A local to global principle for expected values

Micheli, Giacomo ; Schraven, Severin ; Weger, Violetta

DOI: https://doi.org/10.1016/j.jnt.2021.05.018

Originally published at:
Micheli, Giacomo; Schraven, Severin; Weger, Violetta (2022). A local to global principle for expected values. Journal of Number Theory, 238:1-16.
DOI: https://doi.org/10.1016/j.jnt.2021.05.018

Journal of Number Theory 238 (2022) 1–16

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

A local to global principle for expected values

Giacomo Micheli [a], Severin Schraven [b], Violetta Weger [b,*]

[a] *Department of Mathematics, University of South Florida, Tampa, FL 33620, United States of America*
[b] *Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland*

ARTICLE INFO

Article history:
Received 21 August 2020
Received in revised form 16 May 2021
Accepted 17 May 2021
Available online 27 August 2021
Communicated by F. Pellarin

Keywords:
Densities
Mean

ABSTRACT

This paper constructs a new local to global principle for expected values over free $\mathbb{Z}$-modules of finite rank. In our strategy we use the same philosophy as Ekedahl's Sieve for densities, later extended and improved by Poonen and Stoll in their local to global principle for densities. We show that under some additional hypothesis on the system of p-adic subsets used in the principle, one can use p-adic measures also when one has to compute expected values (and not only densities). Moreover, we show that our additional hypotheses are sharp, in the sense that explicit counterexamples exist when any of them is missing. In particular, a system of p-adic subsets that works in the Poonen and Stoll principle is not guaranteed to work when one is interested in expected values instead of densities. Finally, we provide both new applications of the method, and immediate proofs for known results.

* Corresponding author.
E-mail addresses: gmicheli@usf.edu (G. Micheli), severin.schraven@math.uzh.ch (S. Schraven), violetta.weger@math.uzh.ch (V. Weger).

https://doi.org/10.1016/j.jnt.2021.05.018

1. Introduction

Let $\mathbb{Z}$ be the set of integers and d be a positive integer. The problem of computing the "probability", that a randomly chosen element in $\mathbb{Z}^d$ has a certain property, has a long history dating back to Cesáro [2,3].

Since no uniform probability distribution exists over $\mathbb{Z}$, one introduces the notion of density. The density of a set $T \subset \mathbb{Z}^d$ is defined to be

$$\rho(T) = \lim_{H\to\infty} \frac{|T \cap [-H,H]^d|}{(2H)^d},$$

if the limit exists.

Density results over $\mathbb{Z}^d$ have received a great deal of interest recently [4,6–11,13–15,17–20,23,24].

In [21, Lemma 20] Poonen and Stoll show that the computation of densities of many sets $S \subseteq \mathbb{Z}^d$ defined by *local* conditions (in the p-adic sense) can be reduced to measuring the corresponding subsets of the p-adic integers. This technique is an extension of Ekedahl's Sieve [5]. An even more general result is [1, Proposition 3.2]. The general philosophy is that, under some reasonable assumptions, one should be able to treat the p-adic measures of infinitely many sets $U_p \subseteq \mathbb{Z}_p^d$ independently when one looks at the density of the corresponding set $\bigcap_{p\in\mathcal{P}} U_p^C \cap \mathbb{Z}^d$ over the integers.

In [12] the authors computed the expected number of primes, for which an Eisenstein polynomial satisfies the criterion of Eisenstein. In this paper we prove that this is a special case of a much more general principle that allows to compute expected values from p-adic measures of nicely chosen systems of p-adic sets. In fact, in this article we give a new method, in the spirit of Poonen and Stoll's principle, to compute expected values of the "random variable" that counts how many times an element is expected to be in one of the U_p's. First, we show that the hypothesis of Poonen and Stoll is not sufficient to guarantee a local to global principle for expected values (see Example 12). This led us to add two additional hypotheses on the system $(U_p)_{p\in\mathcal{P}}$, that appears in the Poonen and Stoll principle, in order to prove Theorem 13, the main theorem of this article. The additional hypotheses we require are sharp and necessary, as Examples 15 and 16 show.

With this new local to global principle one can for example compute for non-coprime m-tuples of integers how many prime factors they have in common on average, or for rectangular non-unimodular matrices how many primes divide all the basic minors on average. Also the result of [12] considering the number of primes for which an Eisenstein polynomial satisfies the criterion of Eisenstein follows directly.

The paper is organized as follows: in Section 2 we will recall the local to global principle by Poonen and Stoll. In Section 3 we will introduce the definition of expected value of a system of $(U_\nu)_{\nu\in M_\mathbb{Q}}$ and then state and prove Theorem 13, the main theorem of this paper.

In Section 4 we give some applications of our main theorem that allow very fast computations of expected values over $\mathbb{Z}^d$ (see for example [12] compared with Corollary 18).

2. Preliminaries

Definition 1. Let d be a positive integer. The *density* of a set $T \subset \mathbb{Z}^d$ is defined to be

$$\rho(T) = \lim_{H\to\infty} \frac{|T \cap [-H,H]^d|}{(2H)^d},$$

if the limit exists. Then one defines the upper density $\bar{\rho}$ and the lower density $\underline{\rho}$ equivalently with the lim sup and the lim inf respectively.

For convenience, let us restate here the lemma of Poonen and Stoll in [21, Lemma 20]. If S is a set, then we denote by 2^S its powerset and by S^C its complement. Let $\mathcal{P}$ be the set of primes and $M_{\mathbb{Q}} = \{\infty\} \cup \mathcal{P}$ be the set of all places of $\mathbb{Q}$, where we denote by ∞ the unique Archimedean place of $\mathbb{Q}$. Let μ_∞ denote the Lebesgue measure on $\mathbb{R}^d$ and μ_p the normalized Haar measure on $\mathbb{Z}_p^d$. For T a subset of a metric space, let us denote by $\partial(T)$ its boundary. By $\mathbb{R}_{\geq 0}$ we denote the non-negative reals.

