The Erdös Theorem and the Halberstam Theorem in Function Fields

Yu-Ru Liu *

September 24, 2023

1 Introduction.

For $n \in \mathbb{N}$, define $\omega(n)$ to be the number of distinct prime divisors of n. The Turán Theorem [9] is about the second moment of $\omega(n)$ and it implies a result of Hardy and Ramanujan [4] that the normal order of $\omega(n)$ is $\log\log n$. Further development of probabilistic ideas led Erdös and Kac [2] to prove a remarkable refinement of the Hardy-Ramanujan Theorem, namely, the existence of a normal distribution for $\omega(n)$. More precisely, they proved that for $x, \gamma \in \mathbb{R}$,

$$\lim_{x\to\infty} \frac{1}{\#\{n \le x\}} \#\Big\{n \le x, \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \le \gamma\Big\} = G(\gamma) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{\frac{-t^2}{2}} dt.$$

Instead of the sequence of all natural numbers, we consider only the set of primes now. Since $\omega(p) = 1$ for each prime p, the normal order of $\omega(p)$ is not $\log\log p$. However, Erdös [1] proved in 1935 that

$$\sum_{p\le x} \big(\omega(p-1) - \log\log x\big)^2 \ll \pi(x) \log\log x,$$

where $\pi(x) = \#\{p : \text{prime}\,,\, p \le x\}$. It implies that the normal order of $\omega(p-1)$ is $\log\log p$. In 1955, Halberstam [3] improved Erdös' result and proved that

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \#\Big\{p \le x, \frac{\omega(p-1) - \log\log p}{\sqrt{\log\log p}} \le \gamma\Big\} = G(\gamma).$$

This result can be viewed as a 'prime analogue' of the Erdös-Kac Theorem.

Let $\mathbb{F}_q[t]$ be a polynomial ring in one variable over a finite field $\mathbb{F}_q$. Let P be the set of monic irreducible polynomials of $\mathbb{F}_q[t]$. For an element $m \in \mathbb{F}_q[t]$, let $\deg m$ be the degree

*Research partially supported by an NSERC discovery grant..
2000 Mathematics Subjective Classification. 11N60, 11R09.

of the polynomial m. Also, let $\omega(m)$ denote the number of distinct monic irreducible polynomials dividing m, i.e.,

$$\omega(m) = \sum_{\substack{l \in P \\ l \mid m}} 1.$$

We can formulate analogues of the Erdös Theorem and the Halberstam Theorem in $\mathbb{F}_q[t]$.

Theorem 1 *Let P be the set of monic irreducible polynomials of $\mathbb{F}_q[t]$. Fix a non-zero polynomial $a \in \mathbb{F}_q[t]$. For $n \in \mathbb{N}$, we have*

$$\sum_{\substack{p \in P \\ \deg p \leq n}} \big(\omega(p-a) - \log n\big)^2 \ll \pi(n) \log n,$$

where $\pi(n) = \#\{p \in P, \deg p \leq n\}$.

As a direct consequence of Theorem 1, we have

Corollary 1 *Let $\{g_n\}$ be a sequence of real numbers such that $g_n \to \infty$ as $n \to \infty$. We have*

$$\#\left\{p \in P,\ \deg p \leq n,\ \left|\frac{\omega(p-a) - \log(\deg p)}{\sqrt{\log(\deg p)}}\right| > g_n\right\} = \mathrm{o}\big(\pi(n)\big).$$

In particular, given $\epsilon > 0$, we have

$$\#\Big\{\ p \in P,\ \deg p \leq n,\ \big|\omega(p-a) - \log(\deg p)\big| > \epsilon \log(\deg p)\Big\} = \mathrm{o}\big(\pi(n)\big).$$

Thus we conclude that the normal order of $\omega(p-a)$ is $\log(\deg p)$.

As we see from previous examples, Corollary 1 implies a possibility that the quantity

$$\frac{\omega(p-a) - \log(\deg p)}{\sqrt{\log(\deg p)}}$$

distributes normally. This is indeed the case.

