DIVISIBILITY PROPERTIES OF POLYNOMIAL EXPRESSIONS OF RANDOM INTEGERS

ZAKHAR KABLUCHKO[1] AND ALEXANDER MARYNYCH[2]

Abstract. We study divisibility properties of a set $\{f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)})\}$, where $f_1,\dots,f_m$ are polynomials in s variables over $\mathbb{Z}$ and $\mathbf{U}_n^{(s)}$ is a point picked uniformly at random from the set $\{1,\dots,n\}^s$, $s\in\mathbb{N}$. We show that the GCD and the suitably normalized LCM of this set converge in distribution to a.s. finite random variables under mild assumptions on $f_1,\dots,f_m$. Our approach is based on the notion of integer adeles and a known fact that the uniform distribution on $\{1,\dots,n\}$ converges to the Haar measure on the ring of integer adeles combined with the Lang-Weil bounds.

1. Introduction

One of the most classic results in probabilistic number theory, which can be traced back at least to Dirichlet [11], states that probability that two numbers, picked uniformly at random from the set $\{1,2,\dots,n\}$, are coprime converges to

$$\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p^2}\right)=\frac{1}{\zeta(2)}=\frac{6}{\pi^2},$$

as $n\to\infty$. Here $\mathcal{P}$ denotes the set of prime numbers and ζ is the Riemann zeta-function. We refer to [1] for a nice historical account of this result. More generally, it is known [7, 8, 9] that the greatest common divisor, to be denoted in what follows by GCD, of $s\geq 2$ numbers $(U_{n,1},\dots,U_{n,s})=:\mathbf{U}_n^{(s)}$ picked uniformly at random from $\{1,2,\dots,n\}^s$ converges in distribution, as $n\to\infty$, to an $\mathbb{N}$-valued random variable with

[1]Institut für Mathematische Stochastik, Westfälische Wilhelms-Universität Münster, Münster, Germany

[2]Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, Kyiv 01601, Ukraine

2020 *Mathematics Subject Classification.* Primary: 11K65, 11D88; Secondary: 11C08, 13F20.

Key words and phrases. Adele; divisibility; integer-valued polynomials; profinite integers; valuation.

the probability mass function

$$j \longmapsto \frac{1}{\zeta(s) j^s}, \quad j \in \mathbb{N}. \tag{1.1}$$

A recent paper [14] provides a comprehensive overview of results of this kind related to divisibility of random integers.

The motivation for the present paper comes from our attempt to understand the aforementioned result via a continuous mapping approach ubiquitous in probability theory and also to generalize it. In its simplest form, the continuous mapping theorem, see Theorem 2.7 in [4], states that if a sequence of random elements $(X_n)_{n\in\mathbb{N}}$ with values in a metric space M_1 converges in distribution to a random element X_∞ and f is a continuous mapping from M_1 to another metric space M_2, then a sequence of M_2-valued random elements $(f(X_n))_{n\in\mathbb{N}}$ converges in distribution to $f(X_\infty)$. Thus, to derive a convergence of $\mathrm{GCD}(\mathbf{U}_n^{(s)})$ via the continuous mapping approach the crucial step is to pick an appropriate topology, with respect to which the convergence in distribution of $\mathbf{U}_n^{(s)}$ is regarded. In this respect, the notion of integer adeles and a closely related concept of profinite integers turned out to be very useful. An incomplete list of references on various applications of profinite integers and integer adeles in probabilistic number theory includes [3, 12, 13, 20, 24, 25, 31].

Roughly speaking, a ring of integer adeles $\widehat{\mathbb{Z}}$ is a compactification of $\mathbb{Z}$ with respect to which two integers are close, if and only if they possess the same small prime divisors counting multiplicities. The rigorous definition will be recalled below in Section 2. A nice overview of this and other compactifications of $\mathbb{Z}$ in probabilistic number theory can be found in [18, 19]. In particular, a proof of the aforementioned result on the density of coprime pairs using this notion was given in [20]; see also [12, 13, 31] for related results. A rather simple observation which lies in the core of those proofs is the convergence of $U_n := U_{n,1}$ (and, therefore, of $\mathbf{U}_n^{(s)}$), identified with an element of $\widehat{\mathbb{Z}}$ via the canonical embedding, to a random element distributed according to the Haar measure on $\widehat{\mathbb{Z}}$. This result can be found, for example, as Lemma 6 in [20]. We shall recall this fact in a slightly extended form as Proposition 2.1 and give a short proof based on the Chinese Remainder Theorem in Section 2.

In this paper we are concerned with generalizations of the aforementioned and similar results to the following more general setting. Let $f_1, \dots, f_m$ be polynomials in s variables with integer coefficients. What can be said about the greatest common divisor of $\{f_1(\mathbf{U}_n^{(s)}), \dots, f_m(\mathbf{U}_n^{(s)})\}$? Or what is the probability that $f_1(\mathbf{U}_n^{(s)})$ divides $f_2(\mathbf{U}_n^{(s)})$? It

turn out that the approach outlined above can be successfully applied in this setting. For example, our results can be used to conclude that the sequence of random variables

$$n^{-9}\mathrm{LCM}(U_{n,1}^2+U_{n,2}^2, U_{n,1}^3+U_{n,2}^3, U_{n,1}^4+U_{n,2}^4), \tag{1.2}$$

where LCM denotes the least common multiple, converges in distribution to a non-trivial limit, as $n\to\infty$. A direct check of this fact seems to be a challenging problem. To the best of our knowledge, these questions have not been addressed in the literature. A related result on relatively prime values of polynomials can be found in Theorem 3.1 in [28]. Another tangent result is an Erdős-Kac law for the number of prime divisors of a polynomial in several variables which has been established in [32].

The rest of the paper is organized as follows. In Section 2 we recall the definition of integer adeles and reprove a result on convergence of all p-adic expansions of a uniformly sampled integer on $\{1,2,\dots,n\}$ to a random element of $\widehat{\mathbb{Z}}$ distributed according the Haar measure. Section 3 is devoted to the the analysis of arithmetic properties of the set $\{f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)})\}$. One of the central result in Section 3 is Theorem 3.1 which, in particular, provides the limit distribution for the LCM in (1.2). A list of further results in Section 3 includes limit theorems for the GCD and the normalized LCM of the above set. The proofs of these results are given in Section 4 with a one long technical proof being postponed to Section 5. Some short auxiluary results are collected in the Appendix.

2. Ring of integer adeles and convergence to the Haar measure

Let $\mathbb{Q}_p$ be the field of p-adic rational numbers, which is the completion of $\mathbb{Q}$ with respect to the p-adic norm

$$\left\|\frac{a}{b}p^l\right\|_p := p^{-l},\quad l\in\mathbb{Z},\quad a,b \text{ are coprime to } p.$$

Denote also by $\|\cdot\|_\infty$ the usual Euclidean norm on $\mathbb{Q}$ and by $\mathbb{Q}_\infty=\mathbb{R}$ the completion of $\mathbb{Q}$ with respect to $\|\cdot\|_\infty$.

For $p\in\mathcal{P}$ let $\mathbb{Z}_p$ be the ring of p-adic integers in $\mathbb{Q}_p$. Any p-adic integer can be represented as $a_0+a_1p+a_2p^2+\cdots$ with $a_i\in\{0,1,\dots,p-1\}=:\mathbb{Z}/p\mathbb{Z}$. The ring $\mathbb{Z}_p$ is a compact subring of $\mathbb{Q}_p$. Therefore, the direct product

$$\widehat{\mathbb{Z}}=\prod_{p\in\mathcal{P}}\mathbb{Z}_p,$$

is also a compact topological ring by Tychonoff's theorem. The elements of $\widehat{\mathbb{Z}}$ are called *integer adeles* [21], *profinite integers* [2] or *polyadic numbers* [24, 25]. The compact abelian group $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ introduced by H. Prüfer [29]; see also [10, 23, 24, 25].

Since $\mathbb{Z}_p$ is a compact abelian group, for each $p \in \mathcal{P}$, there exists a unique invariant (Haar) probability measure μ_p on $\mathbb{Z}_p$. The explicit probabilistic construction of μ_p is as follows. Take $(u_{k,p})_{k\geq 0}$ independent uniformly distributed on $\{0,1,\ldots,p-1\}$ random variables and put

$$V_p := \sum_{k=0}^{\infty} u_{k,p} p^k \in \mathbb{Z}_p. \tag{2.1}$$

Then μ_p is the distribution of V_p. Let $\widehat{\mu} = \prod_{p\in\mathcal{P}} \mu_p$ be the product measure on $\widehat{\mathbb{Z}}$. Then, $\widehat{\mu}$ is the unique Haar probability measure on the compact group $\widehat{\mathbb{Z}}$.

