SIAM J. DISCRETE MATH.
Vol. 31, No. 3, pp. 2247–2268



# THE SMITH NORMAL FORM DISTRIBUTION OF A RANDOM INTEGER MATRIX*

YINGHUI WANG† AND RICHARD P. STANLEY†

**Abstract.** We show that the density $\mu$ of the Smith normal form (SNF) of a random integer matrix exists and equals a product of densities $\mu_{p^s}$ of SNF over $\mathbb{Z}/p^s\mathbb{Z}$ with $p$ a prime and $s$ some positive integer. Our approach is to connect the SNF of a matrix with the greatest common divisors (gcds) of certain polynomials of matrix entries and develop the theory of multi-gcd distribution of polynomial values at a random integer vector. We also derive a formula for $\mu_{p^s}$ and compute the density $\mu$ for several interesting types of sets. As an application, we determine the probability that the cokernel of a random integer square matrix has at most $\ell$ generators for a positive integer $\ell$, and establish its asymptotics as $\ell \to \infty$, which extends a result of Ekedahl (1991) on the case $\ell = 1$.

**Key words.** Smith normal form, random integer matrix, greatest common divisor distribution

**AMS subject classifications.** Primary, 05A05, 11C20, 15A21, 60B20; Secondary, 11C08, 15B33

**DOI.** 10.1137/16M1098140

## 1. Introduction.

Let $M$ be a nonzero $n \times m$ matrix over a commutative ring $R$ (with identity) and $r$ be the rank of $M$. If there exist invertible $n \times n$ and $m \times m$ matrices $P$ and $Q$ such that the product $PMQ$ is a diagonal matrix (i.e., a matrix that vanishes off the main diagonal) whose main diagonal $(d_1, d_2, \ldots, d_r, 0, 0, \ldots, 0)$ satisfies that $d_i \mid d_{i+1}$ for all $1 \le i \le r-1$, then $PMQ$ is the *Smith normal form (SNF)* of $M$ (named for H. J. S. Smith [19]; see [11, 12, 21] for references on this topic). In general, the SNF does not exist. It does exist when $R$ is a *principal ideal ring*, i.e., a ring (not necessarily an integral domain) for which every ideal is principal. This class of rings includes the integers $\mathbb{Z}$ and their quotients $\mathbb{Z}/q\mathbb{Z}$, which are the rings of interest to us here. In fact, for the rings $\mathbb{Z}/q\mathbb{Z}$ we will be particularly concerned with the case $q = p^s$, a prime power. For principal ideal rings, the diagonal entries (also known as elementary divisors or invariants) are uniquely determined—up to multiplication by a unit—by $g_{i-1}d_i = g_i$ $(1 \le i \le r)$, where $g_0 = 1$ and $g_i$ is the greatest common divisor (gcd) of all $i \times i$ minors of $M$. We have the following algebraic correspondence between the SNF and the cokernel of $M$:

$$\operatorname{coker} M \cong R/d_1R \oplus R/d_2R \oplus \cdots \oplus R/d_rR \oplus R^{n-r}.$$

There has been a huge amount of research on eigenvalues and eigenvectors of a random matrix (see, e.g., [1, 2, 10, 15, 22, 23]). Much less attention has been paid to the SNF of a random matrix. Some basic results in this area are known, but they appear in papers not focused on SNF per se, in particular, some applications to communication theory [8]. We develop the theory in a systematic way, collecting previous work in this area, and providing some new results.

We shall define the *density* $\mu$ of SNF of a random $n \times m$ integer matrix as the limit (if it exists) as $k \to \infty$ of $\mu^{(k)}$, the density of SNF of a random $n \times m$ matrix with

*Received by the editors November 14, 2016; accepted for publication (in revised form) April 27, 2017; published electronically September 28, 2017. Part of this paper was presented at the 2016 International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC).
http://www.siam.org/journals/sidma/31-3/M109814.html
**Funding:** The second author was partially supported by NSF grant DMS-1068625.

†Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139 (yinghui@mit.edu, rstan@math.mit.edu).

entries independent and uniformly distributed over $\{-k, -k+1, \ldots, k\}$ (see Definition 3.1 below for a precise definition).

As a motivating example, the probability that $d_1 = 1$ for a random $n \times m$ integer matrix is the probability that the $nm$ matrix entries are relatively prime, or equivalently, that $nm$ random integers are relatively prime, and thus equals $1/\zeta(nm)$, where $\zeta(\cdot)$ is the Riemann zeta function.

If we regard the minors of an $n \times m$ matrix as polynomials of the $nm$ matrix entries with integer coefficients, then the SNF of a matrix is uniquely determined by the gcds of the values of these polynomials (recall the definition of SNF from the beginning). This motivates us to study the theory of multi-gcd distribution of polynomial values.

Given a collection of relatively prime polynomials in $\mathbb{Z}[x_1, x_2, \ldots, x_d]$, let $g(x)$ be the gcd of the values of these polynomials at $x = (x_1, x_2, \ldots, x_d)$. We shall define the *density* $\lambda$ of $g(x)$ of a random $d$-dimensional integer vector $x$ as the limit (if it exists) as $k \to \infty$ of $\lambda^{(k)}$, the density of $g(x)$ with $x$ uniformly distributed over $\{-k, -k+1, \ldots, k\}^d$ (see Definition 2.1 for a precise definition).

In the spirit of previous work in number theory such as [7, 17, 18] and the Cohen–Lenstra heuristics [4, 5], one might conjecture that $\lambda$ exists and equals the product of density $\lambda_p$ of $g(x)$ over $(\mathbb{Z}/p\mathbb{Z})^d$ over all primes $p$. In fact, we will prove this conjecture with the more general density $\lambda_{p^s}$ of $g(x)$ over $\mathbb{Z}/p^s\mathbb{Z}$ for sets of form (2.4) (see Theorem 2.6), with the aid of a result in number theory [18, Lemma 21]. Note that the special case $s = 0$ or 1 follows from [7, Theorem 2.3] directly. In particular, this result applies to the probability that $g(x) = 1$, in other words, that the polynomial values are relatively prime. Furthermore, all these results hold for the multi-gcd distribution of polynomial values, namely, when $g(x)$ is a vector whose components are the gcds of the values of given collections of polynomials at $x$.

Then we apply this theory to the SNF distribution of a random integer matrix to show that the density $\mu$ (of SNF of a random $n \times m$ integer matrix) equals a product of some densities $\mu_{p^s}$ of SNF over $\mathbb{Z}/p^s\mathbb{Z}$ for sets of form (3.3) (Theorem 3.6). We also derive a formula for $\mu_{p^s}$ (Theorem 3.2), which allows us to compute $\mu_{p^s}$ and hence $\mu$ explicitly (Theorem 4.3). Some special cases of this formula are consistent with [20, Exercise 1.192(b)] and [9, pp. 233, 236]. Other papers related to our work are [14] (on rings $\mathbb{Z}_p$ of $p$-adic integers and $\mathbb{Z}/q\mathbb{Z}$) and [24] (on Laplacian matrices) (see [21, section 4] for a survey on this topic).

On the strength of these results, we determine the value of $\mu$ for some interesting types of sets, specifically, matrices with the first few diagonal entries given, matrices with diagonal entries all equal to 1, and square matrices with at most $\ell\,(= 1, 2, \ldots)$ diagonal entries not equal to 1, i.e., whose corresponding cokernel has at most $\ell$ generators; further, for the last set we establish the asymptotics of $\mu$ as $\ell \to \infty$. In the case $\ell = 1$, which is equivalent to the matrix having a cyclic cokernel, our results echo those of Ekedahl [7, section 3] via a different approach, and the density coincides with that in [16]. We also show that $\mu$ of a finite set is 0 and that the asymptotic probability that a random integer matrix is full rank is 1, which agrees with [13, Theorem 1] in the case of square matrices.

The remainder of this paper is organized as follows. Section 2 develops the theory of multi-gcd distribution of polynomial values. Section 3 applies this theory to the SNF distribution and derives a formula for $\mu_{p^s}$. Finally, section 4 computes the density $\mu$ for several types of sets.

We shall assume that throughout this paper, $p$ represents a prime, $p_j$ is the $j$th smallest prime, $\prod_p$ means a product over all primes $p$, and $\mathbb{Z}^d_{(k)}$ denotes $\{-k, -k+1, \ldots, k\}^d$.

**2. Multi-gcd distribution of polynomial values.** Suppose that $d$ and $h$ are positive integers and $F_1, F_2, \ldots, F_h \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ are nonzero polynomials. Let

$$g(x) := \gcd\big(F_1(x), F_2(x), \ldots, F_h(x)\big), \quad x \in \mathbb{Z}^d,$$

and $g(x) = 0$ if $F_j(x) = 0$ for all $1 \le j \le h$.

We shall define the *density of $g(x)$ of a random $d$-dimensional integer vector $x$* as the limit (if it exists) of the density of $g(x)$ with $x$ uniformly distributed over $\{-k, -k+1, \ldots, k\}^d := \mathbb{Z}^d_{(k)}$ as $k \to \infty$, precisely as follows.

DEFINITION 2.1.

(i) *For $\mathcal{Z} \subseteq \mathbb{Z}$, we denote by $\lambda^{(k)}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z}$ with $x$ uniformly distributed over $\mathbb{Z}^d_{(k)}$. If $\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) = \lambda(\mathcal{Z})$ exists, then we say that the* probability that $g(x) \in \mathcal{Z}$ with $x$ a random $d$-dimensional integer vector *is $\lambda(\mathcal{Z})$. If this is the case, then $\lambda(\mathcal{Z}) \in [0,1]$ since $\lambda^{(k)}(\mathcal{Z}) \in [0,1]$ for all $k$.*

(ii) *We define similarly the* gcd distribution over the ring of integers mod $p^s$ *for prime $p$ and positive integer $s$; more generally, for a finite set $\mathcal{P}$ of prime and positive integer pairs $(p, s)$, we denote*

$$P_{\mathcal{P}} := \prod_{(p,s)\in\mathcal{P}} p^s$$

*and by $\lambda^{(k)}_{P_{\mathcal{P}}}(\mathcal{Z})$ (resp., $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$) the probability that $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$—up to multiplication by a unit—with $x$ uniformly distributed over $\mathbb{Z}^d_{(k)}$ (resp., $(\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$). Note that $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ is the number of solutions to $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ (up to multiplication by a unit) divided by $P^d_{\mathcal{P}}$. In the special case $\mathcal{P} = \{(p, s)\}$, we have $P_{\mathcal{P}} = p^s$.*

(iii) *The above definitions also extend to the* distribution of multi-gcds. *Suppose that $\mathcal{U} = \{U_i\}_{i=1}^w$ is a collection of $w$ nonempty subsets $U_i$ of $\{F_1, F_2, \ldots, F_h\}$. Let*

$$g_i(x) := \gcd\big(F(x) : F \in U_i\big) \quad \text{and} \quad g(x) := (g_1, g_2, \ldots, g_w)(x) \in \mathbb{Z}^w, \quad x \in \mathbb{Z}^d; \tag{2.1}$$

*then we adopt the above definitions of functions $\lambda^{(k)}$, $\lambda$, $\lambda^{(k)}_{P_{\mathcal{P}}}$, and $\lambda_{P_{\mathcal{P}}}$ for $\mathcal{Z} \subseteq \mathbb{Z}^w$ with only one slight modification: replace "up to multiplication by a unit" with "up to multiplication of the* components *of $g$ by units."*

For convenience, we shall always assume that the notion $g(x) \in \mathcal{Z}$ or $\mathcal{Z} = \mathcal{Z}' \pmod{P_{\mathcal{P}}}$ for some $\mathcal{Z}, \mathcal{Z}' \subset \mathbb{Z}^w$ implies the *equivalence of multiplication of components by units* and that the random vector $x$ is *uniformly distributed* on its range (if known, e.g., $\mathbb{Z}^d_{(k)}$ or $(\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$).