Theorem 2 *([21, Lemma 20]). Let d be a positive integer. Let $U_\infty \subset \mathbb{R}^d$, such that $\mathbb{R}_{\geq 0} \cdot U_\infty = U_\infty$ and $\mu_\infty(\partial(U_\infty)) = 0$. Let $s_\infty = \frac{1}{2^d}\mu_\infty(U_\infty \cap [-1,1]^d)$. For each prime p, let $U_p \subset \mathbb{Z}_p^d$, such that $\mu_p(\partial(U_p)) = 0$ and define $s_p = \mu_p(U_p)$. Define the following map*

$$\begin{aligned} P : \mathbb{Z}^d &\to 2^{M_{\mathbb{Q}}}, \\ A &\mapsto \{\nu \in M_{\mathbb{Q}} \mid A \in U_\nu\}. \end{aligned}$$

If the following is satisfied:

$$\lim_{M\to\infty} \bar{\rho}\left(\left\{A \in \mathbb{Z}^d \mid A \in U_p \text{ for some prime } p > M\right\}\right) = 0, \tag{2.1}$$

then:

i) $\sum_{\nu \in M_{\mathbb{Q}}} s_\nu$ *converges.*
ii) *For $\mathcal{S} \subset 2^{M_{\mathbb{Q}}}$, $\rho(P^{-1}(\mathcal{S}))$ exists, and defines a measure on $2^{M_{\mathbb{Q}}}$.*
iii) *For each finite set $S \in 2^{M_{\mathbb{Q}}}$, we have that*

$$\rho(P^{-1}(\{S\})) = \prod_{\nu \in S} s_\nu \prod_{\nu \notin S} (1 - s_\nu),$$

and if $\mathcal{S}$ consists of infinite subsets of $2^{M_{\mathbb{Q}}}$, then $\rho(P^{-1}(\mathcal{S})) = 0$.

Remark 3. Observe that in Theorem 2 one can always choose the finite set S to be the empty set by replacing U_ν by U_ν^C for $\nu \in S$.

To show that (2.1) is satisfied, one can often apply the following useful lemma, that can be deduced from the result in [5].

Lemma 4 *([22, Lemma 2]). Let d and M be positive integers. Let $f, g \in \mathbb{Z}[x_1, \ldots, x_d]$ be relatively prime. Define*

$$S_M(f,g) = \left\{ A \in \mathbb{Z}^d \mid f(A) \equiv g(A) \equiv 0 \mod p \text{ for some prime } p > M \right\},$$

then

$$\lim_{M \to \infty} \bar{\rho}(S_M(f,g)) = 0.$$

3. The local to global principle for expected values

For a fixed $\nu \in M_\mathbb{Q}$ and U_ν as in Theorem 2, the density of $U_\nu \cap \mathbb{Z}^d$ can be computed as follows.

Corollary 5. *Let $\nu \in M_\mathbb{Q}$ and U_ν be chosen as in Theorem 2, then*

$$\rho(U_\nu \cap \mathbb{Z}^d) = s_\nu.$$

Proof. In order to prove the claim, we want to apply Theorem 2 to a suitably chosen system $(U'_{\nu'})_{\nu' \in M_\mathbb{Q}}$. For this we set

$$U'_{\nu'} = \begin{cases} U_\nu & \nu' = \nu, \\ \emptyset & \nu' \neq \nu, \end{cases}$$

and let

$$P' : \mathbb{Z}^d \to 2^{M_\mathbb{Q}}, \quad A \mapsto \{\nu \in M_\mathbb{Q} \mid A \in U'_\nu\}.$$

Then by Theorem 2 we have $\rho(U_\nu \cap \mathbb{Z}^d) = \rho(P'^{-1}(\{\nu\})) = s_\nu$. □

We now introduce the main definition of this paper, namely the mean of a system $(U_\nu)_{\nu \in M_\mathbb{Q}}$.

Definition 6. Let I denote the set of elements living in infinitely many U_ν, i.e.,

$$I = \left\{ A \in \mathbb{Z}^d \mid A \in U_\nu \text{ for infinitely many } \nu \in M_\mathbb{Q} \right\}$$

and denote by $[-H,H]^d_I = ([-H,H]^d \cap \mathbb{Z}^d) \setminus I$. Let H and d be positive integers and assume that $(U_\nu)_{\nu\in M_\mathbb{Q}}$ satisfy the assumptions of Theorem 2, then we define *the expected value of the system* $(U_\nu)_{\nu\in M_\mathbb{Q}}$ to be

$$\mu = \lim_{H\to\infty} \frac{\sum_{A\in[-H,H]^d_I} \mid \{\nu \in M_\mathbb{Q} \mid A \in U_\nu\} \mid}{(2H)^d},$$

if it exists.

This limit essentially gives the expected value of the number of places ν, such that a "random" element in $\mathbb{Z}^d$ is in U_ν.

Remark 7. The reader should notice that the mean of the system $(U_\nu)_{\nu\in M_\mathbb{Q}}$ should be thought of as the "expected value" of the function $A \mapsto |P(A)|$, where P is the map of Theorem 2.

The omission of elements in I, as in Definition 6, is legitimate, as I has density zero.

