Hindawi
Journal of Mathematics
Volume 2021, Article ID 3619347, 6 pages
https://doi.org/10.1155/2021/3619347

Research Article

On the Degree of the GCD of Random Polynomials over a Finite Field

Kui Liu and Meijie Lu

School of Mathematics and Statistics, Qingdao University, 308 Ningxia Road, Shinan District, Qingdao 266000, Shandong, China

Correspondence should be addressed to Meijie Lu; meijie.lu@hotmail.com

Received 28 May 2021; Accepted 17 August 2021; Published 9 September 2021

Academic Editor: Efthymios G. Tsionas

In this paper, we focus on the degree of the greatest common divisor (gcd) of random polynomials over $\mathbb{F}_q$. Here, $\mathbb{F}_q$ is the finite field with q elements. Firstly, we compute the probability distribution of the degree of the gcd of random and monic polynomials with fixed degree over $\mathbb{F}_q$. Then, we consider the waiting time of the sequence of the degree of gcd functions. We compute its probability distribution, expectation, and variance. Finally, by considering the degree of a certain type gcd, we investigate the probability distribution of the number of rational (i.e., in $\mathbb{F}_q$) roots (counted with multiplicity) of random and monic polynomials with fixed degree over $\mathbb{F}_q$.

1. Introduction

1.1. Background. The greatest common divisor (gcd) function is very basic in number theory. It has also been considered in the view of probability theory. For an integer $n \geq 2$, suppose the random variables $X_1, \ldots, X_m, \ldots$ are independent and uniformly distributed on $\{1, 2, \ldots, n\}$. In 1880s, Cesàro [1, 2] first considered the probability distribution of the gcd of random integers and showed that

$$\lim_{n\longrightarrow\infty}\mathbb{P}\left(\gcd\left(X_1, \ldots, X_r\right) = l\right) = \frac{1}{\zeta(r)}\frac{1}{l^r}, \tag{1}$$

for $r \geq 2$ and $1 \leq l \leq n$, where ζ is the Riemann zeta function. Diaconis and Erdös [3] gave a more precise asymptotic formula for the case $r = 2$, which is

$$\mathbb{P}\left(\gcd\left(X_1, X_2\right) = l\right) = \frac{1}{\zeta(2)}\frac{1}{l^2} + O\left(\frac{\log(n/l)}{nl}\right), \tag{2}$$

for $1 \leq l \leq n$ as $n \longrightarrow \infty$. One may refer to [4–7], for more related works. In 2013, Fernández and Fernández [8] considered the waiting time for the gcd sequence:

$$G_1 = X_1, G_2 = \gcd\left(X_1, X_2\right), \ldots, G_m = \gcd\left(X_1, \ldots, X_m\right), \ldots. \tag{3}$$

Let $T^{(n)}$ be the subscript at which the sequence $\{G_m\}_{m\in\mathbb{N}}$ reaches the value 1 for the first time. They computed the expectation of $T^{(n)}$ and showed that

$$\lim_{n\longrightarrow\infty}\mathbb{E}\left(T^{(n)}\right) = 2 + \sum_{m=2}^{\infty}\left(1 - \frac{1}{\zeta(m)}\right) \approx 2.7052. \tag{4}$$

Besides random integers, it is also natural to study random polynomials. One interesting topic in this area is to understand the behavior of the number of certain type of roots of random polynomials. For example, Kac [9] considered the number of real roots of random polynomials over the real number field $\mathbb{R}$. One may refer to [10] for a recent progress.

In this paper, we focus on the degree of the gcd of random polynomials over the finite field $\mathbb{F}_q$, where $q \geq 2$ is a prime power.

1.2. Our Results. In the polynomial ring $\mathbb{F}_q[T]$, we use $\mathscr{M}$ and $\mathscr{M}_n$ to denote the sets of all monic polynomials and monic polynomials with degree $n \geq 0$, respectively. We also use $\deg(f)$ to denote the degree of a polynomial f.

For integers $n \geq 1$ and $r \geq 2$, we define

$$X(n,q,r) \coloneqq \deg\left(\gcd\left(f_1, f_2, \ldots, f_r\right)\right), \tag{5}$$

where f_i, $1 \le i \le r$, are independent and uniformly distributed on $\mathscr{M}_n$. We derive the following probability distribution of $X(n,q,r)$.

