Miskolc Mathematical Notes
Vol. 15 (2014), No 2, pp. 481-488

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2014.1075

Natural density of relative coprime polynomials in $\mathbb{F}_q[x]$

Xiangqian Guo, Fengdan Hou, and Xuewen Liu

Miskolc Mathematical Notes
Vol. 15 (2014), No. 2, pp. 481–488

HU e-ISSN 1787-2413

NATURAL DENSITY OF RELATIVE COPRIME POLYNOMIALS IN $\mathbb{F}_q[x]$

XIANGQIAN GUO, FENGDAN HOU, AND XUEWEN LIU

Received 06 December, 2013

Abstract. Let $\mathbb{F}_q[x]$ be the polynomial ring over the finite field $\mathbb{F}_q$ containing q elements. We compute the probability that n polynomials in $\mathbb{F}_q[x]$ are k-wise relatively coprime, using the concept of natural density. As a special case, we get the probability that n polynomials in $\mathbb{F}_q[x]$ are pairwise coprime.

2010 *Mathematics Subject Classification:* 11B05; 11T06; 11C08; 60B15.

Keywords: natural density, k-wise relatively coprime, irreducible polynomial, q-zeta function

1. INTRODUCTION AND MAIN RESULTS

Let $\mathbb{N}$ be the set of all positive integers. Dirichlet [2] first discovered an interesting result that relates the probability that two randomly chosen integers are relative prime to the Riemann's zeta function, and the probability turns out to be

$$\lim_{N\to\infty} \frac{|\{(m,n) \in \mathbb{N}^2 \mid 1 \le m,n \le N, \gcd(m,n) = 1\}|}{N^2} = \zeta^{-1}(2) = \frac{6}{\pi^2},$$

where $\gcd(m,n)$ denotes the greatest common divisor of m and n, and $\zeta(s)$ is the Riemann's zeta function. This result was generalized to the case of several integers, that is, the probability of n randomly chosen integers to be coprime is given by

$$\lim_{N\to\infty} \frac{|\{(m_1,\dots,m_n) \in \mathbb{N}^n \mid 1 \le m_1,\dots,m_n \le N, \gcd(m_1,\dots,m_n) = 1\}|}{N^n} = \zeta^{-1}(n). \tag{1.1}$$

In [7], Kubota and Sugita gave a rigorous probabilistic interpretation to Dirichlet's theorem. Other probability problems over integers were also considered: L. Tóth [12] obtained that the probability of n positive integers to be pairwise coprime is $\prod_p (1-\frac{1}{p})^{n-1}(1+\frac{n-1}{p})$, where p is a prime number; Hu [4] showed that the probability of n positive integers to be k-wise relatively prime is $\prod_p (\sum_{m=0}^{k-1} \binom{n}{m} (\frac{1}{p})^m (1-\frac{1}{p})^{n-m})$. For deeper links between probability theory and number theory, please refer to Tenenbaum [11], Kubilius [6] and Kac [5].

This notation of probability with respect to the uniform distribution over infinite sets $\mathbb{N}^n, n \in \mathbb{N}$, is also known as **natural density**, which can be defined for any subset A as

$$D(A) = \lim_{N\to\infty} \frac{|A \cap \{1,2,\cdots,N\}^n|}{N^n},$$

provided the limit exists, where $|\cdot|$ denotes the cardinality of the corresponding set. In [8], Maze, Rosenthal and Wagner computed the natural density of the set of $k \times n$ unimodular integer matrices for any positive integers $k \le n$, where a $k \times n$ integer matrix is called unimodular if it can be extended to an invertible $n \times n$ matrix over the integers. Recently, Guo and Yang [3] generalized this result to the matrices of polynomials over finite fields.

Let $\mathbb{F}_q$ be the finite field consisting of q elements, and $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$, where q is a prime power. To define the concept of natural density for certain subsets, we need to enumerate polynomials in $\mathbb{F}_q[x]$. For convenience, denote the elements in $\mathbb{F}_q$ by $a_0 = 0, a_1, \cdots, a_{q-1}$. Let Σ be the set of all vectors $\alpha = (a_{m_0}, a_{m_1}, \cdots)$ with $m_i \in \{0, 1, \cdots, q-1\}$ and $m_i = 0$ for sufficiently large i. Then there is a one-to-one map

$$\chi : \Sigma \to \mathbb{Z}_+ = \mathbb{N} \cup \{0\}, \quad \chi(a_{m_0}, a_{m_1}, \cdots) = \sum_{j=0}^{\infty} m_i q^i.$$

For all $j \in \mathbb{Z}_+$, we set

$$f_j(x) = \sum_{i=0}^{\infty} a_{m_i} x^i, \text{ with } \chi(a_{m_0}, a_{m_1}, \cdots) = j.$$

Then $\mathbb{F}_q[x] = \{f_j(x) \mid j \in \mathbb{Z}_+\}$.