Lemma 8. *Let* $(U_\nu)_{\nu\in M_\mathbb{Q}}$ *be as in Theorem 2. Then we have*

$$\rho(I) = \rho(\{A \in \mathbb{Z}^d \mid A \in U_\nu \textit{ for infinitely many } \nu \in M_\mathbb{Q}\}) = 0.$$

Proof. Since U_ν were chosen as in Theorem 2, Condition (2.1) holds, i.e.,

$$\lim_{M\to\infty} \bar{\rho}\left(\left\{A \in \mathbb{Z}^d \mid A \in U_p \text{ for some prime } p > M\right\}\right) = 0.$$

Let us denote by

$$C_M = \left\{A \in \mathbb{Z}^d \mid A \in U_p \text{ for some prime } p > M\right\}.$$

Clearly $I \subset C_M$ for all $M \in \mathbb{N}$, hence

$$\overline{\rho}(I) \leq \lim_{M\to\infty} \overline{\rho}(C_M) = 0$$

and thus $\rho(I) = 0$. $\square$

Since the quantity $\mid \{\nu \in M_\mathbb{Q} \mid A \in U_\nu\} \mid$ will play a crucial role throughout this paper, we will introduce the following notation: for $U = (U_\nu)_{\nu\in M_\mathbb{Q}}$, we denote by

$$\omega_U(A) =\mid \{\nu \in M_\mathbb{Q} \mid A \in U_\nu\} \mid .$$

Definition 9. For a set T, for which we can compute its density via the local to global principle as in Theorem 2, we say that a *system* $(U_\nu)_{\nu\in M_\mathbb{Q}}$ *corresponds to* T, if $T^C = P^{-1}(\{\emptyset\})$.

Observe that we can restrict Definition 6 to subsets of $\mathbb{Z}^d$, i.e., we define the expected value of the system $(U_\nu)_{\nu\in M_\mathbb{Q}}$ restricted to $T\subset\mathbb{Z}^d$ to be

$$\mu_T=\lim_{H\to\infty}\frac{\sum\limits_{A\in[-H,H]_I^d\cap T}\omega_U(A)}{|\,[-H,H]_I^d\cap T\,|},$$

if it exists. Note, that this is analogous to the conditional expected value.

Remark 10. If $(U_\nu)_{\nu\in M_\mathbb{Q}}$ corresponds to T, then the expected value of the system $(U_\nu)_{\nu\in M_\mathbb{Q}}$ restricted to T should be thought as the “expected value” of the function $A\mapsto|P(A)|$, where P is the map of Theorem 2, when restricted to the elements A of $\mathbb{Z}^d$ such that $|P(A)|\geq 1$.

One can easily pass from μ to μ_T and vice versa:

Lemma 11. *If the density of T exists and is nonzero and T is such that $T^C\subseteq P^{-1}(\{\emptyset\})$, then μ exists iff μ_T exists. Furthermore, in that case it holds that $\mu=\mu_T\rho(T)$.*

Proof. As we assume $T^C\subseteq P^{-1}(\{\emptyset\})$, we have $\omega_U(A)=0$ for all $A\in T^C$ and thus

$$\begin{aligned}\mu_T&=\lim_{H\to\infty}\frac{\sum\limits_{A\in[-H,H]_I^d\cap T}\omega_U(A)}{|\,[-H,H]_I^d\cap T\,|}\\&=\lim_{H\to\infty}\frac{\sum\limits_{A\in[-H,H]_I^d}\omega_U(A)}{(2H)^d}\cdot\frac{(2H)^d}{|\,[-H,H]_I^d\cap T\,|}=\frac{\mu}{\rho(T)}.\quad\square\end{aligned}$$

In the applications of this paper one usually chooses $T^C=P^{-1}(\{\emptyset\})$, and computes the expected value restricted to T. This is a natural choice, since by the definition of T^C it holds that none of its elements lie in any of the U_ν, thus we are only considering the subset T, where nonzero values are added to the expected value.

One would now expect that, if the p-adic measures of the U_p's of Theorem 2 were essentially behaving like probabilities, one would have that the mean of the system $(U_p)_{p\in\mathcal{P}}$, as is defined in Definition 6, would be equal to $\sum_{p\in\mathcal{P}}s_p$, since the density of $U_p\cap\mathbb{Z}^d$ is equal to s_p. For example, this always happens when one has $U_p=\emptyset$ for all but finitely many U_p's. Note that this would also be the result if we could simply move the limit inside the series. This is not the case: in fact, Condition (2.1) of Theorem 2, is not enough to ensure the existence of the mean as in the natural Definition 6. The next example shows a case where Condition (2.1) is verified, but the mean does not exist.

Example 12. We set $U_\infty=\emptyset$ and for all $j\in\mathbb{N}$ with $2^n\leq j<2^{n+1}$ we define $U_{p_j}=\{2^n\}$, where p_j denotes the jth prime number. Clearly, we have $\mu_{p_j}(\partial(U_{p_j}))=0$. Furthermore, we estimate

$$\overline{\rho}\left(\bigcup_{p\in\mathcal{P},\ p>M} U_p\right) \leq \overline{\rho}\left(\bigcup_{\nu\in M_{\mathbb{Q}}} U_\nu\right) = \overline{\rho}(\{2^n \ \mid\ n\in\mathbb{N}\}) = 0.$$

Hence, Condition (2.1) is satisfied, even without taking the limit in M. We have $\omega_U(2^j) = 2^j$ and $\omega_U(A) = 0$ for all A that are not powers of 2. Thus, we have for all $n \in \mathbb{N}$

$$\sum_{A\in[-(2^{n+1}-1),2^{n+1}-1]_I} \frac{\omega_U(A)}{2(2^{n+1}-1)} = \frac{2^{n+1}-1}{2(2^{n+1}-1)} \overset{n\to\infty}{\longrightarrow} \frac{1}{2}$$

and

$$\sum_{A\in[-2^{n+1},2^{n+1}]_I} \frac{\omega_U(A)}{2\cdot 2^{n+1}} = \frac{2^{n+2}-1}{2\cdot 2^{n+1}} \overset{n\to\infty}{\longrightarrow} 1.$$

Hence, the expected value of the system $(U_\nu)_{\nu\in M_{\mathbb{Q}}}$ does not exist, even though it satisfies all conditions of Theorem 2.

