TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 361, Number 9, September 2009, Pages 4519–4539
S 0002-9947(09)04723-0
Article electronically published on April 6, 2009

A CARLITZ MODULE ANALOGUE OF A CONJECTURE OF ERDŐS AND POMERANCE

WENTANG KUO AND YU-RU LIU

ABSTRACT. Let $A = \mathbb{F}_q[T]$ be the ring of polynomials over the finite field $\mathbb{F}_q$ and $0 \neq a \in A$. Let C be the A-Carlitz module. For a monic polynomial $m \in A$, let $C(A/mA)$ and $\bar{a}$ be the reductions of C and a modulo mA respectively. Let $f_a(m)$ be the monic generator of the ideal $\{f \in A, C_f(\bar{a}) = \bar{0}\}$ on $C(A/mA)$. We denote by $\omega(f_a(m))$ the number of distinct monic irreducible factors of $f_a(m)$. If $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $(1+T)$, we prove that there exists a normal distribution for the quantity

$$\frac{\omega(f_a(m)) - \frac{1}{2}(\log \deg m)^2}{\frac{1}{\sqrt{3}}(\log \deg m)^{3/2}}.$$

This result is analogous to an open conjecture of Erdős and Pomerance concerning the distribution of the number of distinct prime divisors of the multiplicative order of b modulo n, where b is an integer with $|b| > 1$, and n a positive integer.

1. INTRODUCTION

For $n \in \mathbb{N} := \{1, 2, 3, \cdots\}$, let $\nu(n)$ denote the number of distinct prime divisors of n. For $x \in \mathbb{N}$, a theorem of Turán [19] states that

$$\sum_{n \leq x} \big(\nu(n) - \log\log x\big)^2 \ll x \log\log x,$$

from which we can derive an earlier result of Hardy and Ramanujan [5] that the normal order of $\nu(n)$ is $\log\log n$. In other words, for any $\epsilon > 0$,

$$\#\Big\{n \leq x \,\Big|\, n \text{ satisfies } |\nu(n) - \log\log n| > \epsilon \log\log n\Big\} = o(x).$$

The idea behind Turán's proof was essentially probabilistic. The further development of probabilistic ideas led Erdős and Kac [2] to prove a remarkable refinement of the Turán Theorem. For $\gamma \in \mathbb{R}$, Erdős and Kac proved that

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{n \leq x \,\middle|\, n \text{ satisfies } \frac{\nu(n) - \log\log n}{\sqrt{\log\log n}} \leq \gamma\right\} = G(\gamma),$$

Received by the editors March 3, 2006 and, in revised form, July 30, 2006.
2000 *Mathematics Subject Classification.* Primary 11K36; Secondary 11R58, 14H05.
Key words and phrases. The Carlitz module, Erdős-Pomerance's conjecture.
The research of the first author was supported by an NSERC discovery grant.
The research of the second author was supported by an NSERC discovery grant.

where $G(\gamma)$ is the Gaussian normal distribution, i.e.,

$$G(\gamma) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} dt.$$

The celebrated theorem of Erdős and Kac opened a door to probabilistic number theory. In the 1960s and 1970s, the theory was refined by many authors, culminating in a generalized Erdős-Kac theorem, proved independently by Kubilius [10] and Shapiro [18]. Their result is applicable to what are called 'strongly additive functions'. An interested reader can find a comprehensive treatment of it in the monograph of Elliott [1].

We can also consider functions that are not strongly additive, say Euler's φ-function. In this case, the result of Kubilius and Shapiro cannot be applied directly. By making a significant transition from $\varphi(n)$ to a strongly additive function, Erdős and Pomerance [3] showed that

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x \,\middle|\, n \text{ satisfies } \frac{\nu(\varphi(n)) - \frac{1}{2}(\log\log n)^2}{\frac{1}{\sqrt{3}}(\log\log n)^{3/2}} \le \gamma \right\} = G(\gamma).$$

Another new type of Erdős-Kac's theorem, which can be described as 'non-abelian', was discovered by M. R. Murty and V. K. Murty [14]. More precisely, they proved that under the assumption of the GRH (i.e., the Riemann Hypothesis for all Dedekind zeta functions of number fields), an analogous result of Erdős and Pomerance holds for $\tau(n)$, where $\tau(n)$ is the Ramanujan τ-function. As shown in [14], their general theorem is applicable to a wider class of functions arising as Fourier coefficients of modular forms. One can also derive from it the result of Erdős and Pomerance on $\nu(\varphi(n))$.

In [3], Erdős and Pomerance proposed the following question. For $b \in \mathbb{Z}, n \in \mathbb{N}$ with $(b, n) = 1$, let $l_b(n)$ be the multiplicative order of b modulo n. Thus $l_b(n)$ is a divisor of $\varphi(n)$. Based on the belief that the difference between $\nu(\varphi(n))$ and $\nu(l_b(n))$ is 'small on average', Erdős and Pomerance conjectured that if $|b| > 1$, then

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x \,\middle|\, n \text{ satisfies } (b,n) = 1 \text{ and } \frac{\nu(l_b(n)) - \frac{1}{2}(\log\log n)^2}{\frac{1}{\sqrt{3}}(\log\log n)^{3/2}} \le \gamma \right\}$$
$$= \frac{\varphi(b)}{|b|} G(\gamma).$$

This conjecture still remains open today. The first breakthrough of the problem was recently achieved by Murty and Saidak [15]. Under the GRH, they proved that the conjecture is true. Subsequently, Li and Pomerance [11] also provided an alternative proof of the same result. The difficulty of this conjecture lies in the intervention of certain non-abelian extensions of $\mathbb{Q}$. More precisely, we need to bound the quantity $\sum \nu(i_b(n))$, where $i_b(n) = \varphi(n)/l_b(n)$, and the estimate involves the distribution of primes in the non-abelian extensions $\mathbb{Q}(\zeta_n, \sqrt[n]{b})$, where ζ_n is a primitive n-th root of unity and $\sqrt[n]{b}$ is an n-th root of b. We can also formulate a prime analogue of Erdős-Pomerance's conjecture for elliptic curves. In [13], the second author proved that under the GRH, an analogous result holds for elliptic curves.

When we see a result involving the GRH, it is natural to ask if its polynomial analogue holds unconditionally. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over the finite field $\mathbb{F}_q$. For $a \in A$, $m \in A$ a monic polynomial with $(a, m) = 1$, let

$l_{a,q}(m)$ be the multiplicative order of a modulo m. We can consider the distribution of $\nu(l_{a,q}(m))$. Let $\varphi_q(m)$ be the order of the multiplicative group $(A/mA)^*$ and $i_{a,q}(m) = \varphi_q(m)/l_{a,q}(m)$. Following the approach of Murty and Saidak, we seek to estimate the quantity $\sum \nu(i_{a,q}(m))$. In this case, we can obtain unconditionally the desired upper bound. Hence, the distribution of $\nu(l_{a,q}(m))$ is the same with that of $\nu(\varphi_q(m))$, if the latter exists. At this point, it is difficult to establish the existence of a normal distribution for $\nu(\varphi_q(m))$. The main obstacle is that the values of $\varphi_q(m)$ involve sums of q-powers, and their prime divisors do not seem to distribute normally. More precisely, following the same principle as in the work of Erdős and Kac, the expectation of $\nu(\varphi_q(m))$ is about

$$\sum_{\deg p \le x} \frac{\nu(\varphi_q(p))}{q^{\deg p}},$$

where $p \in A$ are monic irreducible polynomials. We note that a prime w divides $\varphi_q(p)$ if and only if $q^{\deg p} \equiv 1 \pmod{w}$, which is equivalent to saying that $l_q(w) | \deg p$, where $l_q(w)$ is the order of q modulo w which we defined before. Thus to estimate the above quantity, it involves getting an asymptotic formula for the sum

$$\sum_{w \le x} \frac{1}{l_q(w)}.$$

As M. R. Murty and Srinvasan proved in [16], if the above quantity is bounded by $O(x^{1/4})$, we can conclude that q is a primitive root for infinitely many primes p. In other words, the classical Artin primitive root conjecture holds for q. As the conjecture remains unsolved, and what we need for estimating $\nu(\varphi_q(m))$ is not only an upper bound, but an asymptotic formula for the above sum, it does not seem that there is an easy answer for this problem.