Theorem 2 *Let P be the set of monic irreducible polynomials of $\mathbb{F}_q[t]$. Fix a non-zero polynomial $a \in \mathbb{F}_q[t]$. For $n \in \mathbb{N}$, $\gamma \in \mathbb{R}$, we have*

$$\lim_{n \to \infty} \frac{1}{\pi(n)} \#\left\{p \in P,\ \deg p \leq n,\ \frac{\omega(p-a) - \log(\deg p)}{\sqrt{\log(\deg p)}} \leq \gamma\right\} = G(\gamma).$$

2 Proof of Theorem 1.

We begin with two facts that are essential for the proof of Theorem 1. Let P be the set of monic irreducible polynomials in $\mathbb{F}_q[t]$. The following facts are about elements of P ; their proof can be found in [8].

Fact 1 ([8], p14) *For $d \in \mathbb{N}$, we have*

$$\#\Big\{p \in P, \deg p = d\Big\} = \frac{q^d}{d} + \mathrm{O}\big(\, q^{d/2}\,\big).$$

The next fact is about the arithmetic progression of irreducible polynomials in function fields. It is a theorem of Kornblum [5].

Fact 2 ([8], p40) *Let a, m be polynomials in $\mathbb{F}_q[t]$ that are relatively prime. For any $\epsilon > 0$ and $d \in \mathbb{N}$, we have*

$$\#\Big\{p \in P,\, \deg p = d,\, p \equiv a \pmod{m}\Big\} = \frac{1}{\phi(m)} \cdot \frac{q^d}{d} + \mathrm{O}\big(\, q^{d(1+\epsilon)/2}\,\big),$$

where $\phi(m)$ is the cardinality of $\big(\mathbb{F}_q[t]/m\mathbb{F}_q[t]\big)^*$.

Before proving Theorem 1, we consider its analogous version for monic irreducible polynomials of a fixed degree.

Lemma 1 *Let a be a fixed nonzero polynomial and p a monic irreducible polynomial in $\mathbb{F}_q[t]$. For $d \in \mathbb{N}$, we have*

$$\sum_{\deg p = d} \big(\omega(p-a) - \log d\big)^2 \ll \frac{q^d}{d} \log d.$$

Proof: Let δ be a constant with $0 < \delta < 1$ which will be chosen later. Let l be a monic irreducible polynomial. Notice that

$$\begin{aligned}\omega(p-a) &= \sum_{\substack{l|(p-a)\\ \deg l \le \delta d}} 1 + \sum_{\substack{l|(p-a)\\ \delta d < \deg l \le d}} 1\\ &= \omega_\delta(p-a) + \mathrm{O}\big(\,1/\delta\,\big),\end{aligned}$$

where

$$\omega_\delta(p-a) = \sum_{\substack{l|(p-a)\\ \deg l \le \delta d}} 1.$$

By Facts 1 and 2, we have

$$\begin{aligned}
\sum_{\deg p=d} \omega(p-a) &= \sum_{\deg p=d} \Big(\omega_\delta(p-a) + \mathrm{O}\big(1/\delta\big)\Big) \\
&= \sum_{\deg l \le \delta d} \sum_{\substack{\deg p=d \\ p\equiv a (\mathrm{mod}\, l)}} 1 + \mathrm{O}\big(\, q^d/d\,\big) \\
&= \sum_{\deg l \le \delta d} \left(\frac{1}{q^{\deg l}-1}\cdot\frac{q^d}{d} + \mathrm{O}\big(\, q^{d(1+\epsilon)/2}\,\big)\right) + \mathrm{O}\big(\, q^d/d\,\big).
\end{aligned}$$

By choosing $\delta < 1/2$, Fact 1 implies that

$$\begin{aligned}
\sum_{\deg p=d} \omega(p-a) &= \frac{q^d}{d} \sum_{\deg l \le \delta d} \frac{1}{q^{\deg l}} + \mathrm{O}\big(\, q^d/d\,\big) \\
&= \frac{q^d}{d} \sum_{k \le \delta d} \frac{1}{q^k}\Big(\frac{q^k}{k} + \mathrm{O}\big(\, q^{k/2}\,\big)\Big) + \mathrm{O}\big(\, q^d/d\,\big) \\
&= \frac{q^d}{d}\log d + \mathrm{O}\big(\, q^d/d\,\big).
\end{aligned}$$