From now on, we fix a prime power q and a positive integer $n \ge 2$. Denote $\mathcal{M} = (\mathbb{F}_q[x])^n$ for convenience and let $\mathcal{M}_N$ be the subset of $\mathcal{M}$ consisting of vectors with entries taken from $\{f_0, f_1, \cdots, f_N\}$. For any subset $S \subseteq \mathcal{M}$, we define the **natural density** of S in $\mathcal{M}$ as

$$D(S) = \lim_{N\to\infty} \frac{|S \cap \mathcal{M}_N|}{|\mathcal{M}_N|}.$$

Using a probabilistic method, Sugita and Takanobu [10] determined the probability of two polynomials over $\mathbb{F}_p$ to be coprime for a prime p. Recently, Morrison [9], Benjamin and Bennett [1] computed the probability that n polynomials over $\mathbb{F}_q$ are coprime, which is $1 - q^{1-n}$. They used natural density methods and Euclidean algorithm respectively. Then it is natural to consider the questions: what is the probability that n polynomials in $\mathbb{F}_q[x]$ are pairwise coprime? Generally, what is the probability that n polynomials in $\mathbb{F}_q[x]$ are k-wise relatively coprime?

Our main purpose in this paper is to compute the probabilities mentioned above. More precisely, we determined the natural density of the set of n-dimensional vectors over $\mathbb{F}_q[x]$ whose entries are k-pairwise coprime, for any positive integer $k \leq n$. Our methods are conceptional and the main idea comes from [8] and [3].

Theorem 1. *Let k be a positive integer and $k \leq n$. Denote*

$$G = \{(g_1, \cdots, g_n) \in \mathcal{M} \mid \gcd(g_{i_1}, \cdots, g_{i_k}) = 1, \ \forall\ 1 \leq i_1 < \cdots < i_k \leq n\}.$$

Then the natural density of G is

$$\prod_{m=1}^{\infty} \Big(\sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q^m})^i (1 - \frac{1}{q^m})^{n-i}\Big)^{\phi(m)}, \tag{1.2}$$

where $\phi(m)$ is the number of monic irreducible polynomials with degree m in $\mathbb{F}_q[x]$.

Remark 1. The result of Theorem 1 can be understood as follows: the probability that n polynomials in $\mathbb{F}_q[x]$ are k-wise relatively coprime is

$$\prod_{m=1}^{\infty} \Big(\sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q^m})^i (1 - \frac{1}{q^m})^{n-i}\Big)^{\phi(m)}.$$

Take $k = n$, we get that the probability of n polynomials in $\mathbb{F}_q[x]$ being coprime is the $\prod_{m=1}^{\infty} (1 - \frac{1}{q^{mn}})^{\phi(m)}$. To see what this means, we introduce the following q**-zeta function**

$$\zeta_q(n) := \prod_f (1 - \frac{1}{q^{n \deg(f)}})^{-1} = \prod_{m=1}^{\infty} (1 - \frac{1}{q^{nm}})^{-\phi(m)}, \tag{1.3}$$

where f goes through all monic irreducible polynomials (not including the constant polynomials, as usual) in $\mathbb{F}_q[x]$. Recall the following interesting equation

$$\prod_f (1 - t^{\deg(f)})^{-1} = \sum_{l=0}^{\infty} q^l t^l = \frac{1}{1 - qt}. \tag{1.4}$$

For more details, see [9] and [3]. Putting $t = q^{-n}$ in (1.4), we get

$$\zeta_q^{-1}(n) = 1 - \frac{1}{q^{n-1}}. \tag{1.5}$$

Combining the equations (1.3) and (1.5), we get that the probability of n polynomials in $\mathbb{F}_q[x]$ being coprime is $\zeta_q^{-1}(n) = 1 - \frac{1}{q^{n-1}}$, which is just one of the main results of [9]. In particular, when $n = 2$, the probability that 2 polynomials in $\mathbb{F}_q[x]$ are coprime is $1 - \frac{1}{q}$, which is one of the main results of [1].

Taking $k = 2$ in Theorem 1, we have the following corollary.