*Remark* 2.2. The density $\lambda_p$ defined above in Definition 2.1(ii) is consistent with the normalized *Haar measure* on $\mathbb{Z}^d_p$, as in [18].

In this section, we establish the properties of $\lambda_{P_{\mathcal{P}}}$ and $\lambda$, the existence of $\lambda$, and a connection between $\lambda$ and the $\lambda_{p^s}$'s.

**2.1. Multi-gcd distribution over $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$.** We show that the density $\lambda^{(k)}_{P_{\mathcal{P}}} \to \lambda_{P_{\mathcal{P}}}$ as $k \to \infty$ and that $\lambda_{P_{\mathcal{P}}} = \prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}$.

THEOREM 2.3. *For any $\mathcal{Z} \subseteq \mathbb{Z}^w$, we have*

$$\lim_{k\to\infty} \lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z}) = \lambda_{P_{\mathcal{P}}}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}(\mathcal{Z}). \tag{2.2}$$

*Proof.* For the second equality, we let $N_{P_{\mathcal{P}}}(\mathcal{Z})$ be the number of $x \in (\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$ for which $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$. The Chinese remainder theorem then gives

$$P_{\mathcal{P}}^d\, \lambda_{P_{\mathcal{P}}}(\mathcal{Z}) = N_{P_{\mathcal{P}}}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} N_{p^s}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} p^{sd}\lambda_{p^s}(\mathcal{Z}) = P_{\mathcal{P}}^d \prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}(\mathcal{Z}).$$

Dividing both sides by $P_{\mathcal{P}}^d$ leads to the desired equality.

For the first equality of (2.2), we first observe that if $p \,|\, (2k+1)$, then $\lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z}) = \lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ by definition. If $p \nmid 2(k+1)$, then we proceed by approximating $2k+1$ by a multiple of $P_{\mathcal{P}}$ and estimating $\lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z})$ using $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$.

Let $k \in \mathbb{Z}$ such that $K := 2k+1 \geq P_{\mathcal{P}}$; then there exists $q \in \mathbb{Z}_+$ such that

$$q \cdot P_{\mathcal{P}} \leq K < (q+1) \cdot P_{\mathcal{P}}. \tag{2.3}$$

It follows that for any integer $y$, there are either $q$ or $q+1$ numbers among $\mathbb{Z}_{(k)}$ that equal $y \bmod P_{\mathcal{P}}$. Thus the number of $x \in \mathbb{Z}_{(k)}^d$ for which $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ is between $q^d N'$ and $(q+1)^d N'$, where $N' := N_{P_{\mathcal{P}}}(\mathcal{Z})$. Coupling with (2.3) yields

$$\lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z}) \in \left[\frac{q^d N'}{K^d}, \frac{(q+1)^d N'}{K^d}\right] \subseteq \left[\left(\frac{q}{q+1}\right)^d \frac{N'}{P_{\mathcal{P}}^d}, \left(\frac{q+1}{q}\right)^d \frac{N'}{P_{\mathcal{P}}^d}\right],$$

whose left and right endpoints both converge to $N'/P_{\mathcal{P}}^d = \lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ as $q \to \infty$ or, equivalently, as $k \to \infty$, as desired. ∎

**2.2. Multi-gcd distribution over $\mathbb{Z}$.** We start with some properties of the density $\lambda$ of set unions, subtractions, and complements, which are simple consequences of Definition 2.1 and useful in determining the value of $\lambda$ for specific sets (such as in the explanation below Remark 2.7).

THEOREM 2.4.

(i) *Suppose that $\{\mathcal{Z}_\alpha\}_{\alpha\in\mathcal{A}}$ are pairwise disjoint subsets of $\mathbb{Z}^w$ such that $\lambda(\mathcal{Z}_\alpha)$ exists for all $\alpha \in \mathcal{A}$. If $\mathcal{A}$ is a finite set, then $\lambda(\cup_{\alpha\in\mathcal{A}} \mathcal{Z}_\alpha) = \sum_{\alpha\in\mathcal{A}} \lambda(\mathcal{Z}_\alpha)$.*

(ii) *Suppose that $\mathcal{Z}' \subseteq \mathcal{Z} \subseteq \mathbb{Z}^w$ such that $\lambda(\mathcal{Z}')$ and $\lambda(\mathcal{Z})$ both exist; then $\lambda(\mathcal{Z} \setminus \mathcal{Z}') = \lambda(\mathcal{Z}) - \lambda(\mathcal{Z}')$. In particular, for the complement $\mathcal{Z}^c$ of $\mathcal{Z}$ in $\mathbb{Z}^w$, we have $\lambda(\mathcal{Z}^c) = 1 - \lambda(\mathcal{Z})$.*

(iii) *Suppose that $\mathcal{Y} \in \mathbb{Z}^w$ such that $\lambda(\mathcal{Y}) = 0$; then for any $\mathcal{Y}' \subseteq \mathcal{Y}$, we have $\lambda(\mathcal{Y}') = 0$ as well.*

Now we show that the density $\lambda$ exists and, in fact, equals the product of some $\lambda_{p^s}$'s.

*Assumption* 2.5. For all $1 \leq i \leq w$, we have

$$\gcd(F_1, F_2, \ldots, F_h) = \gcd\,(F : F \in U_i) = 1 \ \text{ in } \ \mathbb{Q}[x_1, x_2, \ldots, x_d].$$

THEOREM 2.6. *Suppose that Assumption* 2.5 *holds. Given positive integers $r \leq w$ and $y_i$ $(1 \leq i \leq r)$, let $y = \prod_{j=1}^{\infty} p_j^{s_j}$ with $p_j$ the $j$th smallest prime and $s_j$ nonnegative*

*integers, $j = 1, 2, \ldots$, such that $y_i \mid y$ for all $1 \le i \le r$; then the probability $\lambda(\mathcal{Z})$ exists for the set*

$$\mathcal{Z} = \left\{(z_1, z_2, \ldots, z_w) \in \mathbb{Z}_+^w : \ z_i = y_i \ \forall \ i \le r\right\}, \tag{2.4}$$

*and in fact*

$$\lambda(\mathcal{Z}) = \prod_{j=1}^{\infty} \lambda_{p_j^{s_j+1}}(\mathcal{Z}). \tag{2.5}$$

*Note that the right-hand side of* (2.5) *is well-defined since $\lambda_{p^s} \in [0, 1]$ for all $p$ and $s$.*

*Remark* 2.7. The special case that all $s_j$'s are either 0 or 1 follows from [7, Theorem 2.3]; in particular, the case $\mathcal{Z} = \{1\}$ gives the probability of relatively prime polynomial values.

We have assumed in Theorem 2.6 that the $y_i$'s are positive. In fact, if $y_i = 0$ for some $i$, then we have $\lambda(\mathcal{Z}) = 0$ on the strength of Theorem 2.4(iii) and the well-known result [17, Lemma 4.1].

THEOREM 2.8. *Let $G \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ be a nonzero polynomial and $\sigma^{(k)}$ the probability that $G(x) = 0$ with $x$ uniformly distributed over $\mathbb{Z}_{(k)}^d$. Then $\sigma^{(k)} \to 0$ as $k \to \infty$; in words, the probability that a nonzero polynomial at a random integer vector equals zero is 0. As a consequence, for any given integer $c$, the probability that $G(x) = c$ is either 0 or 1 (consider the polynomial $G(x) - c$).*

To prove Theorem 2.6, we need Theorem 2.3 and the following two lemmas.

LEMMA 2.9 (see [17, Lemma 5.1] or [18, Lemma 21]). *Suppose that $F, G \in \mathbb{Z}[x_1, \ldots, x_d]$ are relatively prime as elements of $\mathbb{Q}[x_1, \ldots, x_d]$. Let $\nu_\ell^{(k)}$ be the probability that $p \mid F(x), G(x)$ for some prime $p > \ell$ with $x$ uniformly distributed over $\mathbb{Z}_{(k)}^d$, i.e.,*

$$\nu_\ell^{(k)} := \#\left\{x \in \mathbb{Z}_{(k)}^d : \ \exists \text{ prime } p > \ell \text{ s.t. } p \mid F(x), G(x)\right\} / (2k+1)^d.$$

*Then*

$$\lim_{\ell \to \infty} \limsup_{k \to \infty} \nu_\ell^{(k)} = 0.$$

LEMMA 2.10. *Suppose that $G_1, \ldots, G_h \in \mathbb{Q}[x_1, \ldots, x_d]$ ($h \ge 2$) are relatively prime. Then there exists $v = (v_3, \ldots, v_h) \in \mathbb{Z}^{h-2}$ such that $\gcd(G_1, G_2 + \sum_{i=3}^h v_i G_i) = 1$.*

*Proof.* We prove by induction on $h$. See Appendix A for details. ∎

Now we are ready to prove Theorem 2.6.

*Proof of Theorem* 2.6. Let

$$\mathcal{P}_\ell := \{(p_j, s_j + 1)\}_{j=1}^{\ell}, \quad \ell \in \mathbb{Z}_+.$$

Then Theorem 2.3 gives that the right-hand side of (2.5) is

$$\lim_{\ell \to \infty} \prod_{j=1}^{\ell} \lambda_{p_j^{s_j+1}}(\mathcal{Z}) = \lim_{\ell \to \infty} \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}).$$

Therefore it remains to show that

$$\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) = \lim_{\ell\to\infty} \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}). \tag{2.6}$$

Since $y$ is finite, there exists $j^* \in \mathbb{Z}_+$ such that $s_j = 0$ for all $j > j^*$. Then

$$\mathcal{Z} = \mathcal{I} := \left\{(z_1, z_2, \ldots, z_w) \in \mathbb{Z}_+^w : z_1 = z_2 = \cdots = z_r = 1\right\} \pmod{p_j} \quad \forall j > j^*.$$

We define for $\ell > j^*$,

$$A(\ell) := \left\{x \in \mathbb{Z}^d : g(x) \in \mathcal{Z} \,(\mathrm{mod}\, P_{\mathcal{P}_\ell})\right\}, \quad A^{(k)}(\ell) := \left\{x \in \mathbb{Z}^d_{(k)} : g(x) \in \mathcal{Z} \ (\mathrm{mod}\, P_{\mathcal{P}_\ell})\right\},$$
$$A^{(k)} := \left\{x \in \mathbb{Z}^d_{(k)} : g(x) \in \mathcal{Z}\right\} \left(\subseteq A^{(k)}(\ell)\right), \quad \text{and} \quad B^{(k)}(\ell) := A^{(k)}(\ell) \setminus A^{(k)}.$$

Then we have

$$\lambda^{(k)}(\mathcal{Z}) = \frac{\#A^{(k)}}{K^d} \quad \text{and} \quad \lambda^{(k)}_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) = \frac{\#A^{(k)}(\ell)}{K^d} = \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d} \tag{2.7}$$

with $K := 2k + 1$. Therefore

$$\lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) = \lim_{k\to\infty} \lambda^{(k)}_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) = \lim_{k\to\infty} \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d}.$$

Combining with the first equation in (2.7) leads to

$$\limsup_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) \le \limsup_{k\to\infty} \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d} = \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) \tag{2.8}$$

and

$$\begin{aligned} \liminf_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) &\ge \liminf_{k\to\infty} \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d} - \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d} \\ &= \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) - \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d}. \end{aligned} \tag{2.9}$$

Once we show that

$$\limsup_{\ell\to\infty} \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d} = 0, \tag{2.10}$$

taking $\ell \to \infty$ in (2.8) and (2.9) will yield (2.6).

