying Lemma 4.2 to $A(x) = \exp\left(\sum_{n \geq 1} \frac{f_n x^n}{n}\right)$, we find

$$\exp\left(\sum_{n \geq 1} \frac{f_n x^n}{n}\right) = \prod_{k \geq 0} B(x^{2^k})^{2^{-k}}, \quad (5.22)$$

where

$$B(x) = \exp\left(\sum_{2 \nmid n} \frac{q^n x^n}{2n}\right) = \frac{\exp\left(\sum_{n \geq 1} \frac{q^n x^n}{2n}\right)}{\exp\left(\sum_{2|n} \frac{q^n x^n}{2n}\right)} = \frac{(1 - qx)^{-\frac{1}{2}}}{(1 - q^2 x^2)^{-\frac{1}{4}}} = \left(\frac{1 + qx}{1 - qx}\right)^{\frac{1}{4}}. \quad (5.23)$$

Plugging $x = q^{-2}$ in (5.22) and using (5.15), we obtain

$$C_{q,1} = \prod_{k \geq 0} \left(\frac{1 + q^{1-2^{k+1}}}{1 - q^{1-2^{k+1}}} \right)^{-2^{-k-2}}. \quad (5.24)$$

Next we discuss the analogy between (5.24) and (4.36). Let $\eta : \mathbb{F}_q[T] \rightarrow \mathbb{C}$ be the (generalized) Dirichlet character $\eta(f) = (-1)^{\deg(f)}$, and define $|f| = q^{\deg f}$. Let $\zeta_{\mathbb{F}_q[T]}$ be as in (4.49) and

$$L_{\mathbb{F}_q[T]}(s, \eta) = \sum_{f \in \mathcal{M}_q} \eta(f) |f|^{-s}, \quad (5.25)$$

which equals

$$L_{\mathbb{F}_q[T]}(s, \eta) = \sum_{n \geq 0} (-1)^n q^n q^{-ns} = \frac{1}{1 + q^{1-s}}. \quad (5.26)$$

The identity (5.24) may be written differently as an expression which is analogous to (4.36):

$$C_{q,1} = \prod_{n \geq 1} \left(\frac{\zeta_{\mathbb{F}_q[T]}(2^n)}{L_{\mathbb{F}_q[T]}(2^n, \eta)} \right)^{1/2^{n+1}}. \quad (5.27)$$

5.3 Second-order term for fixed q

Consider the functions a, b defined in (5.12). By (5.11), the product $a \cdot b$ is the generating function of $B_1(2n, q)$. Hence, if we apply Theorem 3.3 with $m = 1$ to the functions a, b , we find that in the limit $n \rightarrow \infty$, we may expand $B_1(2n, q)$ as follows:

$$B_1(2n, q) = C_{q,1} \cdot \binom{n - \frac{1}{2}}{n} \cdot q^{2n} \left(1 + \frac{a'(q^{-2})}{2q^2 \cdot a(q^{-2})} \frac{1}{n} + O\left(\frac{1}{q^2 n^2}\right) \right). \quad (5.28)$$

We give a formula for the constant $c'_q = \frac{a'(q^{-2})}{2q^2 \cdot a(q^{-2})} = \frac{1}{2} \sum_{i \geq 1} f_i q^{-2i}$ using the exact formula (5.9) for f_n :

$$c'_q = \frac{1}{2} \sum_{i \geq 1} f_i q^{-2i} = \frac{1}{4} \sum_{i \geq 1} q^{\left(\frac{i}{2^{v_2(i)}}\right) - 2i}. \quad (5.29)$$

In particular, equation (5.29) gives the following estimate for c'_q :

$$c'_q = \frac{1}{4q} + O\left(\frac{1}{q^3}\right). \quad (5.30)$$

6 Counting divisors over function fields

Here we prove Theorem 2.3. First, we prove an auxiliary lemma.

6.1 Counting primes

Lemma 6.1. *Let K be a function field with finite constant field \mathbb{F}_q , i.e. K is a finitely generated field extension of transcendence degree one over \mathbb{F}_q and \mathbb{F}_q is algebraically closed in K . Fix a prime \mathfrak{Q} of K . For any $n \geq 1$, let*

$$\pi_{K, \mathfrak{Q}}(n) = \#\{\text{Primes of degree } n \text{ in } K\} \setminus \{\mathfrak{Q}\}. \quad (6.1)$$

Given integers $r \geq 2$, $\ell \geq 1$, define the following functions:

$$\psi_{r,K}(n) = \sum_{d|n} d \cdot \pi_{K,\Omega}(rd), \quad (6.2)$$

$$f_{r,\ell,K}(n) = \pi_{K,\Omega}(rn) - \underbrace{\pi_{K,\Omega}\left(\frac{rn}{\ell+1}\right)}_{=0 \text{ if } \ell+1 \nmid rn}, \quad (6.3)$$

$$\psi_{r,\ell,K}(n) = \sum_{d|n} d \cdot f_{r,\ell,K}(d), \quad (6.4)$$

$$\xi_{r,K}(n) = \sum_{d|nr} \frac{d \cdot \pi_{K,\Omega}(d)}{(d,r)}. \quad (6.5)$$

Denote by g_K the genus of K and let

$$M_{K,\Omega} = \max\{g_K, \deg \Omega\}. \quad (6.6)$$

Then

$$\psi_{r,K}(n) = \frac{q^{rn}}{r} + O\left(\frac{M_{K,\Omega}}{r} q^{rn/2}\right), \quad (6.7)$$

$$\psi_{r,\ell,K}(n) = \frac{q^{rn}}{r} + O\left(\frac{M_{K,\Omega}}{r} q^{rn/2}\right), \quad (6.8)$$

$$\xi_{r,K}(n) = \frac{q^{rn}}{r} + O\left(\frac{M_{K,\Omega}}{r} q^{rn/2}\right), \quad (6.9)$$

where the implied constants are (at most) 16, 42 and 50, respectively.

Proof. Let

$$\pi_K = \#\{\text{Primes of degree } n \text{ in } K\}. \quad (6.10)$$

The zeta function of K is

$$\zeta_K(u) = \sum_{D \in \text{Div}_{\geq 0}(K)} u^{\deg D} = \prod_{n \geq 1} (1 - u^n)^{-\pi_K(n)} = \prod_{n \geq 1} (1 - u^n)^{-\pi_{K,\Omega}(n)} \cdot (1 - u^{\deg \Omega})^{-1}. \quad (6.11)$$

The function $\zeta_K(u)$ is a rational function in u of the form

$$\zeta_K(u) = \frac{L_K(u)}{(1-u)(1-qu)}, \quad (6.12)$$

where L_K is a polynomial with $L_K(0) = 1$ and of degree twice the genus of K , $2g_K$. The Riemann hypothesis for ζ_K , proved by Weil, shows that the absolute value of the roots of L_K is $q^{-1/2}$ [Ros02, Thm. A.7]. Hence, taking the logarithmic derivative of (6.11), (6.12) and equating coefficients, we find

$$\sum_{d|n} d \cdot \pi_{K,\Omega}(d) = q^n + 1 - \deg \Omega \cdot 1_{\deg \Omega | n} + O(g_K q^{n/2}) = q^n + O(M_{K,\Omega} q^{n/2}), \quad (6.13)$$

with implied constant (at most) 3. We estimate $\psi_{r,K}(n)$ as follows, using (6.13):

$$\begin{aligned} \sum_{d|n} d \cdot \pi_{K,\Omega}(rd) &= \frac{1}{r} \sum_{d|n} rd \cdot \pi_{K,\Omega}(rd) \\ &= \frac{1}{r} \left(\sum_{d'|rn} d' \cdot \pi_{K,\Omega}(d') - \sum_{r \nmid d'|rn} d' \cdot \pi_{K,\Omega}(d') \right) \\ &= \frac{1}{r} \left(q^{rn} + O(M_{K,\Omega} q^{rn/2}) - \sum_{r \nmid d'|rn} d' \cdot \pi_{K,\Omega}(d') \right), \end{aligned} \quad (6.14)$$

where the implied constant is 3. If d' is an integer dividing nr but not divisible by r , it means $d' \mid \frac{nr}{p}$ for some prime p dividing nr . Hence, using (6.13), we see that the sum $\sum_{r \nmid d' \mid nr} d' \cdot \pi_{K,\Omega}(d')$ is at most

$$\begin{aligned}
\sum_{r \nmid d' \mid nr} d' \cdot \pi_{K,\Omega}(d') &\leq \sum_{p \mid nr} \sum_{d' \mid \frac{nr}{p}} d' \cdot \pi_{K,\Omega}(d') \\
&\leq \sum_{p \mid nr} \left(q^{nr/p} + 3M_{K,\Omega} q^{\frac{nr}{2p}} \right) \\
&\leq q^{\lfloor \frac{nr}{2} \rfloor} \left(\sum_{i \geq 0} q^{-i} \right) + 3M_{K,\Omega} q^{\lfloor \frac{nr}{2} \rfloor / 2} \left(\sum_{i \geq 0} q^{-\frac{i}{2}} \right) \\
&\leq \frac{1}{1 - q^{-1}} q^{\lfloor \frac{nr}{2} \rfloor} + 3M_{K,\Omega} \frac{1}{1 - q^{-1/2}} q^{\lfloor \frac{nr}{2} \rfloor} \\
&\leq (2 + \frac{3M_{K,\Omega}}{1 - 2^{-1/2}}) q^{\frac{nr}{2}} \leq 13M_{K,\Omega} q^{\frac{nr}{2}}.
\end{aligned} \tag{6.15}$$