Because of the above complication for polynomials, perhaps we should consider the Erdős-Pomerance problem in a different formulation. Let $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$ be the rational function field. Let τ be the Frobenius element defined by $\tau(X) = X^q$. We denote by $k\{\tau\}$ the 'twisted polynomial ring' whose multiplication is defined by

$$\tau b = b^q \tau, \qquad \forall b \in k.$$

The A-Carlitz module C is the $\mathbb{F}_q$-algebra homomorphism

$$C : A \longrightarrow k\{\tau\}, \qquad f \mapsto C_f,$$

characterized by

$$C_T = T + \tau.$$

Let B be a commutative k-algebra (or more generally, a commutative A-algebra since C_T has coefficients in A) and B_+ the additive group of B. We can view an element of $k\{\tau\}$ as an endomorphism of B_+ in the following way: let $u \in B$ and $\sum b_i \tau^i \in k\{\tau\}$ $(b_i \in k)$,

$$\Big(\sum b_i \tau^i\Big)(u) = \sum b_i u^{q^i}.$$

Using the A-Carlitz module C, we can define a new multiplication on B as follows: for $f \in A$ and $u \in B$,

$$f \cdot u := C_f(u) \in B.$$

This gives B a new A-module structure and we denote it by $C(B)$.

Let $m \in A$ be a monic polynomial and mA the ideal of A generated by m. For $g \in A$, let $\bar{g}$ be the reduction of g modulo mA. Consider the reduction of C modulo mA, i.e., the A-module $C(A/mA)$ given by $C_T(\bar{g}) = \bar{T}\bar{g} + \bar{g}^q$. For a fixed non-zero polynomial $a \in A$, consider the set

$$\{f \in A, C_f(\bar{a}) = \bar{0}\}$$

on $C(A/mA)$. It is indeed an ideal of A because C is a ring homomorphism. Since A is a principle ideal domain, there exists a unique monic polynomial $f_a(m) \in A$ which generates the above ideal. Let $\omega(f_a(m))$ denote the number of distinct monic irreducible factors of $f_a(m)$. Our goal is to study the behavior of $\omega(f_a(m))$.

In the case when $p \in A$ is a monic irreducible polynomial, we will prove that

Theorem 1. *Let $A = \mathbb{F}_q[T]$, C the A-Carlitz module, and $0 \neq a \in A$. For a monic irreducible polynomial $p \in A$, let $C(A/pA)$ and $\bar{a}$ be the reductions of C and a modulo pA respectively. Let $f_a(p)$ be the monic generator of the ideal $\{f \in A, C_f(\bar{a}) = \bar{0}\}$ on $C(A/pA)$. If $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $(1+T)$, for $x \in \mathbb{N}$, we have*

$$\sum_{\deg p = x} \Big(\omega(f_a(p)) - \log x\Big)^2 \ll \pi(x) \log x,$$

where $\pi(x)$ is the number of monic irreducible polynomials in A of degree x.

From Theorem 1, we can derive

Corollary 2. *Let $p \in A$ be a monic irreducible polynomial. For any $\epsilon \in \mathbb{R}, \epsilon > 0$, we have*

$$\#\Big\{\deg p = x \,\Big|\, p \text{ satisfies } \big|\omega(f_a(p)) - \log\deg p\big| > \epsilon \log\deg p\Big\} = o\big(\pi(x)\big).$$

In other words, the normal order of $\omega(f_a(p))$ is $\log\deg p$.

We remark here that the requirement $q \neq 2$ and $a \neq 0$, or $q = 2$ and $a \neq 0, 1, T$, or $(1+T)$ in Theorem 1 is analogous to the condition that an integer b satisfies $|b| > 1$ in the Erdős-Pomerance conjecture. For a rational prime $w \in \mathbb{N}$ with $(b, w) = 1$, we recall that $l_b(w)$ is the multiplicative order of b modulo w. In other words, $l_b(w)$ is the positive generator of the ideal $\{z \in \mathbb{Z},\, b^z \equiv 1 \,(\mathrm{mod}\, w)\}$ of $\mathbb{Z}$. It was proved by Murty and Saidak [15, Theorem 2] that under the GRH, there exists a normal distribution for the quantity

$$\frac{\nu(l_b(w)) - \log\log w}{\sqrt{\log\log w}}.$$

Let $f_a(p)$ be defined as in Theorem 1. Since it is analogous to $l_b(w)$, the following theorem can be viewed as an analogue of the result of Murty and Saidak for the Carlitz module.

Theorem 3. *For a monic irreducible polynomial $p \in A$, let a and $f_a(p)$ be defined as in Theorem 1. For $\gamma \in \mathbb{R}$ and $x \in \mathbb{N}$, we have*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \#\Big\{\deg p = x \,\Big|\, p \text{ satisfies } \frac{\omega(f_a(p)) - \log\deg p}{\sqrt{\log\deg p}} \leq \gamma\Big\} = G(\gamma).$$

In Theorem 1 and Corollary 2, we see that for a monic irreducible polynomial $p \in A$. the normal order of $\omega(f_a(p))$ is $\log\deg p$. We can also consider the normal order of $\omega(f_a(m))$, where $m \in A$ is a general monic polynomial. We will show that

Theorem 4. *Let $A = \mathbb{F}_q[T]$, C the A-Carlitz module, and $0 \neq a \in A$. For a monic polynomial $m \in A$, let $C(A/mA)$ and $\bar{a}$ be the reductions of C and a modulo mA respectively. Let $f_a(m)$ be the monic generator of the ideal $\{f \in A, C_f(\bar{a}) = \bar{0}\}$ on $C(A/mA)$. If $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $(1+T)$, for $x \in \mathbb{N}$, we have*

$$\sum_{\deg m = x} \Big(\omega(f_a(m)) - \frac{1}{2}(\log x)^2\Big)^2 \ll q^x (\log x)^3.$$

As a direct consequence of Theorem 4, we have

Corollary 5. *Let $m \in A$ be a monic polynomial. For any $\epsilon \in \mathbb{R}, \epsilon > 0$, we have*

$$\#\left\{ \deg m = x \,\middle|\, m \text{ satisfies } \left|\omega(f_a(m)) - \frac{1}{2}(\log \deg m)^2\right| > \epsilon(\log \deg m)^2 \right\} = o\big(q^x\big).$$

In other words, the normal order of $\omega(f_a(m))$ is $\frac{1}{2}(\log \deg m)^2$.

We recall that for $b \in \mathbb{Z}, n \in \mathbb{N}$ with $(b, n) = 1$, $l_b(n)$ is the multiplicative order of an integer b modulo n. Since it is the positive generator of the set $\{z \in \mathbb{Z}, b^z \equiv 1 \pmod n\}$, the $f_a(m)$ defined in Theorem 4 can be viewed as the Carlitz module analogue of $l_b(n)$. We remark here that unlike the integer case where we need b and n to be coprime in order to define $l_b(n)$ properly, in the case of the Carlitz module, $f_a(m)$ is well defined for all monic polynomials $m \in A$. Hence, the condition $(a, m) = 1$ is not required in our setting. The next theorem is an analogue of Erdős-Pomerance's conjecture for the Carlitz module.

Theorem 6. *For a monic polynomial $m \in A$, let a and $f_a(m)$ be defined as in Theorem 4. For $\gamma \in \mathbb{R}$ and $x \in \mathbb{N}$, we have*

$$\lim_{x\to\infty} \frac{1}{q^x} \#\left\{ \deg m = x \,\middle|\, m \text{ satisfies } \frac{\omega(f_a(m)) - \frac{1}{2}(\log \deg m)^2}{\frac{1}{\sqrt{3}}(\log \deg m)^{3/2}} \leq \gamma \right\} = G(\gamma).$$

In Section 2, we give a technical lemma that is essential for the proofs of Theorems 1 and 3. We then prove these theorems in Section 3. In Section 4, we show that in order to prove Theorems 4 and 6, it suffices to consider their analogues for $\Omega(F_a(m))$ (see Section 4 for its definition). We prove these results of $\Omega(F_a(m))$ in Section 5 to conclude the paper. Our approach in Section 4 is different from the ones in [3] and [15]. In previous works, the equivalences between Theorems 4 and 6, and their analogues for $\Omega(F_a(m))$, are proved independently from one another. However, by considering the second moment of the difference between $\omega(f_a(m))$ and $\Omega(F_a(m))$ (Lemma 11), we manage to prove these equivalences simultaneously. We also mention here that the above theorems may be generalized to general Drinfeld modules of rank one. Since the details are involved, we intend to return to the problem in a later paper.