We now state the main theorem, which is a new local to global principle for expected values.

Theorem 13. *Let H and d be positive integers. Let $U_\infty \subset \mathbb{R}^d$, such that $\mathbb{R}_{\geq 0}\cdot U_\infty = U_\infty$ and $\mu_\infty(\partial(U_\infty)) = 0$. Let $s_\infty = \frac{1}{2^d}\mu_\infty(U_\infty \cap [-1,1]^d)$. For each prime p, let $U_p \subset \mathbb{Z}_p^d$, such that $\mu_p(\partial(U_p)) = 0$ and define $s_p = \mu_p(U_p)$. Define the following map*

$$P : \mathbb{Z}^d \to 2^{M_{\mathbb{Q}}},$$
$$A \mapsto \{\nu \in M_{\mathbb{Q}} \mid A \in U_\nu\}.$$

If (2.1) is satisfied and for some $\alpha\in[0,\infty)$ there exists an absolute constant $c\in\mathbb{Z}$, such that for all $H \geq 1$ and for all $A\in[-H,H]_I^d$ one has that

$$\left|\left\{p\in\mathcal{P} \mid p > H^\alpha, A\in U_p\cap[-H,H]_I^d\right\}\right| < c \tag{3.1}$$

and that there exists a sequence $(v_p)_{p\in\mathcal{P}}$, such that for all $p < H^\alpha$ one has that

$$|\ U_p \cap [-H,H]_I^d\ | \leq v_p(2H)^d, \tag{3.2}$$

$$\sum_{p\in\mathcal{P}} v_p \quad \text{converges}, \tag{3.3}$$

then it follows that the mean of the system $(U_\nu)_{\nu\in M_{\mathbb{Q}}}$, exists and is given by:

$$\mu = \sum_{\nu\in M_{\mathbb{Q}}} s_\nu.$$

Remark 14. In a nutshell, the additional conditions give control on the number of U_p for which an element in $[-H,H]_I^d$ can live in: Condition (3.1) gives control in the large p regime (and small H), and Condition (3.2) (with (3.3)) gives control in the small p regime (and large H). None of the conditions can be removed, as we will show later with counterexamples in each case.

Proof. For $H, L > 0$ we split

$$\sum_{A\in[-H,H]_I^d} \frac{\omega_U(A)}{(2H)^d} = s_1(H,L) + s_2(H,L) + s_3(H,L),$$

where

$$s_1(H,L) = \sum_{A\in[-H,H]_I^d} \frac{|\,\{p\in\mathcal{P} \mid L \le H^\alpha < p, A\in U_p\}\,|}{(2H)^d},$$

$$s_2(H,L) = \sum_{A\in[-H,H]_I^d} \frac{|\,\{p\in\mathcal{P} \mid L < p < H^\alpha, A\in U_p\}\,|}{(2H)^d},$$

$$s_3(H,L) = \sum_{A\in[-H,H]_I^d} \frac{|\,\{\nu\in\mathcal{P} \mid \nu=\infty \text{ or } \nu\le L, A\in U_\nu\}\,|}{(2H)^d}.$$

We are going to show that for $j\in\{1,2\}$ we have

$$\limsup_{L\to\infty}\limsup_{H\to\infty}|s_j(H,L)| = 0 \quad\text{and}\quad \lim_{L\to\infty}\lim_{H\to\infty} s_3(H,L) = \sum_{\nu_{\nu\in M_{\mathbb{Q}}}} s_\nu,$$

which readily implies that

$$\mu = \lim_{H\to\infty}\frac{\sum\limits_{A\in[-H,H]_I^d}\omega_U(A)}{(2H)^d}$$

exists and that

$$\mu = \sum_{\nu\in M_{\mathbb{Q}}} s_\nu.$$

First we consider the case $\alpha\neq 0$. Let us define for $H>0$ and $A\in\mathbb{Z}^d$

$$|\left\{p\in\mathcal{P} \mid p > H^\alpha, A\in U_p\cap[-H,H]_I^d\right\}| = \ell_{A,H}.$$

Notice that thanks to Condition (3.1) there exists a constant $c>0$ independent of A and H such that

$$\ell_{A,H} < c.$$

Therefore, we get

$$\begin{aligned}
0 &\le \limsup_{L\to\infty}\limsup_{H\to\infty} |s_1(H,L)| \\
&\le \limsup_{L\to\infty}\limsup_{H\to\infty} \sum_{A\in[-H,H]_I^d\cap\bigcup_{L<p\in\mathcal{P}} U_p} \frac{\ell_{A,H}}{(2H)^d} \\
&\le \limsup_{L\to\infty}\limsup_{H\to\infty} \sum_{A\in[-H,H]_I^d\cap\bigcup_{L<p\in\mathcal{P}} U_p} \frac{c}{(2H)^d} \\
&= c\limsup_{L\to\infty}\limsup_{H\to\infty} \frac{|[-H,H]_I^d\cap\bigcup_{L<p\in\mathcal{P}} U_p|}{(2H)^d} \\
&= c\limsup_{L\to\infty}\ \overline{\rho}\left(\bigcup_{L<p\in\mathcal{P}} U_p\right) = 0,
\end{aligned}$$