Theorem 1. *For any integers $n \ge 1$ and $r \ge 2$, the mass function of $X = X(n,q,r)$ is*

$$\mathbb{P}(X = l) = \frac{A_{n,q,r}(l)}{q^{(r-1)l}}, \quad l = 0, 1, \ldots, n, \tag{6}$$

where

$$A_{n,q,r}(l) = \begin{cases} 1 - \dfrac{1}{q^{r-1}}, & 0 \le l \le n-1, \\ 1, & l = n. \end{cases} \tag{7}$$

With the help of Theorem 1, we investigate the waiting time of the sequence:

$$\begin{aligned} G_1^{(n,q)} &= \deg\left(f_1\right), G_2^{(n,q)} = \deg\left(\gcd\left(f_1, f_2\right)\right), \ldots, G_m^{(n,q)} \\ &= \deg\left(\gcd\left(f_1, \ldots, f_m\right)\right), \ldots, \end{aligned} \tag{8}$$

where $f_1, f_2, \ldots$ are independent and uniformly distributed on $\mathscr{M}_n$, $n \ge 1$. Observe that this sequence is decreasing.

For an integer $0 \le s < n$, define the random variable $T_s^{(n,q)}$ to be the subscript at which the sequence $\left\{G_m^{(n,q)}\right\}_{m \in \mathbb{N}}$ reaches a value not exceeding s for the first time. We compute the probability distribution of $T_s^{(n,q)}$ and then derive its expectation $\mathbb{E}(T_s^{(n,q)})$ and variance $\mathbb{V}(T_s^{(n,q)})$.

Theorem 2. *Suppose integer $n \ge 1$; then, for integers $0 \le s < n$ and $m \ge 2$, the mass function of $T_s^{(n,q)}$ is*

$$\mathbb{P}\left(T_s^{(n,q)} = m\right) = \frac{1}{q^{(m-2)(s+1)}}\left(1 - \frac{1}{q^{s+1}}\right), \tag{9}$$

and furthermore, we have

$$\mathbb{E}\left(T_s^{(n,q)}\right) = \frac{2q^{s+1} - 1}{q^{s+1} - 1}, \quad \text{and } \mathbb{V}\left(T_s^{(n,q)}\right) = \frac{q^{s+1}}{\left(q^{s+1} - 1\right)^2}. \tag{10}$$

It is a little bit surprising that the expectation and variance of $T_s^{(n,q)}$ are independent of the degree n. Using SageMath, we verify this for $s = 0, 1$ and some (n,q) by doing numerical experiments with 10^6 times. The results are listed in Table 1 (expectation) and Table 2 (variance).

Enlightened by the proof of Theorem 1, we use the degree of gcd to study the number of rational roots (counted with multiplicity) of a random polynomial $f \in \mathbb{F}_q[T]$, where f is uniformly distributed on $\mathscr{M}_n, n \ge 1$. Denote this number by $N(n,q)$; then, we have the following result.

Theorem 3. *For an integer $n \ge 1$, the mass function of $N = N(n,q)$ is*

$$\mathbb{P}(N = l) = \binom{l+q-1}{q-1}\frac{1}{q^l}\sum_{0 \le i \le \min\{n-l, q\}}\binom{q}{i}\left(-\frac{1}{q}\right)^i, \tag{11}$$

for $0 \le l \le n$.

The method for proving Theorem 3 is also valid if we consider the number of distinct rational roots of a random polynomial $f \in \mathscr{M}_n$. This number is investigated by Leont'ev in [11], where combinational methods are used. Comparatively, our method has more flavor of number theory, and we hope it can be used for other roots' counting problems.

Notations: we use $\mathbb{P}(A)$ to denote the probability of an event A and use $\mathbb{E}(X)$ and $\mathbb{V}(X)$ to denote the expectation and variance of a random variable X. We also use $\mathbb{F}_q$ to denote the finite field with q elements and use $\mathbb{F}_q[T]$ to denote the polynomial ring over $\mathbb{F}_q$.