Notation. For $x \in \mathbb{R}, x > 0$, let $f(x)$ and $g(x)$ be two functions of x. If $g(x)$ is positive and there exists a constant $C > 0$ such that $|f(x)| \leq Cg(x)$, we write either $f(x) \ll g(x)$ or $f(x) = O(g(x))$. If $\lim_{x\to\infty} f(x)/g(x) = 0$, we write $f(x) = o(g(x))$. For $p, m \in A$ and $\alpha \in \mathbb{N}$, we write $p^\alpha \| m$ to denote $p^\alpha | m$ and $p^{\alpha+1} \nmid m$.

2. An important lemma

Let $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$. For $0 \neq a \in A$, $p \in A$ a monic irreducible polynomial, we recall that $f_a(p)$ is the monic generator of the ideal $\{f \in A, C_f(\bar{a}) =$

$\bar{0}\}$ on $C(A/pA)$. Since

$$C(A/pA) \cong A/(p-1)A$$

(see [4, Theorem 3.6.3]), we have

$$(p-1)A \subseteq \{f \in A, C_f(\bar{a}) = \bar{0}\} = f_a(p)A.$$

It follows that $f_a(p)$ divides $(p-1)$ and we can write

$$p - 1 = f_a(p) \cdot i_a(p),$$

where $i_a(p) \in A$. Note that

$$\omega(p-1) - \omega(i_a(p)) \leq \omega(f_a(p)) \leq \omega(p-1).$$

Hence, if the contribution of $\omega(i_a(p))$ is 'small', we can conclude that $\omega(f_a(p))$ has the same distribution with $\omega(p-1)$. In this section, we consider the number of distinct irreducible factors of $i_a(p)$. The following lemma is essential for the proof of Theorems 1 and 3.

Lemma 7. *If $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $(1+T)$, then for $x \in \mathbb{N}$, we have*

$$\sum_{\deg p = x} \omega^2(i_a(p)) \ll \pi(x).$$

Proof. Let δ be a fixed constant with $0 < \delta < 1$ (we will make a choice of δ later). Since $\deg i_a(p) \leq \deg p = x$, there are at most $O(1)$ monic irreducible polynomials $l \in A$ with $l | i_a(p)$ and $\deg l \geq \delta x$. Hence, we have

$$\begin{aligned}
\sum_{\deg p = x} \omega^2(i_a(p)) &= \sum_{\deg p = x} \left(\sum_{l | i_a(p),\, \deg l < \delta x} 1 + O(1) \right)^2 \\
&\ll \sum_{\deg p = x} \left(\sum_{l | i_a(p),\, \deg l < \delta x} 1 \right)^2 + O\big(\pi(x)\big) \\
&= \sum_{\substack{\deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \sum_{\substack{\deg p = x \\ l_1 l_2 | i_a(p)}} 1 + \sum_{\deg l < \delta x} \sum_{\substack{\deg p = x \\ l | i_a(p)}} 1 + O\big(\pi(x)\big),
\end{aligned}$$

where l_1, l_2, and l are monic irreducible polynomials.

For $0 \neq m \in A$, it was proved in [7, Proposition 1.1] that $m | i_a(p)$ if and only if pA splits completely in K_m, where K_m is the Galois extension over k obtained by adjoining roots of $C_m(X) = 0$ and roots of $C_m(X) = a$ to k. Let $\pi_{sc}(x, K_m)$ be the number of monic irreducible polynomials $p \in A$ such that $\deg p = x$ and pA splits completely in K_m. From the above inequality, we have

(1)
$$\sum_{\deg p = x} \omega^2(i_a(p)) \ll \sum_{\substack{\deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \pi_{sc}(x, K_{l_1 l_2}) + \sum_{\deg l < \delta x} \pi_{sc}(x, K_l) + O\big(\pi(x)\big).$$

To estimate $\pi_{sc}(x, K_m)$, we apply the Chebotarev density theorem for function fields. It was proved in [9, p. 55] that

$$\pi_{sc}(x, K_m) = \frac{\pi(x)}{N_m} + O\big(N_m \cdot d_m \cdot q^{x/2}\big),$$

where $N_m = [K_m : k]$ and d_m is the total degree of the discriminant divisor $\Delta(K_m/k)$. Let $l \in A$ be an irreducible polynomial. From [7, Proposition 4.4], there exists a positive integer d_a (depending only on a) such that if $\deg l > d_a$,

$$N_l = (q^{\deg l} - 1)\, q^{\deg l},$$

provided that $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $1 + T$. It was also proved in [7, Theorem 1.7] that for two distinct irreducible polynomials l_1 and l_2, we have $K_{l_1 l_2} = K_{l_1} \cdot K_{l_2}$, and K_{l_1} and K_{l_2} are linearly disjoint over k. Thus if both $\deg l_1, \deg l_2 > d_a$,

$$N_{l_1 l_2} = N_{l_1} \cdot N_{l_2} = (q^{\deg l_1} - 1)\, q^{\deg l_1} \cdot (q^{\deg l_2} - 1)\, q^{\deg l_2}.$$

Moreover, from [7, Theorem 2.4], we have $d_m/N_m = O(\deg m)$ as $\deg m \to \infty$. Thus $N_m \cdot d_m \ll N_m^2 \cdot \deg m$.

For the first sum in the right hand side of (1), we write

$$\begin{aligned}\sum_{\substack{\deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \pi_{sc}(x, K_{l_1 l_2}) \leq & \sum_{\substack{d_a < \deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \pi_{sc}(x, K_{l_1 l_2}) \\ & + 2 \sum_{\deg l_1 \leq d_a} \sum_{d_a < \deg l_2 \leq \delta x} \pi_{sc}(x, K_{l_1 l_2}) \\ & + \sum_{\deg l_1, \deg l_2 \leq d_a} \pi_{sc}(x, K_{l_1 l_2}).\end{aligned} \tag{2}$$

Applying the Chebotarev density theorem in function fields to the first sum on the right hand side of (2), we have

$$\begin{aligned}& \sum_{\substack{d_a < \deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \pi_{sc}(x, K_{l_1 l_2}) \\ &= \sum_{\substack{d_a < \deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \frac{\pi(x)}{(q^{\deg l_1} - 1)\, q^{\deg l_1} \cdot (q^{\deg l_2} - 1)\, q^{\deg l_2}} \\ &\quad + \sum_{\substack{d_a < \deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} O\big(N_{l_1 l_2}^2 \cdot \deg l_1 l_2 \cdot q^{x/2}\big) \\ &\ll \pi(x) \cdot \left(\sum_{n < \delta x} \frac{\pi(n)}{(q^n - 1)\, q^n} \right)^2 + q^{x/2} \cdot 2\delta x \cdot \left(\sum_{n < \delta x} \pi(n)\, (q^n - 1)^2\, q^{2n} \right)^2 \\ &\ll \pi(x) + q^{x/2} \cdot 2\delta x \cdot q^{10\delta x}.\end{aligned}$$

The last inequality holds since $\pi(n) \ll q^n/n$ (see [17, Theorem 2.2]). Choosing $10\delta < 1/2$, say $\delta = 1/21$, it follows that

$$\sum_{\substack{d_a < \deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \pi_{sc}(x, K_{l_1 l_2}) \ll \pi(x) + q^{41/42x} \cdot x \ll \pi(x). \tag{3}$$

For the second sum on the right hand side of (2), we note that if pA splits completely in $K_{l_1 l_2}$, then pA splits completely in K_{l_2}. Thus

$$\begin{aligned} & 2 \sum_{\deg l_1 < d_a} \sum_{d_a < \deg l_2 < \delta x} \pi_{sc}(x, K_{l_1 l_2}) \\ & \ll \sum_{\deg l_2 < \delta x} \pi_{sc}(x, K_{l_2}) \qquad \text{(since } d_a \text{ is a constant)} \\ & \ll \pi(x) \cdot \sum_{n < \delta x} \frac{\pi(n)}{(q^n - 1) \cdot q^n} + q^{x/2} \cdot \delta x \cdot \sum_{n < \delta x} \pi(n) \, (q^n - 1)^2 \, q^{2n} \\ & \ll \pi(x) + q^{x/2} \cdot 2\delta x \cdot q^{5\delta x} \ll \pi(x), \end{aligned} \tag{4}$$

where the last inequality holds if $5\delta < 1/2$. Also, since $\pi_{sc}(x, K_{l_1 l_2}) \leq \pi(x)$,

$$\sum_{\deg l_1, \deg l_2 \leq d_a} \pi_{sc}(x, K_{l_1 l_2}) \ll \pi(x). \tag{5}$$

Combining (2), (3), (4), and (5), and choosing $\delta = 1/21$, we have

$$\sum_{\substack{\deg l_1, \deg l_2 < \delta x \\ l_1 \neq l_2}} \pi_{sc}(x, K_{l_1 l_2}) \ll \pi(x) + q^{41/42x} \cdot x \ll \pi(x). \tag{6}$$

Moreover, we already saw in the proof of (4) that if $5\delta < 1/2$, then

$$\sum_{\deg l < \delta x} \pi_{sc}(x, K_l) \ll \pi(x). \tag{7}$$

Combining (1), (6), and (7), we have

$$\sum_{\deg p = x} \omega^2(i_a(p)) \ll \pi(x).$$

This completes the proof of Lemma 7. □

3. Proofs of Theorems 1 and 3

Now, we are ready to prove Theorems 1 and 3. We start with a proof of Theorem 1. As usual, $p \in A$ is a monic irreducible polynomial.