Combining (6.14) and (6.15), we obtain (6.7) with an implied constant $3 + 13 = 16$. We now prove (6.8). Note that (6.13) implies

$$\pi_{K,\Omega}(n) \leq \frac{4}{n} M_{K,\Omega} q^n. \tag{6.16}$$

If $\ell + 1 \nmid rn$, then $\psi_{r,\ell,K}(n) = \psi_{r,K}(n)$, and (6.8) is established. Otherwise, by (6.16),

$$\begin{aligned}
\sum_{d \mid n, \ell+1 \mid rd} d \cdot \pi_{K,\Omega} \left(\frac{rd}{\ell+1} \right) &\leq 4M_{K,\Omega} \frac{\ell+1}{r} \sum_{d \mid n, \ell+1 \mid rd} q^{\frac{rd}{\ell+1}} \\
&\leq 4M_{K,\Omega} \frac{\ell+1}{r} q^{\frac{rn}{\ell+1}} \sum_{i \geq 0} q^{-i} \\
&\leq 8M_{K,\Omega} \frac{\ell+1}{r} q^{\frac{rn}{\ell+1}}.
\end{aligned} \tag{6.17}$$

If $\ell = 1$, then (6.17) gives

$$\sum_{d \mid n, \ell+1 \mid rd} d \cdot \pi_{K,\Omega} \left(\frac{rd}{\ell+1} \right) \leq 16 \frac{M_{K,\Omega}}{r} q^{\frac{rn}{2}}. \tag{6.18}$$

By (6.18) and (6.7), estimate (6.8) is established with the absolute constant $16+16=32$.

If $\ell > 1$, then (6.17) gives

$$\sum_{d \mid n, \ell+1 \mid rd} d \cdot \pi_{K,\Omega} \left(\frac{rd}{\ell+1} \right) \leq \frac{8M_{K,\Omega}}{r} \cdot rn \cdot q^{\frac{rn}{3}}. \tag{6.19}$$

Note that for any positive x ,

$$x = \frac{6}{e \ln 2} \cdot e \cdot \frac{\ln 2}{6} x \leq \frac{6}{e \ln 2} \cdot e \cdot \exp\left(\left(\frac{\ln 2}{6} x\right) - 1\right) = \frac{6}{e \ln 2} \cdot 2^{x/6} \leq \frac{6}{e \ln 2} \cdot q^{x/6}. \tag{6.20}$$

Using (6.20) with $x = rn$ in (6.19), we obtain

$$\sum_{d \mid n, \ell+1 \mid rd} d \cdot \pi_{K,\Omega} \left(\frac{rd}{\ell+1} \right) \leq \frac{8 \cdot \frac{6}{e \ln 2} M_{K,\Omega}}{r} q^{\frac{rn}{2}}. \tag{6.21}$$

By (6.18) and (6.7), estimate (6.8) is established with the absolute constant $16 + 8 \cdot \frac{6}{e \ln 2} \leq 42$. We now prove (6.9). From (6.2) and (6.5), we have

$$\begin{aligned}
|\xi_{r,K}(n) - \psi_{r,K}(n)| &\leq \sum_{d \mid nr, d \neq nr} \frac{d}{(d,r)} \cdot \pi_{K,\Omega}(d) \\
&\leq \sum_{d \leq \frac{nr}{3}} d \cdot \pi_{K,\Omega}(d) + 1_{2 \mid rn} \cdot \frac{rn/2}{(rn/2, r)} \cdot \pi_{K,\Omega}(rn/2).
\end{aligned} \tag{6.22}$$

From (6.16) and (6.20), we obtain

$$\begin{aligned} \sum_{d \leq \frac{nr}{3}} d \cdot \pi_{K, \Omega}(d) &\leq 4M_{K, \Omega} \sum_{d \leq \frac{nr}{3}} q^d \leq 8M_{K, \Omega} q^{rn/3} \\ &\leq 8M_{K, \Omega} \frac{6}{e \ln 2} \frac{1}{rn} q^{rn/2} \leq \frac{26M_{K, \Omega}}{r} q^{rn/2}. \end{aligned} \quad (6.23)$$

From (6.16), we also have

$$1_{2|rn} \cdot \frac{rn/2}{(rn/2, r)} \cdot \pi_{K, \Omega}(rn/2) \leq n \cdot \frac{8}{rn} M_{K, \Omega} q^{rn/2} = \frac{8M_{K, \Omega}}{r} q^{rn/2}. \quad (6.24)$$

From (6.22), (6.23), (6.24) and (6.7), we arrive at estimate (6.9) with the absolute implied constant $16 + 26 + 8 = 50$. \square

6.2 Proof of Theorem 2.3

We first treat the case $\deg_K \Omega \nmid rn$. The divisors counted by $B_i(rn, rk)$ and $B_3(rn, r, \ell, K)$ satisfy

$$\deg_{\Omega}(D) = rn. \quad (6.25)$$

By (2.15), the condition (6.25) is equivalent to

$$v_{\Omega} = -\frac{rn}{\deg_K \Omega}. \quad (6.26)$$

The right-hand side of (6.26) is not integral when $\deg_K \Omega \nmid rn$, hence

$$B_1(rn, r, K) = B_2(rn, r, K) = B_3(rn, r, \ell, K) = 0. \quad (6.27)$$

From now on we assume

$$\deg_K \Omega \mid rn. \quad (6.28)$$

Given a divisor $D = \sum_{\mathfrak{P} \in \mathbb{P}_K} v_{\mathfrak{P}}(D) \cdot \mathfrak{P} \in \text{Div}_{0, \Omega}(K)$, we define

$$D_0 = \sum_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K} v_{\mathfrak{P}}(D) \cdot \mathfrak{P}, \quad D_{\infty} = -v_{\Omega}(D) \cdot \Omega. \quad (6.29)$$

Note that $D = D_0 - D_{\infty}$. A divisor $D \in \text{Div}_{0, \Omega}(K)$ is counted by $B_1(rn, r, K)/B_2(rn, r, K)/B_3(rn, r, \ell, K)$ if and only if

$$D_{\infty} = \frac{rn}{\deg_K \Omega} \cdot \Omega \quad (6.30)$$

and

$$D_0 \in \left\{ \sum_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K} n_{\mathfrak{P}} \cdot \mathfrak{P}, n_{\mathfrak{P}} \geq 0 : n_{\mathfrak{P}} > 0 \implies \begin{cases} \frac{r}{(r, \deg_K \mathfrak{P})} \mid n_{\mathfrak{P}} & (B_1(rn, r, K)) \\ r \mid \deg_K \mathfrak{P} & (B_2(rn, r, K)) \\ r \mid \deg_K \mathfrak{P} \text{ and } n_{\mathfrak{P}} \leq \ell & (B_3(rn, r, \ell, K)) \end{cases} \right\}. \quad (6.31)$$