There is a unique canonical ring homomorphism

$$\phi : \mathbb{Z} \longrightarrow \widehat{\mathbb{Z}}$$

with $\phi(1) = 1$. It sends an integer n to an infinite vector $\phi(n) := (\phi_p(n))_{p\in\mathcal{P}} \in \widehat{\mathbb{Z}}$ such that $\phi_p(n)$ is the p-adic expansion of n. Let $\pi^{(p)} : \widehat{\mathbb{Z}} \to \mathbb{Z}_p$ and $\pi_j^{(p)} : \widehat{\mathbb{Z}} \to \{0,1,\ldots,p-1\}$ be the canonical projections

$$\pi^{(p)}((x_p)_{p\in\mathcal{P}}) = x_p \quad \text{and} \quad \pi_j^{(p)}\left(\left(\sum_{k=0}^{\infty} a_{k,p} p^k\right)_{p\in\mathcal{P}}\right) = a_{j,p}, \quad j \geq 0, \quad p \in \mathcal{P}. \tag{2.2}$$

We shall use $\xrightarrow{\mathrm{d}}$ to denote convergence in distribution of random elements. Throughout the paper convergence of infinite-dimensional vectors is understood with respect to the product topology, that is, as convergence of all finite-dimensional projections. A version of Proposition 2.1 can be found as Lemma 6 in [20].

Proposition 2.1. *Let U_n be a random variable with the uniform distribution on $\{1,2,\ldots,n\}$. Then we have the convergence in distribution*

$$\left(\phi(U_n), \frac{U_n}{n}\right) \xrightarrow{\mathrm{d}} (\mathcal{V}, U_\infty), \quad n \to \infty,$$

on the space $\widehat{\mathbb{Z}} \times [0,1]$. Here $\mathcal{V} := (V_p)_{p\in\mathcal{P}}$, V_p is given by (2.1), U_∞ has the uniform distribution on $[0,1]$, and $U_\infty, V_2, V_3, V_5, \ldots$ are mutually independent. Note that $(\mathcal{V}, U_\infty)$ is distributed according to the product of the Haar measure $\widehat{\mu}$ on $\widehat{\mathbb{Z}}$ and the Lebesgue measure on $[0,1]$.

Proof. We need to show that

$$\left(\left(\pi_j^{(p)}(\phi(U_n))\right)_{p\in\mathcal{P},j\in\mathbb{N}}, \frac{U_n}{n}\right) \xrightarrow{\mathrm{d}} \left(\left(\pi_j^{(p)}(\mathcal{V})\right)_{p\in\mathcal{P},j\in\mathbb{N}}, U_\infty\right), \quad n\to\infty.$$

Fix pairwise distinct $p_1, p_2, \ldots, p_m \in \mathcal{P}$, arbitrary $l_1, l_2, \ldots, l_m \in \mathbb{N}$, $t \in [0,1]$ and note that by independence

$$\mathbb{P}\{\pi_k^{(p_i)}(\mathcal{V}) = r_{k,p_i}, \quad i = 1,\ldots,m, \quad k = 0,\ldots,l_i - 1\} = \prod_{i=1}^m \frac{1}{p_i^{l_i}},$$

for any $r_{k,p_i} \in \mathbb{Z}/p_i\mathbb{Z}$, $i = 1,\ldots,m$. Thus, it suffices to show that

$$\lim_{n\to\infty} \mathbb{P}\{\pi_k^{(p_i)}(\phi(U_n)) = r_{k,p_i}, \quad i = 1,\ldots,m, \quad k = 0,\ldots,l_i - 1, \quad U_n \le nt\} = t\prod_{i=1}^m \frac{1}{p_i^{l_i}}, \quad (2.3)$$

for any $r_{k,p_i} \in \mathbb{Z}/p_i\mathbb{Z}$, $i = 1,\ldots,m$. Put $r_i := \sum_{j=0}^{l_i-1} r_{j,p_i} p_i^j$ and note that

$$\begin{aligned}
&\mathbb{P}\{\pi_k^{(p_i)}(\phi(U_n)) = r_{k,p_i}, \quad i = 1,\ldots,m, \quad k = 0,\ldots,l_i - 1, \quad U_n \le nt\} \\
&\quad = \mathbb{P}\{U_n \equiv r_i (\mathrm{mod}\, p^{l_i}), \quad i = 1,\ldots,m, \quad U_n \le nt\} \\
&\quad = \frac{1}{n}\#\left\{k \in \{1,2,\ldots,\lfloor nt\rfloor\} : k \equiv r_i \left(\mathrm{mod}\, p_i^{l_i}\right), i = 1,\ldots,m\right\}.
\end{aligned}$$

Put $M := \prod_{i=1}^m p_i^{l_i}$ and let $\mathbb{1}\{A\}$ denote the indicator of the event A. By the Chinese remainder theorem, for some unique $r \in \mathbb{Z}/M\mathbb{Z}$,

$$\begin{aligned}
&\frac{1}{n}\#\left\{k \in \{1,2,\ldots,\lfloor nt\rfloor\} : k \equiv r_i \left(\mathrm{mod}\, p_i^{l_i}\right), i = 1,\ldots,m\right\} \\
&\qquad = \frac{1}{n}\#\{k \in \{1,2,\ldots,\lfloor nt\rfloor\} : k \equiv r\,(\mathrm{mod}\, M)\} = \frac{1}{n}\sum_{l\ge 0} \mathbb{1}\{r + lM \le nt\} = \frac{1}{n}\left\lfloor \frac{nt - r}{M}\right\rfloor,
\end{aligned}$$

and the right-hand side converges to tM^{-1}, as $n \to \infty$. Thus, (2.3) holds and the proof is complete. □

Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1,\ldots,x_s]$ be m polynomials in s variables over $\mathbb{Z}$. Since ϕ is a homomorphism, we have $\phi(f(x_1,\ldots,x_s)) = f(\phi(x_1),\ldots,\phi(x_s))$, for every $f \in \mathbb{Z}[x_1,\ldots,x_s]$. By the continuous mapping theorem we obtain the following corollary. Let $\mathcal{V}_1,\ldots,\mathcal{V}_s$ be independent copies of $\mathcal{V}$ and recall the notation $\mathbf{U}_n^{(s)} = (U_{n,1},\ldots,U_{n,s})$ for a uniformly distributed on $\{1,\ldots,n\}^s$ random vector. Then, with $\mathbf{U}_\infty^{(s)}$ being uniformly distributed on $[0,1]^s$ and independent of $\mathcal{V}_1,\ldots,\mathcal{V}_s$ the following corollary holds true.

Corollary 2.2. *As $n \to \infty$,*

$$\left(\phi(f_1(\mathbf{U}_n^{(s)})),\dots,\phi(f_m(\mathbf{U}_n^{(s)})),\frac{1}{n}\mathbf{U}_n^{(s)}\right) \xrightarrow{\mathrm{d}} \left(f_1(\mathcal{V}_1,\dots,\mathcal{V}_s),\dots,f_m(\mathcal{V}_1,\dots,\mathcal{V}_s),\mathbf{U}_\infty^{(s)}\right).$$

In what follows it is important that, for every fixed $f \in \mathbb{Z}[x_1,\dots,x_s]$, the projections $\pi^{(p)}(f(\mathcal{V}_1,\dots,\mathcal{V}_s))$, $p \in \mathcal{P}$, are mutually independent. This follows from the fact that $\pi^{(p)}(\mathcal{V})$, $p \in \mathcal{P}$, are independent and $\pi^{(p)}$ is a ring homomorphism, thus, commutes with any polynomial.

For $n \in \mathbb{Z} \setminus \{0\}$ and $p \in \mathcal{P}$ let $\lambda_p(n)$ denote the power of prime p in the prime decomposition of $|n|$, so

$$|n| = \prod_{p\in\mathcal{P}} p^{\lambda_p(n)}.$$

We have an obvious relation $\lambda_p(n) = \inf\{k \ge 0 : \pi_k^{(p)}(\phi(n)) > 0\}$, which advocates the usage of the same notation λ_p for the following function defined on $\widehat{\mathbb{Z}}$:

$$\lambda_p(x) = \inf\{k \ge 0 : \pi_k^{(p)}(x) > 0\}, \quad x \in \widehat{\mathbb{Z}}.$$

This definition also shows that it is natural to stipulate $\lambda_p(0) := +\infty$, $p \in \mathcal{P}$. Our main result implies the next two corollaries. The first one is well-known, see, for instance, Lemma 3.1 in [6], the second one seems to be new. Set

$$\mathcal{G}_p := \lambda_p(\mathcal{V}) = \inf\{k \ge 0 : \pi_k^{(p)}(\mathcal{V}) > 0\}, \quad p \in \mathcal{P}.$$

Corollary 2.3. *The random variables $\mathcal{G}_p$, $p \in \mathcal{P}$, and U_∞ are mutually independent and $\mathcal{G}_p$ has a geometric distribution*

$$\mathbb{P}\{\mathcal{G}_p \ge k\} = \frac{1}{p^k}, \quad k \ge 0, \quad p \in \mathcal{P}. \tag{2.4}$$

Furthermore,

$$\left(\left(\lambda_p(U_n)\right)_{p\in\mathcal{P}}, \frac{U_n}{n}\right) \xrightarrow{\mathrm{d}} ((\mathcal{G}_p)_{p\in\mathcal{P}}, U_\infty), \quad n \to \infty.$$

Corollary 2.4. *For polynomials $f_1,\dots,f_m \in \mathbb{Z}[x_1,\dots,x_s]$ with the same notation as in Corollary 2.2 we have*

$$\left(\lambda_p(f_i(\mathbf{U}_n^{(s)}))\right)_{p\in\mathcal{P},i=1,\dots,m} \xrightarrow{\mathrm{d}} \left(\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))\right)_{p\in\mathcal{P},i=1,\dots,m}, \quad n \to \infty.$$

For every $i \in \{1,\dots,m\}$, the limiting random variables $\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))$, $p \in \mathcal{P}$, are mutually independent.