Proof of Theorem 1. It was proved in [12, p. 326] that

$$\sum_{\deg p = x} \omega(p - 1) = \pi(x) \log x + O\big(\pi(x)\big)$$

and

$$\sum_{\deg p = x} \omega^2(p - 1) = \pi(x)(\log x)^2 + O\big(\pi(x) \log x\big).$$

Since

$$\omega(p - 1) - \omega(i_a(p)) \leq \omega(f_a(p)) \leq \omega(p - 1),$$

from Lemma 7, we get

$$\sum_{\deg p = x} \omega(f_a(p)) = \sum_{\deg p = x} \omega(p - 1) + O\left(\sum_{\deg p = x} \omega(i_a(p)) \right) = \pi(x) \log x + O\big(\pi(x)\big). \tag{8}$$

Also, from Lemma 7, we have

(9)
$$\begin{aligned}
&\sum_{\deg p=x} \omega^2(f_a(p)) \\
&= \sum_{\deg p=x} \omega^2(p-1) + O\bigg(\sum_{\deg p=x} \omega(p-1)\,\omega(i_a(p))\bigg) + O\bigg(\sum_{\deg p=x} \omega^2(i_a(p))\bigg) \\
&= \sum_{\deg p=x} \omega^2(p-1) + O\bigg(\Big(\sum_{\deg p=x} \omega^2(p-1)\Big)^{1/2} \Big(\sum_{\deg p=x} \omega^2(i_a(p))\Big)^{1/2}\bigg) + O\big(\pi(x)\big) \\
&= \pi(x)(\log x)^2 + O\big(\pi(x)\log x\big).
\end{aligned}$$

Applying (8) and (9), we have

$$\begin{aligned}
\sum_{\deg p=x} \Big(\omega(f_a(p)) - \log x\Big)^2 &= \sum_{\deg p=x} \omega^2(f_a(p)) - 2\log x \sum_{\deg p=x} \omega(f_a(p)) + \pi(x)(\log x)^2 \\
&\ll \pi(x)\log x.
\end{aligned}$$

This completes the proof of the theorem. □

Now, we prove a prime analogue of the conjecture of Erdős and Pomerance for the Carlitz module.

Proof of Theorem 3. To prove Theorem 3, we need the following result in [12, Theorem 2]: letting $\gamma \in \mathbb{R}$ and $x \in \mathbb{N}$,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \#\bigg\{ \deg p = x \,\big|\, p \text{ satisfies } \frac{\omega(p-1) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma \bigg\} = G(\gamma). \tag{10}$$

We saw in the proof of Theorem 1 that

$$\frac{\omega(p-1) - \log\deg p}{\sqrt{\log\deg p}} - \frac{\omega(i_a(p))}{\sqrt{\log\deg p}} \le \frac{\omega(f_a(p)) - \log\deg p}{\sqrt{\log\deg p}} \le \frac{\omega(p-1) - \log\deg p}{\sqrt{\log\deg p}}.$$

For any $\epsilon > 0$ and $x \in \mathbb{N}$, define

$$E(x,\epsilon) = \#\bigg\{ \deg p = x \,\big|\, p \text{ satisfies } \frac{\omega(i_a(p))}{\sqrt{\log\deg p}} \ge \epsilon \bigg\}.$$

From Lemma 7, we have

$$E(x,\epsilon)\cdot\epsilon\sqrt{\log x} \le \sum_{\deg p=x} \omega(i_a(p)) \le \sum_{\deg p=x} \omega^2(i_a(p)) \ll \pi(x).$$

Since $E(x,\epsilon) = o(\pi(x))$, for $\gamma \in \mathbb{R}$, we obtain

$$\begin{aligned}
&\#\bigg\{ \deg p = x \,\big|\, p \text{ satisfies } \frac{\omega(f_a(p)) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma \bigg\} \\
&\le \#\bigg\{ \deg p = x \,\big|\, p \text{ satisfies } \frac{\omega(p-1) - \log\deg p}{\sqrt{\log\deg p}} - \frac{\omega(i_a(p))}{\sqrt{\log\deg p}} \le \gamma \bigg\} \\
&\le \#\bigg\{ \deg p = x \,\big|\, p \text{ satisfies } \frac{\omega(p-1) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma + \epsilon \bigg\} + o\big(\pi(x)\big).
\end{aligned}$$

Also, we have

$$\begin{aligned}&\#\left\{\deg p = x \,\middle|\, p \text{ satisfies } \frac{\omega(f_a(p)) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma\right\}\\ &\ge \#\left\{\deg p = x \,\middle|\, p \text{ satisfies } \frac{\omega(p-1) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma\right\}.\end{aligned}$$

Using the above two estimates, we can derive from (10) that

$$G(\gamma) \le \lim_{x\to\infty} \frac{1}{\pi(x)} \#\left\{\deg p = x \,\middle|\, p \text{ satisfies } \frac{\omega(f_a(p)) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma\right\} \le G(\gamma+\epsilon).$$

Let $\epsilon \to 0$. Since $G(\gamma)$ is a continuous function, it follows that

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \#\left\{\deg p = x \,\middle|\, p \text{ satisfies } \frac{\omega(f_a(p)) - \log\deg p}{\sqrt{\log\deg p}} \le \gamma\right\} = G(\gamma).$$

This completes the proof of Theorem 3. □

4. Equivalent statements of Theorems 4 and 6

In this section, we will give statements that are equivalent to Theorems 4 and 6. The alternative formulations have the advantage of being 'strongly additive', which is a favorable property in probabilistic number theory.

By the Chinese Remainder Theorem [6, Proposition 1.4], we have

$$C(A/mA) \cong \prod_{p^\alpha \| m} C(A/p^\alpha A).$$

It follows that

$$f_a(m) = \operatorname{lcm}\big\{f_a(p^\alpha),\, p^\alpha \| m\big\}.$$

Instead of $f_a(m)$, it is indeed more convenient to prove our theorems for

$$F_a(m) = \prod_{p^\alpha \| m} f_a(p^\alpha).$$

For $m \in A$, let $\Omega(m)$ denote the total number of irreducible polynomials dividing m, counting multiplicity. Since $f_a(m) = \operatorname{lcm}\{f_a(p^\alpha), p^\alpha \| m\}$, we have

$$\omega(F_a(m)) = \omega(f_a(m)) \le \Omega(f_a(m)) \le \Omega(F_a(m)). \tag{11}$$

In this section, we will show that to obtain Theorems 4 and 6, it suffices to prove their analogues for $\Omega(F_a(m))$. Since $F_a(m)$ is a product of $f_a(p^\alpha)$, we consider first $f_a(p^\alpha)$.