Now, consider $\displaystyle\sum_{\deg p=d} \omega^2(p-a)$. Write

$$\begin{aligned}
\sum_{\deg p=d} \omega^2(p-a) &= \sum_{\deg p=d} \Big(\omega_\delta(p-a) + \mathrm{O}\big(\,1/\delta\,\big)\Big)^2 \\
&= \sum_{\deg p=d} \omega_\delta^2(p-a) + \mathrm{O}\big(\, q^d \log d/d\,\big).
\end{aligned}$$

We have

$$\begin{aligned}
\sum_{\deg p=d} \omega_\delta^2(p-a) &= \sum_{\substack{\deg l_1, \deg l_2 \le \delta d \\ l_1 \ne l_2}} \sum_{\substack{\deg p=d \\ p\equiv a (\mathrm{mod}\, l_1 l_2)}} 1 + \sum_{\deg l \le \delta d} \sum_{\substack{\deg p=d \\ p\equiv a (\mathrm{mod}\, l)}} 1 \\
&= \sum_{\deg l_1, \deg l_2 \le \delta d} \left(\frac{1}{\phi(l_1 l_2)}\cdot\frac{q^d}{d} + \mathrm{O}\big(q^{d(1+\epsilon)/2}\big)\right) \\
&\quad + \mathrm{O}\big(\, q^d \log d/d\,\big).
\end{aligned}$$

By choosing $0 < \delta < 1/4$, we have

$$\begin{aligned}
\sum_{\deg p=d} \omega^2(p-a) &= \frac{q^d}{d} \sum_{\deg l_1, \deg l_2 \le \delta d} \frac{1}{q^{\deg l_1}\cdot q^{\deg l_2}} + \mathrm{O}\big(\, q^d \log d/d\,\big) \\
&= \frac{q^d}{d}(\log d)^2 + \mathrm{O}\big(\, q^d \log d/d\,\big).
\end{aligned}$$

Combine all the above results. Choosing $\delta = 1/5$, we obtain that

$$\begin{aligned}
&\sum_{\deg p = d} (\omega(p-a) - \log d)^2 \\
&= \sum_{\deg p = d} \omega^2(p-a) - 2\log d \sum_{\deg p = d} \omega(p-a) + (\log d)^2 \sum_{\deg p = d} 1 \\
&\ll \frac{q^d \log d}{d}.
\end{aligned}$$

Thus Lemma 1 follows.

Now, we are ready to prove Theorem 1. It follows directly from Lemma 1.

Proof: By Lemma 1, we have

$$\begin{aligned}
&\sum_{\deg p \le n} \big(\omega(p-a) - \log n\big)^2 \\
&= \sum_{d \le n} \sum_{\deg p = d} \big(\omega(p-a) - \log d + \log d - \log n\big)^2 \\
&\ll \sum_{d \le n} \sum_{\deg p = d} \big(\omega(p-a) - \log d\big)^2 + \sum_{d \le n} \sum_{\deg p = d} \big(\log d - \log n\big)^2 \\
&\ll \sum_{d \le n} \frac{q^d}{d} \log d + \sum_{1 \le d \le n/2} \sum_{\deg p = d} (\log n)^2 + \sum_{n/2 < d \le n} \sum_{\deg p = d} \big(\log d - \log n\big)^2.
\end{aligned}$$

The third term of the last inequality is

$$\sum_{n/2 < d \le n} \sum_{\deg p = d} \big(\log d - \log n\big)^2 \ll (\log 2)^2 \sum_{n/2 < d \le n} \sum_{\deg p = d} 1 \ll \pi(n).$$

The second term can be estimated by

$$\sum_{1 \le d \le n/2} \sum_{\deg p = d} (\log n)^2 = (\log n)^2 \pi(n/2) \ll \pi(n).$$

The first term is the main term. It is bounded by

$$\sum_{d \le n} \frac{q^d}{d} \log d \ll \log n \sum_{d \le n} \#\big\{p \in P,\, \deg p = d\big\} \ll \pi(n) \log n.$$

Combining all the above estimates, we obtain

$$\sum_{\deg p \le n} \big(\omega(p-a) - \log n\big)^2 \ll \pi(n) \log n.$$

Hence, Theorem 1 follows. We obtain an analogue of the Erdös Theorem in $\mathbb{F}_q[t]$.