Proposition 2.5. *If $f \in \mathbb{Z}[x_1,\dots,x_s]$ is a non-zero polynomial with integer coefficients, then $\mathbb{P}\{\lambda_p(f(\mathcal{V}_1,\dots,\mathcal{V}_s) = +\infty\} = 0$ for every $p \in \mathcal{P}$.*

Proof. Recall that $(\pi^{(p)}(\mathcal{V}_1),\dots,\pi^{(p)}(\mathcal{V}_s))$ is distributed according to the product measure $\mu_p^{\otimes s}$, where μ_p is the Haar measure on $\mathbb{Z}_p$. Hence, $\mathbb{P}\{\lambda_p(f(\mathcal{V}_1,\dots,\mathcal{V}_s)) = +\infty\} = \mu_p^{\otimes s}(\{x \in \mathbb{Z}_p^s : f(x) = 0\})$. By Lemma 5.7 in the Appendix the right-hand side is equal to zero. □

3. Main results

For a multiset $A := \{a_1,\dots,a_m\} \subset \mathbb{Z}$, let $\mathrm{GCD}(A)$ denote the greatest common divisor, $\mathrm{LCM}(A)$ the least common multiple and $\mathrm{NLCM}(A)$ the normalized least common multiple of a multiset $\{|a_1|,\dots,|a_m|\} \subset \{0,1,2,\dots\}$, respectively. If $0 \notin A$, then $\mathrm{NLCM}(A)$ by definition is equal to

$$\mathrm{NLCM}(A) := \frac{\mathrm{LCM}(A)}{\prod_{i=1}^m |a_i|}.$$

If A contains zero, then we stipulate $\mathrm{GCD}(A) := \mathrm{GCD}(A \setminus \{0\})$, $\mathrm{LCM}(A) := 0$ and $\mathrm{NLCM}(A) := \mathrm{NLCM}(A \setminus \{0\})$.

Theorem 3.1. *Let $f_1,\dots,f_m \in \mathbb{Z}[x_1,\dots,x_s]$ be $m \geq 2$ non-zero polynomials that do not have a common factor of degree > 0. Then*

$$\mathrm{GCD}(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)})) \xrightarrow{\mathrm{d}} G_{f_1,\dots,f_m}, \quad n \to \infty,$$

for some random variable $G_{f_1,\dots,f_m}$ with values in $\mathbb{N}$. More concretely, we have

$$\log G_{f_1,\dots,f_m} = \sum_{p\in\mathcal{P}} \log p \min_{i=1,\dots,m} \lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)),$$

and the series on the right-hand side converges a.s.

The proof of Theorem 3.1 will be given in Section 4.2.

Remark 3.2. *In fact, almost the same proof shows a slightly stronger version of Theorem 3.1 in which the GCD's of all tuples of polynomials without a common factor converge jointly in distribution. More precisely, for integer $m \geq 2$ let $\mathbb{I}_m$ be the set of all m-tuples $(f_1,\dots,f_m)$ of polynomials from $\mathbb{Z}[x_1,\dots,x_s]$ that do not have a common factor of degree > 0. Then, the following distributional convergence of collections of random variables holds:*

$$(\mathrm{GCD}(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)}))_{m\geq 2,(f_1,\dots,f_m)\in\mathbb{I}_m} \xrightarrow{\mathrm{d}} (G_{f_1,\dots,f_m})_{m\geq 2,(f_1,\dots,f_m)\in\mathbb{I}_m}, \quad n \to \infty.$$

Remark 3.3. *Upon setting $s := m$, $f_j(x_1,\dots,x_s) := x_j$, $j = 1,\dots,m$, we recover the result mentioned in the introduction. Namely,*

$$\mathrm{GCD}\,(U_{n,1},\dots,U_{n,s}) \xrightarrow{\mathrm{d}} \prod_{p\in\mathcal{P}} p^{\min_{k=1,\dots,s}\mathcal{G}_{p,k}}, \quad n\to\infty,$$

where $(\mathcal{G}_{p,k})_{p\in\mathcal{P},k=1,\dots,s}$ are mutually independent and $\mathcal{G}_{p,k}$ has the geometric distribution (2.4) *for every $k = 1,\dots,s$ and $p\in\mathcal{P}$. By calculating the moments $\mathbb{E}\left(\prod_{p\in\mathcal{P}} p^{-t\min_{k=1,\dots,s}\mathcal{G}_{p,k}}\right)$, $t>0$, with the aid of Euler's product formula, we see that*

$$\mathbb{P}\left\{\prod_{p\in\mathcal{P}} p^{\min_{k=1,\dots,s}\mathcal{G}_{p,k}} = j\right\} = \frac{1}{\zeta(s)j^s}, \quad j\in\mathbb{N},$$

in full accordance with (1.1). *Interestingly, this distribution has pop up also in the context of profinite integers in* [2].

Corollary 3.4. *Let $f,g\in\mathbb{Z}[x_1,\dots,x_s]$ be two polynomials such that f does not divide g over $\mathbb{Q}[x_1,\dots,x_s]$. Assume that* $\deg f\ge 1$. *Then*

$$\lim_{n\to\infty}\mathbb{P}\{f(\mathbf{U}_n^{(s)}) \text{ divides } g(\mathbf{U}_n^{(s)})\} = 0.$$

The proof of Corollary 3.4 will be given in Section 4.3.

Theorem 3.5. *Let $f_1,\dots,f_m\in\mathbb{Z}[x_1,\dots,x_s]$ be $m\ge 2$ non-zero polynomials such that any pair does not share a common factor of degree >0. Put $d_i := \deg f_i$. Then*

$$\mathrm{NLCM}\,(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)})) \xrightarrow{\mathrm{d}} L_{f_1,\dots,f_m}, \quad n\to\infty, \tag{3.1}$$

for some random variable $L_{f_1,\dots,f_m}$ with values in $1/\mathbb{N} := \{1,1/2,1/3,\dots\}$. More concretely, we have

$$\log L_{f_1,\dots,f_m} = \sum_{p\in\mathcal{P}} \log p\left(\max_{i=1,\dots,m}\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)) - \sum_{i=1}^m \lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))\right),$$

and the series on the right-hand side converges a.s. Moreover, with $\bar{f}_i\in\mathbb{Z}[x_1,\dots,x_s]$ denoting a homogeneous polynomial of the same degree as f_i obtained from f_i by dropping all monomials except those having the highest degree d_i, it holds

$$\frac{\mathrm{LCM}\,(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)}))}{n^{d_1+\cdots+d_m}} \xrightarrow{\mathrm{d}} L_{f_1,\dots,f_m}\prod_{i=1}^m \bar{f}_i(\mathbf{U}_\infty^{(s)}), \tag{3.2}$$

where $\mathbf{U}_\infty^{(s)}$ is independent of $L_{f_1,\dots,f_m}$ and has the uniform distribution on $[0,1]^s$.

The proof of Theorem 3.5 will be given in Section 4.4.

4. Proofs for Section 3

4.1. **Preliminaries: algebraic sets and varieties.** Here we recall some basic notions from algebraic geometry and prove several auxiliary results needed for the proof of Theorem 3.1. We refer to Chapter VI in [30] for the definitions given below and further properties of algebraic sets and varieties.

Let $\mathbb{K}$ be a field and denote by $\overline{\mathbb{K}}$ its algebraic closure. For a subset S of the ring $\mathbb{K}[x_1,\dots,x_s]$ of polynomials over $\mathbb{K}$ the set

$$A_{\mathbb{K}}(S) := \{x \in \overline{\mathbb{K}}^s : g(x) = 0 \ \forall g \in S\} \tag{4.1}$$

is called an (affine) $\mathbb{K}$-algebraic set. A $\mathbb{K}$-algebraic set is called irreducible (or an affine $\mathbb{K}$-algebraic variety) if it is not the union of two strictly smaller $\mathbb{K}$-algebraic sets. Every $\mathbb{K}$-algebraic set is a finite union of irreducible $\mathbb{K}$-algebraic varieties, called irreducible components. This decomposition is unique, see Theorems 1I and 1J in [30, Chapter VI]. The dimension of a $\mathbb{K}$-algebraic variety $A_{\mathbb{K}}(S)$ is the maximal length $d \in \{0,1,\dots,s\}$ of the chains $V_0 \subset V_1 \subset \cdots \subset V_d$ of distinct nonempty $\mathbb{K}$-algebraic subvarieties of $A_{\mathbb{K}}(S)$. The dimension of a $\mathbb{K}$-algebraic set is the maximum of the dimensions of its irreducible components. The algebraic varieties of dimension $s-1$ are called hypersurfaces.

Lemma 4.1. *Assume that $f_1,\dots,f_m \in \mathbb{Z}[x_1,\dots,x_s]$ are $m \geq 2$ non-zero polynomials that do not have a common factor of degree > 0, then*

$$\dim\left(A_{\mathbb{Q}}(f_1,\dots,f_m)\right) \leq s-2.$$

For $s = 1$ this means that $A_{\mathbb{Q}}(f_1,\dots,f_m)$ is empty.