Now let us prove (2.10). For any $x \in B^{(k)}(\ell)$, by definition there exists $j > \ell\,(> j^*)$ such that $g(x) \notin \mathcal{Z}\,(= \mathcal{I}) \pmod{p_j}$. Hence $p_j \,|\, g_\eta(x)$ for some $\eta \le r$.

Recall that $g_\eta$ is the gcd of some relatively prime $F_i$'s. If two or more $F_i$'s are involved, then applying Lemma 2.10 to these $F_i$'s leads to two relatively prime linear combinations $\mathcal{G}_\eta$ and $\mathcal{H}_\eta$ of these $F_i$'s with integer coefficients. If there is only one $F_i$ involved, then it must be a constant since the gcd of itself is 1 in $\mathbb{Q}[x_1, x_2, \ldots, x_d]$; in this case, we take $\mathcal{G}_\eta = \mathcal{H}_\eta = F_i$ so that $\gcd(\mathcal{G}_\eta, \mathcal{H}_\eta) = 1$ still holds.

Since $p_j \,|\, g_\eta(x)$, we have $p_j \,|\, \mathcal{G}_\eta(x), \mathcal{H}_\eta(x)$. Hence

$$B^{(k)}(\ell) \subseteq \bigcup_{\eta=1}^{r} \overline{B}^{(k)}_\eta(\ell) \text{ with } \overline{B}^{(k)}_\eta(\ell) := \left\{x \in \mathbb{Z}^d_{(k)} : \exists\, j > \ell \text{ s.t. } p_j \,|\, \mathcal{G}_\eta(x), \mathcal{H}_\eta(x)\right\}. \tag{2.11}$$

Applying Lemma 2.9 to $\mathcal{G}_\eta$ and $\mathcal{H}_\eta$ gives

$$\lim_{\ell\to\infty}\limsup_{k\to\infty}\frac{\#\overline{B}_\eta^{(k)}(\ell)}{K^d}=0\ \ \forall\ \eta.$$

Combining with (2.11) and the fact that $\#B^{(k)}(\ell)\geq 0$, we obtain

$$0\leq\limsup_{\ell\to\infty}\limsup_{k\to\infty}\frac{\#B^{(k)}(\ell)}{K^d}\leq\sum_{\eta=1}^{r}\limsup_{\ell\to\infty}\limsup_{k\to\infty}\frac{\#\overline{B}_\eta^{(k)}(\ell)}{K^d}=0.$$

Hence (2.10) indeed holds. ∎

**3. SNF distribution.** Let $m\leq n$ be two positive integers. We shall define the *density* of SNF of a random $n\times m$ integer matrix as the limit (if it exists) of the density of SNF of a random $n\times m$ matrix with entries independent and uniformly distributed over $\mathbb{Z}_{(k)}$ as $k\to\infty$ (see Definition 3.1 below for a precise definition).

If we regard the minors of an $n\times m$ matrix as polynomials of the $nm$ matrix entries with integer coefficients, then the SNF of a matrix is uniquely determined by the values of these polynomials. Specifically, let $x_1,x_2,\ldots,x_{nm}$ be the $nm$ entries of an $n\times m$ matrix, $F_j$'s be the minors of an $n\times m$ matrix as elements in $\mathbb{Z}[x_1,x_2,\ldots,x_{nm}]$, and $U_i$ be the set of $i\times i$ minors ($1\leq i\leq m$). Then the SNF of this matrix is the diagonal matrix whose $i$th diagonal entry is 0 if $g_i(x)=0$ and $g_i(x)/g_{i-1}(x)$ otherwise, where $x=(x_1,x_2,\ldots,x_{nm})$ and $g_i(x)$ is defined in (2.1).

In this spirit, the multi-gcd distribution as well as the results in sections 2.1 and 2.2 have analogues for the SNF distribution of a random integer matrix. This section presents these analogues and the next section will use them to compute the density $\mu$ for some interesting types of sets.

Conventionally, the SNF is only defined for a nonzero matrix; however, for convenience, we shall define the SNF of a zero matrix to be itself, so that SNF is well-defined for all matrices. Clearly this definition does not change the density (if it exists) of SNF of a random $n\times m$ integer matrix.

We denote the SNF of an $n\times m$ matrix $M$ by $\mathrm{SNF}(M)=(\mathrm{SNF}(M)_{i,j})_{n\times m}$ and let $\mathbb{S}$ be the set of all candidates for SNF of an $n\times m$ integer matrix, i.e., the set of $n\times m$ diagonal matrices whose diagonal entries $d_1,d_2,\ldots,d_m$ are nonnegative integers such that $d_{i+1}$ is a multiple of $d_i$ $(i=1,2,\ldots,m-1)$.

For convenience, we shall always assume that the matrix entries are *independent and uniformly distributed* on its range (if known, e.g., $\mathbb{Z}_{(k)}$ or $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$) and that the notion $\mathrm{SNF}(M)\in\mathcal{S}$ or $\mathrm{SNF}(M)=D\pmod{P_{\mathcal{P}}}$ for some $\mathcal{S}\subseteq\mathbb{S}$ and $D\in\mathbb{S}$ implies the *equivalence of multiplication of the entries of $M$ by units* in $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$. Thus we can assume that the entries of $\mathrm{SNF}(M)\pmod{P_{\mathcal{P}}}$ are zero or divisors of $P_{\mathcal{P}}$.

Definition 3.1.

(i) *For $\mathcal{S}\subseteq\mathbb{S}$, we denote by $\mu^{(k)}(\mathcal{S})$ the probability that* $\mathrm{SNF}(M)\in\mathcal{S}$ *with entries of $M$ from $\mathbb{Z}_{(k)}$. If $\lim_{k\to\infty}\mu^{(k)}(\mathcal{S})=\mu(\mathcal{S})$ exists, then we say that the* probability that $\mathrm{SNF}(M)\in\mathcal{S}$ with $M$ a random $n\times m$ integer matrix *is $\mu(\mathcal{S})$. If this is the case, then $\mu(\mathcal{S})\in[0,1]$ since $\mu^{(k)}(\mathcal{S})\in[0,1]$ for all $k$.*

(ii) *We define similarly the* SNF distribution over the ring of integers mod $p^s$ *for prime $p$ and positive integer $s$; more generally, for a finite set $\mathcal{P}$ of prime and positive integer pairs $(p,s)$, we denote by $\mu_{P_{\mathcal{P}}}^{(k)}(\mathcal{S})$ (resp., $\mu_{P_{\mathcal{P}}}(\mathcal{S})$) the probability that* $\mathrm{SNF}(M)\in\mathcal{S}\pmod{P_{\mathcal{P}}}$ *with entries of $M$ from $\mathbb{Z}_{(k)}$ (resp., $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$). Note that $\mu_{P_{\mathcal{P}}}(\mathcal{S})$ is the number of matrices $M$ over $P_{\mathcal{P}}$ such that*

$\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_{\mathcal{P}}}$ *divided by* $P_{\mathcal{P}}^{nm}$. *In the special case* $\mathcal{P} = \{(p,s)\}$, *we have* $P_{\mathcal{P}} = p^s$.

In this section, we establish a formula for $\mu_{p^s}$, discuss the properties of $\mu_{P_{\mathcal{P}}}$ and $\mu$, show the existence of $\mu$, and represent it as a product of $\mu_{p^s}$'s.

**3.1. SNF distribution over $\mathbb{Z}/\boldsymbol{P_{\mathcal{P}}}\mathbb{Z}$.** We have the following formula for $\mu_{p^s}$ and analogue of Theorem 2.3 for SNFs.

THEOREM 3.2.

(i) *Given a prime* $p$, *a positive integer* $s$, *and integers* $0 = a_0 \le a_1 \le \cdots \le a_s \le a_{s+1} = m$, *let* $\boldsymbol{a} := (a_1, a_2, \ldots, a_s)$ *and* $D_{\boldsymbol{a}} \in \mathbb{S}$ *be the diagonal matrix with exactly* $(a_i - a_{i-1})$ $p^{i-1}$*'s, i.e.,* $a_i$ *non-*$p^i$*-multiples,* $1 \le i \le s$ *on its diagonal. Then*

$$\mu_{p^s}(\{D_{\boldsymbol{a}}\}) = p^{-\sum_{i=1}^{s}(n-a_i)(m-a_i)} \cdot \frac{[p,n][p,m]}{[p,n-a_s][p,m-a_s]\prod_{i=1}^{s}[p,a_i-a_{i-1}]}, \tag{3.1}$$

*where*

$$[p,0] = 1, \quad [p,\ell] := \prod_{j=1}^{\ell}\left(1-p^{-j}\right), \quad \ell \in \mathbb{Z}_+.$$

(ii) *For any* $\mathcal{S} \subseteq \mathbb{S}$, *we have*

$$\lim_{k\to\infty} \mu_{P_{\mathcal{P}}}^{(k)}(\mathcal{S}) = \mu_{P_{\mathcal{P}}}(\mathcal{S}) = \prod_{(p,s)\in\mathcal{P}} \mu_{p^s}(\mathcal{S}).$$

*Proof.* Part (ii) is a direct application of Theorem 2.3 to SNFs. For (i), we compute the number, denoted by $N$, of $n \times m$ matrices over $\mathbb{Z}/p^s\mathbb{Z}$ whose SNF is $D_{\boldsymbol{a}}$ by [8, Theorem 2] and simplify it to

$$N = p^{\sum_{i=1}^{s}\left[(n+m)a_i - a_i^2\right]} \cdot \frac{\prod_{i=0}^{a_s-1}(1-p^{-n+j})(1-p^{-m+j})}{\prod_{i=0}^{s-1}\prod_{j=1}^{a_{i+1}-a_i}(1-p^{-j})}. \tag{3.2}$$

Notice that $\mu_{p^s}(\{D_{\boldsymbol{a}}\}) = p^{-snm}N$, and thus (3.1) follows. ∎

*Remark* 3.3. When $s = 1$, formula (3.2) gives the number of $n \times m$ matrices over $\mathbb{Z}/p\mathbb{Z}$ of rank $a_1$ and is consistent with [20, Exercise 1.192(b)], whereas in the case $n = m$, formula (3.2) is consistent with [9, pp. 233, 236] (their $|\mathrm{Aut}\, H|$ is our $N$).

**3.2. SNF distribution over $\mathbb{Z}$.** The properties of $\lambda$ of set unions, subtractions, and complements in section 2.2 also carry over to SNFs. They will be useful in determining the value of $\mu$ for some specific sets (for instance, in section 4.2).