Corollary 1. *Denote* $E = \{(g_1, \cdots, g_n) \in \mathcal{M} \mid \gcd(g_i, g_j) = 1,\ \forall\ 1 \le i < j \le n\}$. *Then*

$$D(E) = \prod_{m=1}^{\infty} \big((1 - \frac{1}{q^m})^{n-1}(1 + \frac{n-1}{q^m})\big)^{\phi(m)}. \tag{1.6}$$

Similarly, the value in (1.6) can be interpreted as the probability that n polynomials in $\mathbb{F}_q[x]$ are pairwise coprime.

2. Results

In this section, we will give the proof of Theorem 1. Before this, we need some preparations.

Fix a positive integer $k \le n$. Let T be a finite set of monic irreducible polynomials in $\mathbb{F}_q[x]$, denote

$$G_T = \{(g_1, \cdots, g_n) \in \mathcal{M} \mid f \nmid \gcd(g_{i_1}, \cdots, g_{i_k}), \\ \forall\ f \in T, 1 \le i_1 < \cdots < i_k \le n\}.$$

Clearly we have $G = \bigcap_T G_T$. Denote by $\langle f \rangle$ the ideal generated by $f \in \mathbb{F}_q[x]$.

Lemma 1. *Let* G_T *be defined as above, then we have*

$$D(G_T) = \prod_{f \in T} \sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q^{\deg(f)}})^i (1 - \frac{1}{q^{\deg(f)}})^{n-i}.$$

Proof. Denote $f^{(T)} = \prod_{f \in T} f$ and $d_T = \deg(f^{(T)})$. Given $g \in \mathbb{F}_q[x]$ let $\bar{g}$ be its image in $\mathbb{F}_q[x]/\langle f^{(T)} \rangle$. Then for any positive integer N, we have the canonical maps

$$\pi: \mathcal{M}_N \to (\mathbb{F}_q[x]/\langle f^{(T)} \rangle)^n, \quad (g_1, \cdots, g_n) \mapsto (\bar{g}_1, \cdots, \bar{g}_n),$$

and

$$\varphi: \Big(\mathbb{F}_q[x]/\langle f^{(T)} \rangle\Big)^n \to \Big(\prod_{f \in T} \mathbb{F}_q[x]/\langle f \rangle\Big)^n \to \prod_{f \in T} \big(\mathbb{F}_q[x]/\langle f \rangle\big)^n,$$

where the first part of φ is induced from the isomorphism

$$\mathbb{F}_q[x]/\langle f^{(T)} \rangle \cong \prod_{f \in T} \mathbb{F}_q[x]/\langle f \rangle,$$

a consequence of the Chinese Remainder Theorem and the second part of φ is an obvious isomorphism of vector spaces.

First suppose that $N = mq^{d_T} - 1$ for some $m \in \mathbb{N}$. Then it is easy to see

$$\{f_l(x) \mid 0 \le l \le N\} = \{f_s(x)x^{d_T} + f_t(x) \mid 0 \le s \le m-1, 0 \le t \le q^{d_T} - 1\}.$$

For any fixed $0 \le s \le m-1$, the following projection is one-to-one:

$$\{f_s(x)x^{d_T} + f_t(x) \mid 0 \le t \le q^{d_T} - 1\} \longrightarrow \mathbb{F}_q[x]/\langle f^{(T)} \rangle,$$

and the canonical projection

$$\{f_l(x) \mid 0 \le l \le N\} \longrightarrow \mathbb{F}_q[x]/\langle f^{(T)} \rangle$$

is m-to-one. Thus the projection map π is m^n-to-one.

For any $f \in T$, let φ_f be the canonical projection from $(\mathbb{F}_q[x]/\langle f^{(T)} \rangle)^n$ to $(\mathbb{F}_q[x]/\langle f \rangle)^n$ via φ. Given any $A \in \mathcal{M}_N$, we see that $A \in G_T$ if and only if at most $k-1$ entries of $\varphi_f \circ \pi(A)$ is zero for all $f \in T$. Noticing that $|\mathbb{F}_q[x]/\langle f \rangle| = q^{\deg(f)}$, it is easy to deduce that

$$|\varphi \circ \pi(\mathcal{M}_N)| = \prod_{f \in T} \sum_{i=0}^{k-1} \binom{n}{i} (q^{\deg(f)} - 1)^{n-i}.$$

As a result we have

$$\begin{aligned} |G_T \bigcap \mathcal{M}_N| &= m^n |\varphi \circ \pi(\mathcal{M}_N)| \\ &= (mq^{d_T})^n \prod_{f \in T} \sum_{i=0}^{k-1} \binom{n}{i} \Big(\frac{1}{q^{\deg(f)}}\Big)^i \Big(1 - \frac{1}{q^{\deg(f)}}\Big)^{n-i}. \end{aligned}$$