Proof. We argue by contradiction. At least one of the polynomials is non-zero, therefore $\dim\left(A_{\mathbb{Q}}(f_1,\dots,f_m)\right) < s$. Assume that $\dim\left(A_{\mathbb{Q}}(f_1,\dots,f_m)\right) = s-1$, then at least one irreducible component of $A_{\mathbb{Q}}(f_1,\dots,f_m)$ is a hypersurface, say H. According to Theorem 2C(ii) in [30, Chapter VI], there exists an irreducible polynomial $h \in \mathbb{Q}[x_1,\dots,x_s]$ such that

$$H := A_{\mathbb{Q}}(h) = \{x \in \overline{\mathbb{Q}}^s : h(x) = 0\}, \quad \deg h \geq 1.$$

Since $f_1,\dots,f_m$ vanish on H, Hilbert's Nullstellensatz yields that

$$f_i^{r_i} = hg_i, \quad i = 1,\dots,m,$$

for some $g_1,\dots,g_m \in \mathbb{Q}[x_1,\dots,x_s]$ and $r_1,\dots,r_m \in \mathbb{N}$. Thus, h is a common factor of $f_1,\dots,f_m$ giving the desired contradiction. □

Any set of polynomials $f_1,\dots,f_m \in \mathbb{Q}[x_1,\dots,x_s]$ with rational coefficients can be regarded also as a set of polynomials over finite fields $\mathbb{F}_p$, $p \in \mathcal{P}$, by reducing their coefficients modulo p. The next result shows that basic characteristics of the $\mathbb{Q}$-algebraic set $A_{\mathbb{Q}}(f_1,\dots,f_m)$, such as the number of irreducible components and the dimension, are preserved when passing to $\mathbb{F}_p$-algebraic sets $A_{\mathbb{F}_p}(f_1,\dots,f_m)$, for all but finitely many primes $p \in \mathcal{P}$.

Proposition 4.2. *Let $f_1,\dots,f_m \in \mathbb{Q}[x_1,\dots,x_s]$ be such that the algebraic set $A_{\mathbb{Q}}(f_1,\dots,f_m)$ has ℓ irreducible components and dimension d. Then, for all but finitely many primes p, the variety $A_{\mathbb{F}_p}(f_1,\dots,f_m)$ has m irreducible components and the same dimension d.*

Proof. The claim about the number of components follows from Proposition 5 in [17]. Thus, we may assume that $\ell = 1$, that is, $A_{\mathbb{Q}}(f_1,\dots,f_m)$ is a $\mathbb{Q}$-algebraic variety of dimension d. By Corollary 10.4.3 in [15] the dimension of $A_{\mathbb{F}_p}(f_1,\dots,f_m)$ is equal to d for all but finitely many primes $p \in \mathcal{P}$. □

A complexity of a $\mathbb{K}$-algebraic set $A_{\mathbb{K}}(f_1,\dots,f_m)$, for $f_1,\dots,f_m \in \mathbb{K}[x_1,\dots,x_s]$, is defined as the maximum of s, m and the degrees of $f_1,\dots,f_m$. Proposition 4.2 in conjunction with the classical Lang-Weil bound, see the original work [22] or Theorem 4.1 in [16], yields the following.

Proposition 4.3 (The Lang-Weil bound)**.** *For $f_1,\dots,f_m \in \mathbb{Z}[x_1,\dots,x_s]$, consider a $\mathbb{Q}$-algebraic set $V := A_{\mathbb{Q}}(f_1,\dots,f_m)$ of complexity at most M. Then, for all but finitely many $p \in \mathcal{P}$,*

$$\#\{x \in \mathbb{F}_p^s : f_1(x) = \dots = f_m(x) = 0\} = (\ell(V) + O(p^{-1/2}))p^{\dim(V)},$$

where $\ell(V) \in \mathbb{N}$ is the number of irreducible components of V of dimension $\dim(V)$ and a constant in the Landau symbol O depends only on the complexity M. In particular, if V is irreducible than $\ell(V) = 1$.

4.2. **Proof of Theorem 3.1.**

Proof. By Proposition 2.5 $\mathbb{P}\{\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)) < \infty\} = 1$ for all $p \in \mathcal{P}$. By Lemma 4.1 the dimension of a $\mathbb{Q}$-variety $A_{\mathbb{Q}}(f_1,\dots,f_m)$ is at most $s-2$. According to Proposition 4.3, for all p large enough,

$$\begin{aligned}\mathbb{P}\{\min_{i=1,\dots,m} \lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)) \geq 1\} &= \mathbb{P}\{\pi_0^{(p)}(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)) = 0 \ \forall i = 1,\dots,m\} \\ &= p^{-s}\#\{(x_1,\dots,x_s) \in \mathbb{F}_p^s : f_i(x_1,\dots,x_s) = 0 \ \forall i = 1,\dots,m\} = O(p^{-2}), \quad (4.2)\end{aligned}$$

provided $s \geq 2$. For $s = 1$, the probability vanishes for sufficiently large p. By the Borel-Cantelli lemma, this implies the a.s. convergence of the series defining $\log G_{f_1,\dots,f_m}$.

Fix $N \in \mathbb{N}$ and write, for $n \geq N$,

$$\log \mathrm{GCD}\,(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)})) = \left(\sum_{p\in\mathcal{P},p\leq N} + \sum_{p\in\mathcal{P},N<p\leq n} + \sum_{p\in\mathcal{P},p>n}\right)\log p \min_{i=1,\dots,m} \lambda_p(f_i(\mathbf{U}_n^{(s)}))$$
$$=: Y_1(n,N) + Y_2(n,N) + Y_3(n).$$

By Corollary 2.4 and the continuous mapping theorem

$$Y_1(n,N) \xrightarrow{\mathrm{d}} \sum_{p\in\mathcal{P},p\leq N} \log p \min_{i=1,\dots,m} \lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)), \quad n\to\infty.$$

As we have already shown, the right-hand side converges a.s. to $\log G_{f_1,\dots,f_m}$, as $N\to\infty$. Using Theorem 3.2 in [4] we see that it suffices to check that

$$\lim_{N\to\infty} \limsup_{n\to\infty} \mathbb{P}\{Y_2(n,N)\neq 0\} = 0, \tag{4.3}$$
$$\lim_{n\to\infty} \mathbb{P}\{Y_3(n)\neq 0\} = 0. \tag{4.4}$$

The proof of (4.4) is postponed to Proposition 5.1 in Section 5. Let us prove (4.3). For $p\in\mathcal{P}$ and $k = 1,\dots,s$, put $Z_{n,p}^{(k)} := U_{n,k} (\mathrm{mod}\, p)$ and note that

$$\begin{aligned}
&\mathbb{P}\{Y_2(n,N)\neq 0\}\\
&\leq \mathbb{P}\{\exists p\in\mathcal{P}: N<p\leq n, \lambda_p(f_i(\mathbf{U}_n^{(s)}))\geq 1\ \forall i=1,\dots,m\}\\
&\leq \sum_{p\in\mathcal{P},N<p\leq n} \mathbb{P}\{\lambda_p(f_i(\mathbf{U}_n^{(s)}))\geq 1\ \forall i=1,\dots,m\}\\
&= \sum_{p\in\mathcal{P},N<p\leq n} \mathbb{P}\{f_1(Z_{n,p}^{(1)},\dots,Z_{n,p}^{(s)}) \equiv \dots \equiv f_m(Z_{n,p}^{(1)},\dots,Z_{n,p}^{(s)}) \equiv 0 (\mathrm{mod}\, p)\}\\
&\leq \sum_{p\in\mathcal{P},N<p\leq n} \left(\max_{j=0,\dots,p-1} \mathbb{P}\{Z_{n,p}^{(1)} = j\}\right)^s \#\{(x_1,\dots,x_s)\in\mathbb{F}_p^s : f_1(x_1,\dots,x_s) = \cdots\\
&\qquad\qquad = f_m(x_1,\dots,x_s) = 0\}.
\end{aligned}$$

Note that, for $p\leq n$,

$$\max_{j=0,\dots,p-1} \mathbb{P}\{Z_{n,p}^{(1)} = j\} = \max_{j=0,\dots,p-1} \mathbb{P}\{U_{n,1}\in\{j,j+p,\dots,j+\lfloor (n-j)/p\rfloor p\}$$
$$\leq n^{-1} \max_{j=0,\dots,p-1} (\lfloor (n-j)/p\rfloor + 1) \leq \frac{1}{p} + \frac{1}{n} \leq \frac{2}{p}.$$

Thus, applying the Lang-Weil bound from Proposition 4.3 we see that

$$\lim_{N\to\infty}\limsup_{n\to\infty}\mathbb{P}\{Y_2(n,N)\neq 0\}\le\lim_{N\to\infty}O\left(\sum_{p>N}p^{-2}\right)=0.$$

This completes the proof of (4.3) and of Theorem 3.1. □

Remark 4.4 (Ekedahl-Poonen density formula)**.** *Theorem 3.1, in particular, implies that the set*

$$\mathcal{R}:=\{(x_1,\dots,x_s)\in\mathbb{Z}^s:\mathrm{GCD}\,(f_1(x_1,\dots,x_s),\dots,f_m(x_1,\dots,x_s))=1\}$$

possesses the asymptotic density, which is equal to

$$\begin{aligned}\mathbb{P}\left\{\sum_{p\in\mathcal{P}}\log p\min_{i=1,\dots,m}\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))=0\right\}&=\prod_{p\in\mathcal{P}}\mathbb{P}\{\min_{i=1,\dots,m}\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))=0\}\\&=\prod_{p\in\mathcal{P}}\Big(1-\mathbb{P}\{\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))\ge 1\ \forall i=1,\dots,m\}\Big)=\prod_{p\in\mathcal{P}}\left(1-\frac{s_p}{p^s}\right),\end{aligned}$$

where $s_p:=\#\{(x_1,\dots,x_s)\in\mathbb{F}_p^s:f_i(x_1,\dots,x_s)\equiv 0(\mathrm{mod}\,p)\ \forall i=1,\dots,m\}$. *For the last passage we used the second equality in* (4.2). *This result is known in the literature as Ekedahl–Poonen formula, see* [5, 28].