2. Preliminaries

The Mö bius function for monic polynomials is defined by $\mu(f) = (-1)^r$ if f is a product of r distinct monic irreducible polynomials and $\mu(f) = 0$ if f is not square free. For any $f \in \mathscr{M}$, we have

$$\sum_{\substack{d \in \mathscr{M} \\ d \mid f}} \mu(d) = \begin{cases} 1, & f = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

For the mean value of $\mu(f)$ over $\mathscr{M}_n$, it is well known that

$$\sum_{f \in \mathscr{M}_n} \mu(f) = \begin{cases} 1, & n = 0, \\ -q, & n = 1, \\ 0, & n \ge 2. \end{cases} \tag{13}$$

For a polynomial f in $\mathbb{F}_q[T]$, we defined its norm by $\|f\| \coloneqq q^{\deg(f)}$. We derive the following two results, which are needed in proving Proposition 1.

Lemma 1. *For integers $r, k \ge 1$, we have*

$$\begin{aligned} \sum_{\substack{h \in \mathscr{M} \\ 0 \le \deg(h) \le n}} \frac{\deg^k(h)}{\|h\|^r} &= \sum_{0 \le l \le n} \frac{l^k}{q^{(r-1)l}}, \quad \text{for } n \ge 0, \\ \sum_{\substack{d \in \mathscr{M} \\ 0 \le \deg(d) \le n}} \frac{\mu(d)}{\|d\|^r} &= 1 - \frac{1}{q^{r-1}}, \quad \text{for } n \ge 1. \end{aligned} \tag{14}$$

Table 1: Numerical results for the expectation $\mathbb{E}(T_s^{(n,q)})$.

n	$(q,s)=(2,0)$	$(q,s)=(3,0)$	$(q,s)=(4,1)$	$(q,s)=(5,1)$
1	3.000922	2.500092	NA.	NA.
2	3.002260	2.500115	2.066650	2.041783
3	2.998854	2.500166	2.066424	2.041758
4	2.998771	2.499346	2.066466	2.041767
5	2.999041	2.500160	2.066895	2.041485
⋮	⋮	⋮	⋮	⋮
Theoretical	3.000000	2.500000	2.066666	2.041666

Table 2: Numerical results for the variance $\mathbb{V}(T_s^{(n,q)})$.

n	$(q,s)=(2,0)$	$(q,s)=(3,0)$	$(q,s)=(4,1)$	$(q,s)=(5,1)$
1	2.006609	0.748455	NA.	NA.
2	2.013104	0.748523	0.071244	0.043498
3	1.992205	0.747423	0.070657	0.043345
4	1.988979	0.747273	0.070883	0.043402
5	1.997586	0.749603	0.071586	0.043045
⋮	⋮	⋮	⋮	⋮
Theoretical	2.000000	0.750000	0.071111	0.043402

Proof. Note that

$$\sum_{\substack{h\in\mathcal{M}\\ 0\le\deg(h)\le n}}\frac{\deg^k(h)}{\|h\|^r}=\sum_{\substack{h\in\mathcal{M}\\ 0\le\deg(h)\le n}}\frac{\deg^k(h)}{q^{r\deg(h)}}=\sum_{0\le l\le n}\frac{l^k}{q^{rl}}\sum_{h\in\mathcal{M}_l}1. \tag{15}$$

Then, the first statement follows by noting

$$\sum_{h\in\mathcal{M}_l}1=q^l. \tag{16}$$

For the second statement, we have

$$\sum_{\substack{d\in\mathcal{M}\\ 0\le\deg(d)\le n}}\frac{\mu(d)}{\|d\|^r}=\sum_{\substack{d\in\mathcal{M}\\ 0\le\deg(d)\le n}}\frac{\mu(d)}{q^{r\deg(d)}}=\sum_{0\le l\le n}\frac{1}{q^{rl}}\sum_{d\in\mathcal{M}_l}\mu(d). \tag{17}$$

This together with (13) gives our desired result. □

The following lemma is used in the proof of Proposition 2.

Lemma 2. *For integer $n\ge 1$, suppose $Q=Q_{n,q}(T):=\prod_{\alpha\in\mathbb{F}_q}(T-\alpha)^n$ and $h\in\mathcal{M}$ with $h|Q$ and $0\le \deg(h)\le n-1$. Then, we have*

$$\sum_{\substack{d\in\mathcal{M},d|Q/h\\ 0\le\deg(d)\le n-\deg(h)}}\frac{\mu(d)}{\|d\|}=\sum_{0\le i\le\min\{n-\deg(h),q\}}\binom{q}{i}\left(-\frac{1}{q}\right)^i. \tag{18}$$