THEOREM 3.4.

(i) *Suppose that* $\{\mathcal{S}_\alpha\}_{\alpha\in\mathcal{A}}$ *are pairwise disjoint subsets of* $\mathbb{S}$ *such that* $\mu(\mathcal{S}_\alpha)$ *exists for all* $\alpha \in \mathcal{A}$. *If* $\mathcal{A}$ *is a finite set, then* $\mu(\cup_{\alpha\in\mathcal{A}}\mathcal{S}_\alpha) = \sum_{\alpha\in\mathcal{A}}\mu(\mathcal{S}_\alpha)$.

(ii) *Suppose that* $\mathcal{S}' \subseteq \mathcal{S} \subseteq \mathbb{S}$ *such that* $\mu(\mathcal{S}')$ *and* $\mu(\mathcal{S})$ *both exist. Then* $\mu(\mathcal{S} \setminus \mathcal{S}') = \mu(\mathcal{S}) - \mu(\mathcal{S}')$. *In particular for the complement* $\mathcal{S}^c$ *of* $\mathcal{S}$ *in* $\mathbb{S}$, *we have* $\mu(\mathcal{S}^c) = 1 - \mu(\mathcal{S})$.

(iii) *Suppose that* $\mathcal{T} \in \mathbb{S}$ *such that* $\mu(\mathcal{T}) = 0$. *Then for any* $\mathcal{T}' \subseteq \mathcal{T}$, *we have* $\mu(\mathcal{T}') = 0$ *as well.*

Theorem 2.6 has an analogue for SNFs as well, by virtue of the following well-known lemma (see [3, Theorem 61.1] for an easy proof).

LEMMA 3.5. *Fix a positive integer $r$. The determinant of an $r \times r$ matrix as a polynomial of its $r^2$ entries $x_1, x_2, \ldots, x_{r^2}$ is irreducible in $\mathbb{Q}[x_1, x_2, \ldots, x_{r^2}]$.*

For any $i \le m \wedge (n-1)$ (i.e., $\min\{m, n-1\}$), the set $U_i$ contains at least two different minors, which are both irreducible as polynomials of the entries Lemma 3.5 and therefore relatively prime. Hence Assumption 2.5 holds with $w = m \wedge (n-1)$. This allows us to apply Theorem 2.6 to SNFs and obtain the following analogue. In addition, we will compute the density $\mu(\mathcal{S})$ explicitly later in section 4.1.

THEOREM 3.6. *Given positive integers $r \le m \wedge (n-1)$ and $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$, let $z = \prod_{j=1}^{\infty} p_j^{s_j}$ with $p_j$ the $j$th smallest prime and $s_j$ nonnegative integers $(j = 1, 2, \ldots)$ such that $d_r \,|\, z$, then the probability $\mu(\mathcal{S})$ exists for the set*

$$\mathcal{S} = \{D := (D_{i,j})_{n\times m} \in \mathbb{S} : \ D_{i,i} = d_i \ \forall\ i \le r\}, \tag{3.3}$$

*and in fact*

$$\mu(\mathcal{S}) = \prod_{j=1}^{\infty} \mu_{p_j^{s_j+1}}(\mathcal{S}). \tag{3.4}$$

*Note that the right-hand side of* (3.4) *is well-defined since $\mu_{p^s} \in [0,1]$ for all $p$ and $s$.*

We have assumed that $r \le m \wedge (n-1)$; otherwise, we must have $r = m = n$ (note that $r \le m \le n$) and $\mu(\mathcal{S}) = 0$. In fact, any matrix $M$ with $\mathrm{SNF}(M) \in \mathcal{S}$ satisfies $|M| = \pm d_1 d_2 \cdots d_n$. We will show later (Theorem 4.5) that the probability that the determinant of a random $n \times n$ integer matrix equals $c$ is 0 for all constant $c$. It then follows from Theorem 3.4(iii) that $\mu(\mathcal{S}) = 0$.

We have also assumed that the $d_i$'s are positive; in fact, we have $\mu(\mathcal{S}) = 0$ otherwise. If $d_i = 0$ for some $i$, then all $i \times i$ minors of any matrix $M$ with $\mathrm{SNF}(M) \in \mathcal{S}$ are zero. Thus Theorems 3.4(iii) and 4.5 with $c = 0$ lead to $\mu(\mathcal{S}) = 0$.

**4. Applications.** Now we apply Theorems 3.2 and 3.6 to compute the density $\mu$ explicitly for the following subsets of $\mathbb{S}$: matrices with first few diagonal entries given (i.e., with the form of (3.3)), full rank matrices, a finite subset (in particular, matrices with diagonal entries all equal to 1), and square matrices with at most $\ell\,(= 1, 2, \ldots, n)$ diagonal entries not equal to 1.

**4.1. Density of the set** (3.3)**.** For the set $\mathcal{S}$ of (3.3), i.e., of matrices with first $r$ diagonal entries given, we take $z = d_r$ in Theorem 3.6 and compute $\mu_{p^{s+1}}(\mathcal{S})$ for each $(p, s) = (p_j, s_j)$. Working modulo $p^{s+1}$, the set $\mathcal{S}$ has $m - r + 1$ elements (see (4.12) below), and formula (3.1) gives the density $\mu_{p^{s+1}}$ of each element of $\mathcal{S}$. Thus one can take the sum over $\mathcal{S}$ to get an expression for $\mu_{p^{s+1}}(\mathcal{S})$, and compute this sum explicitly when $m - r$ is small, such as in Theorems 4.8 and 4.9 below. However, this sum is hard to compute when $m - r$ is large, for example, when $m$ is large and $r$ is fixed; in this case, we recast $\mathcal{S}$ as the difference between a subset of $\mathbb{S}$ and the union of other $r - 1$ subsets such that for each of these $r$ sets, its density $\mu_{p^{s+1}}$ is given directly by (3.1).

We work out two examples to illustrate this idea and then deal with the general case.

**4.1.1. The first example: Relatively prime entries.** Our approach reproduces the following result mentioned at the beginning of this paper.

THEOREM 4.1. *Let $\mathcal{S}$ be the set of* (3.3) *with $r = 1$ and $d_1 = 1$. Then we have*

$$\mu(\mathcal{S}) = \frac{1}{\zeta(nm)}, \tag{4.1}$$

*where $\zeta(\cdot)$ is the Riemann zeta function.*

*Proof.* Applying Theorem 3.6 with $r = 1$, $d_1 = 1$, and $s_j = 0$, $j = 1, 2, \ldots$, gives

$$\mu(\mathcal{S}) = \prod_p \mu_p(\mathcal{S}), \tag{4.2}$$

so it reduces to computing $\mu_p(\mathcal{S})$ for each $p$.

Recalling the equivalence of multiplication by units, we see that the matrix entries modulo $p$ can only be 1 or 0. Thus the set $\mathcal{S} \pmod p$ consists of all the matrices in $\mathbb{S}$ whose first diagonal entry is 1, i.e., $\mathcal{S} = \{D_{(a_1)} : a_1 \geq 1\} \pmod p$ (recall the notation $D_{(a_1,a_2,\ldots,a_s)}$ from Theorem 3.2). Therefore

$$\mu_p(\mathcal{S}) = 1 - \mu_p(\{D_{(0)}\}) = 1 - p^{-nm}$$

by applying (3.1) to $\mu_p(\{D_{(0)}\})$. Plugging into (4.2) with the Euler product formula

$$\prod_p \left(1 - p^{-i}\right) = \frac{1}{\zeta(i)} \in (0, 1), \quad i \geq 2, \tag{4.3}$$

yields (4.1). ∎

**4.1.2. Another example.**

THEOREM 4.2. *Let $\mathcal{S}$ be the set of* (3.3) *with $r = 2$, $d_1 = 2$, and $d_2 = 6$. Then*

$$\mu(\mathcal{S}) = \mu_{2^2}(\mathcal{S})\, \mu_{3^2}(\mathcal{S}) \prod_{p>3} \mu_p(\mathcal{S}), \tag{4.4}$$

*where*

$$\mu_{2^2}(\mathcal{S}) = 2^{-nm} \left(1 - 2^{-nm} - 2^{-(n-1)(m-1)} \cdot \frac{(1 - 2^{-n})\,(1 - 2^{-m})}{1 - 2^{-1}}\right), \tag{4.5}$$

$$\mu_{3^2}(\mathcal{S}) = 3^{-(n-1)(m-1)} \left(1 - 3^{-(n-1)(m-1)}\right) \frac{(1 - 3^{-n})\,(1 - 3^{-m})}{1 - 3^{-1}}, \tag{4.6}$$

$$\begin{aligned} \mu_p(\mathcal{S}) &= 1 - p^{-nm} - p^{-(n-1)(m-1)} \cdot \frac{(1 - p^{-n})\,(1 - p^{-m})}{1 - p^{-1}} \\ &= 1 - \sum_{i=(n-1)(m-1)}^{(n-1)m} p^{-i} + \sum_{i=n(m-1)+1}^{nm-1} p^{-i}. \end{aligned} \tag{4.7}$$

*Proof.* The first equation (4.4) follows directly from Theorem 3.6 with $r = 2$, $d_1 = 2$, $d_2 = z = 6$, $s_1 = s_2 = 1$, $s_j = 0$, $j \geq 3$. Therefore it reduces to calculating $\mu_{p^s}(\mathcal{S})$ for $(p, s) = (2, 2)$, $(3, 2)$, and $(p, 1)$ with $p > 3$.

*Case* 1. $p > 3$ and $s = 1$. The matrix entries modulo $p$ (up to multiplication by units) can only be 1 or 0. Thus the set $\mathcal{S} \pmod p$ consists of all the matrices in $\mathbb{S}$ whose first two diagonal entries are 1, i.e., $\mathcal{S} = \{D_{(a_1)} : a_1 \geq 2\} \pmod p$ (recall the notation $D_{(a_1,a_2,\ldots,a_s)}$ from Theorem 3.2). Therefore

$$\mu_p(\mathcal{S}) = 1 - \mu_p(\{D_{(0)}\}) - \mu_p(\{D_{(1)}\}).$$

Then we apply (3.1) to $\mu_p(\{D_{(0)}\})$ and $\mu_p(\{D_{(1)}\})$, and (4.7) follows.

*Case* 2. $p = 2$ and $s = 2$. The matrix entries modulo $2^2$ can be 1, 2 or 0. Thus the set $\mathcal{S} \pmod{2^2}$ consists of all the matrices in $\mathbb{S}$ whose first two diagonal entries are 2, i.e., $\mathcal{S} = \{D_{(a_1,a_2)} : a_1 = 0,\ a_2 \geq 2\} \pmod{2^2}$. Therefore

$$\mu_{2^2}(\mathcal{S}) = \mu_{2^2}(\{D_{(a_1,a_2)} : a_1 = 0\}) - \mu_{2^2}(\{D_{(0,0)}\}) - \mu_{2^2}(\{D_{(0,1)}\}). \tag{4.8}$$

Notice that the set $\{D_{(a_1,a_2)} : a_1 = 0\} \pmod{2^2}$ consists of all the matrices in $\mathbb{S}$ whose diagonal entries are all multiples of 2 (i.e., 2 or 0) or, equivalently, the zero matrix in mod 2. Hence

$$\mu_{2^2}(\{D_{(a_1,a_2)} : a_1 = 0\}) = \mu_2(\{D_{(0)}\}).$$

Plugging into (4.8) and applying (3.1) to $\mu_2(\{D_{(0)}\})$, $\mu_{2^2}(\{D_{(0,0)}\})$, and $\mu_{2^2}(\{D_{(0,1)}\})$, we obtain (4.5).