where the last equality follows from Condition (2.1). Using (3.2) and (3.3) we get

$$\begin{aligned}
0 \le \limsup_{L\to\infty}\limsup_{H\to\infty} |s_2(H,L)| &= \limsup_{L\to\infty}\limsup_{H\to\infty} \sum_{p\in\mathcal{P},\ L<p<H^\alpha} \frac{|U_p\cap[-H,H]_I^d|}{(2H)^d} \\
&\le \limsup_{L\to\infty}\limsup_{H\to\infty} \sum_{p\in\mathcal{P},\ L<p<H^\alpha} v_p = 0.
\end{aligned}$$

For $\alpha = 0$ on the other hand, we have for $L > 1$ that $s_1(H,L) = 0 = s_2(H,L)$. Using Corollary 5 we get

$$\begin{aligned}
\lim_{L\to\infty}\lim_{H\to\infty} s_3(H,L) &= \lim_{L\to\infty}\lim_{H\to\infty} \sum_{\nu\in M_\mathbb{Q},\ \nu\le L \text{ or } \nu=\infty} \frac{|\,[-H,H]_I^d\cap U_\nu\,|}{(2H)^d} \\
&= \lim_{L\to\infty} \sum_{\nu\in M_\mathbb{Q},\ \nu\le L \text{ or } \nu=\infty} \rho(U_\nu\cap\mathbb{Z}^d) \\
&= \lim_{L\to\infty} \sum_{\nu\in M_\mathbb{Q},\ \nu\le L \text{ or } \nu=\infty} s_\nu \\
&= \sum_{\nu\in M_\mathbb{Q}} s_\nu. \quad \square
\end{aligned}$$

A natural question is whether some of the conditions in Theorem 13 are redundant. This is not the case as the next two examples show.

Example 15. In this example, we construct $(U_\nu)_{\nu\in M_\mathbb{Q}}$ such that Conditions (3.1) and (2.1) are verified but the conclusion of Theorem 13 does not hold. As in Example 12, we denote by p_j the jth prime. We choose

$$U_\infty = \emptyset, \quad U_{p_j} = \{p_j, p_{j+1}, \dots, p_{2^j}\}.$$

Clearly, we have $\mu_{p_j}(\partial(U_{p_j})) = 0$. By the prime number theorem we have that $\mathcal{P}$ has density zero and thus our choice satisfies Condition (2.1) even without taking the limit in M.

Note that for $p_j > H > 0$ we have $U_{p_j} \cap [-H, H] = \emptyset$ and thus Condition (3.1) is satisfied with $c = 1$. Now we will show that the conclusion of the theorem does not hold. First we show that $\mu = \infty$, if the limit exists. Note that for this example $[-H, H]_I = [-H, H]$ for all $H > 0$. Let $L \in \mathbb{N}$, then we compute

$$\begin{aligned}
\sum_{A \in [-p_{2^L}, p_{2^L}]} \frac{\omega_U(A)}{2p_{2^L}} &= \sum_{j=1}^{2^L} \frac{|U_{p_j} \cap [-p_{2^L}, p_{2^L}]|}{2p_{2^L}} \\
&= \sum_{j=1}^{L} \frac{|\{p_j, \dots, p_{2^j}\}|}{2p_{2^L}} + \sum_{j=L+1}^{2^L} \frac{|\{p_j, \dots, p_{2^L}\}|}{2p_{2^L}} \\
&\geq \sum_{j=L+1}^{2^L} \frac{2^L - j}{2p_{2^L}} \geq \frac{2^{2L} - L2^L - \frac{2^L(2^L+1)}{2}}{2p_{2^L}}.
\end{aligned}$$

Hence, for L sufficiently large we get

$$\sum_{A \in [-p_{2^L}, p_{2^L}]} \frac{\omega_U(A)}{2p_{2^L}} \geq \frac{1}{5p_{2^L}} 2^{2L}.$$

Thus, using the prime number theorem, we obtain

$$\begin{aligned}
\limsup_{H \to \infty} \sum_{A \in [-H, H]_I} \frac{\omega_U(A)}{(2H)} &\geq \limsup_{L \to \infty} \sum_{A \in [-p_{2^L}, p_{2^L}]} \frac{\omega_U(A)}{2p_{2^L}} \\
&\geq \limsup_{L \to \infty} \frac{1}{5p_{2^L}} 2^{2L} \\
&= \limsup_{L \to \infty} \frac{2^L}{5\ln(2)L} = \infty.
\end{aligned}$$

All finite sets are null sets for the p-adic Haar measure. Thus, we have $s_p = 0$ for all $p \in \mathcal{P}$ and $s_\infty = \frac{1}{2}\mu_\infty(\emptyset) = 0$ and hence

$$\sum_{\nu \in M_{\mathbb{Q}}} s_\nu = 0.$$

This means the conclusion of Theorem 13 does not hold, if we only assume Conditions (2.1) and (3.1).