Note that condition (6.31) does not depend on $\deg_K \Omega$, so we may assume $\deg_K \Omega = 1$ without loss of generality. The generating function of $\{B_1(rn, r, K)\}_{n \geq 0}$ is, by definition,

$$\begin{aligned}
G_{r,K}(x) &= \prod_{\mathfrak{P} \in \mathbb{P}_K \setminus \{\Omega\}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{-1} \\
&= \prod_{d|r} \prod_{\substack{\mathfrak{P} \in \mathbb{P}_K \setminus \{\Omega\} \\ (r, \deg_K \mathfrak{P}) = d}} (1 - x^{\frac{\deg_K \mathfrak{P}}{d}})^{-1} \\
&= \exp \left(\sum_{d|r} \sum_{m \geq 1} \frac{x^m}{m} \frac{\sum_{\substack{\mathfrak{P} \in \mathbb{P}_K \setminus \{\Omega\} \\ (\deg_K \mathfrak{P}, r) = d}} \deg_K \mathfrak{P}}{\deg_K \mathfrak{P} | md} \right) \\
&= \exp \left(\sum_{m \geq 1} \frac{\xi_{r,K}(m) x^m}{m} \right).
\end{aligned} \tag{6.32}$$

The generating function $F_{r,K}$ of $\{B_2(rm, r, K)\}_{m \geq 0}$ is, by definition,

$$\begin{aligned}
F_{r,K}(x) &= \prod_{m \geq 1} (1 + x^m + x^{2m} + \dots)^{\pi_{K,\Omega}(rm)} \\
&= \prod_{m \geq 1} (1 - x^m)^{-\pi_{K,\Omega}(rm)} \\
&= \exp \left(\sum_{m \geq 1} \frac{\psi_{r,K}(m) x^m}{m} \right),
\end{aligned} \tag{6.33}$$

where $\pi_{K,\Omega}$ is defined in (6.1) and $\psi_{r,K}$ is defined in (6.2). The generating function $F_{r,\ell,K}$ of $\{B_3(rm, r, \ell, K)\}_{n \geq 0}$ is, by definition,

$$\begin{aligned}
F_{r,\ell,K}(x) &= \prod_{m \geq 1} (1 + x^m + \dots + x^{m\ell})^{\pi_{K,\Omega}(rm)} \\
&= \prod_{m \geq 1} \left(\frac{1 - x^{m(\ell+1)}}{1 - x^m} \right)^{\pi_{K,\Omega}(rm)}.
\end{aligned} \tag{6.34}$$

We may rearrange (6.34) as follows:

$$F_{r,\ell,K}(x) = \prod_{m \geq 1} (1 - x^m)^{-f_{r,\ell,K}(m)} = \exp \left(\sum_{m \geq 1} \frac{\psi_{r,\ell,K}(m) x^m}{m} \right), \tag{6.35}$$

where $f_{r,\ell,K}$ and $\psi_{r,\ell,K}$ are defined in (6.3) and (6.4), respectively. The estimates (6.7), (6.8) and (6.9) of Lemma 6.1 show that we may write $G_{r,K}$, $F_{r,K}$ and $F_{r,\ell,K}$ as

$$\begin{aligned}
G_{r,K} &= a_1 \cdot b, \\
F_{r,K} &= a_2 \cdot b, \\
F_{r,\ell,K} &= a_3 \cdot b,
\end{aligned} \tag{6.36}$$

where

$$\begin{aligned}
b(x) &= \exp \left(\sum_{m \geq 1} \frac{q^{rm} x^m}{m} \right) = (1 - q^r x)^{-\frac{1}{r}}, \\
a_1 &= \frac{G_{r,K}}{b} = \exp \left(\sum_{m \geq 1} \frac{\widetilde{a_{1,m}} x^m}{m} \right), \\
a_2 &= \frac{F_{r,K}}{b} = \exp \left(\sum_{m \geq 1} \frac{\widetilde{a_{2,m}} x^m}{m} \right), \\
a_3 &= \frac{F_{r,\ell,K}}{b} = \exp \left(\sum_{m \geq 1} \frac{\widetilde{a_{3,m}} x^m}{m} \right),
\end{aligned} \tag{6.37}$$

$$i = 1, 2, 3 : |\widetilde{a_{i,m}}| = O \left(\frac{M_{K,\Omega}}{r} q^{rm/2} \right), \tag{6.38}$$

where the implied constant in (6.38) is (at most) 50.

We apply Corollary 3.4 to the pairs (a_1, b) , (a_2, b) and (a_3, b) with the following parameters, given by (6.37) and (6.38):

$$c_1 = \frac{1}{r}, c_2 \leq \frac{50M_{K,\Omega}}{r}, \alpha = q^{-r/2}, \beta = q^{-r}. \tag{6.39}$$

We obtain that the estimates (2.27), (2.28) and (2.29) of Theorem 2.3 hold with an absolute implied constant, as long as

$$n \geq \max \left\{ 5 \cdot \left(\frac{\frac{4 \cdot 50 \cdot M_{K,\Omega}}{r} + 8}{r \ln q} + 1 \right) \ln \left(\frac{\frac{4 \cdot 50 \cdot M_{K,\Omega}}{r} + 8}{r \ln q} + 1 \right) + 1, \frac{4}{\ln q} \frac{\ln r}{r} + 1 \right\}, \tag{6.40}$$

and the constants $C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K}$ are given by

$$C_{1,r,K} = a_1(q^{-r}), \quad C_{2,r,K} = a_2(q^{-r}), \quad C_{r,\ell,K} = a_3(q^{-r}). \tag{6.41}$$

By Remark 3.6,

$$C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K} = \exp \left(O \left(\frac{M_{K,\Omega}}{r q^{r/2}} \right) \right) = 1 + O_{M_{K,\Omega}} \left(\frac{1}{r q^{r/2}} \right). \tag{6.42}$$

Since

$$\frac{4}{\ln q} \frac{\ln r}{r} + 1 = O(1) \text{ and } \frac{\frac{4 \cdot 50 \cdot M_{K,\Omega}}{r} + 8}{r \ln q} + 1 = O \left(\frac{M_{K,\Omega}}{r^2 \ln q} + 1 \right),$$

we get that the range (6.40) may be replaced with the range (2.30) of Theorem 2.3, as needed.

6.3 The constants $C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K}$

Here we give an expression for the constants $C_{1,r,K}, C_{2,r,K}$ and $C_{r,\ell,K}$, involving a product over primes of K . The Euler products for the generating functions $G_{r,K}, F_{r,K}, F_{r,\ell,K}$ defined in §6.2 are given by

$$\begin{aligned}
G_{r,K}(x) &= \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{-1}, \\
F_{r,K}(x) &= \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K, r \mid \deg_K \mathfrak{P}} (1 - x^{\deg_K \mathfrak{P}/r})^{-1}, \\
F_{r,\ell,K}(x) &= \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K, r \mid \deg_K \mathfrak{P}} \frac{1 - x^{\deg_K \mathfrak{P}(\ell+1)/r}}{1 - x^{\deg_K \mathfrak{P}/r}}.
\end{aligned} \tag{6.43}$$

Let K_r be the constant field extension of K of degree r , and let

$$\mathcal{Z}_{K_r}(u) = \prod_{\mathfrak{P} \in \mathbb{P}_{K_r}} (1 - u^{\deg_{K_r} \mathfrak{P}})^{-1} \quad (6.44)$$

be its zeta function. When $r = 1$, $\mathcal{Z}_{K_r} = \mathcal{Z}_K$ is just the zeta function of K . By [Ros02, Lem. 8.14 and Thm. 8.15],

$$\mathcal{Z}_{K_r}(u^r) = \prod_{\omega: \omega^r=1} \mathcal{Z}_K(\omega u) = \prod_{\mathfrak{P} \in \mathbb{P}_K} (1 - u^{\frac{r \deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{-(r, \deg_K \mathfrak{P})}. \quad (6.45)$$

We separate the product in (6.45) into a product over primes of degree divisible by r and the rest, and replace u^r with x :

$$\mathcal{Z}_{K_r}(x) = \prod_{\mathfrak{P} \in \mathbb{P}_K, r | \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{r}})^{-r} \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{-(r, \deg_K \mathfrak{P})}. \quad (6.46)$$

Let $\mathcal{Z}_{K_r}(x)^{1/r}$ be chosen so that the constant term is 1. By (6.46),

$$\mathcal{Z}_{K_r}(x)^{1/r} = \prod_{\mathfrak{P} \in \mathbb{P}_K, r | \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{r}})^{-1} \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{-(r, \deg_K \mathfrak{P})/r}. \quad (6.47)$$

Dividing the expressions in (6.43) by (6.47), we obtain

$$\begin{aligned} \frac{G_{r,K}(x)}{\mathcal{Z}_{K_r}(x)^{1/r}} &= (1 - x^{\frac{\deg_K \Omega}{(r, \deg_K \Omega)}}) \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r-1}, \\ \frac{F_{r,K}(x)}{\mathcal{Z}_{K_r}(x)^{1/r}} &= \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - x^{\deg_K \Omega/r}) & r | \deg_K \Omega, \end{cases} \\ \frac{F_{r,\ell,K}(x)}{\mathcal{Z}_{K_r}(x)^{1/r}} &= \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - x^{\deg_K \Omega/r}) & r | \deg_K \Omega \end{cases} \\ &\quad \cdot \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K, r | \deg_K \mathfrak{P}} (1 - x^{\deg_K \mathfrak{P}(\ell+1)/r}). \end{aligned} \quad (6.48)$$