Lemma 8. *For a monic irreducible polynomial $p \in A$ and $\alpha \ge 1$, we have*

$$f_a(p^\alpha) = f_a(p)p^\beta \qquad \text{where} \quad 0 \le \beta \le \alpha - 1.$$

Proof. To prove this lemma, since p is irreducible, it suffices to show $f_a(p) | f_a(p^\alpha)$ and $f_a(p^\alpha) | f_a(p)p^{\alpha-1}$. Since

$$\big\{f \in A, C_f(\bar a) = \bar 0\big\} \text{ on } C(A/p^\alpha A) \;\subseteq\; \big\{f \in A, C_f(\bar a) = \bar 0\big\} \text{ on } C(A/pA),$$

we have

$$f_a(p) | f_a(p^\alpha).$$

Consider the polynomial $f_a(p)p^{\alpha-1}$. For $g \in A$, $n \in \mathbb{N}$, since $C_p(X)/X$ is an Eisenstein polynomial in X, i.e., $C_p(X)$ is of the form [17, p. 203],

$$X^{q^{\deg p}} + c_1 \cdot p \cdot X^{q^{\deg p - 1}} + c_2 \cdot p \cdot X^{q^{\deg p - 2}} + \cdots + c_{\deg p} \cdot p \cdot X \qquad \text{with} \quad c_i \in A,$$

we have

$$C_p(p^n g) = (p^n g)^{q^{\deg p}} + c_1 \cdot p \cdot (p^n g)^{q^{\deg p - 1}} + \cdots + c_{\deg p} \cdot p \cdot (p^n g) \in p^{n+1} A. \tag{12}$$

Since $C_{f_a(p)}(a) \in pA$, we can write $C_{f_a(p)}(a) = p^n g$ with $n \geq 1$ and $g \in A$. Applying (12) repeatedly, we have

$$C_{p^{\alpha-1} f_a(p)}(a) = C_{p^{\alpha-1}}\big(C_{f_a(p)}(a)\big) = C_{p^{\alpha-1}}(p^n g) \in p^{n+\alpha-1} A \subseteq p^\alpha A.$$

Hence, on $C(A/p^\alpha A)$, we obtain

$$f_a(p^\alpha) | f_a(p) p^{\alpha-1}.$$

This completes the proof of the lemma. □

From Lemma 8, we have

$$\sum_{p|m} \Omega(f_a(p)) \leq \Omega(F_a(m)) \leq \sum_{p|m} \Omega(f_a(p)) + \Omega(m). \tag{13}$$

We will see later that from (11) and (13), one can derive

$$\sum_{\deg m = x} \omega(f_a(m)) \sim \sum_{\deg m = x} \sum_{p|m} \Omega(f_a(p)).$$

Since the double sums are equal to

$$q^x \cdot \sum_{\deg p \leq x} \frac{\Omega(f_a(p))}{q^{\deg p}},$$

to study $\omega(f_a(m))$, we need to consider $\frac{\Omega(f_a(p))}{q^{\deg p}}$ on average. We prove that

Lemma 9. *Let a and $f_a(p)$ be defined as in Theorem 1. For $x \in \mathbb{N}$, we have*

$$\sum_{\deg p \leq x} \frac{\Omega(f_a(p))}{q^{\deg p}} = \frac{1}{2} (\log x)^2 + O(\log x)$$

and

$$\sum_{\deg p \leq x} \frac{\Omega^2(f_a(p))}{q^{\deg p}} = \frac{1}{3} (\log x)^3 + O\big((\log x)^2\big).$$

Proof. Let $l \in A$ be a monic irreducible polynomial. From (8), we have

$$\begin{aligned}
\sum_{\deg p = x} \Omega(f_a(p)) &= \sum_{\deg p = x} \sum_{l^\beta \| f_a(p)} \beta \\
&= \sum_{\deg p = x} \omega(f_a(p)) + \sum_{\deg p = x} \sum_{\substack{l^\beta \| f_a(p) \\ \beta \geq 2}} (\beta - 1) \\
&= \pi(x) \log x + O\big(\pi(x)\big) + \sum_{\deg p = x} \sum_{\substack{l^\beta \| f_a(p) \\ \beta \geq 2}} (\beta - 1).
\end{aligned}$$

Using the Brun-Titchmarsh theorem in function fields [8, Theorem 4.3], we have

$$\begin{aligned}\sum_{\deg p=x}\sum_{\substack{l^\beta \| f_a(p)\\ \beta\geq 2}}(\beta-1) &\leq \sum_{\deg p=x}\sum_{\substack{l^\gamma\|(p-1)\\ \gamma\geq 2}}(\gamma-1) \quad (\text{since } \beta\leq\gamma)\\ &\ll \sum_{\deg l^2\leq x}\left(\frac{\pi(x)}{q^{2\deg l}}+\frac{2\pi(x)}{q^{3\deg l}}+\cdots\right)\\ &\ll \pi(x)\cdot\sum_{n\leq x}\pi(n)\left(\frac{1}{q^{2n}}+\frac{2}{q^{3n}}+\cdots\right)\ll \pi(x).\end{aligned}$$

Combining the above two estimates, we obtain

$$\sum_{\deg p=x}\Omega(f_a(p))=\pi(x)\log x+O\big(\pi(x)\big). \tag{14}$$

Similarly, we can derive from (9) that

$$\sum_{\deg p=x}\Omega^2(f_a(p))=\pi(x)(\log x)^2+O\big(\pi(x)\log x\big). \tag{15}$$

By a partial summation and (14), we can obtain

$$\begin{aligned}\sum_{\deg p\leq x}\frac{\Omega(f_a(p))}{q^{\deg p}} &= \sum_{n\leq x}\frac{1}{q^n}\sum_{\deg p=n}\Omega(f_a(p))\\ &= \sum_{n\leq x}\frac{1}{q^n}\Big(\pi(n)\log n+O\big(\pi(n)\big)\Big)\\ &= \sum_{n\leq x}\frac{\log n}{n}+O\bigg(\sum_{n\leq x}\frac{\log n}{q^{n/2}}\bigg)+O\bigg(\sum_{n\leq x}\frac{1}{n}\bigg)\\ &= \frac{1}{2}(\log x)^2+O\big(\log x\big).\end{aligned}$$

Similarly, applying a partial summation to (15), we get

$$\sum_{\deg p\leq x}\frac{\Omega^2(f_a(p))}{q^{\deg p}}=\frac{1}{3}(\log x)^3+O\big((\log x)^2\big).$$

This completes the proof of the lemma. □

The following lemma is essential when we make a transition from $\omega(f_a(m))$ to $\Omega(F_a(m))$.

Lemma 10. *Let $p\in A$ be a monic irreducible polynomial and $m\in A$ a monic polynomial with $\deg m\geq 1$. Then we have*

$$\sum_{\substack{\deg p\leq x\\ p\equiv 1(\mathrm{mod}\, m)}}\frac{1}{q^{\deg p}}=\frac{\log x}{\varphi(m)}+O(1),$$

where $\varphi(m)$ is the order of the multiplicative group $(A/mA)^*$.

Proof. From Dirichlet's theorem on monic irreducible polynomials in an arithmetic progression (see [17, Theorem 4.8]), we have

$$\pi(n,1,m):=\#\Big\{\deg p=n\,\Big|\,p\equiv 1(\mathrm{mod}\, m)\Big\}=\frac{1}{\varphi(m)}\cdot\frac{q^n}{n}+O\big(q^{n/2}/n\big).$$

Thus it follows that

$$\sum_{\substack{\deg p\le x\\ p\equiv 1 \,(\mathrm{mod}\, m)}} \frac{1}{q^{\deg p}} = \sum_{n\le x}\left(\frac{1}{\varphi(m)\,n} + O\big(q^{-n/2}/n\big)\right) = \frac{\log x}{\varphi(m)} + O(1).$$

This completes the proof of the lemma. □

The following lemma estimates the difference between $\omega(f_a(m))$ and $\Omega(F_a(m))$.

Lemma 11. *Let $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $(1+T)$. For $x \in \mathbb{N}$, we have*

$$\sum_{\deg m = x}\Big(\Omega(F_a(m)) - \omega(f_a(m))\Big)^2 \ll q^x\,(\log x)^2.$$

Proof. We saw in (11) that $\omega(f_a(m)) = \omega(F_a(m))$. Hence, to prove this lemma, it suffices to consider the difference between $\Omega(F_a(m))$ and $\omega(F_a(m))$. For $1 \le y \le x$ and $l \in A$ a monic irreducible polynomial, we define the truncated functions

$$\omega_y(F_a(m)) = \sum_{\substack{l\mid F_a(m)\\ \deg l\le y}} 1 \qquad \text{and} \qquad \Omega_y(F_a(m)) = \sum_{\substack{l^\alpha \| F_a(m)\\ \deg l\le y}} \alpha.$$

Let $\omega_y^+(F_a(m))$ be the number of distinct divisors of $F_a(m)$ whose degrees are $> y$ and $\Omega_y^+(F_a(m))$ defined similarly. Then we have

(16)

$$\begin{aligned}
&\sum_{\deg m = x}\Big(\Omega(F_a(m)) - \omega(F_a(m))\Big)^2\\
&= \sum_{\deg m = x}\Big(\Omega_y(F_a(m)) + \Omega_y^+(F_a(m)) - \omega_y(F_a(m)) - \omega_y^+(F_a(m))\Big)^2\\
&\ll \sum_{\deg m = x}\Big(\Omega_y^+(F_a(m)) - \omega_y^+(F_a(m))\Big)^2 + \sum_{\deg m = x}\Omega_y^2(F_a(m)) + \sum_{\deg m = x}\omega_y^2(F_a(m)).
\end{aligned}$$

Applying (13) and Lemma 9 to the last two sums, we get

(17)

$$\begin{aligned}
\sum_{\deg m = x}\omega_y^2(F_a(m)) &\le \sum_{\deg m = x}\Omega_y^2(F_a(m))\\
&\ll \sum_{\deg m = x}\left\{\left(\sum_{p\mid m,\,\deg p\le y}\Omega(f_a(p))\right)^2 + \Omega_y^2(m)\right\}\\
&\ll \sum_{\deg p_1, \deg p_2 \le y}\Omega(f_a(p_1))\,\Omega(f_a(p_2))\,\frac{q^x}{q^{\deg p_1}\,q^{\deg p_2}} + O\big(q^x(\log y)^2\big)\\
&\ll q^x\left(\sum_{\deg p\le y}\frac{\Omega(f_a(p))}{q^{\deg p}}\right)^2 + O\big(q^x(\log y)^2\big) \ll q^x(\log y)^4.
\end{aligned}$$

Let $y = \delta \log x$ for some $\delta > 0$. From (16) and (17), it remains to prove an analogue of the lemma for $\Omega_y^+(F_a(m))$ and $\omega_y^+(F_a(m))$.