Now let N be any positive integer. There exist $m, r \in \mathbb{Z}_+$ such that $N + 1 = mq^{d_T} + r$, where $0 \le r < q^{d_T}$ and m, r are not both 0. For convenience, set $\widetilde{N} = mq^{d_T} - 1$. Then by the definition of the natural density, we have

$$\begin{aligned} D(G_T) &= \lim_{N \to \infty} \frac{|G_T \cap \mathcal{M}_N|}{|\mathcal{M}_N|} \\ &= \lim_{N \to \infty} \frac{|G_T \bigcap \mathcal{M}_{\widetilde{N}}| + |G_T \bigcap (\mathcal{M}_N - \mathcal{M}_{\widetilde{N}})|}{|\mathcal{M}_N|}. \end{aligned}$$

Note that $|\mathcal{M}_N - \mathcal{M}_{\widetilde{N}}| \le rn(N+1)^{n-1}$, that is

$$\lim_{N \to \infty} \frac{|G_T \bigcap (\mathcal{M}_N - \mathcal{M}_{\widetilde{N}})|}{|\mathcal{M}_N|} \le \lim_{N \to \infty} \frac{rn(N+1)^{n-1}}{(N+1)^n} = 0.$$

So, we obtain

$$\begin{aligned} D(G_T) &= \lim_{N \to \infty} \frac{|G_T \bigcap \mathcal{M}_{\widetilde{N}}|}{(N+1)^n} \\ &= \lim_{N \to \infty} \frac{(mq^{d_T})^n \prod_{f \in T} \sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q^{\deg(f)}})^i (1 - \frac{1}{q^{\deg(f)}})^{n-i}}{(N+1)^n} \\ &= \prod_{f \in T} \sum_{i=0}^{k-1} \binom{n}{i} \Big(\frac{1}{q^{\deg(f)}}\Big)^i \Big(1 - \frac{1}{q^{\deg(f)}}\Big)^{n-i}. \end{aligned}$$

This completes the proof. □

Proof of Theorem 1.1. For any irreducible polynomial $f \in \mathbb{F}_q[x]$, denote

$$K_f = \{(g_1,\cdots,g_n) \mid f \,|\, \gcd(g_{i_1},\cdots,g_{i_k}), 1 \le i_1 < \cdots < i_k \le n\}.$$

Let $q_f = q^{\deg(f)}$, then by Lemma 2.1 we have

$$\begin{aligned} D(K_f) &= 1 - D(G_{\{f\}}) \\ &= 1 - \sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q_f})^i (1-\frac{1}{q_f})^n \\ &\le 1 - (1-\frac{n-1}{q_f})(1+\frac{n-1}{q_f}) \\ &= (\frac{n-1}{q_f})^2. \end{aligned}$$

Let T_t be the set of all monic irreducible polynomials with degree no more than t, and denote $\widehat{T}$ the set of all monic irreducible polynomials in $\mathbb{F}_q[x]$. For convenience, we set $G_t = G_{T_t}$. Since

$$(G_t \setminus G) \subseteq \bigcup_{f \in \hat{T}\setminus T_t} K_f,$$

we have

$$\begin{aligned} \limsup_{N\to\infty} \frac{|(G_t \setminus G) \bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} &\le \limsup_{N\to\infty} \frac{|(\bigcup_{f\in\hat{T}\setminus T_t} K_f) \bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} \\ &\le \limsup_{N\to\infty} \frac{\sum_{f\in\hat{T}\setminus T_t} |K_f \bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} \\ &\le \sum_{f\in\hat{T}\setminus T_t} \limsup_{N\to\infty} \frac{|K_f \bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} \\ &= \sum_{f\in\hat{T}\setminus T_t} D(K_f) < \sum_{f\in\hat{T}\setminus T_t} (\frac{n-1}{q_f})^2 \\ &= \sum_{m=t+1}^{\infty} \frac{(n-1)^2}{q^{2m}} \phi(m), \end{aligned}$$

where $\phi(m)$ denotes the number of monic irreducible polynomials with degree m in $\mathbb{F}_q[x]$.