From [Ros02, Thm. 5.9] we know that $\mathcal{Z}_{K_r}(x)$ is a rational function of x of the form

$$\mathcal{Z}_{K_r}(x) = \frac{L_{K_r}(x)}{(1 - q^r x)(1 - x)}, \quad (6.49)$$

where L_{K_r} is a polynomial of degree $2g_{K_r} = 2g_K$ satisfying

$$L_{K_r}(u) = L_{K_r}\left(\frac{1}{q^r u}\right) (q^r u^2)^{g_K} \quad (6.50)$$

and

$$L_{K_r}(q^{-r}) = q^{-r \cdot g_K} L_{K_r}(1) = q^{-r \cdot g_K} h_{K_r}, \quad (6.51)$$

where h_{K_r} is the class number of K_r . Combining (6.48) and (6.49), we obtain

$$\begin{aligned} G_{r,K}(x) &= (1 - q^r x)^{-1/r} \left(\frac{L_{K_r}(x)}{1 - x} \right)^{1/r} \cdot (1 - x^{\frac{\deg_K \Omega}{(r, \deg_K \Omega)}}) \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r-1} \\ F_{r,K}(x) &= (1 - q^r x)^{-1/r} \left(\frac{L_{K_r}(x)}{1 - x} \right)^{1/r} \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - x^{\deg_K \Omega/r}) & r | \deg_K \Omega, \end{cases} \\ F_{r,\ell,K}(x) &= (1 - q^r x)^{-1/r} \left(\frac{L_{K_r}(x)}{1 - x} \right)^{1/r} \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - x^{\deg_K \Omega/r}) & r | \deg_K \Omega \end{cases} \\ &\quad \cdot \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K, r | \deg_K \mathfrak{P}} (1 - x^{\deg_K \mathfrak{P}(\ell+1)/r}). \end{aligned} \quad (6.52)$$

We deduce that the functions a_1, a_2, a_3 defined in (6.36) are given by

$$\begin{aligned}
a_1(x) &= \left(\frac{L_{K_r}(x)}{1-x} \right)^{1/r} \cdot (1 - x^{\frac{\deg_K \Omega}{(r, \deg_K \Omega)}}) \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r-1}, \\
a_2(x) &= \left(\frac{L_{K_r}(x)}{1-x} \right)^{1/r} \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - x^{\deg_K \Omega/r}) & r \mid \deg_K \Omega, \end{cases} \\
a_3(x) &= \left(\frac{L_{K_r}(x)}{1-x} \right)^{1/r} \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - x^{\frac{\deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{(r, \deg_K \mathfrak{P})/r} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - x^{\deg_K \Omega/r}) & r \mid \deg_K \Omega \end{cases} \\
&\quad \cdot \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K, r \mid \deg_K \mathfrak{P}} (1 - x^{\deg_K \mathfrak{P}(\ell+1)/r}).
\end{aligned} \tag{6.53}$$

From (6.53) and (6.51), we get that the constants $C_{1,r,K}, C_{2,r,K}, C_{r,\ell,K}$ defined in (6.41) are given by

$$\begin{aligned}
C_{1,r,K} &= a_1(q^{-r}) = q^{-g_K} \sqrt[r]{\frac{h_K}{1-q^{-r}}} \cdot (1 - q^{-\frac{r \cdot \deg_K \Omega}{(r, \deg_K \Omega)}}) \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - q^{-\frac{r \cdot \deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{\frac{(r, \deg_K \mathfrak{P})}{r}-1}, \\
C_{2,r,K} &= a_2(q^{-r}) = q^{-g_K} \sqrt[r]{\frac{h_K}{1-q^{-r}}} \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - q^{-\frac{r \cdot \deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{\frac{(r, \deg_K \mathfrak{P})}{r}} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - q^{-\deg_K \Omega}) & r \mid \deg_K \Omega, \end{cases} \\
C_{r,\ell,K} &= a_3(q^{-r}) = q^{-g_K} \sqrt[r]{\frac{h_K}{1-q^{-r}}} \cdot \prod_{\mathfrak{P} \in \mathbb{P}_K, r \nmid \deg_K \mathfrak{P}} (1 - q^{-\frac{r \cdot \deg_K \mathfrak{P}}{(r, \deg_K \mathfrak{P})}})^{\frac{(r, \deg_K \mathfrak{P})}{r}} \cdot \begin{cases} 1 & r \nmid \deg_K \Omega, \\ (1 - q^{-\deg_K \Omega}) & r \mid \deg_K \Omega \end{cases} \\
&\quad \cdot \prod_{\Omega \neq \mathfrak{P} \in \mathbb{P}_K, r \mid \deg_K \mathfrak{P}} (1 - q^{-(\ell+1) \cdot \deg_K \mathfrak{P}}).
\end{aligned} \tag{6.54}$$

7 Polynomials with prime factors in an arithmetic progression

Let $a, m \in \mathbb{F}_q[T]$ be a pair of coprime polynomials with $\deg m > 0$, m monic. Let $G_{a,m} \subseteq \mathbb{F}_q[T]$ be the set of monic polynomials whose monic prime factors lie in the arithmetic progression $a(T) \bmod m(T)$. Let $\pi_q(n; a, m)$ count the number of monic primes of degree n in the arithmetic progression $a(T) \bmod m(T)$. The generating function of $S(n; a, m)$ (counting function of $G_{a,m}$, defined in (2.33)) is

$$F_{G_{a,m}}(x) = \prod_{n \geq 1} (1 - x^n)^{-\pi_q(n; a, m)}. \tag{7.1}$$

As before, one sees that

$$F_{G_{a,m}}(x) = \exp \left(\sum_{n \geq 1} \frac{\psi_{G_{a,m}}(n) x^n}{n} \right), \tag{7.2}$$

where

$$\psi_{G_{a,m}}(n) = \sum_{d \mid n} d \cdot \pi_q(d; a, m). \tag{7.3}$$

We estimate $\psi_{G_{a,m}}(n)$. By a result of Wan [Wan97, Thm. 5.1],

$$\left| n \cdot \pi_q(n; a, m) - \frac{q^n}{\phi(m)} \right| \leq (\deg(m) + 1) q^{\frac{n}{2}}. \tag{7.4}$$

Hence,

$$\left| \psi_{G_{a,m}}(n) - \frac{q^n}{\phi(m)} \right| \leq (\deg(m) + 1) q^{\frac{n}{2}} + \sum_{d \mid n, d < n} d \cdot \pi_q(d; a, m). \tag{7.5}$$

The tail $\sum_{d|n, d < n} d \cdot \pi_q(d; a, m)$ is easily bounded:

$$\begin{aligned} \sum_{d|n, d < n} d \cdot \pi_q(d; a, m) &\leq \sum_{d|n, d < n} d \cdot \pi_q(d) \leq \sum_{d|n, d < n} q^d \\ &\leq q^{\frac{n}{2}} \frac{1}{1 - q^{-1}} \leq 2q^{\frac{n}{2}}. \end{aligned} \quad (7.6)$$

By (7.5) and (7.6),

$$\left| \psi_{G_{a,m}}(n) - \frac{q^n}{\phi(m)} \right| \leq (\deg(m) + 3)q^{\frac{n}{2}}. \quad (7.7)$$

Hence we may write

$$F_{G_{a,m}}(x) = a(x) \cdot b(x), \quad (7.8)$$

where

$$\begin{aligned} a(x) &= \exp \left(\sum_{n \geq 1} \frac{\widetilde{a_n} x^n}{n} \right), \\ |\widetilde{a_n}| &\leq (\deg(m) + 3)q^{\frac{n}{2}}, \\ b(x) &= (1 - qx)^{-\frac{1}{\phi(m)}}. \end{aligned} \quad (7.9)$$

The conditions of Corollary 3.4 then hold with the following parameters:

$$\alpha = \frac{1}{\sqrt{q}}, \beta = \frac{1}{q}, c_1 = \frac{1}{\phi(m)} \geq q^{-\deg m}, c_2 = \deg(m) + 3, \quad (7.10)$$

and so estimate (2.39) holds with an implied constant at most 48, whenever

$$n \geq \max \left\{ 5 \left(\frac{2(2c_2 + 4)}{\ln(q)} + 1 \right) \ln \left(\frac{2(2c_2 + 4)}{\ln(q)} + 1 \right) + 1, 4 \frac{\ln(c_1^{-1})}{\ln q} + 1 \right\}. \quad (7.11)$$

By plugging the parameters (7.10) in (7.11), and replacing $\ln(q)$ with the lower bound $\ln(2)$, the range (7.11) may be replaced with the smaller range

$$n \geq \max \left\{ 5 \left(\frac{4 \deg(m) + 20 + \ln(2)}{\ln(2)} \right) \ln \left(\frac{4 \deg(m) + 20 + \ln(2)}{\ln(2)} \right) + 1, 4 \deg(m) + 1 \right\}. \quad (7.12)$$

Replacing $\frac{4 \deg(m) + 20 + \ln(2)}{\ln(2)}$ with the upper bound $6 \deg(m) + 30$, Theorem 2.6 follows.