4.3. **Proof of Corollary 3.4.** We start by writing factorizations over $\mathbb{Q}$:

$$f=c_f\prod_{i=1}^{L}h_i^{u_i}\quad\text{and}\quad g=c_g\prod_{i=1}^{L}h_i^{v_i},\tag{4.5}$$

where $\{h_1,\dots,h_L\}$ is the set of irreducible factors of f and g without multiplicities, $c_f,c_g\in\mathbb{Z}$ and $u_i,v_i\ge 0$. The assumption that f does not divide g implies $u_i>v_i$, for some $i=1,\dots,L$. Clearly,

$$\mathbb{P}\{f(\mathbf{U}_n^{(s)})\text{ divides }g(\mathbf{U}_n^{(s)})\}=\mathbb{P}\{\mathrm{GCD}\,(f(\mathbf{U}_n^{(s)}),g(\mathbf{U}_n^{(s)}))=f(\mathbf{U}_n^{(s)})\}.$$

Let $\bar f\in\mathbb{Z}[x_1,\dots,x_s]$ be a homogeneous polynomial of the same degree as f obtained from f by dropping all monomials except those having the highest degree $\deg f$. Recall that $\deg f\ge 1$, so that $\bar f$ is not constant. Then, by the continuous mapping theorem combined with Slutsky's lemma,

$$\frac{f(\mathbf{U}_n^{(s)})}{n^{\deg f}}\xrightarrow{\mathrm{d}}\bar f(\mathbf{U}_\infty^{(s)}),\quad n\to\infty.\tag{4.6}$$

Therefore, it suffices to show that

$$\frac{\mathrm{GCD}\,(f(\mathbf{U}_n^{(s)}), g(\mathbf{U}_n^{(s)}))}{n^{\deg f}} \xrightarrow{\mathbb{P}} 0, \quad n \to \infty. \tag{4.7}$$

Using (4.5) and Lemma 5.6 in the Appendix we obtain, for some $c_{f,g} \in \mathbb{Z}$,

$$\begin{aligned}\mathrm{GCD}\,(f(\mathbf{U}_n^{(s)}), g(\mathbf{U}_n^{(s)})) &\le c_{f,g} \prod_{i,j=1}^{L} \mathrm{GCD}\,(h_i^{u_i}(\mathbf{U}_n^{(s)}), h_j^{v_j}(\mathbf{U}_n^{(s)})) \\ &= c_{f,g} \prod_{i=1}^{L} \mathrm{GCD}\,(h_i^{u_i}(\mathbf{U}_n^{(s)}), h_i^{v_i}(\mathbf{U}_n^{(s)})) \prod_{i \ne j} \mathrm{GCD}\,(h_i^{u_i}(\mathbf{U}_n^{(s)}), h_j^{v_j}(\mathbf{U}_n^{(s)})). \end{aligned} \tag{4.8}$$

For every pair of indices $i \ne j$, by Theorem 3.1 $\mathrm{GCD}\,(h_i^{u_i}(\mathbf{U}_n^{(s)}), h_j^{v_j}(\mathbf{U}_n^{(s)}))$ converges in distribution to an a.s. finite random variable, since h_i and h_j do not have a common factor. Thus, the last product in (4.8) is bounded in probability[1]. Therefore, (4.7) is a consequence of

$$\frac{1}{n^{\deg f}} \prod_{i=1}^{L} \mathrm{GCD}\,(h_i^{u_i}(\mathbf{U}_n^{(s)}), h_i^{v_i}(\mathbf{U}_n^{(s)})) = \frac{1}{n^{\deg f}} \prod_{i=1}^{L} (h_i(\mathbf{U}_n^{(s)}))^{\min(u_i, v_i)} \xrightarrow{\mathbb{P}} 0, \quad n \to \infty. \tag{4.9}$$

It remains to note that the degree of the polynomial $\prod_{i=1}^{L} h_i^{\min(u_i, v_i)}$ is strictly smaller than $\deg f$ because $u_i > v_i$ for at least one $i = 1, \dots, L$. This immediately implies (4.9). The proof is complete.

4.4. **Proof of Theorem 3.5.** As in the proof of Theorem 3.1 we start by checking that the random series defining $L_{f_1,\dots,f_m}$ converges a.s. By Proposition 2.5 all summands in the definition of $L_{f_1,\dots,f_m}$ are a.s. finite. Let us show that the series converges a.s. To this end, note that for any set of nonnegative integers $a_1, \dots, a_m \in \{0, 1, 2 \dots\}$ we have

$$\max_{i=1,\dots,m} a_i \ne \sum_{i=1}^{m} a_i \implies \exists i, j \in \{1, 2, \dots, m\}, i \ne j : \ a_i \ge 1, a_j \ge 1. \tag{4.10}$$

Thus, by the Borel-Cantelli lemma the series converges a.s. provided that

$$\sum_{p \in \mathcal{P}} \mathbb{P}\left\{\exists i, j \in \{1, 2, \dots, m\}, i \ne j : \ \lambda_p(f_i(\mathcal{V}_1, \dots, \mathcal{V}_s)) \ge 1, \lambda_p(f_j(\mathcal{V}_1, \dots, \mathcal{V}_s)) \ge 1\right\} < \infty. \tag{4.11}$$

[1]It actually converges because $(\mathrm{GCD}\,(h_i^{u_i}(\mathbf{U}_n^{(s)}), h_j^{v_j}(\mathbf{U}_n^{(s)})))_{i \ne j}$ converge jointly as is readily seen from Remark 3.2.

Eq. (4.2) implies

$$\sum_{p\in\mathcal{P}} \mathbb{P}\left\{\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)) \geq 1, \lambda_p(f_j(\mathcal{V}_1,\dots,\mathcal{V}_s)) \geq 1\right\} < \infty, \quad i \neq j,$$

where we used that f_i and f_j do not share a common factor of degree > 0. Thus, (4.11) follows by the union bound.

In order to prove (3.1) we fix $N \in \mathbb{N}$ and decompose NLCM similarly as in the proof of Theorem 3.1

$$\begin{aligned}\log \mathrm{NLCM}(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)})) &= \sum_{p\in\mathcal{P}} \log p \left(\max_{i=1,\dots,m} \lambda_p(f_i(\mathbf{U}_n^{(s)})) - \sum_{i=1}^m \lambda_p(f_i(\mathbf{U}_n^{(s)}))\right)\\ &= \left(\sum_{p\in\mathcal{P},p\leq N} + \sum_{p\in\mathcal{P},N<p\leq n} + \sum_{p\in\mathcal{P},p>n}\right) \log p \left(\max_{i=1,\dots,m} \lambda_p(f_i(\mathbf{U}_n^{(s)})) - \sum_{i=1}^m \lambda_p(f_i(\mathbf{U}_n^{(s)}))\right)\\ &=: \widetilde{Y}_1(n,N) + \widetilde{Y}_2(n,N) + \widetilde{Y}_3(n).\end{aligned}$$

By the continuous mapping theorem

$$\widetilde{Y}_1(n,N) \xrightarrow{\mathrm{d}} \sum_{p\in\mathcal{P},p\leq N} \log p \left(\max_{i=1,\dots,m} \lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s)) - \sum_{i=1}^m \lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))\right), \quad n\to\infty, \tag{4.12}$$

and the right-hand side, in turn, converges a.s. to $\log L_{f_1,\dots,f_m}$, as $N\to\infty$. Using (4.10) and the union bound we obtain

$$\begin{aligned}\mathbb{P}\{\widetilde{Y}_3(n)\neq 0\} &\leq \mathbb{P}\left\{\exists p\in\mathcal{P}: p>n, \max_{i=1,\dots,m} \lambda_p(f_i(\mathbf{U}_n^{(s)})) \neq \sum_{i=1}^m \lambda_p(f_i(\mathbf{U}_n^{(s)}))\right\}\\ &\leq \sum_{i,j=1,i\neq j}^m \mathbb{P}\left\{\exists p\in\mathcal{P}: p>n, \lambda_p(f_i(\mathbf{U}_n^{(s)}))\geq 1, \lambda_p(f_j(\mathbf{U}_n^{(s)}))\geq 1\right\}. \end{aligned}\tag{4.13}$$

The right-hand side converges to 0, as $n\to\infty$, by Proposition 5.1. By the union bound,

$$\mathbb{P}\{\widetilde{Y}_2(n,N) \neq 0\} \leq \sum_{i,j=1,i\neq j}^m \sum_{p\in\mathcal{P},N<p\leq n} \mathbb{P}\{\lambda_p(f_i(\mathbf{U}_n^{(s)})) \geq 1, \lambda_p(f_j(\mathbf{U}_n^{(s)})) \geq 1\}. \tag{4.14}$$

Thus, repeating verbatim the proof of (4.3), we obtain $\lim_{N\to\infty}\limsup_{n\to\infty}\mathbb{P}\{\widetilde{Y}_2(n,N)\neq 0\} = 0$. This finishes the proof of Eq. (3.1).