*Case* 3. $p = 3$ and $s = 2$. The matrix entries in mod $3^2$ can be 1, 3, or 0. Thus the set $\mathcal{S} \pmod{3^2}$ consists of all the matrices in $\mathbb{S}$ whose first two diagonal entries are 1 and 3, respectively, i.e., $\mathcal{S} = \{D_{(a_1,a_2)} : a_1 = 1,\ a_2 \geq 2\} \pmod{3^2}$. Therefore

$$\mu_{3^2}(\mathcal{S}) = \mu_{3^2}(\{D_{(a_1,a_2)} : a_1 = 1\}) - \mu_{3^2}(\{D_{(1,1)}\}). \tag{4.9}$$

Notice that the set $\{D_{(a_1,a_2)} : a_1 = 1\} \pmod{3^2}$ consists of all the matrices in $\mathbb{S}$ whose first diagonal entry is 1 and all other diagonal entries are multiples of 3 (i.e., 3 or 0), equivalently, the $\mathrm{diag}(1, 0, 0, \ldots, 0)$ in mod 3. Hence

$$\mu_{3^2}(\{D_{(a_1,a_2)} : a_1 = 1\}) = \mu_3(\{D_{(1)}\}).$$

Plugging into (4.9) and applying (3.1) to $\mu_3(\{D_{(1)}\})$ and $\mu_{3^2}(\{D_{(1,1)}\})$, we obtain (4.6). ∎

### 4.1.3. The general case.

THEOREM 4.3. *Let $\mathcal{S}$ be the set of* (3.3) *in Theorem* 3.6 *with $d_r = \prod_{j=1}^{\infty} p_j^{s_j}$. Then for $(p, s) = (p_j, s_j)$, $j = 1, 2, \ldots$, we have*

$$\begin{aligned}\mu_{p^{s+1}}(\mathcal{S}) = {} & \frac{p^{-\sum_{i=1}^{s}(n-\tilde{a}_i)(m-\tilde{a}_i)} \cdot [p,n][p,m]}{[p,n-\tilde{a}_s][p,m-\tilde{a}_s]\prod_{i=1}^{s}[p,\tilde{a}_i-\tilde{a}_{i-1}]} \\ & - \sum_{\ell=\tilde{a}_s}^{r-1} \frac{p^{-(n-\ell)(m-\ell)-\sum_{i=1}^{s}(n-\tilde{a}_i)(m-\tilde{a}_i)} \cdot [p,n][p,m]}{[p,n-\ell][p,m-\ell][p,\ell-\tilde{a}_s]\prod_{i=1}^{s}[p,\tilde{a}_i-\tilde{a}_{i-1}]},\end{aligned} \tag{4.10}$$

*where $\tilde{a}_i$ $(0 \leq i \leq s)$ is the number of non-$p^i$-multiples among $d_1, d_2, \ldots, d_r$ (thus $\tilde{a}_s \leq r-1$). In particular, when $s = 0$ (which holds for all but finitely many $j$'s), we have*

$$\mu_p(\mathcal{S}) = 1 - \sum_{\ell=0}^{r-1} p^{-(n-\ell)(m-\ell)} \cdot \frac{[p,n][p,m]}{[p,n-\ell][p,m-\ell][p,\ell]}\,. \tag{4.11}$$

*The value of $\mu(\mathcal{S})$ is then given by Theorem* 3.6 *with $z = d_r$.*

*Proof.* Recalling from Theorem 3.2 the notation of $D_{(a_1,a_2,\ldots,a_{s+1})}$, we recast $\mathcal{S}$ as

$$\mathcal{S} = \{D_{(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\,,\ a_{s+1} \ge r\} \pmod{p^{s+1}}, \tag{4.12}$$

and therefore

$$\begin{aligned}\mu_{p^{s+1}}(\mathcal{S}) = {} & \mu_{p^{s+1}}(\{D_{(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\}) \\ & - \sum_{\ell=\tilde{a}_s}^{r-1} \mu_{p^{s+1}}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s,\ell)}\}).\end{aligned} \tag{4.13}$$

Notice that the set $\{D_{(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\} \pmod{p^{s+1}}$ in the first term on the right-hand side of (4.13) consists of all the matrices in $\mathbb{S}$ with exactly $\tilde{a}_i$ $(1 \le i \le s)$ non-$p^i$-multiples on its diagonal, equivalently, the diagonal matrix in $\mathbb{S}$ with exactly $\tilde{a}_i$ non-$p^i$-multiples $(1 \le i \le s)$ in mod $p^s$. Hence

$$\mu_{p^{s+1}}(\{D_{(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\}) = \mu_{p^s}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s)}\}).$$

Plugging into (4.13) and applying (3.1) to get formulas for $\mu_{p^s}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s)}\})$ and $\mu_{p^{s+1}}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s,\ell)}\})$ for $1 \le \ell \le r-1$, we obtain (4.10). ∎

*Remark* 4.4. We notice that the density $\mu_{p^s}(\{D_{\boldsymbol{a}}\})$ of (3.1) is a polynomial in $p^{-1}$ with integer coefficients since $m - a_s + \sum_{i=1}^{s}(a_i - a_{i-1}) = m$. The $\mu_p(\mathcal{S})$ of (4.11) is also a polynomial in $p^{-1}$ with integer coefficients and with constant term 1 (see the $\mu_p(\mathcal{S})$ of (4.7) as an example). If we replace each occurrence of $p$ by $p^{\boldsymbol{z}}$, where $\boldsymbol{z}$ is a complex variable, and plug into (3.4) of Theorem 3.6, we get an Euler product for some kind of generalized zeta function.

For instance, when $m = n = 3$, for the set $\mathcal{S}$ in Theorem 4.2, we apply (4.7),

$$\mu_p(\mathcal{S}) = 1 - p^{-4} - p^{-5} - p^{-6} + p^{-7} + p^{-8} = \left(1 - p^{-2}\right)\left(1 - p^{-3}\right)\left(1 + p^{-2} + p^{-3}\right),$$

take the product over all primes $p$, and apply the Euler product formula (4.3) to get

$$\prod_p \mu_p(\mathcal{S}) = \frac{1}{\zeta(2)\zeta(3)} \prod_p \left(1 + p^{-2} + p^{-3}\right).$$

Plugging into (4.4), we see that to obtain the density $\mu(\mathcal{S})$, it reduces to computing $\prod_p(1 + p^{-2} + p^{-3})$, or to understanding the Euler product $\prod_p(1 + p^{-2\boldsymbol{z}} + p^{-3\boldsymbol{z}})$.

It would be interesting to study whether such an Euler product for some generalized zeta function, first, has any interesting properties relevant to SNF, second, extends to a meromorphic function on all of $\mathbb{C}$, and third, satisfies a functional equation.

**4.2. The determinant.** The determinant of an $m \times m$ matrix can be regarded as a polynomial $G$ of its $m^2$ entries. Since $G$ is not a constant we can apply Theorem 2.8 to $G$ and obtain the following result.

THEOREM 4.5. *Let $c$ be an integer. The probability that the determinant equals $c$ for an $m \times m$ matrix with entries from $\mathbb{Z}_{(k)}$ goes to* 0 *as $k \to \infty$; in other words, the density of the determinant of a random $m \times m$ integer matrix is always* 0.

This result agrees with [13, Theorem 1] for the case $c = 0$ and [6, Theorem 1.2 and Example 1.6] for the case $c \neq 0$. It also leads to the following two corollaries. The first of them shows that the probability of a full rank integer matrix is 1.

COROLLARY 4.6. *If $\mathcal{S} \subseteq \mathbb{S}$ satisfies $D_{m,m} = 0$ for all $D = (D_{i,j})_{n\times m} \in \mathcal{S}$, then we have $\mu(\mathcal{S}) = 0$; in other words, the probability of a full rank $n \times m$ matrix with entries from $\mathbb{Z}_{(k)}$ goes to 1 as $k \to \infty$.*

*Proof.* If $\mathrm{SNF}(M) \in \mathcal{S}$, then all $m \times m$ minors of $M$ are zero. The result then follows from Theorem 4.5 with $c = 0$ and Theorem 3.4(iii). ∎

When $m = n$, we can generalize Corollary 4.6 to any finite subset $\mathcal{S} \subset \mathbb{S}$.

COROLLARY 4.7. *Suppose that $m = n$ and $\mathcal{S} \subset \mathbb{S}$. Then we have $\mu(\mathcal{S}) = 0$ if the set $\{D_{n,n} : D = (D_{i,j})_{n\times n} \in \mathcal{S}\}$ is finite; in particular, this holds for any finite subset $\mathcal{S} \subset \mathbb{S}$.*

*Proof.* For any $M$ such that $D = \mathrm{SNF}(M) \in \mathcal{S}$, we have $|M| = \pm D_{1,1} \cdots D_{n,n}$. If $D_{n,n} = 0$, then $|M| = 0$; if $D_{n,n} \neq 0$, then the $D_{i,i}$'s are divisors of $D_{n,n}$ and therefore $|M|$ has finitely many choices. We then conclude by Theorems 4.5 and 3.4(iii). ∎

**4.3. Probability that all diagonal entries of an SNF are 1.** Corollary 4.7 with Theorem 3.4(iii) implies that the probability that all diagonal entries of an SNF are 1 is 0 if $m = n$; however, this probability is positive if $m < n$.

THEOREM 4.8. *Let $E$ be the $n \times m$ matrix* $\mathrm{diag}(1, 1, \ldots, 1)$. *If $m < n$, then*

$$\mu(\{E\}) = \frac{1}{\prod_{i=n-m+1}^{n} \zeta(i)} \to \begin{cases} 1 & \text{if } m \text{ is fixed} \\ \frac{1}{\prod_{i=n-m+1}^{\infty} \zeta(i)} & \text{if } n-m \text{ is fixed} \end{cases} \quad \text{as} \quad n \to \infty\,.$$

*Proof.* Apply Theorem 3.6 with $\mathcal{S} = \{E\}$, $r = m$, $d_i = z = 1$, $s_j = 0$ for all $i, j$, Theorem 3.2 with $s = 1$, $a_1 = m$, and finally the Euler product formula (4.3):

$$\mu(\{E\}) = \prod_p \mu_p(\{E\}) = \prod_p \frac{[p,n]}{[p,n-m]} = \prod_{i=n-m+1}^{n} \prod_p \left(1 - p^{-i}\right) = \frac{1}{\prod_{i=n-m+1}^{n} \zeta(i)}\,,$$

thanks to $n > m$. Then we derive the limits from the fact that $\zeta(i) \downarrow 1$ as $i \to \infty$. ∎

**4.4. Probability that at most $\ell$ diagonal entries of an SNF are not 1.** In this section, we assume that $m = n$. We provide a formula for the probability that an SNF has at most $\ell$ diagonal entries not equal to 1 and a formula for the limit of this probability as $n \to \infty$. In particular, when $\ell = 1$, this limit is the reciprocal of a product of values of the Riemann zeta function at positive integers and equals $0.846936\ldots$. For bigger $\ell$, we prove that this limit converges to 1 as $\ell \to \infty$ and find its asymptotics (see Theorem 4.13).