Since all irreducible polynomials with degree m can divide $x^{q^m} - x$, which has no multiple roots, thus $m\phi(m) \le q^m$ and

$$\limsup_{N\to\infty} \frac{|(G_t \setminus G)\bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} \le \sum_{m=t+1}^{\infty} \frac{(n-1)^2}{mq^m} \le \frac{(n-1)^2}{q^t(q-1)}.$$

Note that $G\bigcap \mathcal{M}_N \subseteq G_t \bigcap \mathcal{M}_N$ and $G\bigcap \mathcal{M}_N = G_t\bigcap \mathcal{M}_N - (G_t \setminus G)\bigcap \mathcal{M}_N$, which imply that

$$\limsup_{N\to\infty} \frac{|G\bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} \le \limsup_{N\to\infty} \frac{|G_t\bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} \le D(G_t).$$

and

$$\begin{aligned}\liminf_{N\to\infty} \frac{|G\bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} &\ge \liminf_{N\to\infty} \frac{|G_t\bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} - \limsup_{N\to\infty} \frac{(G_t \setminus G)\bigcap \mathcal{M}_N}{|\mathcal{M}_N|} \\ &\ge D(G_t) - \frac{(n-1)^2}{q^t(q-1)},\end{aligned}$$

for all $t \in \mathbb{N}$. Let t tend to ∞, from Lemma 2.1, we can conclude that

$$\begin{aligned}\lim_{N\to\infty} \frac{|G\bigcap \mathcal{M}_N|}{|\mathcal{M}_N|} &= \lim_{t\to\infty} D(G_t) \\ &= \lim_{t\to\infty} \prod_{f\in T_t} \sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q_f})^i (1-\frac{1}{q_f})^{n-i} \\ &= \lim_{t\to\infty} \prod_{m=1}^{t} \sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q^m})^i (1-\frac{1}{q^m})^{n-i} \\ &= \prod_{m=1}^{\infty} \Big(\sum_{i=0}^{k-1} \binom{n}{i} (\frac{1}{q^m})^i (1-\frac{1}{q^m})^{n-i}\Big)^{\phi(m)}.\end{aligned}$$

This completes the proof. □

Acknowledgement

This work is partially supported by the NSF of China (Grant No. 11101380, 11471294). The authors would like to express their gratitude to the referees for valuable suggestions.

References

[1] A. T. Benjamin and C. D. Bennett, "The probability of relatively prime polynomials," *Math. Mag.*, vol. 80, pp. 196–202, 2007.

[2] G. L. Dirichlet, *Über die Bestimmung der mittleren Werthe in der Zahlentheorie*. Abhandlungen Königlich Preuss, Akad. Wiss., 1849.
[3] X. Guo and G. Yang, "The probability of rectangular unimodular matrices over $\mathbb{F}_q[x]$," *Linear Algebra Appl.*, vol. 438, pp. 2657–2682, 2013.
[4] J. Hu, "The probability that random positive integers are k-wise relatively prime," *Int. J. Number Theory*, vol. 09, 2013.
[5] M. Kac, *Statistical independence in probability, analysis and number theory*, ser. The Carus Mathematical Monographs. New York: Mathematical Association of America, John Wiley and Sons, Inc., 1959, vol. 16.
[6] J. Kubilius, "Probabilistic methods in the theory of numbers," *Amer. Math. Soc. Transl. (2)*, vol. 19, pp. 47–85, 1962.
[7] H. Kubota and H. Sugita, "Probabilistic proof of limit theorems in number theory by means of adeles," *Kyushu J. Math.*, vol. 56, pp. 391–404, 2002.
[8] G. Maze, J. Rosenthal, and U. Wagner, "Natural density of rectangular unimodular integer matrices," *Linear Algebra Appl.*, vol. 434, pp. 1319–1324, 2011.
[9] K. E. Morrison, "Random polynomials over finite fields," *http://www.calpoly.edu/∼kmorriso/Research/RPFF.pdf*, 1999.
[10] H. Sugita and S. Takanobu, "The probability of two $\mathbb{F}_q$-polynomials to be coprime," *Adv. Stud. Pure Math.*, vol. 49, pp. 455–478, 2007.
[11] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, ser. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 1995, vol. 46.
[12] L. Tóth, "The probability that k positive integers are pairwise relatively prime," *Fibonacci Quart.*, vol. 40, pp. 13–18, 2002.

Authors' addresses

Xiangqian Guo

Zhengzhou University, School of Mathematics and Statistics, 100 Science Road, 450001 Zhengzhou, P. R. China

E-mail address: guoxq@ZZu.edu.cn

Fengdan Hou

Zhengzhou University, School of Mathematics and Statistics, 100 Science Road, 450001 Zhengzhou, P. R. China

E-mail address: houfd@zzu.ps.edu.cn

Xuewen Liu

Zhengzhou University, School of Mathematics and Statistics, 100 Science Road, 450001 Zhengzhou, P. R. China

E-mail address: liuxw@zzu.edu.cn