Example 16. Next we construct an example that satisfies Conditions (2.1), (3.2), (3.3), and we show that the conclusion of Theorem 13 does not hold. We set $U_\infty = \emptyset$ and for $p \in \mathcal{P} \setminus \{p_{2^n} \mid n \in \mathbb{N}\}$ we define $U_p = \emptyset$. Inductively, we define the remaining $U_{p_{2^n}}$. We start with $U_{p_1} = \{1\}$. If $U_{p_{2^n}} = \{m^2\}$ for $m \in \mathbb{N}$, then we define

$$U_{p_{2^{n+1}}} = \begin{cases} \{m^2\} & \text{if } |\{j \in \mathbb{N} \mid j \leq n, U_{p_{2^j}} = \{m^2\}\}| < m^3, \\ \{(m+1)^2\} & \text{else.} \end{cases}$$

Clearly we have $\mu_{p_j}(\partial(U_{p_j})) = 0$. We compute

$$\overline{\rho}\left(\bigcup_{\nu \in M_{\mathbb{Q}}} U_\nu\right) = \overline{\rho}\left(\{n^2 \mid n \in \mathbb{N}\}\right) = \limsup_{H\to\infty} \frac{|\{n \in \mathbb{N} \mid n^2 < H\}|}{2H}$$
$$\leq \limsup_{H\to\infty} \frac{\sqrt{H}}{2H} = 0.$$

Hence, Condition (2.1) is satisfied. We have for $H > p_n$

$$|[-H, H] \cap U_{p_n}| = \begin{cases} 1 & \text{if } n = 2^k \text{ for some } k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we may pick

$$v_{p_n} = \begin{cases} \frac{1}{p_n} & \text{if } n = 2^k \text{ for some } k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

By the prime number theorem, there exists some constant $D > 0$, such that

$$\sum_{p_n \in \mathcal{P}} v_{p_n} = \sum_{k \geq 1} \frac{1}{p_{2^k}} = \sum_{k \geq 1} \frac{2^k \ln(2^k)}{p_{2^k}} \cdot \frac{1}{2^k \ln(2^k)} \leq \sum_{k \geq 1} \frac{D}{2^k \ln(2^k)} < \infty.$$

Thus, Conditions (3.2) and (3.3) are satisfied.
By construction, we have

$$\omega_U(A) = \begin{cases} m^3 & \text{if } A = m^2 \text{ for some } m \in \mathbb{N}_{>0}, \\ 0 & \text{else.} \end{cases}$$

Therefore, we get

$$\sum_{A \in [-H,H]_I} \frac{\omega_U(A)}{2H} \geq \sum_{m=1}^{\lfloor\sqrt{H}\rfloor} \frac{m^3}{2H} = \frac{1}{2H} \cdot \frac{\lfloor\sqrt{H}\rfloor^2}{4} (\lfloor\sqrt{H}\rfloor + 1)^2$$
$$\geq \frac{1}{32} (\lfloor\sqrt{H}\rfloor + 1)^2.$$

Hence,

$$\limsup_{H\to\infty} \sum_{A\in[-H,H]_I} \frac{\omega_U(A)}{(2H)} = \infty.$$

On the other hand, by the same argument as in the previous example we obtain

$$\sum_{\nu\in M_{\mathbb{Q}}} s_\nu = 0.$$

4. Applications

We can apply Theorem 13 to sets, whose densities were computed via the local to global principle of Theorem 2 and fulfill Conditions (3.1), (3.2) and (3.3).

For the next example we need the notion of a basic minor. A minor of a matrix is called basic, if it is the determinant of a submatrix of maximal size. We will now compute the expected number of common prime divisors of all basic minors of a rectangular non-unimodular matrix.

Corollary 17. *Let $n < m$ be positive integers, and let us denote by R the set of rectangular unimodular matrices in $\mathbb{Z}^{n\times m}$. Then the corresponding system $(U_\nu)_{\nu\in M_{\mathbb{Q}}}$ is given as in [19], i.e., $U_\infty = \emptyset$ and for $p \in \mathcal{P}$ denote by U_p the set of all matrices in $\mathbb{Z}_p^{n\times m}$ whose basic minors are all divisible by p.*

Then the expected value of the system $(U_\nu)_{\nu\in M_{\mathbb{Q}}}$ exists and is given by

$$\mu = \sum_{\nu\in M_{\mathbb{Q}}} s_\nu = \sum_{p\in\mathcal{P}} \left(1 - \prod_{i=0}^{n-1}\left(1 - \frac{1}{p^{m-i}}\right)\right). \tag{4.1}$$

And the average number of primes that divide all basic minors of a rectangular non-unimodular matrix is given by

$$\mu_{R^C} = \frac{\mu}{1 - \prod_{i=0}^{n-1} \frac{1}{\zeta(m-i)}}, \tag{4.2}$$

where ζ denotes the Riemann zeta function.

Proof. By [19], we have that all conditions of Theorem 2 are satisfied for the corresponding system $(U_\nu)_{\nu\in M_{\mathbb{Q}}}$ and for $p \in \mathcal{P}$ we have that

$$s_p = \left(1 - \prod_{i=0}^{n-1}\left(1 - \frac{1}{p^{m-i}}\right)\right)$$

and thus

$$\rho(R) = \rho(P^{-1}(\{\emptyset\})) = \prod_{i=0}^{n-1} \frac{1}{\zeta(m-i)}.$$

Thanks to Lemma 11 we are left with proving that the additional assumptions on the system $(U_\nu)_{\nu \in M_\mathbb{Q}}$ of Theorem 13 are satisfied.

For this, let us choose $\alpha = 1$ and denote by f_i the function associating to $A \in \mathbb{Z}^{n\times m}$ some fixed basic minor. Then we have for all $A \in [-H,H]^{n\times m}$ the inequality $f_i(A) \leq (2H)^n$ for all i. We exclude that $f_i(A)$ vanishes for all i, since then we land in I.