Proof. Note that

$$\sum_{\substack{d\in\mathcal{M},d|Q/h\\ 0\le\deg(d)\le n-\deg(h)}}\frac{\mu(d)}{\|d\|}=1+\sum_{\substack{d\in\mathcal{M},d|Q/h\\ 1\le\deg(d)\le n-\deg(h)}}\frac{\mu(d)}{q^{\deg(d)}}. \tag{19}$$

Let $\deg(d)=i$; then, by the definition of $\mu(d)$ and Q, we have that d is of the form

$$d=\prod_{j=1}^{i}(T-\alpha_j),\quad 1\le i\le\min\{n-\deg(h),q\}, \tag{20}$$

for some distinct $\alpha_j\in\mathbb{F}_q$, $1\le j\le i$. From this, we derive that

$$\sum_{\substack{d\in\mathcal{M},d|Q/h\\ 1\le\deg(d)\le n-\deg(h)}}\frac{\mu(d)}{q^{\deg(d)}}=\sum_{1\le i\le\min\{n-\deg(h),q\}}\left(-\frac{1}{q}\right)^i\sum_{\substack{d\text{ satisfies (20)}\\ d|Q/h}}1. \tag{21}$$

Note that $\deg(h)\le n-1$; then, we have

$$\sum_{\substack{d\text{ satisfies (20)}\\ d|Q/h}}1=\binom{q}{i}. \tag{22}$$

Then, our required result follows by combining (21) and (22) with (19). □

3. Proof of Theorem 1

We first compute the kth power moments of $X=X(n,q,r)$.

Proposition 1. *For any integers $n,k\ge 1$ and $r\ge 2$, we have*

$$\mathbb{E}\left(X^k(n,q,r)\right) = \sum_{0\le l\le n} \frac{A_{n,q,r}(l)l^k}{q^{(r-1)l}}, \tag{23}$$

where $A_{n,q,r}(l)$ is given by (7).

Proof. By the definition of the kth moment, we have

$$\mathbb{E}\left(X^k\right) = \frac{1}{q^{rn}} \sum_{f_i\in\mathcal{M}_n, 1\le i\le r} \deg^k\left(\gcd\left(f_1,\ldots,f_r\right)\right). \tag{24}$$

It follows that

$$\mathbb{E}\left(X^k\right) = \frac{1}{q^{rn}} \sum_{\substack{h\in\mathcal{M}\\ 0\le \deg(h)\le n}} \deg^k(h) \sum_{\substack{f_i\in\mathcal{M}_n, 1\le i\le r\\ \gcd\left(f_1,\ldots,f_r\right)=h}} 1. \tag{25}$$

Then, for the inner sum on the right-hand side of (25), we can write

$$\sum_{\substack{f_i\in\mathcal{M}_n, 1\le i\le r\\ \gcd\left(f_1,\ldots,f_r\right)=h}} 1 = \sum_{\substack{f_i\in\mathcal{M}_n, h\mid f_i\\ 1\le i\le r}} \sum_{d\mid \gcd\left(f_1/h,\ldots,f_r/h\right)} \mu(d), \tag{26}$$

where we have used (12). Changing the order of the summations, we obtain

$$\sum_{\substack{f_i\in\mathcal{M}_n, 1\le i\le r\\ \gcd\left(f_1,\ldots,f_r\right)=h}} 1 = \sum_{\substack{d\in\mathcal{M}\\ 0\le \deg(d)\le n-\deg(h)}} \mu(d)\left(\sum_{\substack{f\in\mathcal{M}_n\\ dh\mid f}} 1\right)^r = \sum_{\substack{d\in\mathcal{M}\\ 0\le \deg(d)\le n-\deg(h)}} \mu(d)q^{r(n-\deg(dh))}. \tag{27}$$

It follows that

$$\sum_{\substack{f_i\in\mathcal{M}_n, 1\le i\le r\\ \gcd\left(f_1,\ldots,f_r\right)=h}} 1 = \frac{q^{rn}}{\|h\|^r} \sum_{\substack{d\in\mathcal{M}\\ 0\le \deg(d)\le n-\deg(h)}} \frac{\mu(d)}{\|d\|^r}. \tag{28}$$

Inserting (28) to (25) gives

$$\mathbb{E}\left(X^k\right) = \sum_{\substack{h\in\mathcal{M}\\ 0\le \deg(h)\le n}} \frac{\deg^k(h)}{\|h\|^r} \sum_{\substack{d\in\mathcal{M}\\ 0\le \deg(d)\le n-\deg(h)}} \frac{\mu(d)}{\|d\|^r}. \tag{29}$$