To check (3.2) we note that Corollaries 2.2 and 2.4 actually imply a stronger version of (4.12), namely

$$\left(\widetilde{Y}_1(n,N),\frac{\mathbf{U}_n^{(s)}}{n}\right)\xrightarrow{\mathrm{d}}\left(\sum_{p\in\mathcal{P},p\le N}\log p\left(\max_{i=1,\dots,m}\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))-\sum_{i=1}^{m}\lambda_p(f_i(\mathcal{V}_1,\dots,\mathcal{V}_s))\right),\mathbf{U}_\infty^{(s)}\right),$$

for every fixed $N\in\mathbb{N}$. Thus, by (4.13) and (4.14),

$$\left(\frac{\mathrm{LCM}(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)}))}{\prod_{j=1}^m f_j(\mathbf{U}_n^{(s)})},\frac{\mathbf{U}_n^{(s)}}{n}\right)\xrightarrow{\mathrm{d}}(L_{f_1,\dots,f_m},\mathbf{U}_\infty^{(s)}),\quad n\to\infty.$$

As in the proof of (4.6), the continuous mapping theorem and Slutsky's lemma imply

$$\left(\frac{\mathrm{LCM}(f_1(\mathbf{U}_n^{(s)}),\dots,f_m(\mathbf{U}_n^{(s)}))}{\prod_{j=1}^m f_j(\mathbf{U}_n^{(s)})},\frac{f_1(\mathbf{U}_n^{(s)})}{n^{\deg f_1}},\dots,\frac{f_m(\mathbf{U}_n^{(s)})}{n^{\deg f_m}}\right)$$
$$\xrightarrow{\mathrm{d}}(L_{f_1,\dots,f_m},\bar{f}_1(\mathbf{U}_\infty^{(s)}),\dots,\bar{f}_m(\mathbf{U}_\infty^{(s)})),\quad n\to\infty,$$

which immediately yields (3.2).

5. Absence of large common prime divisors

Proposition 5.1. *Let $f_1,\dots,f_m\in\mathbb{Z}[x_1,\dots,x_s]$ be $m\in\mathbb{N}$ non-zero polynomials that do not have a common factor of degree >0. Let $\mathbf{U}_n^{(s)}$ be uniformly distributed on $\{1,\dots,n\}^s$. Then,*

$$\lim_{n\to\infty}\mathbb{P}\{\exists p\in\mathcal{P}:p\ge n,f_1(\mathbf{U}_n^{(s)})\equiv\dots\equiv f_m(\mathbf{U}_n^{(s)})\equiv 0(\mathrm{mod}\,p)\}=0.$$

For the proof we need several lemmas.

Lemma 5.2. *For every number $M\in\mathbb{N}$ there is a number $B=B(M)$ depending only on M such that the following holds for every $n\in\mathbb{N}$. Let $g_1,\dots,g_m\in\mathbb{Z}[x]$ be polynomials in one variable such that:*

(a) *$m\le M$ and $\deg g_i\le M$ for all $i=1,\dots,m$;*
(b) *the absolute values of all coefficients of $g_1,\dots,g_m$ are bounded above by $M\cdot n^M$;*
(c) *$g_1,\dots,g_m$ do not have a common factor in $\mathbb{Q}[x]$ of degree >0.*

Then, we can find polynomials $a_1,\dots,a_m\in\mathbb{Z}[x]$ and a number $A\in\mathbb{N}$ with $A\le Bn^B$ such that $a_1g_1+\dots+a_mg_m=A$.

Let us note that since $\mathbb{Q}[x]$ is a principal ideal domain, there exist polynomials $b_1,\dots,b_m\in\mathbb{Q}[x]$ with rational coefficients such that $b_1g_1+\dots+b_mg_m=1$. Multiplying these polynomials by a suitable number A we can make their coefficients integer.

Thus, the only nontrivial claim in the above lemma is the bound $A \le Bn^B$, which we claim to hold uniformly over all $g_1,\dots,g_m$ and n satisfying the above conditions. This uniformity will be crucial in what follows.

Proof. Essentially, we apply the Euclidean algorithm while tracking the size of coefficients. We use induction over $\deg g_1 + \dots + \deg g_m$ (where we put $\deg 0 := 0$). If this number is 0, then all polynomials g_i are constant but not all of them are zero by Condition (c). We can put $\alpha_i := 1$ if $g_i \ge 0$ and $\alpha_i := -1$ if $g_i \le 0$. Then, $A = |g_1| + \dots + |g_m| \le mMn^M$, so that we can put $B := M^2$.

Let now $\deg g_1 + \dots + \deg g_m \ge 1$ and suppose that we proved the lemma for smaller values of this sum. Without loss of generality let $\deg g_1 \ge \max\{\deg g_2,\dots,\deg g_m\}$. Then, $\deg g_1 \ge 1$. By Condition (c), some of the polynomials $g_2,\dots,g_m$ is not identically zero. Let $g_2 \not\equiv 0$. Write

$$g_1(x) = c_p x^p + \dots + c_0, \quad g_2(x) = d_q x^q + \dots + d_0, \quad c_i, d_j \in \mathbb{Z}, \quad p \ge q, \quad p \ge 1.$$

Consider now instead of the tuple $(g_1, g_2, \dots, g_m)$ the tuple $(d_q g_1 - c_q g_2 x^{p-q}, g_2, \dots, g_m)$. Note that $\deg(d_q g_1 - c_q g_2 x^{p-q}) < \deg g_1$. Also, the coefficients of the polynomials from the new tuple are integer and bounded above by $2M^2 n^{2M}$, so , so that we can apply the induction assumption to the new tuple with M replaced by $2M^2$. It follows that

$$\tilde{a}_1(x) \cdot (d_q g_1(x) - c_q g_2(x) x^{p-q}) + \tilde{a}_2(x) g_2(x) + \dots + \tilde{a}_m(x) g_m(x) = A$$

for suitable $\tilde{a}_1,\dots,\tilde{a}_m \in \mathbb{Z}[x]$ and a number $A \in \mathbb{N}$, $A \le Bn^B$. After regrouping the terms this gives the claim. □

Lemma 5.3. *For every number $M \in \mathbb{N}$ there is $C = C(M)$ depending only on M such that the following holds for all $n \in \mathbb{N}$. Let $g_1,\dots,g_m \in \mathbb{Z}[x]$ be polynomials satisfying Conditions (a), (b), (c) of Lemma 5.2 and such that, additionally,*

(d) *There is no prime number $p \ge n$ dividing all coefficients of $g_1,\dots,g_m$.*

Then, for the random variable U_n uniformly distributed on $\{1,\dots,n\}$ we have

$$\mathbb{P}\{\exists p \in \mathcal{P} : p \ge n, g_1(U_n) \equiv \dots \equiv g_m(U_n) \equiv 0 (\mathrm{mod}\, p)\} \le C/n.$$

Proof. By Lemma 5.2 we have $a_1 g_1 + \dots + a_m g_m = A$ for some $A \in \mathbb{N}$ with $A \le Bn^B$ and some polynomials $a_1,\dots,a_m \in \mathbb{Z}[x]$ with integer coefficients. So, every common prime divisor $p \ge n$ of $g_1(U_n),\dots,g_m(U_n)$ must be a divisor of A. The number A has at most $B+1$ distinct prime divisors $p_1,\dots,p_\ell \ge n$, where we assumed that $n \ge B$. (For $n \le B$ the

claim is trivial since there are only finitely many choices for $g_1, \dots, g_m$.) So,

$$\mathbb{P}\{\exists p \in \mathcal{P} : p \geq n, g_1(U_n) \equiv \dots \equiv g_m(U_n) \equiv 0 (\mathrm{mod}\, p)\} \\ \leq \sum_{i=1}^{\ell} \mathbb{P}\{g_1(U_n) \equiv \dots \equiv g_m(U_n) \equiv 0 (\mathrm{mod}\, p_i)\}.$$

Fix some $i \in \{1, \dots, \ell\}$. Some of the coefficients of some polynomial g_j is not divisible by p_i, by Condition (d). So, the reduction of g_j modulo p_i is a non-zero polynomial. Thus, it has at most $\deg g_j \leq M$ zeros over $\mathbb{F}_{p_i}$. Since $p_i \geq n$ and hence all numbers $1, \dots, n$ have different remainders modulo p_i, there are at most M possible values of U_n for which $g_j(U_n)$ is divisible by p_i. It follows that

$$\mathbb{P}(g_1(U_n) \equiv \dots \equiv g_m(U_n) \equiv 0 \mod p_i) \leq M/n.$$

The claim follows with $C := (B+1)M$ since $\ell \leq B+1$. □

It is well known that the property of 2 univariate polynomials to have a non-constant common divisor can be expressed as a polynomial condition on their coefficients. Given next is a generalization to any finite number of polynomials which is also a standard result in algebra, see [26, 27].