Since

$$F_a(m) \,\Big|\, \prod_{p^\alpha \| m} f_a(p) p^{\alpha-1},$$

if $l^2|F_a(m)$, it implies that either (A) $l^2|f_a(p)$ for some irreducible polynomial $p|m$, (B) there exist two distinct irreducible polynomials p_1, p_2 such that $l|f_a(p_1)$, $l|f_a(p_2)$, and $p_1p_2|m$, or (C) $l|m$. We will use the notation $m \in \mathcal{A}$ (resp. $\mathcal{B}$ or $\mathcal{C}$) to refer to the case (A) (resp. (B) or (C)). Note that if there is no such $l^2|F_a(m)$ with $\deg l > y$ (write $m \notin \mathcal{A}, \mathcal{B}, \mathcal{C}$), we have

$$\sum_{\substack{\deg m = x \\ m \notin \mathcal{A},\mathcal{B},\mathcal{C}}} \Big(\Omega_y^+(F_a(m)) - \omega_y^+(F_a(m))\Big)^2 = 0. \tag{18}$$

In cases (A) and (B), we have

$$\omega_y^+(F_a(m)) \le \Omega_y^+(F_a(m)) \le \omega_y^+(F_a(m)) + \Omega(F_a(m))\delta(m),$$

where $\delta(m) = 1$, if there exists $l^2|F_a(m)$ with $\deg l > y$, and $\delta(m) = 0$ otherwise. It follows that

$$\Omega_y^+(F_a(m)) = \omega_y^+(F_a(m)) + O\Big(\Omega(F_a(m))\delta(m)\Big).$$

Hence, we have

$$\sum_{\substack{\deg m = x \\ m \in \mathcal{A} \text{ or } \mathcal{B}}} \Big(\Omega_y^+(F_a(m)) - \omega_y^+(F_a(m))\Big)^2 \ll \sum_{\substack{\deg m = x \\ m \in \mathcal{A} \text{ or } \mathcal{B}}} \delta(m)\Omega^2(F_a(m)).$$

Note that if $F_a(m) = l_1^{\beta_1} \cdots l_r^{\beta_r}$, then

$$\Omega(F_a(m)) = \sum_{i=1}^{r} \beta_i \le \deg F_a(m) \le \deg m.$$

Thus for case (A), by Lemma 10, we have

$$\begin{aligned}
\sum_{\substack{\deg m = x \\ m \in \mathcal{A}}} \delta(m)\Omega^2(F_a(m)) &\le x^2 \sum_{\substack{\deg m = x \\ m \in \mathcal{A}}} \delta(m) = x^2 \sum_{\deg l > y} \sum_{\substack{\deg m = x \\ l^2 | f_a(p),\, p|m}} 1 \\
&\le x^2 \sum_{\deg l > y} \sum_{\substack{\deg p \le x \\ p \equiv 1 \pmod{l^2}}} \frac{q^x}{q^{\deg p}} \\
&\ll x^2\, q^x \sum_{\deg l > y} \frac{\log x}{q^{2\deg l}} \ll x^2\, q^x\, \frac{\log x}{q^y y}.
\end{aligned}$$

Choosing $y = 2\log x$, we have

$$\sum_{\substack{\deg m = x \\ m \in \mathcal{A}}} \delta(m)\Omega^2(F_a(m)) \ll q^x.$$

Similarly, by Lemma 10, one can show that if $y = 2\log x$, then

$$\begin{aligned}
\sum_{\substack{\deg m = x \\ m \in \mathcal{B}}} \delta(m)\Omega^2(F_a(m)) &\le x^2 \sum_{\deg l > y} \sum_{\substack{\deg p_1, \deg p_2 \le x \\ p_1 \equiv 1 \pmod{l} \\ p_2 \equiv 1 \pmod{l}}} \frac{q^x}{q^{\deg p_1} q^{\deg p_2}} \\
&\ll x^2\, q^x \sum_{\deg l > y} \left(\frac{\log x}{q^{\deg l}}\right)^2 \ll q^x\, \log x.
\end{aligned}$$

Hence, we have

$$\sum_{\substack{\deg m=x \\ m\in\mathcal{A}\text{ or }\mathcal{B}}} \left(\Omega_y^+(F_a(m)) - \omega_y^+(F_a(m))\right)^2 \ll q^x \log x. \tag{19}$$

In case (C), if $l^2 \nmid f_a(p)$ for any $p|m$ and there is no distinct $p_1|m, p_2|m$ such that $l|f_a(p_1)$ and $l|f_a(p_2)$, we have

$$\omega_y^+(F_a(m)) \le \Omega_y^+(F_a(m)) \le \omega_y^+(F_a(m)) + \Omega(m).$$

Hence,

$$\sum_{\substack{\deg m=x \\ m\in\mathcal{C}\setminus(\mathcal{A}\cup\mathcal{B})}} \left(\Omega_y^+(F_a(m)) - \omega_y^+(F_a(m))\right)^2 \ll \sum_{\deg m=x} \Omega^2(m) \ll q^x(\log x)^2. \tag{20}$$

From (18), (19), and (20), we have

$$\sum_{\deg m=x} \left(\Omega_y^+(F_a(m)) - \omega_y^+(F_a(m))\right)^2 \ll q^x(\log x)^2.$$

Combining this equation with (16) and (17), the lemma follows. □

Now, we are ready to give an equivalent statement of Theorem 4.

Lemma 12. *Let $q \neq 2$ or $q = 2$ and $a \neq 1, T$, or $(1+T)$. For $x \in \mathbb{N}$,*

$$\sum_{\deg m=x} \left(\omega(f_a(m)) - \frac{1}{2}(\log x)^2\right)^2 \ll q^x\,(\log x)^3$$

if and only if

$$\sum_{\deg m=x} \left(\Omega(F_a(m)) - \frac{1}{2}(\log x)^2\right)^2 \ll q^x\,(\log x)^3.$$

Proof. We observe that

$$\begin{aligned}
&\sum_{\deg m=x} \left(\omega(f_a(m)) - \frac{1}{2}(\log x)^2\right)^2 \\
&= \sum_{\deg m=x} \left(\omega(f_a(m)) - \Omega(F_a(m)) + \Omega(F_a(m)) - \frac{1}{2}(\log x)^2\right)^2 \\
&\ll \sum_{\deg m=x} \left(\Omega(F_a(m)) - \omega(F_a(m))\right)^2 + \sum_{\deg m=x} \left(\Omega(F_a(m)) - \frac{1}{2}(\log x)^2\right)^2.
\end{aligned}$$

Similarly,

$$\begin{aligned}
&\sum_{\deg m=x} \left(\Omega(F_a(m)) - \frac{1}{2}(\log x)^2\right)^2 \\
&\ll \sum_{\deg m=x} \left(\Omega(F_a(m)) - \omega(F_a(m))\right)^2 + \sum_{\deg m=x} \left(\omega(f_a(m)) - \frac{1}{2}(\log x)^2\right)^2.
\end{aligned}$$