The contribution of those h with $\deg(h) = n$ is equal to

$$\sum_{h\in\mathcal{M}_n} \frac{\deg^k(h)}{\|h\|^r} = \frac{n^k}{q^{rn}} \sum_{h\in\mathcal{M}_n} 1 = \frac{n^k}{q^{(r-1)n}}. \tag{30}$$

By Lemma 1, the contribution of those h with $0\le \deg(h)\le n-1$ is equal to

$$\left(1-\frac{1}{q^{r-1}}\right) \sum_{0\le l\le n-1} \frac{l^k}{q^{(r-1)l}}. \tag{31}$$

Hence, we have

$$\mathbb{E}\left(X^k\right) = \frac{n^k}{q^{(r-1)n}} + \left(1-\frac{1}{q^{r-1}}\right) \sum_{0\le l\le n-1} \frac{l^k}{q^{(r-1)l}}, \tag{32}$$

which is our desired result. □

Now, we are ready to prove Theorem 1. Suppose $M_X(t) := \mathbb{E}(e^{tX})$ is the moment generating function of X; then, we have

$$M_X(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!} \mathbb{E}\left(X^k\right). \tag{33}$$

It follows from Proposition 1 that

$$M_X(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!} \left(\sum_{0\le l\le n} \frac{A_{n,q,r}(l)l^k}{q^{(r-1)l}}\right) = \sum_{0\le l\le n} \frac{A_{n,q,r}(l)}{q^{(r-1)l}} e^{lt}. \tag{34}$$

Then, our desired result follows from the relationship between the moment generating function and the generating function of X.

4. Proof of Theorem 2

For an integer $0\le s<n$, note that the event $\left\{G_m^{(n,q)}\le s\right\} = \left\{X(n,q,m)\le s\right\}$ coincides with the event $\left\{T_s^{(n,q)}\le m\right\}$ for each $m\ge 2$. Hence, by Theorem 1, we have

$$\mathbb{P}\left(T_s^{(n,q)}\le m\right) = \sum_{0\le l\le s} \mathbb{P}(X(n,q,m)=l) = 1-\frac{1}{q^{(m-1)(s+1)}}. \tag{35}$$

This gives the mass function in Theorem 2.

By the definition of the expectation of $T_s^{(n,q)}$, we have

$$\mathbb{E}\left(T_s^{(n,q)}\right) = \sum_{m=2}^{\infty} m\mathbb{P}\left(T_s^{(n,q)}=m\right) = 2\mathbb{P}\left(T_s^{(n,q)}>1\right) + \sum_{m=2}^{\infty} \mathbb{P}\left(T_s^{(n,q)}>m\right). \tag{36}$$

It follows from (35) that

$$\mathbb{E}\left(T_s^{(n,q)}\right) = 2 + \sum_{m=2}^{\infty} \frac{1}{q^{(m-1)(s+1)}} = \frac{2q^{s+1}-1}{q^{s+1}-1}. \tag{37}$$

To deal with $\mathbb{V}(T_s^{(n,q)})$, we write

$$\mathbb{V}\left(T_s^{(n,q)}\right) = \mathbb{E}\left(\left(T_s^{(n,q)}\right)^2\right) - \left(\mathbb{E}\left(T_s^{(n,q)}\right)\right)^2. \tag{38}$$

For $\mathbb{E}((T_s^{(n,q)})^2)$, we have

$$\mathbb{E}\left(\left(T_s^{(n,q)}\right)^2\right) = \sum_{m=2}^{\infty} m^2 \mathbb{P}\left(T_s^{(n,q)} = m\right) = 4\mathbb{P}\left(T_s^{(n,q)} > 1\right) + \sum_{m=2}^{\infty} (2m+1)\mathbb{P}\left(T_s^{(n,q)} > m\right). \tag{39}$$

It follows from (35) again that

$$\mathbb{E}\left(\left(T_s^{(n,q)}\right)^2\right) = 4 + 2\sum_{m=2}^{\infty} \frac{m}{q^{(m-1)(s+1)}} + \sum_{m=2}^{\infty} \frac{1}{q^{(m-1)(s+1)}} = \frac{4q^{2(s+1)} - 3q^{s+1} + 1}{\left(q^{s+1}-1\right)^2}, \tag{40}$$

where we have used

$$\sum_{m=2}^{\infty} \frac{m}{q^{(m-1)(s+1)}} = \frac{2q^{s+1}-1}{\left(q^{s+1}-1\right)^2}. \tag{41}$$

Inserting (37) and (40) into (38) yields our desired result.