8 Asymptotics

Here we prove Theorem 3.3, a theorem in analysis on which we relied in previous sections, and whose proof implies Corollary 3.4. We break the proof into several auxiliary lemmas.

8.1 Basic identities and inequalities

Lemma 8.1. *For any $c_1 \notin \mathbb{Z}$ and integers $n \geq i \geq 0$, the following identity holds:*

$$(-1)^i \frac{\binom{-c_1}{n-i}}{\binom{-c_1}{n}} = \sum_{k=0}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}}. \quad (8.1)$$

Proof. Define the forward difference operator $\Delta(f)(x) := f(x+1) - f(x)$, acting on $\mathbb{C}[x]$. For $f(x) = \binom{x}{n}$ we have $\Delta(f)(x) = \binom{x}{n-1}$ (Pascal's identity $\binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}$) and so by induction we arrive at

$$\Delta(f)^{(i)}(x) = \binom{x}{n-i}. \quad (8.2)$$

On the other hand, we have in general

$$\Delta(f)^{(i)}(x) = \sum_{k=0}^i \binom{i}{k} (-1)^{i-k} f(x+k). \quad (8.3)$$

Plugging $x = -c_1$ in (8.2), (8.3) and comparing the results, we obtain

$$\binom{-c_1}{n-i} = \sum_{k=0}^i \binom{i}{k} (-1)^{i-k} \binom{k-c_1}{n}. \quad (8.4)$$

Dividing both sides of (8.4) by $(-1)^i \binom{-c_1}{n}$, we obtain

$$(-1)^i \frac{\binom{-c_1}{n-i}}{\binom{-c_1}{n}} = \sum_{k=0}^i \binom{i}{k} (-1)^k \frac{\binom{k-c_1}{n}}{\binom{-c_1}{n}}. \quad (8.5)$$

The proof concludes by observing

$$(-1)^k \frac{\binom{k-c_1}{n}}{\binom{-c_1}{n}} = \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}}. \quad (8.6)$$

□

Before the next lemma we recall that $(x)_n$ stands for $x(x-1)\cdots(x-(n-1))$, the falling factorial.

Lemma 8.2. *The following bound holds for any $m < i \leq n$ and $c_1 \in (0, 1)$:*

$$\sum_{k=m+1}^i \frac{\binom{i}{k} \binom{k-c_1}{n+c_1-1}}{\binom{-c_1}{n}} \leq \begin{cases} \frac{(i)_{m+1}}{(n+c_1-1)_{m+1}} (i-m) & i < n, \\ n \left(\ln(n-m) + \frac{2}{c_1} \right) & i = n. \end{cases} \quad (8.7)$$

Proof. Since $\binom{k-c_1}{n} = \prod_{i=1}^k (1 - \frac{c_1}{i}) \leq 1$, we can bound the left-hand side of (8.7) from above by

$$\sum_{k=m+1}^i \frac{\binom{i}{k} \binom{k-c_1}{n+c_1-1}}{\binom{-c_1}{n}} \leq \sum_{k=m+1}^i \frac{(i)_k}{(n+c_1-1)_k} \quad (8.8)$$

$$= \frac{(i)_{m+1}}{(n+c_1-1)_{m+1}} \sum_{k=m+1}^i \frac{(i-m-1)_{k-m-1}}{(n+c_1-m-2)_{k-m-1}}. \quad (8.9)$$

The case $i < n$ follows by observing that each of the terms in the sum in (8.9) is at most 1.

For the case $i = n$, note that the right-hand side of (8.8) is equal to

$$\sum_{k=m+1}^n \frac{\binom{n}{k}}{\binom{n+c_1-1}{k}}. \quad (8.10)$$

The term $k = n$ in (8.10) gives $\frac{\binom{n}{n}}{\binom{n+c_1-1}{n}} = \frac{n}{c_1} \frac{1}{\binom{n+c_1-1}{n-1}} \leq \frac{n}{c_1}$. The sum of the rest of the terms is bounded from above by

$$\sum_{k=m+1}^{n-1} \frac{\binom{n}{k}}{\binom{n-1}{k}} = \sum_{k=m+1}^{n-1} \frac{n}{n-k} = n \sum_{i=1}^{n-m-1} \frac{1}{i} \leq n (\ln(n-m) + 1) \leq n \left(\ln(n-m) + \frac{1}{c_1} \right), \quad (8.11)$$

as needed. □

Lemma 8.3. *Let $a(x) = \exp\left(\sum_{n \geq 1} \frac{\widetilde{a_n x^n}}{n}\right) = \sum a_n x^n$ be a power series satisfying (3.12) for some $\alpha, c_2 > 0$. We have the following for any $i \geq 0$ and any $0 \leq x < \alpha$:*

$$\left| a^{(i)}(x) \right| \leq \alpha^{-i} (c_2 + i - 1)_i \left(1 - \frac{x}{\alpha}\right)^{-c_2-i}. \quad (8.12)$$

Proof. Property (3.12) allows us to bound $|a^{(i)}(x)|$ from above by $|G^{(i)}(x)|$ for $0 \leq x < \alpha$, where

$$G(x) = \exp \left(\sum_{n \geq 1} \frac{c_2 \alpha^{-n} x^n}{n} \right) = \exp \left(-c_2 \log \left(1 - \frac{x}{\alpha} \right) \right) = \left(1 - \frac{x}{\alpha} \right)^{-c_2}. \quad (8.13)$$

By repeated differentiation and using $(-c_2)_i = (c_2 + i - 1)_i (-1)^i$, we find

$$|G^{(i)}(x)| = \alpha^{-i} (c_2 + i - 1)_i \left(1 - \frac{x}{\alpha} \right)^{-c_2 - i}, \quad (8.14)$$

as needed. \square

Lemma 8.4. *Let $t > 0$. If n is a positive integer satisfying*

$$n \geq 1 + 5(t + 1) \ln(t + 1), \quad (8.15)$$

then the inequality

$$\frac{n - 1}{\ln(n) + 1} \geq t \quad (8.16)$$

holds.

Proof. Let $f(x) = \frac{x-1}{\ln(x)+1}$. Note f is monotone increasing on $[1, \infty)$:

$$f'(x) = \frac{\ln(x) + \frac{1}{x}}{(\ln(x) + 1)^2} > 0. \quad (8.17)$$

Thus, to prove (8.16), it is enough to show that

$$f(1 + 5(t + 1) \ln(t + 1)) \geq t, \quad (8.18)$$

that is,

$$\frac{5(t + 1) \ln(t + 1)}{\ln(1 + 5(t + 1) \ln(t + 1)) + 1} \geq t. \quad (8.19)$$

Let

$$g(t) = (t + 1) \ln(t + 1). \quad (8.20)$$

Note that $g(t) - t$ is monotone increasing for $t > 0$, since

$$\text{for all } t > 0 : (g(t) - t)' = \ln(t + 1) > 0. \quad (8.21)$$

In particular, (8.21) implies

$$\text{for all } t \geq 0 : g(t) \geq t + g(0) = t \quad (8.22)$$

and $g(t)$ is monotone increasing in $[0, \infty)$. We split the proof of (8.19) into two cases. If $t \leq 4$, then by (8.22) we obtain

$$\frac{5(t + 1) \ln(t + 1)}{\ln(1 + 5(t + 1) \ln(t + 1)) + 1} \geq \frac{5t}{\ln(1 + 5(4 + 1) \ln(4 + 1)) + 1} \geq t. \quad (8.23)$$