Lemma 5.4 (Resultant)**.** *Let R be an integral domain, $m \in \mathbb{N}_0$. Fix "degrees" $d_1, \dots, d_m \in \mathbb{N}_0$. There exist $L \in \mathbb{N}$ and polynomials $W_1, \dots, W_L$ in $d_1 + \dots + d_m + m$ variables (having integer coefficients) with the property that polynomials $Q_1, \dots, Q_m \in R[x]$ with $\deg Q_1 = d_1, \dots, \deg Q_m = d_m$ have a nonconstant common divisor in $R[x]$ if and only if all polynomials $W_1, \dots, W_L$, evaluated at the coefficients of $Q_1, \dots, Q_m$, vanish.*

Proof. For $m = 2$ polynomials, we can take $L = 1$ and W_1 to be the Sylvester resultant of Q_1 and Q_2. For $m \geq 3$, we introduce new variables $u_2, \dots, u_m$ and observe that $Q_1, \dots, Q_m$ have a common factor in $R[x]$ if and only if Q_1 and $u_2 Q_2 + \dots + u_m Q_m$ have a common factor in $R[x, u_1, \dots, u_m] \equiv R'[x]$, where $R' = R[u_1, \dots, u_m]$ is also an integral domain. The Sylvester resultant of Q_1 and $u_2 Q_2 + \dots + u_m Q_m$, considered as elements of $R'[x]$, is a polynomial in the coefficients of $Q_1, \dots, Q_m$ and the variables $u_2, \dots, u_m$. The resultant can be written as a sum of finitely many monomials of the form $u_2^{\ell_2} \dots u_m^{\ell_m}$ multiplied by certain polynomials in the coefficients of $Q_1, \dots, Q_m$. Denote these polynomials (in some order) by $W_1, \dots, W_L$. Then, $W_1 = \dots = W_L = 0$ if and only if the resultant of Q_1 and $u_2 Q_2 + \dots + u_m Q_m$ vanishes, which is the case if and only if the polynomials $Q_1, \dots, Q_m$ have a common factor. □

Remark 5.5. *If* $\deg Q_1 \le d_1, \dots, \deg Q_m \le d_m$*, then the "only if" direction of the above claim holds with the same proof: if* $Q_1, \dots, Q_m$ *have a common factor, then* $W_1, \dots, W_L$*, evaluated at the coefficients of* $Q_1, \dots, Q_m$*, vanish.*

Proof of Proposition 5.1. We use induction over the number of variables s. For $s = 1$, the claim follows immediately from Lemma 5.3.

Take some $s \in \{2, 3, \dots\}$ and assume we proved the proposition for polynomials of $s-1$ variables. We prove it for polynomials with s variables. The idea is to fix the numbers $x_1, \dots, x_{s-1} \in \{1, \dots, n\}$ and consider the polynomials $g_i(x_s) := f_i(x_1, \dots, x_{s-1}, x_s)$ as univariate polynomials in x_s. Clearly, $g_i \in \mathbb{Z}[x_s]$. For a sufficiently large $M \in \mathbb{N}$, Conditions (a) and (b) of Lemma 5.2 are fulfilled. Let C_n, respectively D_n, be the sets of all $(x_1, \dots, x_{s-1}) \in \{1, \dots, n\}^{s-1}$ for which $g_1, \dots, g_m$ fail to satisfy Condition (c), respectively, (d). Let G_n be the complement of $C_n \cup D_n$, that is the set of all $(x_1, \dots, x_{s-1}) \in \{1, \dots, n\}^{s-1}$ for which both Conditions (c) and (d) are fulfilled. Write $\Pi(x_1, \dots, x_s) = (x_1, \dots, x_{s-1})$ for the projection map removing the last coordinate. Then,

$$\begin{aligned}
&\mathbb{P}\{\exists p \in \mathcal{P} : p \ge n, f_1(\mathbf{U}_n^{(s)}) \equiv \dots \equiv f_m(\mathbf{U}_n^{(s)}) \equiv 0 \mod p, \Pi\mathbf{U}_n^{(s)} \in G_n)\} \\
&= \frac{1}{n^{s-1}} \sum_{(x_1,\dots,x_{s-1}) \in G_n} \mathbb{P}\{\exists p \in \mathcal{P} : p \ge n, f_1(x_1, \dots, x_{s-1}, U_n) \equiv \dots \\
&\qquad\qquad \equiv f_m(x_1, \dots, x_{s-1}, U_n) \equiv 0 (\mathrm{mod}\, p)\} \\
&\le \frac{1}{n^{s-1}} \sum_{(x_1,\dots,x_{s-1}) \in G_n} \frac{C}{n} \le \frac{C}{n},
\end{aligned}$$

where we applied Lemma 5.3 to the polynomials $g_i(x_s) = f_i(x_1, \dots, x_{s-1}, x_s)$. Note that the constant C in Lemma 5.3 does not depend on the choice of $x_1, \dots, x_{s-1} \in \{1, \dots, n\}$.

Let us check that $\mathbb{P}\{\Pi\mathbf{U}_n^{(s)} \in D_n\} \to 0$ as $n \to \infty$. Recall that $\Pi\mathbf{U}_n^{(s)} \in D_n$ means that all coefficients of the univariate polynomials $g_1(\Pi\mathbf{U}_n^{(s)}, x_s), \dots, g_m(\Pi\mathbf{U}_n^{(s)}, x_s)$ have a common prime divisor $p \ge n$. Consider the ring $R = \mathbb{Z}[x_1, \dots, x_{s-1}]$. Then, we can view $h_i(x_s) := f_i(x_1, \dots, x_{s-1}, x_s) \in R[x_s]$ as a polynomial in x_s with coefficients in R. Let $q_1, \dots, q_L \in R$ be the coefficients of the polynomials $h_1(x_s), \dots, h_m(x_s)$ listed in some order. Then, $q_1, \dots, q_L$ have no nonconstant common divisor in R since otherwise $f_1, \dots, f_m$ would have a nonconstant common divisor. We can then apply the induction assumption to $q_1, \dots, q_L$ (which depend on $s-1$ variables and for which we assume Proposition 5.1 to hold). This yields

$$\lim_{n\to\infty} \mathbb{P}\{\exists p \in \mathcal{P} : p \ge n, q_1(\Pi\mathbf{U}_n^{(s)}) \equiv \dots \equiv q_L(\Pi\mathbf{U}_n^{(s)}) \equiv 0 (\mathrm{mod}\, p)\} = 0.$$

This proves that $\mathbb{P}\{\Pi\mathbf{U}_n^{(s)} \in D_n\} \to 0$ as $n \to \infty$.

Let us check that $\mathbb{P}\{\Pi\mathbf{U}_n^{(s)} \in C_n\} \to 0$, $n \to \infty$. We again consider $h_i(x_s) \in R[x_s]$ as polynomials in x_s with coefficients in the integral domain $R = \mathbb{Z}[x_1, \dots, x_{s-1}]$. By the hypothesis of Proposition 5.1, these polynomials do not have a common factor in $R[x_s] = \mathbb{Z}[x_1, \dots, x_s]$ of degree > 0. By Lemma 5.4 this implies that certain polynomial, say W_1, of their coefficients (which are elements in R) does not vanish in R. Inserting in W_1 the coefficients (which are polynomials in $x_1, \dots, x_{s-1}$), we obtain certain *non-zero* polynomial $W_2 \in \mathbb{Z}[x_1, \dots, x_{s-1}]$. Now, $\Pi\mathbf{U}_n \in C_n$ means that the polynomials $g_1(\Pi\mathbf{U}_n, x_s), \dots, g_m(\Pi\mathbf{U}_n, x_s)$, viewed as elements in $\mathbb{Z}[x_s]$, have a common non-constant factor, which, by Lemma 5.4 and Remark 5.5, implies that $W_2(\Pi\mathbf{U}_n) = 0$. Since $W_2 \not\equiv 0$, we can apply Lemma 5.8 from the Appendix, which yields

$$\mathbb{P}\{\Pi\mathbf{U}_n^{(s)} \in C_n\} \le \mathbb{P}\{W_2(\Pi\mathbf{U}_n^{(s)} = 0\} \le \frac{\deg W_2}{n},$$

which converges to 0 as $n \to \infty$. □

Appendix

Lemma 5.6. *For $a_1, \dots, a_n, b_1, \dots, b_m \in \mathbb{N}$ we have*

$$\mathrm{GCD}\,(a_1 \cdots a_n, b_1 \cdots b_m) \le \prod_{i=1}^{n} \prod_{j=1}^{m} \mathrm{GCD}\,(a_i, b_j).$$