5. Proof of Theorem 3

We first compute the kth power moments of $N = N(n,q)$.

Proposition 2. *For any integers $n, k \geq 1$, we have*

$$\mathbb{E}\left(N^k(n,q)\right) = \sum_{0 \leq l \leq n} \binom{l+q-1}{q-1} \frac{l^k}{q^l} \sum_{0 \leq i \leq \min\{n-l,q\}} \binom{q}{i} \left(-\frac{1}{q}\right)^i. \tag{42}$$

Proof. Proof. Let $Q = Q_{n,q}(T) := \prod_{\alpha \in \mathbb{F}_q} (T-\alpha)^n$. Notice that

$$N(n,q) = \deg(\gcd(f,Q)), \tag{43}$$

where f is random and uniformly distributed on $\mathcal{M}_n$. Then, by the definition of the kth moment, we have

$$\mathbb{E}\left(N^k\right) = \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \deg^k(\gcd(f,Q)). \tag{44}$$

It follows that

$$\mathbb{E}\left(N^k\right) = \frac{1}{q^n} \sum_{\substack{h \in \mathcal{M}, h|Q \\ 0 \leq \deg(h) \leq n}} \deg^k(h) \sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=h}} 1. \tag{45}$$

For the inner sum on the right-hand side of (45), we have

$$\sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=h}} 1 = \sum_{\substack{f \in \mathcal{M}_n \\ h|f}} \sum_{\substack{d \in \mathcal{M} \\ d \mid \gcd(f/h, Q/h)}} \mu(d), \tag{46}$$

where we have used (12). Changing the order of the summations, we derive

$$\sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=h}} 1 = \sum_{\substack{d \in \mathcal{M}, d|Q/h \\ 0 \leq \deg(d) \leq n - \deg(h)}} \mu(d) \sum_{\substack{f \in \mathcal{M}_n \\ dh|f}} 1 = \sum_{\substack{d \in \mathcal{M}, d|Q/h \\ 0 \leq \deg(d) \leq n - \deg(h)}} \mu(d) q^{n - \deg(dh)}. \tag{47}$$

By (45) and (47), we obtain

$$\mathbb{E}\left(N^k\right) = \sum_{\substack{h \in \mathcal{M}, h|Q \\ 0 \leq \deg(h) \leq n}} \frac{\deg^k(h)}{\|h\|} \sum_{\substack{d \in \mathcal{M}, d|Q/h \\ 0 \leq \deg(d) \leq n - \deg(h)}} \frac{\mu(d)}{\|d\|}. \tag{48}$$

Breaking the above sum into two sums according to $\deg(h) = n$ or not, we have

$$\mathbb{E}\left(N^k\right) = \sum_1 + \sum_2, \tag{49}$$

where

$$\begin{aligned} \sum_1 &= \frac{n^k}{q^n} \sum_{\substack{h \in \mathcal{M}_n \\ h|Q}} 1, \\ \sum_2 &= \sum_{\substack{h \in \mathcal{M}, h|Q \\ 0 \leq \deg(h) \leq n-1}} \frac{\deg^k(h)}{\|h\|} \sum_{\substack{d \in \mathcal{M}, d|Q/h \\ 0 \leq \deg(d) \leq n - \deg(h)}} \frac{\mu(d)}{\|d\|}. \end{aligned} \tag{50}$$

To deal with $\sum_1$, note that $h|Q$ and $\deg(h) = n$; then, h is of the form

$$h = \prod_{j=1}^{q} \left(T - \alpha_j\right)^{r_j}, \tag{51}$$

for distinct $\alpha_j \in \mathbb{F}_q$, $1 \le j \le q$, where $0 \le r_j \le n$ and $r_1 + \cdots + r_q = n$. Thus, we have

$$\sum_1 = \frac{n^k}{q^n} \sum_{\substack{0 \le r_j \le n, 1 \le j \le q \\ r_1 + \cdots + r_q = n}} 1 = \binom{n+q-1}{q-1} \frac{n^k}{q^n}. \tag{52}$$