Recall, that

$$\ell_{A,H} = |\{p \in \mathcal{P} \mid p > H,\ A \in U_p \cap [-H,H]_I^{nm}\}|.$$

Thus, we have that

$$H^{\ell_{A,H}} \leq \prod_{\substack{p\in\mathcal{P} \\ p>H,\ A\in U_p\cap[-H,H]_I^{nm}}} p.$$

Further, observe that

$$\prod_{\substack{p\in\mathcal{P} \\ p>H,\ A\in U_p\cap[-H,H]_I^{nm}}} p = \gcd((f_i(A))_i) \leq (2H)^n.$$

Hence, we get that $H^{\ell_{A,H}} \leq (2H)^n$, and thus Condition (3.1) is satisfied.

To verify Condition (3.2) we want to show that there exists a sequence $(v_p)_{p\in\mathcal{P}}$ such that for all $p < H$ we have that $| U_p \cap [-H,H]_I^{nm} | \leq v_p (2H)^{nm}$. The set of non-full rank matrices over $\mathbb{F}_p$ has size

$$p^{nm} - \prod_{i=0}^{n-1}(p^m - p^i) \leq 2^n p^{m(n-1)+n-1} = 2^n p^{(m+1)(n-1)}.$$

We can fix one non-full rank $n \times m$ matrix over $\mathbb{F}_p$, for which we have less than or equal to $2^n p^{(m+1)(n-1)}$ choices. For this fixed matrix there are less than or equal to $(\lceil \frac{2H}{p} \rceil)^{nm}$ lifts to $\mathbb{Z}^{n\times m} \cap [-H,H]^{nm}$. Hence, we have for $p < H$

$$\begin{aligned} | U_p \cap [-H,H]_I^{nm} | &\leq 2^n \left(\left\lceil \frac{2H}{p} \right\rceil\right)^{nm} p^{(m+1)(n-1)} \\ &\leq 2^n \left(\frac{2H}{p} + 1\right)^{nm} p^{(m+1)(n-1)} \\ &\leq 2^n (3H)^{nm} p^{nm-m+n-1-nm} \\ &\leq 6^{nm} H^{nm} \frac{1}{p^2}. \end{aligned}$$

Thus $(v_p)_{p\in\mathcal{P}}$ can be chosen to be $(\frac{6^{nm}}{p^2})_{p\in\mathcal{P}}$, which also satisfies Condition (3.3). Hence, (4.1) follows and Lemma 11 implies (4.2). □

By choosing $n = 1$ we get the mean of numbers of primes dividing non-coprime m-tuples of integers and of course choosing $n = 1$ and $m = 2$ will give the mean of numbers of primes dividing non-coprime pairs of integers.

The results of [12] regarding the average amount of primes for which an Eisenstein polynomial satisfies the criterion of Eisenstein follow immediately as corollary using Theorem 13. We say that a polynomial is p-Eisenstein, if it satisfies the criterion of Eisenstein for this prime p.

Corollary 18. *Let $d \geq 2$ be an integer. The expected number of primes p for which an Eisenstein polynomial of degree d is p-Eisenstein, is given by*

$$\left(1-\prod_{p\in\mathcal{P}}\left(1-\frac{(p-1)^2}{p^{d+2}}\right)\right)^{-1}\sum_{p\in\mathcal{P}}\frac{(p-1)^2}{p^{d+2}}.$$

Proof. In Theorem 13 simply use the system $U_p = (p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p) \times p\mathbb{Z}_p^{d-1} \times (\mathbb{Z}_p \setminus p\mathbb{Z}_p)$ and choose $\alpha = 1$. With this, Condition (2.1) is clearly satisfied, as $U_p \subset (p\mathbb{Z}_p)^2 \times \mathbb{Z}_p^{d-1}$ and using Lemma 4 on $f(x_1,\dots,x_{d+1}) = x_1$ and $g(x_1,\dots,x_{d+1}) = x_2$.

Also Condition (3.1) is trivially verified, as no polynomial can be Eisenstein with respect to a prime larger than its height. Finally, Condition (3.3) is verified thanks to the rough estimate

$$|U_p \cap [-H,H]_I^{d+1}| \leq \lceil 2H/p \rceil^d \cdot H,$$

and this is enough for our purposes because $\sum_{p\in\mathcal{P}} 1/p^d$ converges for $d \geq 2$. □

Moreover, we can obtain the expected number of primes for which a given polynomial $f(x)$ is Eisenstein for some shift $f(x+i)$. For this result we choose the system $(U_p)_{p\in\mathcal{P}}$ as in [16], i.e., U_p is the set of polynomials f of degree d in $\mathbb{Z}_p[x]$, such that there exists $i \in \mathbb{N}$ for which $f(x+i)$ is p-Eisenstein. Clearly, we will see U_p as a subset of $\mathbb{Z}_p^{d+1}$.

Corollary 19. *For $d \geq 3$, the expected value of the system $(U_p)_{p\in\mathcal{P}}$, given as in [16], is*

$$\sum_{p\in\mathcal{P}}\frac{(p-1)^2}{p^{d+1}}. \tag{4.3}$$

The average number of primes p for which a shifted Eisenstein polynomial f is such that $f(x+i)$ is p-Eisenstein for some $i \in \mathbb{Z}$ is

$$\left(1-\prod_{p\in\mathcal{P}}\left(1-\frac{(p-1)^2}{p^{d+1}}\right)\right)^{-1}\sum_{p\in\mathcal{P}}\frac{(p-1)^2}{p^{d+1}}. \tag{4.4}$$

Proof. By [16], where the density of the set of shifted Eisenstein polynomials is computed, we have that Condition (2.1) is verified.