**4.4.1. Cyclic SNFs ($\ell = 1$).** We shall say that an SNF is *cyclic* if it has at most one diagonal entry not equal to 1, i.e., if the corresponding cokernel is cyclic. Denote the set of $n \times n$ cyclic SNFs by $\mathcal{T}_n$. We will compute the probability $\mu(\mathcal{T}_n)$ of having a cyclic SNF and show that this probability strictly decreases to $1/(\zeta(6)\prod_{i=4}^{\infty}\zeta(i)) \approx 0.846936$ as $n \to \infty$. As mentioned above, this result was first obtained by Ekedahl [7, section 3]. We present a complete and more detailed proof via a slightly different approach (in particular, for the second equality of (4.16) below).

THEOREM 4.9. *Let $Z_n = \mu(\mathcal{T}_n)$. Then we have*

$$Z_n = \frac{\prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^n}\right)}{\prod_{i=2}^{n} \zeta(i)} \downarrow \frac{1}{\zeta(6)\prod_{i=4}^{\infty}\zeta(i)} \approx 0.846936 \quad \text{as} \quad n \to \infty\,. \tag{4.14}$$

*In particular, when $n = 2$, we have $Z_2 = 1/\zeta(4) = 90/\pi^4 \approx 0.923938$.*

*Proof.*

(i) For the first equality, we apply Theorem 3.6 with $\mathcal{S} = \mathcal{T}_n$, $r = n-1$, $d_i = z = 1$, $s_j = 0$ for all $i, j$, and then Theorem 3.2 with $s = 1$, $a_1 = n$, $n-1$:

$$Z_n = \prod_p \mu_p(\mathcal{T}_n) = \prod_p \frac{[p,n]}{[p,1]} \left(1 - p^{-1} + \frac{p^{-1}(1-p^{-n})}{1-p^{-1}}\right) = \frac{\prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^n}\right)}{\prod_{i=2}^n \zeta(i)}.$$

Here in the last equality we used the Euler product formula (4.3):

$$\prod_p \frac{[p,n]}{[p,1]} = \prod_p \prod_{i=2}^n \left(1 - p^{-i}\right) = \prod_{i=2}^n \prod_p \left(1 - p^{-i}\right) = \frac{1}{\prod_{i=2}^n \zeta(i)}. \tag{4.15}$$

(ii) For the monotonicity of $Z_n$, we consider the ratio $Z_{n+1}/Z_n$ and see that

$$\frac{Z_{n+1}}{Z_n} = \prod_p \left(1 - p^{-(n+1)}\right) \frac{\left(1 + p^{-2} + p^{-3} + \cdots + p^{-n}\right) + p^{-(n+1)}}{1 + p^{-2} + p^{-3} + \cdots + p^{-n}} < 1,$$

since for each $p$, the factor is at most $(1 - p^{-(n+1)})(1 + p^{-(n+1)}) = 1 - p^{-2(n+1)} < 1$.

(iii) To find $\lim_{n\to\infty} Z_n$, we assume that $n \geq 3$. It suffices to show that

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)} = \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) = \lim_{n\to\infty} \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^n}\right). \tag{4.16}$$

For ease of notation, let $t := p^{-1}$. For the first equality of (4.16), we observe that

$$1 + t^2 + t^3 + \cdots = 1 + \frac{t^2}{1-t} = \frac{1 - t + t^2}{1-t} = \frac{1+t^3}{(1+t)(1-t)} = \frac{1-t^6}{(1-t^2)(1-t^3)}. \tag{4.17}$$

Taking the product of this equation over all reciprocals $t$ of primes and applying the Euler product formula (4.3) yields the desired equality.

For the second equality of (4.16), we see that

$$1 > \prod_t \frac{1 + t^2 + t^3 + \cdots + t^n}{1 + t^2 + t^3 + \cdots} = \prod_t \left(1 - \frac{t^{n+1} + t^{n+2} + \cdots}{1 + t^2 + t^3 + \cdots}\right) > \prod_t (1 - t^{n-1}) = \frac{1}{\zeta(n-1)}$$

which converges to 1 as $n \to \infty$. Here $\prod_t$ represents a product over all reciprocals $t$ of primes.

One can also show the second equality of (4.16) using the fact that

$$1 < 1 + p^{-2} + p^{-3} + \cdots + p^{-n} \uparrow 1 + p^{-2} + p^{-3} + \cdots \quad \text{as } n \to \infty$$

and the following version of the monotone convergence theorem (which will also be useful in Theorem 4.14(iii)) with $x_{i,j} = 1 + p_i^{-2} + p_i^{-3} + \cdots + p_i^{-j}$ and $x_i = 1 + p_i^{-2} + p_i^{-3} + \cdots$. ∎

LEMMA 4.10. *If real numbers $x_{i,j}$ $(i, j = 1, 2, \ldots)$ satisfy $1 \leq x_{i,j} \uparrow x_i$ as $j \to \infty$ for all $i$, then we have*

$$\lim_{j\to\infty} \prod_{i=1}^{\infty} x_{i,j} = \prod_{i=1}^{\infty} x_i.$$

*Here we allow the products and the limit to be infinity.*

*Proof.* Apply the monotone convergence theorem to $\log x_{i,j}$ ($\geq 0$).

(iv) When $n = 2$, we derive from the first equality of (4.14) along with (4.3) that

$$Z_2 = \prod_p \left(1 - p^{-2}\right)\left(1 + p^{-2}\right) = \prod_p \left(1 - p^{-4}\right) = \frac{1}{\zeta(4)}\,.$$

∎

*Remark* 4.11.

(1) The proof of the convergence result in Theorem 4.9 is reminiscent of (though not directly related to) [20, Exercise 1.186(c)].

(2) Later Nguyen and Shparlinski [16, (1.2)] showed that if we take a subgroup of $\mathbb{Z}^n$ uniformly among all subgroups of index at most $V$ and let $V \to \infty$, then the probability that the quotient group is cyclic is also $\mu(\mathcal{T}_n)$. This result is equivalent to computing the probability that an $n \times n$ integer matrix has a cyclic cokernel using a certain probability distribution different from $\mu$. We do not know a simple reason why these two probability distributions yield the same probability of a cyclic cokernel. Perhaps there is a universality result which gives the same conclusion for a wide class of probability distributions.

**4.4.2. More generators (general $\ell$).** Now we consider the SNFs with at most $\ell\,(\leq n)$ diagonal entries not equal to 1, i.e., whose corresponding cokernel has at most $\ell$ generators. Denote the set of such $n \times n$ SNFs by $\mathcal{T}_n(\ell)$. In particular, when $\ell = n$, we have $\mu(\mathcal{T}_n(n)) = 1$. The above discussion on cyclic SNFs is for the case $\ell = 1$. We will compute the density $\mu(\mathcal{T}_n(\ell))$ and its limit as $n \to \infty$, show that this limit increases to 1 as $\ell \to \infty$, and establish its asymptotics.

We start with a lemma which will play an important role in our proof.

LEMMA 4.12. *For any real number $x \in (0, 1/2]$, the positive sequence $\{[1/x, k] := \prod_{j=1}^{k}(1 - x^j)\}_{k=1}^{\infty}$ is decreasing and thus has a limit as $k \to \infty$:*

$$C(x) := (1 - x)\,(1 - x^2)\cdots \in \left[e^{-2x/(1-x)}, 1\right). \tag{4.18}$$

*This also implies that $C(x) \to 1$ as $x \to 0$ and that $[1/x, k] \in [e^{-2x/(1-x)}, 1)$ for all $x \in (0, 1/2]$ and $k \geq 1$.*

*In particular, when $x = 1/p$, we have*

$$[p, k] \downarrow C_p := C(1/p) \in \left[e^{-2/(p-1)}, 1\right) \subseteq \left[e^{-2}, 1\right) \quad \text{as} \quad k \to \infty\,, \tag{4.19}$$

*$C_p \to 1$ as $p \to \infty$, and $[p, k] \in [e^{-2/(p-1)}, 1)$ for all $p$ and $k \geq 1$.*

*Proof.* The sequence $[1/x, k]$ is decreasing in $k$ because $0 < 1 - x^j < 1$ for all $j$.

To get the lower bound for $C(x)$, we will use the following inequality:

$$\ln y \geq -\frac{1 - y}{y}\,, \quad y \in (0, 1]. \tag{4.20}$$

To see this, let $\psi(y) := \ln y + (1 - y)/y$. Then $\psi'(y) = 1/y - 1/y^2 \leq 0$. Hence $\psi(y) \leq \psi(1) = 0$.

Applying (4.20) with $y = 1 - x^j$ ($j = 1, 2, \ldots, k$) yields

$$\ln [1/x, k] = \sum_{j=1}^{k} \ln\left(1 - x^j\right) \geq -\sum_{j=1}^{k} \frac{x^j}{1 - x^j} \geq -\sum_{j=1}^{k} 2x^j = -\frac{2x}{1 - x}\,,$$

since $x^j \leq x \leq 1/2$. Hence $C(x) = \lim_{k\to\infty}[1/x, k] \geq e^{-2x/(1-x)}$. ∎

The main results of this subsection are as follows.

THEOREM 4.13. *We have*

$$\mu(\mathcal{T}_n(\ell)) = \frac{1}{\prod_{i=2}^{n}\zeta(i)}\prod_p [p,1]\sum_{i=0}^{\ell}\frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]} \to \prod_p C_p \sum_{i=0}^{\ell}\frac{p^{-i^2}}{[p,i]^2} \quad \text{as} \quad n\to\infty$$

*and*

$$\lim_{n\to\infty}\mu(\mathcal{T}_n(\ell)) \uparrow 1 \text{ and } \lim_{n\to\infty}\mu(\mathcal{T}_n(\ell)) = 1 - C_2^{-1}\cdot 2^{-(\ell+1)^2}\big[1-2^{-\ell}+O\big(4^{-\ell}\big)\big] \text{ as } \ell\to\infty,$$

*where* $C_2^{-1} = 1/((1-2^{-1})(1-2^{-2})\cdots) \approx 3.46275$.

We split the proof into the following five parts.