Proof. Using a crude bound

$$\min(x_1 + \cdots + x_n, y_1 + \cdots + y_m) \le \sum_{i=1}^{n} \sum_{j=1}^{m} \min(x_i, y_j), \quad x_i, y_j \ge 0,$$

we obtain

$$\begin{aligned}\mathrm{GCD}\,(a_1 \cdots a_n, b_1 \cdots b_m) &= \prod_{p \in \mathcal{P}} p^{\min(\sum_{i=1}^n \lambda_p(a_i), \sum_{j=1}^m \lambda_p(b_j))} \le \prod_{p \in \mathcal{P}} p^{\sum_{i=1}^n \sum_{j=1}^m \min(\lambda_p(a_i), \lambda_p(b_j))} \\ &\le \prod_{i=1}^{n} \prod_{j=1}^{m} \prod_{p \in \mathcal{P}} p^{\min(\lambda_p(a_i), \lambda_p(b_j))} = \prod_{i=1}^{n} \prod_{j=1}^{m} \mathrm{GCD}\,(a_i, b_j).\end{aligned}$$

□

Lemma 5.7. *Fix $p \in \mathcal{P}$. Let $f \in \mathbb{Q}_p[x_1, \dots, x_s]$ be a non-zero polynomial over p-adic rationals and μ_p be the Haar measure on $\mathbb{Z}_p$. Then*

$$\mu_p^{\otimes s}(\{x = (x_1, \dots, x_s) \in \mathbb{Z}_p^s : f(x) = 0\}) = 0.$$

Proof. We use induction over s. For $s = 1$, the polynomial f has only finitely many zeros in $\mathbb{Z}_p$ since $f \not\equiv 0$, hence the claim is true. Suppose the claim is true for polynomials of $s-1$ variables. Consider some non-zero polynomial $f \in \mathbb{Q}_p[x_1,\dots,x_s]$. One of the variables (without loss of generality, x_1) appears in f in degree ≥ 1. Write $f(x_1,\dots,x_s) = \sum_{j=0}^{d} x_1^j a_j(x_2,\dots,x_s)$, where $d \geq 1$, $a_j \in \mathbb{Q}_p[x_2,\dots,x_s]$ and $a_d \not\equiv 0$. By induction hypothesis, the set $E \subset \mathbb{Z}_p^{s-1}$ consisting of the zeros of the polynomial $a_d(x_2,\dots,x_s)$ is a $\mu_p^{\otimes(s-1)}$-zero set. Hence,

$$\mu_p^{\otimes s}(\{x \in \mathbb{Z}_p^s : f(x) = 0, (x_2,\dots,x_s) \in E\}) = 0.$$

On the other hand, for every fixed $(x_2,\dots,x_s) \in \mathbb{Z}_p^{s-1} \setminus E$, the polynomial $x_1 \mapsto f(x_1,\dots,x_s)$ is non-zero and has at most d roots. By Fubini's theorem,

$$\mu_p^{\otimes s}(\{x \in \mathbb{Z}_p^s : f(x) = 0, (x_2,\dots,x_s) \notin E\}) = 0,$$

and the proof is complete. □

Proposition 5.8 (The Schwartz-Zippel bound)**.** *Let $Q \in \mathbb{Z}[x_1,\dots,x_s]$ be a non-zero polynomial and let $\mathbf{U}_n^{(s)} = (U_{n,1},\dots,U_{n,s})$ be uniformly distributed on $\{1,\dots,n\}^s$. Then,*

$$\mathbb{P}\{Q(\mathbf{U}_n^{(s)}) = 0\} \leq \frac{\deg Q}{n}.$$

Acknowledgments

This work has been accomplished during AM's visit to Queen Mary University of London as Leverhulme Visiting Professor in July-December 2023. AM gratefully acknowledges financial support from the Leverhulme Trust. ZK has been supported by the German Research Foundation under Germany's Excellence Strategy EXC 2044 – 390685587, Mathematics Münster: Dynamics - Geometry - Structure.

References

[1] Abramovich, S., and Nikitin, Y. Y. (2017). On the probability of co-primality of two natural numbers chosen at random: from Euler identity to Haar measure on the ring of adeles, *Bernoulli News* **24**, pp. 7–13.

[2] Alexander, K. S. and Baclawski, K. and Rota, G.-C. (1993). A stochastic interpretation of the Riemann zeta function, *Proc. Nat. Acad. Sci. U.S.A.*, **90**, pp. 697–699.

[3] Avdeeva, M. and Cellarosi, F. and Sinai, Ya. G. (2016). Ergodic and statistical properties of $\mathcal{B}$-free numbers, *Teor. Veroyatn. Primen.*, **61**, pp. 805–829.

[4] Billingsley, P. (2013). *Convergence of probability measures*. John Wiley & Sons.

[5] Bodin, A. and Débes, P. (2022). Coprime values of polynomials in several variables, ArXiv preprint available at .

[6] Bostan, A., Marynych, A. and Raschel, K. (2019). On the least common multiple of several random integers, *J. Number Theory*, **204**, pp. 113–133.

[7] Cesaro, E. (1885). Sur le plus grand commun diviseur de plusieurs nombres, *Annali di Matematica Pura ed Applicata* , **13**, pp. 291–294.

[8] Christopher, J. (1956). The asymptotic density of some k-dimensional sets, *Amer. Math. Monthly*, **63**, pp. 399–401.

[9] Cohen, E. (1960). Arithmetical functions of a greatest common divisor. I. *Proc. Amer. Math. Soc.*, **11**, pp. 164–171.

[10] Demangos, L. and Longhi, I. (2021). Densities on Dedekind domains, completions and Haar measure, ArXiv preprint available at .

[11] Dirichlet, G. L. (1849). Über die Bestimmung der mittleren Werthe in der Zahlentheorie, *Abhandlungen der Königlich Preussischen Akademie der Wissenschaften*, pp. 69–83.

[12] Duy, T. K. (2011). On the distribution of k-th power free integers, *Osaka J. Math.*, **48**, pp. 1027–1045.

[13] Duy, T. K. and Takanobu, S. (2013). On the distribution of k-th power free integers, II, *Osaka J. Math.*, **50**, pp. 687–713.

[14] Fernández, J. L. and Fernández, P. (2021). Divisibility properties of random samples of integers, *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, **115**, paper no. 26, 35.

[15] Fried, M. and Jarden, M. (2005). *Field arithmetic*. Springer.

[16] Ghorpade, S. R. and Lachaud, G. (2002). Ghorpade, S. R. and Lachaud, G. (2002). Number of Solutions of Equations over Finite Fields and a Conjecture of Lang and Weil. In: Agarwal, A.K., Berndt, B.C., Krattenthaler, C.F., Mullen, G.L., Ramachandra, K., Waldschmidt, M. (eds) Number Theory and Discrete Mathematics. Trends in Mathematics. Birkhäuser, Basel.

[17] Greenleaf, N. (1965). Irreducible Subvarieties and Rational Points, *American J. Math.*, **87**, pp. 25–31.

[18] Indlekofer, K.-H. (2002). New approach to probabilistic number theory, *Theory Stoch. Process.*, **8**, pp. 136–153.

[19] Indlekofer, K.-H. (2002). Number theory—probabilistic, heuristic, and computational approaches, *Comput. Math. Appl.*, **43**, pp. 1035–1061.

[20] Kubota, H. and Sugita, H. (2002). Probabilistic proof of limit theorems in number theory by means of adeles, *Kyushu J. Math.*, **56**, pp. 391–404.

[21] Lang, S. (1986). *Algebraic Number Theory*, Springer.

[22] Lang, S. and Weil, A. (1954). Number of points of varieties in finite fields, *American J. Math.*, **76**, pp. 819–827.

[23] Lovas, R. L. and Mező, I. (2015). Some observations on the Furstenberg topological space, *Elem. Math.*, **70**, pp. 103–116.

[24] Novoselov, E. V. (1961). Integration on a bicompact ring and its applications to number theory, *Izv. Vysš. Učebn. Zaved. Matematika*, **3**, pp. 66–79.

[25] Novoselov, E. V. (1964). A new method in probabilistic number theory, *Izv. Akad. Nauk SSSR Ser. Mat.* **28**, pp. 307–364.

[26] McCallum, S. and and Winkler F. (2018). Resultants: algebraic and differential. Techn. Rep. RISC-18-08, J. Kepler University, Linz, Austria.

[27] McCallum, S. (1999). Factors of iterated resultants and discriminants, *J.Symb. Comp.*, **27**, pp. 367–385.

[28] Poonen, B. (2003). Squarefree values of multivariable polynomials, *Duke Mathematical Journal*, **118**, pp. 353–373.

[29] Prüfer, H. (1925). Neue Begründung der algebraischen Zahlentheorie, *Math. Ann.*, **94**, pp. 198–243.

[30] Schmidt, W. (1976). *Equations over Finite Fields: An Elementary Approach*, Springer.

[31] Sugita, H. and Takanobu, S. (2003). The probability of two integers to be co-prime, revisited—on the behavior of CLT-scaling limit, *Osaka J. Math.*, **40**, pp. 945–976.

[32] Xiong, M. (2009). The Erdős-Kac theorem for polynomials of several variables, *Proc. Amer. Math. Soc.*, **137**, pp. 2601–2608.