3 Proof of Theorem 2.

In this section, we shall prove that the quantity

$$\frac{\omega(p-a)-\log(\deg p)}{\sqrt{\log(\deg p)}}$$

distributes normally. This result follows from Theorem 1 in [6]. Instead of stating that theorem in its general form, we state below its application in $\mathbb{F}_q[t]$. Let P be the set of monic irreducible polynomials of $\mathbb{F}_q[t]$. For $m \in \mathbb{F}_q[t]$, define $N(m) := q^{\deg m}$. Take $X = \{q^z, z \in \mathbb{Z}\}$. Let S be a subset of infinitely many elements of $\mathbb{F}_q[t]$. For $x \in X$, define

$$S(x) = \big\{m \in S,\, N(m) \le x\big\}.$$

We assume that S satisfies the following condition:

$$\text{(C)} \quad |S(x^{1/2})| = \mathrm{o}\big(|S(x|\big), \text{ for all } x \in X.$$

Let f be a map from S to M. For each $l \in P$, we write

$$\frac{1}{|S(x)|}\,\#\big\{m \in S(x),\, l \mid f(m)\big\} = \lambda_l(x) + e_l(x),$$

where $\lambda_l = \lambda_l(x)$ can be thought of as a main term (and is usually chosen to be independent of x) and $e_l = e_l(x)$ is an error term. For any sequence of distinct elements $l_1, l_2, \cdots, l_u \in P$, we write

$$\frac{1}{|S(x)|}\,\#\Big\{m \in S(x),\, l_i | \, f(m) \text{ for all } i = 1 \cdots u\Big\} = \lambda_{l_1} \cdot \lambda_{l_2} \cdots \lambda_{l_u} + e_{l_1 l_2 \cdots l_u}(x).$$

We will use $e_{l_1 l_2 \cdots l_u}$ to abbreviate $e_{l_1 l_2 \cdots l_u}(x)$ below.

Suppose for all $x \in X$, there exist a constant β with $0 < \beta \le 1$ and $y = y(x) < x^\beta$ such that the following conditions hold:

(1) $\#\Big\{l \in P,\, N(l) > x^\beta,\, l \mid f(m)\Big\} = \mathrm{O}(1)$, for each $m \in S(x)$.

(2) $\displaystyle\sum_{y < N(l) \le x^\beta} \lambda_l = \mathrm{o}\big((\log\log x)^{1/2}\big)$.

(3) $\displaystyle\sum_{y < N(l) \le x^\beta} |e_l| = \mathrm{o}\big((\log\log x)^{1/2}\big)$.

(4) $\displaystyle\sum_{N(l) \le y} \lambda_l = \log\log x + \mathrm{o}\big((\log\log x)^{1/2}\big)$.

(5) $\displaystyle\sum_{N(l) \le y} \lambda_l^2 = \mathrm{o}\big((\log\log x)^{1/2}\big)$.

(6) For $r \in \mathbb{N}$, let $u = 1, 2, \cdots r$. We have

$$\sum\nolimits'' \left| e_{l_1 \cdots l_u} \right| = \mathrm{o}\big((\log\log x)^{-r/2} \big),$$

where $\sum''$ extends over all u-tuples $(l_1, l_2, \cdots, l_u)$ with $N(l_i) \leq y$ and l_i are all distinct.

It was proved in [6] that there is a generalization of the Erdös-Kac Theorem in $\mathbb{F}_q[t]$.