THEOREM 4.14. *Let*

$$Z_n(\ell) = \mu(\mathcal{T}_n(\ell)), \quad Z_n(p,\ell) = \mu_p(\mathcal{T}_n(\ell)) = [p,n]\sum_{i=0}^{\ell}\frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]} \tag{4.21}$$

*and*

$$Y_n(p,\ell) = \frac{[p,1]}{[p,n]}Z_n(p,\ell) = [p,1]\sum_{i=0}^{\ell}\frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]}\,. \tag{4.22}$$

*Then we have the following results:*

(i)

$$Z_n(\ell) = \prod_p Z_n(p,\ell) = \frac{1}{\prod_{i=2}^{n}\zeta(i)}\prod_p Y_n(p,\ell);$$

(ii)

$$Y_n(p,\ell) \uparrow [p,1]\sum_{i=0}^{\ell}\frac{p^{-i^2}}{[p,i]^2} =: Y(p,\ell) \quad \text{as} \quad n\to\infty \tag{4.23}$$

*and*

$$Y(p,\ell) \uparrow \frac{[p,1]}{C_p} \quad \text{as} \quad \ell\to\infty, \tag{4.24}$$

*where* $C_p = (1-p^{-1})(1-p^{-2})\cdots$ *as defined in* (4.19) *and* (4.18)*; further, combining with definition* (4.22) *and Lemma* 4.12*, it follows that*

$$Z_n(p,\ell) = \frac{[p,n]}{[p,1]}Y_n(p,\ell) \to \frac{C_p}{[p,1]}Y(p,\ell) = C_p\sum_{i=0}^{\ell}\frac{p^{-i^2}}{[p,i]^2} =: Z(p,\ell) \text{ as } n\to\infty \tag{4.25}$$

*and*

$$Z(p,\ell) \uparrow 1 \quad \text{as} \quad \ell\to\infty; \tag{4.26}$$

(iii)

$$Z_n(\ell) \to \frac{\prod_p Y(p,\ell)}{\prod_{i=2}^{\infty}\zeta(i)} = \prod_p \frac{C_p}{[p,1]} Y(p,\ell) = \prod_p Z(p,\ell) := Z(\ell) \quad \text{as} \quad n \to \infty \tag{4.27}$$

*and*

$$Z(\ell) \uparrow 1 \quad \text{as} \quad \ell \to \infty\,;$$

(iv)

$$Z(p,\ell) = 1 - C_p^{-1} \cdot p^{-(\ell+1)^2}\left[1 - \frac{2}{p^2-p}\cdot p^{-\ell} + O\left(p^{-2\ell}\right)\right] \quad \text{as} \quad \ell \to \infty\,, \tag{4.28}$$

*and more precisely, this* $O(p^{-2\ell}) \in (0, 2p^{-2\ell})$*;*

(v)

$$Z(\ell) = 1 - C_2^{-1} \cdot 2^{-(\ell+1)^2}\left[1 - 2^{-\ell} + O\left(4^{-\ell}\right)\right] \quad \text{as} \quad \ell \to \infty\,, \tag{4.29}$$

*where* $C_2^{-1} = 1/((1-2^{-1})(1-2^{-2})\cdots) \approx 3.46275$.

Figure 1 and Table 1 illustrate the asymptotics (4.29) of $Z(\ell)$ and the fast rate of convergence.

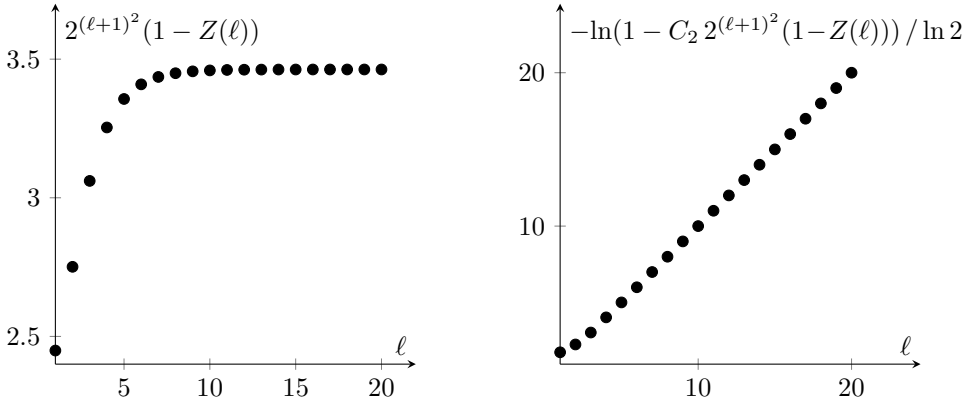


FIG. 1. *Asymptotics of* $Z(\ell)$.

TABLE 1
*Asymptotics of* $Z(\ell)$ *with* $f(\ell) := -\ln\left[1 - C_2\,2^{(\ell+1)^2}(1-Z(\ell))\right]/\ln 2$.

| $\ell$ | $Z(\ell)$ | $1-Z(\ell)$ | $2^{(\ell+1)^2}(1-Z(\ell))$ | $f(\ell)$ |
|---|---|---|---|---|
| 1 | 0.846935901735 | $1.53064098265 \times 10^{-1}$ | 2.44902557224 | 1.77225611430 |
| 2 | 0.994626883543 | $5.37311645734 \times 10^{-3}$ | 2.75103562616 | 2.28255339912 |
| 3 | 0.999953295075 | $4.67049248389 \times 10^{-5}$ | 3.06085395424 | 3.10703467197 |
| 4 | 0.999999903035 | $9.69645493161 \times 10^{-8}$ | 3.25359037644 | 4.04926385851 |
| 5 | 0.999999999951 | $4.88413458245 \times 10^{-11}$ | 3.35635172814 | 5.02441603986 |
| 6 | 1.000000000000 | $6.05577286766 \times 10^{-15}$ | 3.40909705378 | 6.01220652280 |
| 7 | 1.000000000000 | $1.86255532064 \times 10^{-19}$ | 3.43580813230 | 7.00610418193 |
| 8 | 1.000000000000 | $1.42657588960 \times 10^{-24}$ | 3.44924885316 | 8.00305233425 |
| 9 | 1.000000000000 | $2.72629586798 \times 10^{-30}$ | 3.45599059345 | 9.00152622794 |
| 10 | 1.000000000000 | $1.30126916909 \times 10^{-36}$ | 3.45936681921 | 10.0007631292 |

*Proof.*

(i) The first equality follows from Theorem 3.6 with $\mathcal{S} = \mathcal{T}_n(\ell)$, $r = n - \ell$, $d_i = z = 1$, $s_j = 0$ for all $i, j$, and Theorem 3.2 with $s = 1$, $a_1 = n, n-1, \ldots, n-\ell$. The second equality follows from definition (4.22) and (4.15).

(ii) The first result (4.23) follows from the observation

$$\frac{[p,n]}{[p,n-i]} = \left(1-p^{-n}\right)\left(1-p^{-(n-1)}\right)\cdots\left(1-p^{-(n-i+1)}\right) \uparrow 1 \quad \text{as} \quad n \to \infty\,.$$

For the second result (4.24), by definition we see that

$$Y_n(p,n) = \frac{[p,1]}{[p,n]}\mu_p(\mathcal{T}_n(n)) = \frac{[p,1]}{[p,n]} \quad \text{and, similarly,} \quad Y_\ell(p,\ell) = \frac{[p,1]}{[p,\ell]}\,.$$

Since $Y_n(p,\ell)$ is also increasing in $\ell$ by definition (4.22), so is $Y(p,\ell)$. Thus we have

$$\frac{[p,1]}{[p,\ell]} = Y_\ell(p,\ell) \le Y_n(p,\ell) \le Y_n(p,n) = \frac{[p,1]}{[p,n]} < \frac{[p,1]}{C_p} \quad \forall\, \ell \le n\,.$$

Taking $n \to \infty$ yields

$$\frac{[p,1]}{[p,\ell]} \le Y(p,\ell) \le \frac{[p,1]}{C_p}\,.$$

Then taking $\ell \to \infty$ and applying Lemma 4.12 leads to (4.24).

(iii) It follows from definitions (4.21) and (4.22) that

$$Z_n(\ell) = \prod_p Z_n(p,\ell) = \left(\prod_p \frac{[p,n]}{[p,1]}\right)\prod_p Y_n(p,\ell). \tag{4.30}$$

By virtue of (4.15), the first product on the right-hand side of (4.30) becomes

$$\prod_p \frac{[p,n]}{[p,1]} = \frac{1}{\prod_{i=2}^n \zeta(i)} \to \frac{1}{\prod_{i=2}^\infty \zeta(i)} \approx 0.435757 \quad \text{as} \quad n \to \infty\,, \tag{4.31}$$

and further, by (4.3) this limit is given by

$$\frac{1}{\prod_{i=2}^\infty \zeta(i)} = \prod_{i=2}^\infty \prod_p \left(1-p^{-i}\right) = \prod_p \prod_{i=2}^\infty \left(1-p^{-i}\right) = \prod_p \frac{C_p}{[p,1]}\,. \tag{4.32}$$

One can also deduce $\prod_p \frac{[p,n]}{[p,1]} \to \prod_p \frac{C_p}{[p,1]}$ as $n \to \infty$ from Lemma 4.10 with $x_{i,j} = [p_i,1]/[p_i,j]$ and $x_i = [p_i,1]/C_{p_i}$, on the strength of Lemma 4.12.

For the second product on the right-hand side of (4.30), by definition $Y_n(p,\ell) \ge Y_n(p,1) = 1 + p^{-2} + p^{-3} + \cdots + p^{-n} > 1$ (see proof (i) of Theorem 4.9). Thanks to (4.23), we can apply Lemma 4.10 with $x_{i,j} = Y_j(p_i,\ell)$ and $x_i = Y(p_i,\ell)$:

$$\prod_p Y_n(p,\ell) \uparrow \prod_p Y(p,\ell) \quad \text{as} \quad n \to \infty\,. \tag{4.33}$$

Plugging (4.31), (4.32), and (4.33) into (4.30) yields (4.27).

Since $Y_n(p,\ell) > 1$ and is increasing in $\ell$, so is its limit $Y(p,\ell)$. Thus we can apply Lemma 4.10 with $x_{i,j} = Y(p_i, j)$ and $x_i = [p_i, 1]/C_{p_i}$:

$$\prod_p Y(p,\ell) \uparrow \prod_p \frac{[p,1]}{C_p} \quad \text{as} \quad \ell \to \infty\,.$$

Plugging into the second expression of $Z(\ell)$ in (4.27) leads to $Z(\ell) \uparrow 1$ as $\ell \to \infty$.

(iv) We prove the more general case $p = 1/x$ with $x \in (0, 1/2]$. Note that the proof of (ii) also holds for this case; in particular, (4.25) and (4.26) extend to

$$V(x,\ell) := Z(1/x,\ell) = C(x)\sum_{i=0}^{\ell} \frac{x^{i^2}}{[1/x,i]^2} \uparrow 1 \quad \text{as} \quad \ell \to \infty\,.$$

Recall that $C(x) = (1-x)(1-x^2)\cdots$ and $[1/x, i] = (1-x)\cdots(1-x^i)$. Thus

$$\frac{1}{C(x)} = \sum_{i=0}^{\infty} \frac{x^{i^2}}{[1/x,i]^2} = \sum_{i=0}^{\ell} \frac{x^{i^2}}{[1/x,i]^2} + \sum_{i=\ell+1}^{\infty} \frac{x^{i^2}}{[1/x,i]^2} = \frac{V(x,\ell)}{C(x)} + \sum_{i=\ell+1}^{\infty} \frac{x^{i^2}}{[1/x,i]^2}\,.$$

After rearrangements, we obtain

$$\begin{aligned}\frac{C(x)[1-V(x,\ell)]}{x^{(\ell+1)^2}} &= \sum_{i=\ell+1}^{\infty} \frac{C^2(x)x^{i^2-(\ell+1)^2}}{[1/x,i]^2} = \prod_{j=\ell+2}^{\infty}\left(1-x^j\right)^2 + \sum_{i=\ell+2}^{\infty} x^{i^2-(\ell+1)^2}\prod_{j=i+1}^{\infty}\left(1-x^j\right)^2 \\ &= \left(1 - 2\sum_{j=\ell+2}^{\infty} x^j + \Delta_1\right) + \Delta_2 = 1 - \frac{2x^{\ell+2}}{1-x} + \Delta_1 + \Delta_2\,, \end{aligned} \tag{4.34}$$

where

$$\Delta_1 := \prod_{j=\ell+2}^{\infty}\left(1-x^j\right)^2 - \left(1 - 2\sum_{j=\ell+2}^{\infty} x^j\right) \text{ and } \Delta_2 := \sum_{i=\ell+2}^{\infty} x^{i^2-(\ell+1)^2}\prod_{j=i+1}^{\infty}\left(1-x^j\right)^2.$$

Let us show that $0 \le \Delta_1 \le x^{2\ell}$ and $0 < \Delta_2 < x^{2\ell}$ for $x \in (0, 1/2]$. Then combining with (4.34) will lead to (4.28) with $p = 1/x$.