Applying Lemma 11 to the above equation, the lemma follows. □

Lemma 13. *For $\gamma \in \mathbb{R}$ and $x \in \mathbb{N}$, we have*

$$\lim_{x\to\infty} \frac{1}{q^x} \# \left\{ \deg m = x \,\middle|\, m \text{ satisfies } \frac{\omega(f_a(m)) - \frac{1}{2}(\log\deg m)^2}{\frac{1}{\sqrt{3}}(\log\deg m)^{3/2}} \le \gamma \right\} = G(\gamma)$$

if and only if

$$\lim_{x\to\infty} \frac{1}{q^x} \# \left\{ \deg m = x \,\middle|\, m \text{ satisfies } \frac{\Omega(F_a(m)) - \frac{1}{2}(\log\deg m)^2}{\frac{1}{\sqrt{3}}(\log\deg m)^{3/2}} \le \gamma \right\} = G(\gamma).$$

Proof. To prove this lemma, it suffices to show that for all but $o(q^x)$ monic polynomials $m \in A$ with $\deg m = x$, we have

$$\Omega(F_a(m)) - \omega(f_a(m)) = o\big((\log x)^{3/2}\big).$$

We will actually prove something much stronger. Define

$$E_1(x) = \#\Big\{ \deg m = x \,\Big|\, m \text{ satisfies } \Omega(F_a(m)) - \omega(f_a(m)) \ge \log x \log\log x \Big\}.$$

Using Lemma 11, we have

$$E_1(x) \cdot (\log x \log\log x)^2 \le \sum_{\deg m = x} \Big(\Omega(F_a(m)) - \omega(f_a(m))\Big)^2 \ll q^x\,(\log x)^2.$$

Since $E_1(x) = o(q^x)$, the lemma follows. □

5. Proofs of Theorems 4 and 6

Let $m \in A$ be a monic polynomial. We are now ready to prove Theorems 4 and 6.

Proof of Theorem 4. From Lemma 12, to prove Theorem 4, it suffices to consider its analogue for $\Omega(F_a(m))$. From (13), we have

$$\sum_{\deg m = x} \Omega(F_a(m)) = \sum_{\deg m = x} \sum_{p \mid m} \Omega(f_a(p)) + O\bigg(\sum_{\deg m = x} \Omega(m) \bigg).$$

Using Lemma 9, we can obtain

$$\sum_{\deg m = x} \sum_{p\mid m} \Omega(f_a(p)) = \sum_{\deg p \le x} \Omega(f_a(p)) \cdot \frac{q^x}{q^{\deg p}} = \frac{1}{2}\, q^x (\log x)^2 + O\big(q^x \log x\big).$$

Since

$$\sum_{\deg m = x} \Omega(m) \ll q^x \log x,$$

combining the above estimates, we get

$$\sum_{\deg m = x} \Omega(F_a(m)) = \frac{1}{2}\, q^x (\log x)^2 + O\big(q^x\, \log x\big). \tag{21}$$

From (13), we have

$$\begin{aligned} \sum_{\deg m = x} \Omega(F_a(m))^2 &= \sum_{\deg m = x} \bigg(\sum_{p\mid m} \Omega(f_a(p)) + O\big(\Omega(m)\big) \bigg)^2 \\ &= \sum_{\deg m = x} \bigg(\sum_{p\mid m} \Omega(f_a(p)) \bigg)^2 + O\big(E(x)\big), \end{aligned} \tag{22}$$

where

$$E(x) = \max\left\{ \sum_{\deg m = x} \sum_{p \mid m} \Omega(f_a(p))\Omega(m), \sum_{\deg m = x} \Omega^2(m) \right\}.$$

From Lemma 9, we have

$$\begin{aligned}\sum_{\deg m = x} \sum_{p \mid m} \Omega(f_a(p))\Omega(m) &= \sum_{\deg p \le x} \Omega(f_a(p)) \sum_{\substack{\deg m = x \\ p \mid m}} \Omega(m) \\ &\ll q^x \log x \sum_{\deg p \le x} \frac{\Omega(f_a(p))}{q^{\deg p}} \ll q^x (\log x)^3.\end{aligned}$$

The last two inequalities hold since

$$\sum_{\substack{\deg m = x \\ p \mid m}} \Omega(m) = \sum_{\deg n = x - \deg p} \big(1 + \Omega(n)\big) \ll q^{x - \deg p} \log x.$$

Also,

$$\sum_{\deg m = x} \Omega^2(m) \ll q^x (\log x)^2.$$

Hence, we have

$$E(x) \ll q^x (\log x)^3. \tag{23}$$

We consider the main term in (22):

(24)

$$\begin{aligned}\sum_{\deg m = x} \left(\sum_{p \mid m} \Omega(f_a(p)) \right)^2 &= q^x \sum_{\substack{\deg p_1 + \deg p_2 \le x \\ p_1 \ne p_2}} \frac{\Omega(f_a(p_1))\Omega(f_a(p_2))}{q^{\deg p_1} q^{\deg p_2}} \\ &\quad + q^x \sum_{\deg p \le x} \frac{\Omega^2(f_a(p))}{q^{\deg p}} \\ &= q^x \sum_{\deg p_1 + \deg p \le x} \frac{\Omega(f_a(p_1))\Omega(f_a(p_2))}{q^{\deg p_1} q^{\deg p_2}} + O\big(q^x (\log x)^3\big).\end{aligned}$$

The last equality follows from Lemma 9 and the following estimate:

$$\sum_{\deg p \le x} \frac{\Omega^2(f_a(p))}{q^{2 \deg p}} = \sum_{n \le x} \frac{1}{q^n} \sum_{\deg p = n} \frac{\Omega^2(f_a(p))}{q^{\deg p}} \ll \sum_{n \le x} \frac{(\log n)^3}{q^n} \ll 1.$$

Consider

$$\begin{aligned}\sum_{\deg p_1 + \deg p_2 \le x} \frac{\Omega(f_a(p_1))\Omega(f_a(p_2))}{q^{\deg p_1} q^{\deg p_2}} &= \sum_{\deg p_1 \le x/2} \frac{\Omega(f_a(p_1))}{q^{\deg p_1}} \sum_{\deg p_2 \le x - \deg p_1} \frac{\Omega(f_a(p_2))}{q^{\deg p_2}} \\ &\quad + \sum_{x/2 < \deg p_1 \le x} \frac{\Omega(f_a(p_1))}{q^{\deg p_1}} \sum_{\deg p_2 \le x - \deg p_1} \frac{\Omega(f_a(p_2))}{q^{\deg p_2}}.\end{aligned}$$

Applying Lemma 9, we have

$$\begin{aligned}
&\sum_{\deg p_1 \le x/2} \frac{\Omega(f_a(p_1))}{q^{\deg p_1}} \sum_{\deg p_2 \le x-\deg p_1} \frac{\Omega(f_a(p_2))}{q^{\deg p_2}} \\
&= \sum_{\deg p_1 \le x/2} \frac{\Omega(f_a(p_1))}{q^{\deg p_1}} \cdot \left(\frac{1}{2} \big(\log(x - \deg p_1) \big)^2 + O(\log x) \right) \\
&= \sum_{\deg p_1 \le x/2} \frac{\Omega(f_a(p_1))}{q^{\deg p_1}} \cdot \left(\frac{1}{2} (\log x)^2 + O(\log x) \right) \quad (\text{since } \deg p_1 \le x/2) \\
&= \frac{1}{4} (\log x)^4 + O\big((\log x)^3 \big).
\end{aligned}$$

Also, by Lemma 9,

$$\begin{aligned}
&\sum_{x/2 < \deg p_1 \le x} \frac{\Omega(f_a(p_1))}{q^{\deg p_1}} \sum_{\deg p_2 \le x-\deg p_1} \frac{\Omega(f_a(p_2))}{q^{\deg p_2}} \\
&\ll \left(\frac{1}{2} (\log x)^2 + O(\log x) - \frac{1}{2} (\log x/2)^2 \right) \cdot (\log x)^2 \\
&\ll (\log x)^3.
\end{aligned}$$

Combining the above two estimates, we have

$$\sum_{\deg p_1 + \deg p_2 \le x} \frac{\Omega(f_a(p_1))\Omega(f_a(p_2))}{q^{\deg p_1} q^{\deg p_2}} = \frac{1}{4} (\log x)^4 + O\big((\log x)^3 \big). \tag{25}$$

Combining (22), (23), (24), and (25), we obtain

$$\sum_{\deg m = x} \Omega(F_a(m))^2 = \frac{1}{4} q^x (\log x)^4 + O\big(q^x (\log x)^3 \big). \tag{26}$$

Using (21) and (26), we get

$$\sum_{\deg m = x} \left(\Omega(F_a(m)) - \frac{1}{2} (\log x)^2 \right)^2 \ll q^x (\log x)^3.$$

Applying Lemma 12, the theorem follows. □

We now prove Theorem 6.