Theorem 3 (Theorem 1 in [6]) *Let P and X be defined as before. Let S be a subset of $\mathbb{F}_q[t]$ satisfying* Condition (C). *Let $f : S \to \mathbb{F}_q[t]$. Suppose there exist a constant β with $0 < \beta \leq 1$ and $y = y(x) < x^{\beta}$ such that* Conditions (1) *to* (6) *hold. Then for $\gamma \in \mathbb{R}$, we have*

$$\lim_{x \to \infty} \frac{1}{|S(x)|} \#\Big\{ m \in S(x),\ \frac{\omega(f(m)) - \log\log N(m)}{\sqrt{\log\log N(m)}} \leq \gamma \Big\} = G(\gamma).$$

Now, we are ready to prove Theorem 2. Let $S = P$ and $f : p \mapsto (p - a)$. By Fact 1, Condition (C) follows. Choose $y = x^{1/\log\log x}$ and β be any constant such that $0 < \beta < 1/2$. Since for $N(p) \leq x = q^n$ with x large (say $> N(a)$), we have

$$\#\big\{ l \in P,\ N(l) > x^{\beta},\ l \,|(p - a) \big\} \leq 1/\beta,$$

Condition (1) is satisfied. For a monic irreducible polynomial l, Fact 2 implies that

$$\#\big\{ p \in P,\ \deg p \leq n,\ p \equiv a \,(\mathrm{mod}\, l) \big\} = \frac{1}{\phi(l)} \cdot \pi(n) + \mathrm{O}\big(\pi(n)^{1/2+\epsilon} \big).$$

Take $\lambda_l = 1/\phi(l)$. Lemmas 1 and 2 in [7] state that

$$\sum_{N(l) \leq x} \frac{1}{N(l)} = \log\log x + \mathrm{O}(1)$$

and

$$\sum_{N(l) \leq x} \frac{1}{N(l)^2} \ll 1.$$

Thus Conditions (2) , (4), and (5) follow. Also, we have

$$\sum_{y < N(l) \leq x^{\beta}} |e_l| \ll \pi(n)^{-1/2+\epsilon} \cdot \pi(n)^{\beta} \ll 1,$$

since $\beta < 1/2$. Thus, Condition (3) follows. For distinct primes $l_1, l_2, \cdots, l_u$ with $N(l_i) \leq y$, by Fact 2, we have

$$|e_{l_1 l_2 \cdots l_u}| \ll \pi(n)^{-1/2+\epsilon}.$$

Since $y = \mathrm{o}(x^{\epsilon})$, Condition (6) is satisfied. Combining all the above results, Theorem 3 implies that

$$\lim_{n \to \infty} \frac{1}{\pi(n)} \#\Big\{ p \in P,\ \deg p \leq n,\ \frac{\omega(p - a) - \log(\deg p)}{\sqrt{\log(\deg p)}} \leq \gamma \Big\} = G(\gamma).$$

We obtain an analogue of the Halberstam Theorem in $\mathbb{F}_q[t]$.

Acknowledgement I would like to thank Prof. B Mazur and Prof. R Murty for their comments about this work.

References

[1] P. Erdös, *On the normal order of prime factors of* $(p-1)$ *and some related problems concerning Euler's* ϕ*-functions*, Quart. J. Math.(Oxford), 6 (1935), 205-213.

[2] P. Erdös & M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math., 62 (1940), 738-742.

[3] H. Halberstam, *On the distribution of additive number theoretic functions*, I., II., & III., J. London Math. Soc., 30 (1955), 43-53; 31 (1956), 1-14, 15-27.

[4] G.H. Hardy & S. Ramanujan, *The normal number of prime factors of a number* n, Quar. J. Pure. Appl. Math., 48 (1917), 76-97.

[5] H. Kornblum, *Über die primfunktionen in einer arithmetischen progression,* Math. Z. 5 (1919), 100-111.

[6] Y.-R. Liu, *A generalization of the Erdös-Kac Theorem and its applications* II, submitted.

[7] Y.-R. Liu, *A generalization of the Turán Theorem and its applications*, to appear in Canadian Mathematical Bulletin.

[8] M. Rosen, *Number theory in function fields*, Springer Verlag (2002).

[9] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), 274-276.

Departments of Mathematics, Harvard University, Cambridge, MA, USA 02138
Email: yrliu@math.harvard.edu