If $t \geq 4$, then $5(t + 1) \ln(t + 1) \geq 1$. In particular, using $\ln(t + 1) \leq t < t + 1$, we obtain the following when $t \geq 4$:

$$\begin{aligned} \frac{5(t + 1) \ln(t + 1)}{\ln(1 + 5(t + 1) \ln(t + 1)) + 1} &\geq \frac{5t \ln(t + 1)}{\ln(10(t + 1) \ln(t + 1)) + 1} \\ &\geq \frac{5t \ln(t + 1)}{\ln(10(t + 1)^2) + 1} = 5t \left(\frac{1}{2} - \frac{\ln(10) + 1}{4 \ln(t + 1) + 2 \ln(10) + 2} \right) \\ &\geq 5t \left(\frac{1}{2} - \frac{\ln(10) + 1}{4 \ln(4 + 1) + 2 \ln(10) + 2} \right) \geq t, \end{aligned} \quad (8.24)$$

as needed. \square

8.2 Main sum inequality

Lemma 8.5. *Let $a(x) = \exp\left(\sum_{n \geq 1} \frac{\widetilde{a_n} x^n}{n}\right) = \sum a_n x^n$ be a power series satisfying (3.12) for some $\alpha, c_2 > 0$. Let $\beta > 0$ be a real number such that $r = \beta/\alpha$ satisfies (3.11). Let $0 \leq m < n$ and define*

$$S_1 = \sum_{i=m+1}^n \beta^i \left(\sum_{k=m+1}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!}. \quad (8.25)$$

Then

$$|S_1| \ll_m \binom{n+c_2-1}{n} r^n \left(n \ln(n) + \frac{2n}{c_1} \right) + \left(\frac{r}{n} \right)^{m+1} (c_2+m)_{m+1} (1-r)^{-c_2} (1+c_2 r). \quad (8.26)$$

For $m = 0$, the implicit constant in (8.26) is (at most) 24.

Proof. We split $S_1 = S' + S''$ into two parts, according to $i = n$ and $i < n$:

$$S' = \beta^n \left(\sum_{k=m+1}^n \frac{\binom{n}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(n)}(0)}{n!}, \quad (8.27)$$

$$S'' = \sum_{i=m+1}^{n-1} \beta^i \left(\sum_{k=m+1}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!}. \quad (8.28)$$

By Lemmas 8.2 and 8.3, we obtain

$$|S'| \leq \beta^n \left(n \ln(n) + \frac{2n}{c_1} \right) \frac{\alpha^{-n} (c_2 + n - 1)_n}{n!} = \binom{n+c_2-1}{n} r^n \left(n \ln(n) + \frac{2n}{c_1} \right). \quad (8.29)$$

If $m = n - 1$, we have $S'' = 0$. Otherwise, Lemmas 8.2 and 8.3 give

$$\begin{aligned} |S''| &\leq \frac{1}{(n+c_1-1)_{m+1}} \sum_{i=m+1}^{n-1} \beta^i (i)_{m+1} (i-m) \alpha^{-i} \binom{c_2+i-1}{i} \\ &= \frac{1}{(n+c_1-1)_{m+1}} \sum_{i=m+1}^{n-1} r^i (i)_{m+1} (i-m) \binom{c_2+i-1}{i}. \end{aligned} \quad (8.30)$$

We bound the sum in (8.30) from above by the infinite series

$$\sum_{i=m+1}^{\infty} r^i (i)_{m+1} (i-m) \binom{c_2+i-1}{i}. \quad (8.31)$$

We can compute (8.31). We differentiate the identity

$$\sum_{i \geq 0} (-x)^i \binom{c_2+i-1}{i} = (1+x)^{-c_2} \quad (8.32)$$

$m+1$ times, multiply by x^{m+1} and obtain

$$\sum_{i \geq m+1} (-x)^i (i)_{m+1} \binom{c_2+i-1}{i} = (-c_2)_{m+1} x^{m+1} (1+x)^{-c_2-m-1}. \quad (8.33)$$

We apply the linear operator $f \mapsto x \cdot f' - m \cdot f$ to both sides of (8.33):

$$\sum_{i \geq m+1} (-x)^i (i)_{m+1} (i-m) \binom{c_2+i-1}{i} = (-c_2)_{m+1} x^{m+1} (1+x)^{-c_2-m-1} \left(1 - (c_2+m+1) \frac{x}{1+x} \right). \quad (8.34)$$

We plug $x = -r$ in (8.34) and find the following formula for (8.31):

$$(-c_2)_{m+1}(-r)^{m+1}(1-r)^{-c_2-m-1} \left(1 + \frac{r}{1-r}(c_2+m+1)\right). \quad (8.35)$$

Dividing (8.35) by the denominator appearing in (8.30), we obtain the following upper bound on $|S''|$:

$$|S''| \leq \frac{(c_2+m)_{m+1}}{(n+c_1-1)_{m+1}} \left(\frac{r}{1-r}\right)^{m+1} (1-r)^{-c_2} \left(1 + \frac{r}{1-r}(c_2+m+1)\right). \quad (8.36)$$

Using (3.11) and the estimate $(n+c_1-1)_{m+1} = \Omega_m(n^{m+1})$, we may simplify (8.36) as

$$|S''| \ll_m \left(\frac{r}{n}\right)^{m+1} (c_2+m)_{m+1} (1-r)^{-c_2} (1+c_2r). \quad (8.37)$$

By combining (8.29) and (8.37), we establish (8.26).

Now we assume that $m = 0$. If $n = 1$, we have $S'' = 0$. Otherwise, plugging $m = 0$ in (8.36), we obtain

$$|S''| \leq \frac{c_2r}{n} (1-r)^{-c_2} \frac{n}{n+c_1-1} \frac{1+c_2r}{(1-r)^2}. \quad (8.38)$$

Since $\frac{n}{n+c_1-1} \leq 2$ and (3.11) implies that $\frac{1+c_2r}{(1-r)^2} \leq \frac{1+c_2r}{(1-\frac{1}{\sqrt{2}})^2} \leq 12(1+c_2r)$, equation (8.38) implies that

$$|S''| \leq 24 \frac{c_2r}{n} (1-r)^{-c_2} (1+c_2r). \quad (8.39)$$

By (8.29) and (8.39), we find that the implicit constant in (8.26) is at most 24, as needed. \square

8.3 Integral bound

Lemma 8.6. *Let $a(x) = \exp\left(\sum_{n \geq 1} \frac{\tilde{a}_n x^n}{n}\right) = \sum a_n x^n$ be a power series satisfying (3.12) for some $\alpha, c_2 > 0$. Let $\beta > 0$ be a real number such that $r = \beta/\alpha$ satisfies (3.11). Let $0 \leq m < n$. Define*

$$S_2 = \sum_{k=0}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \frac{\beta^k}{k!} \int_0^\beta \frac{(\beta-x)^{n-k}}{(n-k)!} a^{(n+1)}(x) dx. \quad (8.40)$$

Then

$$|S_2| \ll_m \binom{n+c_2-1}{n} r^n (1+c_2r) (1-r)^{-c_2}. \quad (8.41)$$

For $m = 0$, the implicit constant in (8.41) is (at most) 12.

Proof. In (8.40), we replace $\binom{k-c_1}{k}$ by the upper bound 1 and $\binom{n+c_1-1}{k}$ by the lower bound $\binom{n-1}{k}$:

$$|S_2| \leq \sum_{k=0}^m \frac{1}{\binom{n-1}{k}} \frac{\beta^n}{k!} \int_0^\beta \frac{(1-\frac{x}{\beta})^{n-k}}{(n-k)!} |a^{(n+1)}(x)| dx. \quad (8.42)$$

We use Lemma 8.3 to replace the number $|a^{(n+1)}(x)|$ appearing in the integrand of (8.42) with $(c_2+n)_{n+1} (1-\frac{x}{\alpha})^{-c_2-n-1} \alpha^{-n-1}$:

$$\begin{aligned} |S_2| &\leq \sum_{k=0}^m \frac{1}{\binom{n-1}{k}} \frac{\beta^n}{k!} \int_0^\beta \frac{(1-\frac{x}{\beta})^{n-k}}{(n-k)!} (c_2+n)_{n+1} \alpha^{-n-1} \left(1-\frac{x}{\alpha}\right)^{-c_2-n-1} dx \\ &= \sum_{k=0}^m \frac{(c_2+n)_{n+1}}{\binom{n-1}{k} k! (n-k)!} \beta^n \alpha^{-n-1} \int_0^\beta \left(1-\frac{x}{\beta}\right)^{n-k} \left(1-\frac{x}{\alpha}\right)^{-c_2-n-1} dx. \end{aligned} \quad (8.43)$$