Notice that Condition (3.1) is verified with $\alpha = 1$: in fact, the primes p for which a polynomial is p-Eisenstein divide the discriminant of the polynomial. More in detail, one observes that $f(x+i)$ has the same discriminant as $f(x)$, which is bounded by CH^{2d-2} (as the discriminant is homogeneous of degree $2d-2$), for some absolute constant C. Thus, one obtains that the product of the primes p larger than H for which $f(x+i)$ is p-Eisenstein for some i is bounded by an absolute constant.

Also Condition (3.3) is easy to verify. First, observe that if $f(x+i)$ is p-Eisenstein for some $i \in \mathbb{N}$, then i can be chosen less than p (see for example [16, Lemma 6]). So that the set of shifted p-Eisenstein polynomials in $[-H,H]^{d+1}$ is absolutely bounded by $|E_p(H)|\cdot p$, where $E_p(H)$ is the set of p-Eisenstein polynomials of degree $d+1$ and height at most H. Finally, we have the rough estimate

$$|U_p \cap [-H,H[_I^{d+1}| \leq| E_p(H) \mid \cdot p \leq \lceil 2H/p\rceil^d \cdot H \cdot p,$$

which is enough for our purposes as $\sum_{p\in\mathcal{P}} 1/p^{d-1}$ converges for $d \geq 3$. Thus, Theorem 13 implies (4.3) and Lemma 11 further implies (4.4). □

Acknowledgments

The authors would like to thank the anonymous reviewer for the helpful comments. This work has been partially supported by the Swiss National Science Foundation grant number 172623, grant number 188430 and grant number 195290.

References

[1] Martin Bright, Tim Daniel Browning, Daniel Loughran, Failures of weak approximation in families, Compos. Math. 152 (7) (2016) 1435–1475.
[2] Ernesto Cesaro, Question 75 (solution), Mathesis 3 (1883) 224–225.
[3] Ernesto Cesaro, Probabilité de certains faits arithméthiques, Mathesis 4 (1884) 150–151.
[4] Edoardo Dotti, Giacomo Micheli, Eisenstein polynomials over function fields, Appl. Algebra Eng. Commun. Comput. 27 (2) (2016) 159–168.
[5] Torsten Ekedahl, An infinite version of the Chinese remainder theorem, Comment. Math. Univ. St. Pauli 40 (1) (1991) 53–59.
[6] Andrea Ferraguti, The set of stable primes for polynomial sequences with large Galois group, Proc. Am. Math. Soc. (2018).
[7] Andrea Ferraguti, Giacomo Micheli, On the Mertens–Cesáro theorem for number fields, Bull. Aust. Math. Soc. 93 (02) (2016) 199–210.
[8] Xiangqian Guo, Guangyu Yang, The probability of rectangular unimodular matrices over $F_q[x]$, Linear Algebra Appl. 438 (6) (2013) 2675–2682.
[9] Randell Heyman, Igor E. Shparlinski, On the number of Eisenstein polynomials of bounded height, Appl. Algebra Eng. Commun. Comput. 24 (2) (2013) 149–156.

[10] Randell Heyman, Igor E. Shparlinski, On shifted Eisenstein polynomials, Period. Math. Hung. 69 (2) (2014) 170–181.
[11] Julia Lieb, Uniform probability and natural density of mutually left coprime polynomial matrices over finite fields, Linear Algebra Appl. 539 (2018) 134–159.
[12] Shilin Ma, Kevin McGown, Devon Rhodes, Mathias Wanner, On the number of primes for which a polynomial is Eisenstein, Integers 18 (2018) 2.
[13] Gérard Maze, Natural density distribution of Hermite normal forms of integer matrices, J. Number Theory 131 (12) (2011) 2398–2408.
[14] Franz Mertens, Ueber einige asymptotische Gesetze der Zahlentheorie, J. Reine Angew. Math. 77 (1874) 289–338.
[15] Giacomo Micheli, A local to global principle for densities over function fields, arXiv preprint, arXiv:1701.01178, 2017.
[16] Giacomo Micheli, Reto Schnyder, The density of shifted and affine Eisenstein polynomials, Proc. Am. Math. Soc. 144 (11) (2016) 4651–4661.
[17] Giacomo Micheli, Reto Schnyder, The density of unimodular matrices over integrally closed subrings of function fields, in: Contemporary Developments in Finite Fields and Applications, World Scientific, 2016, pp. 244–253.
[18] Giacomo Micheli, Reto Schnyder, On the density of coprime m-tuples over holomorphy rings, Int. J. Number Theory 12 (03) (2016) 833–839.
[19] Giacomo Micheli, Violetta Weger, On rectangular unimodular matrices over the algebraic integers, SIAM J. Discrete Math. 33 (1) (2019) 425–437.
[20] James E. Nymann, On the probability that k positive integers are relatively prime, J. Number Theory 4 (5) (1972) 469–473.
[21] Bjorn Poonen, Michael Stoll, The Cassels-Tate pairing on polarized Abelian varieties, Ann. Math. 150 (3) (1999) 1109–1149.
[22] Bjorn Poonen, Michael Stoll, A local-global principle for densities, in: Scott D. Ahlgren, George E. Andrews, K. Ono (Eds.), Topics in Number Theory, in: Mathematics and Its Applications, vol. 467, Springer US, 1999, pp. 241–244.
[23] Brian D. Sittinger, The probability that random algebraic integers are relatively r-prime, J. Number Theory 130 (1) (2010) 164–171.
[24] Yinghui Wang, Richard P. Stanley, The Smith normal form distribution of a random integer matrix, SIAM J. Discrete Math. 31 (3) (2017) 2247–2268.