For $\Delta_1$, thanks to the inequality (proved easily by induction on $u$)

$$0 \le \prod_{i=1}^{u}(1-\delta_i) - \left(1 - \sum_{i=1}^{u}\delta_i\right) \le \sum_{1\le i<j\le u}\delta_i\delta_j \quad \text{for} \quad \delta_1,\delta_2,\ldots,\delta_u \in [0,1], \tag{4.35}$$

applying to $x^{\ell+2}, x^{\ell+2}, x^{\ell+3}, x^{\ell+3}, \ldots, x^{\ell'}, x^{\ell'}$ and letting $\ell' \to \infty$, we see that

$$0 \le \Delta_1 \le 4\sum_{j,j'\ge\ell+2} x^{j+j'} = \frac{4x^{2\ell+4}}{(1-x)^2} \le x^{2\ell} \quad \text{for} \quad 0 < x \le \frac{1}{2}\,.$$

For $\Delta_2$, we have

$$0 < \Delta_2 < \sum_{i=\ell+2}^{\infty} x^{i^2-(\ell+1)^2} < \sum_{i=2\ell+3}^{\infty} x^i = \frac{x^{2\ell+3}}{1-x} < x^{2\ell} \quad \text{for} \quad 0 < x \le \frac{1}{2}\,.$$

Thus it follows from (4.34) that (4.28) holds for $p = 1/x$ with $x \in (0, 1/2]$.

(v) By definition $0 \le Z(p,\ell) \le 1$ for all $p$, and $Z(\ell) = \prod_p Z(p,\ell) \le Z(2,\ell)$. On the other hand, the $O(p^{-2\ell})$ in (4.28) is at most $2p^{-2\ell} < \frac{2}{p^2-p} \cdot p^{-\ell}$ when $\ell \ge 2$, thus

$$Z(p,\ell) > 1 - C_p^{-1} p^{-(\ell+1)^2}.$$

Take the product of this inequality over $p \ge 3$ and apply the left inequality of (4.35):

$$Z(\ell) = \prod_p Z(p,\ell) \ge 1 - \big(1 - Z(2,\ell)\big) - \sum_{p\ge 3} C_p^{-1} p^{-(\ell+1)^2} = Z(2,\ell) - 2^{-(\ell+1)^2} o(4^{-\ell}).$$

Here we used the following estimate. Since $C_p^{-1} \le e^2$ by (4.19), the positive sum

$$2^{(\ell+1)^2} \sum_{p\ge 3} C_p^{-1} p^{-(\ell+1)^2} \le e^2 \sum_{p\ge 3} \left(\frac{2}{p}\right)^{(\ell+1)^2} < e^2 \sum_{p\ge 3} \left(\frac{2}{3}\right)^{\ell^2} \left(\frac{2}{p}\right)^2 = o(4^{-\ell}).$$

Finally, we apply (iv) to $Z(2,\ell)$ and arrive at (4.29). ∎

*Remark* 4.15.

(1) The proof of (ii) and (iv) holds with $p = 1/x$ for any $x \in (0, 1/2]$. The convergence result (4.26) in (ii) with $p = 1/x$ implies Euler's identity:

$$\sum_{i=0}^{\infty} \frac{x^{i^2}}{(1-x)^2(1-x^2)^2\cdots(1-x^i)^2} = \frac{1}{(1-x)(1-x^2)\cdots}.$$

(2) When $\ell = 1$, in the proof of Theorem 4.9 we wrote $Y(1/x, 1)$ as $(1-x^6)/(1-x^2)(1-x^3)$ (see (4.17)) in order to represent $Z(1) = \prod_p Y(p,1) \,/\, \prod_{i=2}^{\infty} \zeta(i)$ as the reciprocal of a product of values of the Riemann zeta function at positive integers. However, this is not the case when $\ell > 1$; in fact, in general $Y(1/x, \ell)$ is not even a symmetric function in $x$, for instance,

$$Y\left(\frac{1}{x}, 2\right) = \frac{1 - x - x^2 + 2x^3 - x^5 + x^6}{(1-x)^3(1+x)^2},$$

$$Y\left(\frac{1}{x}, 3\right) = \frac{1 - x - x^2 + 2x^4 + x^5 - 2x^6 - x^7 + x^8 + x^9 - x^{11} + x^{12}}{(1-x)^5(1+x)^2(1+x+x^2)^2}.$$

## Appendix A. Proof of Lemma 2.10.

*Proof.* We prove by induction on $h$. The case $h = 2$ is trivial as $\gcd(G_1, G_2) = 1$.

We prove the base case $h = 3$ by contradiction. Assume to the contrary that $\gcd(G_1, G_2 + zG_3) \ne 1$ for all $z \in \mathbb{Z}$. Suppose that the polynomial factorization of $G_1$ is $\phi_1\phi_2\cdots\phi_u$. Then each $G_2 + zG_3$ is a multiple of some nonconstant factor $\phi_{u(z)}$ of $G_1$ ($1 \le u(z) \le u$). Since there are infinitely many $z$'s, by the pigeonhole principle, there exist distinct $z$ and $z'$ such that $u(z) = u(z')$. Then $\phi_{u(z)} \,|\, (G_2 + zG_3) - (G_2 + z'G_3) = (z - z')G_3$. Thus $\phi_{u(z)} \,|\, G_3$, and hence $\phi_{u(z)} \,|\, (G_2 + zG_3) - zG_3 = G_2$. Recall that $\phi_{u(z)} \,|\, G_1$ as well. This contradicts the condition that $\gcd(G_1, G_2, G_3) = 1$.

Assume that the statement holds for $h - 1$ ($\ge 3$). Let $H := (G_2, G_3, \ldots, G_h)$ and $H_i := G_i/H$ ($2 \le i \le h$). Then

$$\gcd(G_1, H) = \gcd(G_1, G_2, \ldots, G_h) = 1 = \gcd(H_2, H_3, \ldots, H_h). \tag{A.1}$$

According to the induction hypothesis for $H_2, H_3, \ldots, H_h$, there exists $v = (v_4, \ldots, v_h) \in \mathbb{Z}^{h-3}$ such that

$$\gcd(H_2, H_3') = 1 \quad \text{for} \quad H_3' := H_3 + \sum_{i=4}^{h} v_i H_i \,. \tag{A.2}$$

Combining with (A.1) gives

$$\gcd(G_1, G_2, H_3'H) = \gcd(G_1, H_2H, H_3'H) = \gcd(G_1, \gcd(H_2H, H_3'H)) = \gcd(G_1, H) = 1.$$

Thus we can apply the base case $h = 3$ to $G_1, G_2, H_3'H$ to get an integer $z$ such that $\gcd(G_1, G_2 + zH_3'H) = 1$. Finally, we represent $zH_3'H$ back to a linear combination of the $G_i$'s with integer coefficients by definitions (A.2) and by $H_i = G_i/H$ $(2 \le i \le h)$:

$$zH_3'H = zH_3H + z\sum_{i=4}^{h} v_i H_i H = zG_3 + \sum_{i=4}^{h} zv_i G_i \,.$$

Therefore, the statement holds for $h$ with the new $v = (z, zv_4, \ldots, zv_h)$. ∎

**Acknowledgments.** The authors are grateful to Professor Bjorn Poonen for advice on the literature on the subject of this paper.

## REFERENCES

[1] G. Akemann, J. Baik, and P. Di Francesco, *The Oxford Handbook of Random Matrix Theory*, Oxford University Press, Oxford, UK, 2011.
[2] G. W. Anderson, A. Guionnet, and O. Zeitouni, *An Introduction to Random Matrices*, Cambridge University Press, Cambridge, UK, 2010.
[3] M. Bôcher, *Introduction to Higher Algebra*, Dover, New York, 1964.
[4] H. Cohen and H. W. Lenstra, Jr., *Heuristics on Class Groups*, in Number Theory (New York 1982), Springer, Berlin, 1984, pp. 26–36.
[5] H. Cohen and H. W. Lenstra, Jr., *Heuristics on Class Groups of Number Fields*, in Number Theory (Noordwijkerhout 1983), Springer, Berlin, 1984, pp. 33–62.
[6] W. Duke, Z. Rudnick, and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J., 71 (1993), pp. 143–179.
[7] T. Ekedahl, *An infinite version of the Chinese remainder theorem*, Comment. Math. Univ. St. Paul., 40 (1991), pp. 53–59.
[8] C. Feng, R. W. Nóbrega, F. R. Kschischang, and D. Silva, *Communication over finite-chain-ring matrix channels*, IEEE Trans. Inform. Theory, 60 (2014), pp. 5899–5917.
[9] E. Friedman and L. C. Washington, *On the Distribution of Divisor Class Groups of Curves over a Finite Field*, in Théorie des Nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239.
[10] J. Fulman, *Random matrix theory over finite fields*, Bull. Amer. Math. Soc. (N.S.), 39 (2002), pp. 51–85.
[11] F. R. Gantmacher, *The Theory of Matrices*, Vol. 1, AMS, Providence, RI, 1998.
[12] I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc., 66 (1949), pp. 464–491.
[13] Y. R. Katznelson, *Singular matrices and a uniform bound for congruence groups of* $\mathrm{SL}_n(\mathbf{Z})$, Duke Math. J., 69 (1993), pp. 121–136.
[14] K. Maples, *Cokernels of Random Matrices Satisfy the Cohen–Lenstra Heuristics*, preprint, arXiv:1301.1239, 2013.
[15] M. L. Mehta, *Random Matrices*, 3rd ed., Elsevier/Academic Press, Amsterdam, 2004.
[16] P. Q. Nguyen and I. E. Shparlinski, *Counting co-cyclic lattices*, SIAM J. Discrete Math., 30 (2016), pp. 1358–1370.
[17] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J., 118 (2003), pp. 353–373.
[18] B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. (2), 150 (1999), pp. 1109–1149.

[19] H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Philos. Trans. R. Soc. London, 151 (1861), pp. 293–326.
[20] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, 2nd ed., Cambridge University Press, Cambridge, UK, 2012.
[21] R. P. Stanley, *Smith normal form in combinatorics*, J. Combin. Theory Ser. A, 144 (2016), pp. 476–495.
[22] T. Tao, *Topics in Random Matrix Theory*, AMS, Providence, RI, 2012.
[23] V. H. Vu, ed., *Modern Aspects of Random Matrix Theory*, Proc. Sympos. Appl. Math. 72, AMS, Providence, RI, 2014.
[24] M. M. Wood, *Random Integral Matrices and the Cohen Lenstra Heuristics*, preprint, arXiv:1504.04391, 2015.