For $\sum_2$, using Lemma 2, we derive

$$\sum_2 = \sum_{\substack{h \in \mathcal{M}, h|Q \\ 0 \le \deg(h) \le n-1}} \frac{\deg^k(h)}{\|h\|} \sum_{0 \le i \le \min\{n - \deg(h), q\}} \binom{q}{i} \left(-\frac{1}{q}\right)^i. \tag{53}$$

Let $\deg(h) = l$; then, we have

$$\sum_2 = \sum_{0 \le l \le n-1} \frac{l^k}{q^l} \sum_{0 \le i \le \min\{n-l, q\}} \binom{q}{i} \left(-\frac{1}{q}\right)^i \sum_{\substack{h \in \mathcal{M}_l \\ h|Q}} 1$$

$$= \sum_{0 \le l \le n-1} \binom{l+q-1}{q-1} \frac{l^k}{q^l} \sum_{0 \le i \le \min\{n-l, q\}} \binom{q}{i} \left(-\frac{1}{q}\right)^i. \tag{54}$$

Plugging (52) and (54) into (49) yields our required result. □

Now, we are ready to prove Theorem 3. Suppose $M_N(t) := \mathbb{E}(e^{tN})$ is the moment generating function of N; then, we have

$$M_N(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!} \mathbb{E}\left(N^k\right). \tag{55}$$

By Proposition 2, we derive

$$M_N(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!} \left(\sum_{0 \le l \le n} \binom{l+q-1}{q-1} \frac{l^k}{q^l} \sum_{0 \le i \le \min\{n-l, q\}} \binom{q}{i} \left(-\frac{1}{q}\right)^i \right), \tag{56}$$

which gives

$$M_N(t) = \sum_{0 \le l \le n} \binom{l+q-1}{q-1} \frac{1}{q^l} \sum_{0 \le i \le \min\{n-l, q\}} \binom{q}{i} \left(-\frac{1}{q}\right)^i e^{tl}. \tag{57}$$

Then, our desired result follows from the relationship between the moment generating function and the generating function of N.

Data Availability

The date in the chart in our paper can be verifies by using SageMath.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The first listed author was partially supported by National Natural Science Foundation of China (NSFC, Grant no. 12071238) and Shandong Provincial Natural Science Foundation, China (Grant no. ZR2019BA028). The second listed author was partially supported by National Natural Science Foundation of China (NSFC, Grant no. 12071238).

References

[1] E. Cesàro, "Probabilite de certains faits arithméthiques," *Mathesis*, vol. 4, pp. 150-151, 1884.

[2] E. Cesàro, "Sur le plus grand commun diviseur de plusieurs nombres," *Annali Di Matematica Pura Ed Applicata*, vol. 13, no. 1, pp. 291–294, 1885.

[3] P. Diaconis and P. Erdös, "On the distribution of the greatest common divisor," Technical Report No. 12, Department of Statistics, Stanford University, Stanford, CL, USA, 1977.

[4] E. Cohen, "Arithmetical functions of greatest common divisor. I," *Proceedings of the American Mathematical Society*, vol. 11, no. 2, p. 164, 1960.

[5] J. L. Fernández and P. Fernández, "Divisibility properties of random samples of integers," *Revista de la Real Academia de Ciencias Exactas Fisicas y Naturales Serie A-Matematicas*, vol. 115, no. 26, 2021.

[6] T. Hilberdink and L. Tóth, "On the average value of the least common multiple of k positive integers," *Journal of Number Theory*, vol. 169, pp. 327–341, 2016.

[7] J. E. Nymann, "On the probability that k positive integers are relatively prime," *Journal of Number Theory*, vol. 4, no. 5, pp. 469–473, 1972.

[8] J. L. Fernández and P. Fernández, "On the probability distribution of the gcd and lcm of r-tuples of integers," 2013, https://arxiv.org/abs/1305.0536.

[9] M. Kac, "On the average number of real roots of a random algebraic equation," *Bulletin of the American Mathematical Society*, vol. 49, no. 4, pp. 314–321, 1943.

[10] O. Nguyen and V. Vu, "Random polynomials: central limit theorems for the real roots," 2019, https://arxiv.org/abs/1904.04347.

[11] V. K. Leont'ev, "Roots of random polynomials over a finite field," *Mathematical Notes*, vol. 80, no. 2, pp. 300–304, 2006.