We simplify the expression outside the integral:

$$\begin{aligned}
\frac{(c_2 + n)_{n+1}}{\binom{n-1}{k} k! (n-k)!} \beta^n \alpha^{-n-1} &= \binom{c_2 + n}{n+1} (n+1)n \cdot r^{n+1} \cdot \frac{\beta^{-1}}{n-k} \\
&= \binom{n+c_2-1}{n} n((n+c_2)r) \cdot r^n \cdot \frac{\beta^{-1}}{n-k} \\
&\leq \binom{n+c_2-1}{n} (1+c_2r)n^2 \cdot r^n \cdot \frac{\beta^{-1}}{n-k}.
\end{aligned} \tag{8.44}$$

Plugging (8.44) back in (8.43), we see

$$|S_2| \leq \binom{n+c_2-1}{n} (1+c_2r)n^2 \cdot r^n \sum_{k=0}^m \int_0^\beta \frac{1}{n-k} \left(1 - \frac{x}{\beta}\right)^{n-k} \left(1 - \frac{x}{\alpha}\right)^{-c_2-n-1} \frac{dx}{\beta}. \tag{8.45}$$

We perform the change of variables $s := x/\beta$ in the right-hand side of (8.45), and obtain

$$|S_2| \leq \binom{n+c_2-1}{n} (1+c_2r)n^2 \cdot r^n \sum_{k=0}^m \int_0^1 \frac{(1-s)^{n-k}}{n-k} (1-rs)^{-c_2-n-1} ds. \tag{8.46}$$

We rewrite the integrand $\frac{(1-s)^{n-k}}{n-k} (1-rs)^{-c_2-n-1}$ as

$$\frac{1}{n-k} \left(\frac{1-s}{1-rs} \right)^{n-k} (1-rs)^{-c_2-k-1}. \tag{8.47}$$

We apply two basic inequalities to (8.47), which hold for $s \in [0, 1]$: $0 \leq \frac{1-s}{1-rs} \leq 1 + s(r-1)$ and $(1-rs)^{-1} \leq (1-r)^{-1}$. This allows us to bound the right-hand side of (8.46) from above by

$$\binom{n+c_2-1}{n} (1+c_2r)n^2 \cdot r^n \sum_{k=0}^m \frac{1}{n-k} (1-r)^{-c_2-k-1} \int_0^1 (1+s(r-1))^{n-k} ds. \tag{8.48}$$

The integral in (8.48) can be evaluated precisely as $\frac{1-r^{n-k+1}}{1-r} \frac{1}{n-k+1}$, which we bound from above by $\frac{1}{(1-r)(n-k+1)}$. Thus, we obtain

$$|S_2| \leq \binom{n+c_2-1}{n} (1+c_2r)n^2 \cdot r^n \sum_{k=0}^m \frac{1}{(n-k)(n-k+1)} (1-r)^{-c_2-k-2}. \tag{8.49}$$

Since $k \leq m$, we may replace $(1-r)^{-c_2-k-2}$ in (8.49) by $(1-r)^{-c_2-m-2}$:

$$|S_2| \leq \binom{n+c_2-1}{n} (1+c_2r)n^2 \cdot r^n (1-r)^{-c_2-m-2} \sum_{k=0}^m \frac{1}{(n-k)(n-k+1)}. \tag{8.50}$$

The sum in (8.50) telescopes as follows:

$$\begin{aligned}
\sum_{k=0}^m \frac{1}{(n-k)(n-k+1)} &= \sum_{k=0}^m \left(\frac{1}{n-k} - \frac{1}{n-k+1} \right) \\
&= \frac{1}{n-m} - \frac{1}{n+1} = \frac{1+m}{(n-m)(n+1)}.
\end{aligned} \tag{8.51}$$

Thus, (8.50) becomes

$$|S_2| \leq \binom{n+c_2-1}{n} (1+c_2r) \frac{n(1+m)}{n-m} r^n (1-r)^{-c_2-m-2}. \tag{8.52}$$

Since $\frac{n(1+m)}{n-m} \leq (1+m)^2 \ll_m 1$ and $r \leq 1/\sqrt{2}$ by (3.11), the bound (8.52) may be simplified as

$$|S_2| \ll_m \binom{n+c_2-1}{n} r^n (1+c_2r) (1-r)^{-c_2}, \tag{8.53}$$

where the implied constant is $(1+m)^2(1-1/\sqrt{2})^{-m-2}$. This establishes (8.41). For $m = 0$, the implied constant is less than 12. \square

8.4 Proof of Theorem 3.3

Proof. Recall $b_n = [x^n](1 - x/\beta)^{-c_1} = (-1/\beta)^n \binom{-c_1}{n} = \beta^{-n} \binom{n+c_1-1}{n}$. We have

$$\begin{aligned} f_n &= \sum_{i=0}^n a_i b_{n-i} = \sum_{i=0}^n \frac{a^{(i)}(0)}{i!} \cdot \left(-\frac{1}{\beta}\right)^{n-i} \binom{-c_1}{n-i} \\ &= \left(-\frac{1}{\beta}\right)^n \binom{-c_1}{n} \sum_{i=0}^n \left(-\frac{1}{\beta}\right)^{-i} \frac{\binom{-c_1}{n-i}}{\binom{-c_1}{n}} \frac{a^{(i)}(0)}{i!} \\ &= b_n \cdot \left(\sum_{i=0}^n \beta^i (-1)^i \frac{\binom{-c_1}{n-i}}{\binom{-c_1}{n}} \frac{a^{(i)}(0)}{i!} \right). \end{aligned} \quad (8.54)$$

By Lemma 8.1, we may replace $(-1)^i \frac{\binom{-c_1}{n-i}}{\binom{-c_1}{n}}$ in (8.54) with $\sum_{k=0}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}}$ and split the sum according to small and large k :

$$\begin{aligned} f_n &= b_n \cdot \sum_{i=0}^n \beta^i \left(\sum_{k=0}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!} \\ &= b_n \cdot \sum_{i=0}^n \beta^i \left(\sum_{k=0}^m \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!} + b_n \cdot \sum_{i=m+1}^n \beta^i \left(\sum_{k=m+1}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!}. \end{aligned} \quad (8.55)$$

We denote the first sum by S_0 and the second sum by S_1 :

$$\begin{aligned} S_0 &= \sum_{i=0}^n \beta^i \left(\sum_{k=0}^m \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!}, \\ S_1 &= \sum_{i=m+1}^n \beta^i \left(\sum_{k=m+1}^i \frac{\binom{i}{k} \binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \right) \frac{a^{(i)}(0)}{i!}. \end{aligned} \quad (8.56)$$

We rearrange the terms of S_0 as follows:

$$\begin{aligned} S_0 &= \sum_{k=0}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \sum_{i=k}^n \binom{i}{k} \frac{a^{(i)}(0)}{i!} \beta^i \\ &= \sum_{k=0}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \frac{\beta^k}{k!} \sum_{j=0}^{n-k} \frac{a^{(j+k)}(0)}{j!} \beta^j. \end{aligned} \quad (8.57)$$

Let

$$\begin{aligned} M &= \sum_{k=0}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta), \\ S_2 &= \sum_{k=0}^m \frac{\binom{k-c_1}{k}}{\binom{n+c_1-1}{k}} \frac{\beta^k}{k!} \int_0^\beta \frac{(\beta-x)^{n-k}}{(n-k)!} a^{(n+1)}(x) dx. \end{aligned} \quad (8.58)$$

By the integral formula for the remainder in a Taylor series, we may replace $\sum_{j=0}^{n-k} \frac{a^{(j+k)}(0)}{j!} \beta^j$ in (8.57) with

$$a^{(k)}(\beta) - \int_0^\beta \frac{(\beta-x)^{n-k}}{(n-k)!} a^{(n+1)}(x) dx,$$

and obtain

$$S_0 = M - S_2. \quad (8.59)$$

Summarizing (8.55) and (8.59), we see

$$f_n = b_n \cdot (M + S_1 - S_2). \quad (8.60)$$

Note that $b_n \cdot M$ is the main term of (3.13). The expression E , as defined in (3.13), equals $S_1 - S_2$. The sums S_1, S_2 are bounded in Lemmas 8.5 and 8.6, respectively, and these bounds give

$$\begin{aligned} |E| &\ll_m \left(\frac{r}{n}\right)^{m+1} (1-r)^{-c_2} (1+c_2r)(c_2+m)_{m+1} \\ &\quad + \binom{n+c_2-1}{n} r^n \left(n \ln(n) + \frac{2n}{c_1} + (1-r)^{-c_2} (1+c_2r)\right). \end{aligned} \quad (8.61)$$