Proof of Theorem 6. From Lemma 13, to prove Theorem 6, it suffices to show that for $m \in A, \deg m = x$, the quantity

$$\frac{\Omega(F_a(m)) - \frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}} (\log x)^{3/2}}$$

distributes normally. We recall that in (13), we have

$$\Omega(F_a(m)) = \sum_{p \mid m} \Omega(f_a(p)) + O\big(\Omega(m) \big).$$

Since the normal order of $\Omega(m)$ is $\log m$, we have for all but $o(q^x)$ monic polynomials $m \in A$ with $\deg m = x$,

$$\Omega(m) = (1 + o(1)) \log x = o\big((\log x)^{3/2} \big).$$

Define

$$g(m) = \sum_{p|m} \Omega(f_a(p)).$$

From the above discussion, to prove Theorem 6, it suffices to prove that the quantity

$$\frac{g(m) - \frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}}(\log x)^{3/2}}$$

distributes normally.

We need the following result of Zhang [20]: Let $h(m)$ be a real-valued strongly additive function on A. In other words, for $m_1, m_2 \in A$ with $(m_1, m_2) = 1$, $p \in A$ an irreducible polynomial, and $\alpha \geq 1$, we have

$$h(m_1 m_2) = h(m_1) + h(m_2) \qquad \text{and} \qquad h(p^\alpha) = h(p).$$

For $x \in \mathbb{N}$, define

$$A(x) = \sum_{\deg p \leq x} \frac{h(p)}{q^{\deg p}} \qquad \text{and} \qquad B(x) = \left(\sum_{\deg p \leq x} \frac{h^2(p)}{q^{\deg p}} \right) \geq 0.$$

If for each fixed $\epsilon > 0$,

$$\lim_{x \to \infty} \frac{1}{B^2(x)} \sum_{\substack{\deg p \leq x \\ |h(p)| \geq \epsilon B(x)}} \frac{h^2(p)}{q^{\deg p}} = 0, \tag{27}$$

then we have

$$\lim_{x \to \infty} \frac{1}{q^x} \# \left\{ \deg m = x \,\middle|\, m \text{ satisfies } \frac{h(m) - A(x)}{B(x)} \leq \gamma \right\} = G(\gamma).$$

Apply the result of Zhang to the strongly additive function $g(m)$. From Lemma 9, we have

$$A(x) = \frac{1}{2}(\log x)^2 + O(\log x) \qquad \text{and} \qquad B(x) = \frac{1}{\sqrt{3}}(\log x)^{3/2} + O(\log x).$$

Hence, to conclude that

$$\frac{g(m) - \frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}}(\log x)^{3/2}}$$

distributes normally, it remains to check that condition (27) holds for $g(p)$. Let

$$\alpha(p) = \begin{cases} 1 & \text{if } \Omega(f_a(p)) \geq \epsilon B(x), \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$\begin{aligned} \sum_{\substack{\deg p \leq x \\ |g(p)| \geq \epsilon B(x)}} \frac{g^2(p)}{q^{\deg p}} &= \sum_{\deg p \leq x} \alpha(p) \cdot \frac{\Omega^2(f_a(p))}{q^{\deg p}} \\ &\leq \left(\sum_{\deg p \leq x} \frac{\alpha(p)}{q^{\deg p}} \right)^{1/2} \left(\sum_{\deg p \leq x} \frac{\Omega^4(f_a(p))}{q^{\deg p}} \right)^{1/2}. \end{aligned}$$

Using (14) and (15), we have

$$\sum_{\deg p=x} \Big(\Omega(f_a(p)) - \log\deg p\Big)^2 \ll \pi(x)\log x.$$

As a direct consequence of the above inequality, we have

$$\sum_{\deg p=x} \alpha(p) = \#\Big\{ \deg p = x \,\Big|\, p \text{ satisfies } \Omega(f_a(p)) > \epsilon B(x)\Big\} \ll \frac{\pi(x)}{(\log x)^2}.$$

By a partial summation, we have

$$\sum_{\deg p\le x} \frac{\alpha(p)}{q^{\deg p}} \ll \sum_{n\le x} \frac{1}{q^n}\cdot\frac{\pi(n)}{(\log n)^2} \ll 1.$$

Also, using the same method as in the proof of (15), we can show that

$$\sum_{\deg p=x} \Omega^4(f_a(p)) \ll \pi(x)(\log x)^4.$$

By a partial summation, we have

$$\sum_{\deg p\le x} \frac{\Omega^4(f_a(p))}{q^{\deg p}} \ll \sum_{n\le x} \frac{1}{q^n}\cdot\pi(n)(\log n)^4 \ll (\log x)^5.$$

Combining the above estimates, we have

$$\sum_{\substack{\deg p\le x\\ |g(p)|\ge\epsilon B(x)}} \frac{g^2(p)}{q^{\deg p}} \ll (\log x)^{5/2} = o\big(B^2(x)\big).$$

Hence, the condition (27) is satisfied and we have

$$\lim_{x\to\infty}\frac{1}{q^x}\#\left\{ \deg m = x \,\Big|\, m \text{ satisfies } \frac{g(m)-\frac{1}{2}(\log x)^2}{\frac{1}{\sqrt{3}}(\log x)^{3/2}} \le \gamma\right\} = G(\gamma).$$

This completes the proof of the theorem. □

Acknowledgement

The authors wish to thank the referee for his/her valuable comments, and also for supplying us a simplified proof of Lemma 10.

References

[1] P. D. T. A. Elliott, *Probabilistic number theory*, Vols. I. & II., Springer-Verlag (1979). MR551361 (82h:10002a); MR560507 (82h:10002b)
[2] P. Erdős & M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. 62 (1940), 738-742. MR0002374 (2:42c)
[3] P. Erdős & C. Pomerance, *On the normal number of prime factors of $\varphi(n)$*, Rocky Mountain J. Math. 15 (1985), 343-352. MR823246 (87e:11112)
[4] D. Goss, *Basic structures of function field arithmetic*, Springer-Verlag (1996). MR1423131 (97i:11062)
[5] G. H. Hardy & S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), 76-92. MR2280878
[6] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77-91. MR0330106 (48:8444)
[7] C.-N. Hsu, *On Artin's conjecture for the Carlitz module*, Compositio Math. 106 (1997), 247-266. MR1457105 (98c:11053)

[8] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory 58 (1996), 267-287. MR1393616 (97e:11147)
[9] M. Ishibashi, *Effective version of the Tschebotareff density theorem in function fields over finite fields*, Bull. London Math. Soc. 24 (1992), 52-56. MR1139057 (92k:11135)
[10] J. Kubilius, *Probabilistic methods in the theory of numbers*, Transl. Math. Monogr. 11, Amer. Math. Soc., Providence, RI, 1964. MR160745 (28:3956)
[11] S. Li & C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. 556 (2003), 205-224. MR1971146 (2004c:11177)
[12] Y.-R. Liu, *The Erdős theorem and the Halberstam theorem in function fields*, Acta. Arith. 114 (2004), 323-330. MR2101821 (2005h:11218)
[13] Y.-R. Liu, *A prime analogue of the Erdős-Pomerance conjecture for elliptic curves*, Comment. Math. Helv. 80 (2005), 755–769. MR2182699 (2006f:11119)
[14] M. R. Murty & V. K. Murty, *An analogue of the Erdős-Kac theorem for Fourier coefficients of modular forms*, Indian J. Pure App. Math., 15 (1984), 1090-1101. MR765015 (86d:11039)
[15] M. R. Murty & F. Saidak, *Non-abelian generalizations of the Erdős-Kac theorem*, Canadian J. Math. 56 (2004), 356-372. MR2040920 (2005a:11114)
[16] M. R. Murty & S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. Vol. 30 (1987), 80-85. MR879875 (88e:11094)
[17] M. Rosen, *Number theory in function fields*, Graduate Texts in Math. 210, Springer (2002). MR1876657 (2003d:11171)
[18] H. Shapiro, *Distribution functions of additive arithmetic functions*, Proc. Nat. Acad. Sci. USA 42 (1956), 426-430. MR0079609 (18:113c)
[19] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), 274-276.
[20] W.-B. Zhang, *Probabilistic number theory in additive arithmetic semigroups*, In: Analytic Number Theory (B. C. Berndt et al. eds.) Prog. Math., Birkhäuser (1996), 839-884. MR1409397 (97h:11088)

Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
E-mail address: wtkuo@math.uwaterloo.ca

Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
E-mail address: yrliu@math.uwaterloo.ca