We simplify (8.61) using the following two inequalities:

$$1 + c_2r \leq \exp(c_2r), \quad (8.62)$$

and, since $-\ln(1-r) \leq 2r$ for $0 \leq r \leq 1/\sqrt{2}$ by simple calculus, we have

$$(1-r)^{-c_2} = \exp(-c_2 \ln(1-r)) \leq \exp(2c_2r). \quad (8.63)$$

Plugging (8.62) and (8.63) into (8.61), we obtain

$$\begin{aligned} |E| &\ll_m \left(\frac{r}{n}\right)^{m+1} \exp(3c_2r)(c_2+m)_{m+1} \\ &\quad + \binom{n+c_2-1}{n} r^n \left(n \ln(n) + \frac{2n}{c_1} + \exp(3c_2r)\right). \end{aligned} \quad (8.64)$$

We note that

$$n \ln(n) + \frac{2n}{c_1} + \exp(3c_2r) \leq \exp(3c_2r) \frac{4n^2}{c_1}. \quad (8.65)$$

Plugging (8.65) in (8.64), we obtain

$$|E| \ll_m \exp(3c_2r) \left(\left(\frac{r}{n}\right)^{m+1} (c_2+m)_{m+1} + \binom{n+c_2-1}{n} \frac{4n^2}{c_1} r^n \right), \quad (8.66)$$

as needed. For $m = 0$, the implied coefficient is the maximum of the two implied constants of Lemmas 8.5 and 8.6, i.e. 24. \square

8.5 Proof of Corollary 3.4

We apply Theorem 3.3 with $m = 0$, and obtain

$$|E| \ll \exp(3c_2r) \left(\frac{c_2r}{n} + \binom{n+c_2-1}{n} \frac{4n^2}{c_1} r^n \right), \quad (8.67)$$

where the implied constant is 24. We find a range of n where the first term of the right-hand side of (8.67) dominates the error, i.e. we want to solve

$$\frac{c_2r}{n} \geq \binom{n+c_2-1}{n} \frac{4n^2}{c_1} r^n. \quad (8.68)$$

For n for which (8.68) holds, (3.17) holds with an implied constant (at most) $24 + 24 = 48$. We find a range of n for which (8.68) holds by making several simplifications. Note that

$$\begin{aligned} \binom{n+c_2-1}{n} n^2 &= \binom{n+c_2-1}{n-1} c_2 n = \prod_{i=1}^{n-1} \left(1 + \frac{c_2}{i}\right) c_2 n \\ &\leq \exp\left(c_2 \sum_{i=1}^{n-1} \frac{1}{i}\right) c_2 n \leq \exp(c_2 (\ln(n) + 1)) c_2 n \\ &= (ne)^{c_2+1} \frac{c_2}{e}, \end{aligned} \quad (8.69)$$

so we may replace (8.68) by the following stricter inequality:

$$\frac{r}{n} \geq (ne)^{c_2+1} \frac{1}{c_1} \frac{4}{e} r^n, \quad (8.70)$$

or, equivalently,

$$\left(\frac{1}{r}\right)^{n-1} \geq (ne)^{c_2+2} \frac{1}{c_1} \frac{4}{e^2}. \quad (8.71)$$

Inequality (8.71) holds when the following two inequalities hold simultaneously:

$$\left(\frac{1}{r}\right)^{(n-1)/2} \geq (ne)^{c_2+2}, \quad \left(\frac{1}{r}\right)^{(n-1)/2} \geq \frac{1}{c_1}. \quad (8.72)$$

The first inequality of (8.72) holds whenever $\frac{n-1}{\ln(n)+1} \geq \frac{2c_2+4}{\ln(\frac{1}{r})}$, which, by Lemma 8.4, is satisfied when

$$n \geq 1 + 5 \left(\frac{2c_2 + 4}{\ln(\frac{1}{r})} + 1 \right) \ln \left(\frac{2c_2 + 4}{\ln(\frac{1}{r})} + 1 \right). \quad (8.73)$$

The second inequality of (8.72) holds whenever $n \geq \frac{2 \ln(c_1^{-1})}{\ln(\frac{1}{r})} + 1$. This establishes Corollary 3.4.

Acknowledgments

I thank my advisor, Lior Bary-Soroker, for introducing me to Landau's theorem, for helpful discussions and for teaching me, patiently, how to write. Also, I thank Amotz Oppenheim and Zeév Rudnick for their useful comments on this paper, Mikhail Sodin for a helpful discussion related to the analytic part of the paper, and the anonymous referee for her/his valuable remarks. This research was partially supported by the Israel Science Foundation grants no. 952/14 and no. 382/15.

References

- [Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. I. *Math. Z.*, 19(1):153–206, 1924.
- [BJ12] Sunghan Bae and Hwanyup Jung. On the 4-rank of ideal class groups of quadratic function fields. *Acta Arith.*, 151(4):325–360, 2012.
- [BSSW16] Lior Bary-Soroker, Yotam Smilansky, and Adva Wolf. On the function field analogue of Landau's theorem on sums of squares. *Finite Fields Appl.*, 39:195–215, 2016.
- [Che51] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951.
- [CKY15] Chih-Yun Chuang, Yen-Liang Kuan, and Jing Yu. On counting polynomials over finite fields. *Proc. Amer. Math. Soc.*, 143(10):4305–4316, 2015.
- [FK10] Étienne Fouvry and Jürgen Klüners. On the negative Pell equation. *Ann. of Math. (2)*, 172(3):2035–2104, 2010.
- [FS09] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.
- [FV96] Philippe Flajolet and Ilan Vardi. Zeta function expansions of classical constants. *Unpublished manuscript*, <http://algo.inria.fr/flajolet/Publications/landau.ps>, 1996.
- [Hen77] Peter Henrici. *Applied and computational complex analysis. Vol. 2*. Wiley Interscience [John Wiley & Sons], New York-London-Sydney, 1977. Special functions—integral transforms—asymptotics—continued fractions.

- [Jam13] G. J. O. Jameson. Inequalities for gamma function ratios. *Amer. Math. Monthly*, 120(10):936–940, 2013.
- [Kno90] John Knopfmacher. *Abstract analytic number theory*. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, second edition, 1990.
- [KW89] Donald E. Knuth and Herbert S. Wilf. A short proof of Darboux’s lemma. *Appl. Math. Lett.*, 2(2):139–140, 1989.
- [KZ01] John Knopfmacher and Wen-Bin Zhang. *Number theory arising from finite fields*, volume 241 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 2001. Analytic and probabilistic theory.
- [Lan08] Edmund Landau. Über die einteilung der positiven ganzen zahlen in vier klassen nach der mindestzahl der zu ihrer additiven zusammensetzung erforderlichen quadrate. *Arch. Math. Phys.*, 13:305–312, 1908.
- [Lea67] William Leahey. Sums of squares of polynomials with coefficients in a finite field. *Amer. Math. Monthly*, 74:816–819, 1967.
- [Mat17] Vlad Matei. A geometric perspective on landau’s problem over function fields. *Online preprint*, <http://www.math.wisc.edu/~mvlad/landau.pdf>, 2017.
- [MS93] E. Manstavičius and R. Skrabutėnas. Summation of values of multiplicative functions on semi-groups. *Lithuanian Mathematical Journal*, 33(3):255–264, 1993.
- [Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [Sha64] Daniel Shanks. The second-order term in the asymptotic expansion of $B(x)$. *Math. Comp.*, 18:75–86, 1964.
- [Shi00] D. K. L. Shiu. Strings of congruent primes. *J. London Math. Soc. (2)*, 61(2):359–373, 2000.
- [Ste93] Peter Stevenhagen. The number of real quadratic fields having units of negative norm. *Experiment. Math.*, 2(2):121–136, 1993.
- [Tho08] Frank Thorne. Irregularities in the distributions of primes in function fields. *J. Number Theory*, 128(6):1784–1794, 2008.
- [Wan97] Daqing Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.
- [War92] Richard Warlimont. Arithmetical semigroups. V. Multiplicative functions. *Manuscripta Math.*, 77(4):361–383, 1992.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, P. O. Box 39040, Tel Aviv 6997801, Israel. E-mail address: ofir.goro@gmail.com