RANDOM PARTITIONS AND COHEN-LENSTRA HEURISTICS

JASON FULMAN AND NATHAN KAPLAN

Abstract. We investigate combinatorial properties of a family of probability distributions on finite abelian $p$-groups. This family includes several well-known distributions as specializations. These specializations have been studied in the context of Cohen-Lenstra heuristics and cokernels of families of random $p$-adic matrices.

1. Introduction

Friedman and Washington study a distribution on finite abelian $p$-groups $G$ of rank at most $d$ in [12]. In particular, a finite abelian $p$-group $G$ of rank $r \leq d$, is chosen with probability

$$P_d(G) = \frac{1}{|\text{Aut}(G)|} \left( \prod_{i=1}^{d} (1 - 1/p^i) \right) \left( \prod_{i=d-r+1}^{d} (1 - 1/p^i) \right).$$

Let $\lambda = (\lambda_1, \ldots, \lambda_r)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$ be a partition. A finite abelian $p$-group $G$ has type $\lambda$ if

$$G \cong \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\lambda_r}\mathbb{Z}.$$ 

Note that $r$ is equal to the rank of $G$.

There is a correspondence between measures on the set of integer partitions and on isomorphism classes of finite abelian $p$-groups. Let $\mathcal{L}$ denote the set of isomorphism classes of finite abelian $p$-groups. Given a measure $\nu$ on partitions, we get a corresponding measure $\nu'$ on $\mathcal{L}$ by setting $\nu'(G) = \nu(\lambda)$ where $G \in \mathcal{L}$ is the isomorphism class of finite abelian $p$-groups of type $\lambda$. We analogously define a measure on partitions given a measure on $\mathcal{L}$. When $G$ is a finite abelian group of type $\lambda$, we write $|\text{Aut}(\lambda)|$ for $|\text{Aut}(G)|$, and
from page 181 of [19],

\begin{equation}
|\text{Aut}(\lambda)| = p^{\sum(\lambda_i)^2} \prod_{i}(1/p)_{m_i(\lambda)}.
\end{equation}

The notation used in (2) is standard, and we review it in Section 1.2.

We introduce and study a more general distribution on integer partitions and on finite abelian $p$-groups $G$ of rank at most $d$. We choose a partition $\lambda$ with $r \leq d$ parts with probability

\begin{equation}
P_{d,u}(\lambda) = \frac{u^{|\lambda|}}{p^{\sum(\lambda_i)^2} \prod_{i}(1/p)_{m_i(\lambda)}} \prod_{i=1}^{d}(1 - u/p^i) \prod_{i=d-r+1}^{d}(1 - 1/p^i).
\end{equation}

This gives a distribution on partitions for all real $p > 1$ and $0 < u < p$. We can include $p$ as an additional parameter and write $P_{d,u}^p(\lambda)$. For clarity, we will suppress this additional notation except in Section 3. When $p$ is prime, we can interpret (3) as a distribution on $L$. When $p$ is not prime it does not make sense to talk about automorphisms of a finite abelian $p$-group, but in this case we can take (2) as the definition of $|\text{Aut}(\lambda)|$.

The main goal of this paper is to investigate combinatorial properties of the family of distributions of (3). We begin by noting six interesting specializations of this measure.

- Setting $u = 1$ in $P_{d,u}$ recovers $P_d$.
- We define a distribution $P_{\infty,u}$ by

\[ \lim_{d \to \infty} P_{d,u}(\lambda) = P_{\infty,u}(\lambda) = \frac{u^{|\lambda|}}{|\text{Aut}(\lambda)|} \prod_{i \geq 1}(1 - u/p^i). \]

It is not immediately clear that this limit defines a distribution on partitions, but this follows from the sentence after Proposition 2.1, from Theorem 2.2, or from Theorem 5.3 by taking $\mu$ to be the trivial partition.

For $0 < u < 1$, this probability measure arises by choosing a random non-negative integer $N$ with probability $P(N = n) = (1 - u)u^n$, and then looking at the $z - 1$ piece of a random element of the finite group $GL(N,p)$. See [13] for details.

- Note that

\[ P_{\infty,1}(\lambda) = \frac{1}{|\text{Aut}(\lambda)|} \prod_{i \geq 1}(1 - 1/p^i). \]

This is the measure on partitions corresponding to the usual Cohen-Lenstra measure on finite abelian $p$-groups [5]. It also arises from studying the $z - 1$ piece of a random element of the finite group $GL(d,p)$ in the $d \to \infty$ limit [13], or from studying the cokernel of a random $d \times d$ $p$-adic matrix in the $d \to \infty$ limit [12].
• Let $w$ be a positive integer and $\lambda$ a partition. The $w$-probability of $\lambda$, denoted by $P_w(\lambda)$, is the probability that a finite abelian $p$-group of type $\lambda$ is obtained by the following three step random process:
  - Choose randomly a $p$-group $H$ of type $\mu$ with respect to the measure $P_{\infty,1}(\mu)$.
  - Then choose $w$ elements $g_1, \ldots, g_w$ of $H$ uniformly at random.
  - Finally, output $H/\langle g_1, \ldots, g_w \rangle$, where $\langle g_1, \ldots, g_w \rangle$ denotes the group generated by $g_1, \ldots, g_w$.

From Example 5.9 of Cohen and Lenstra [5], it follows that $P_w(\lambda)$ is a special case of (3):

$$P_w(\lambda) = P_{\infty,1/p^w}(\lambda).$$

• We now mention two analogues of Proposition 1 of [12] for rectangular matrices. Let $w$ be a non-negative integer. Friedman and Washington do not discuss this explicitly, but using the same methods as in [12] one can show that taking the limit as $d \to \infty$ of the probability that a randomly chosen $d \times (d + w)$ matrix over $\mathbb{Z}_p$ has cokernel isomorphic to a finite abelian $p$-group of type $\lambda$ is given by $P_{\infty,1/p^w}(\lambda)$. See the discussion above Proposition 2.3 of [26].

Similarly, Tse considers rectangular matrices with more rows than columns and shows that $P_{\infty,1/p^w}(\lambda)$ is equal to the $d \to \infty$ probability that a randomly chosen $(d + w) \times d$ matrix over $\mathbb{Z}_p$ has cokernel isomorphic to $\mathbb{Z}_p^w \oplus G$, where $G$ is a finite abelian $p$-group of type $\lambda$ [23].

• In Section 3 we see that the measure on partitions studied by Bhargava, Kane, Lenstra, Poonen and Rains [1], arising from taking the cokernel of a random alternating $p$-adic matrix is also a special case of $P_{d,u}$. Taking a limit as the size of the matrix goes to infinity gives a distribution consistent with heuristics of Delaunay for Tate-Shafarevich groups of elliptic curves defined over $\mathbb{Q}$ [8].

A few of these specializations have received extensive attention in prior work:

• When $p$ is an odd prime, Cohen and Lenstra conjecture that $P_{\infty,1}$ models the distribution of $p$-parts of class groups of imaginary quadratic fields and $P_{\infty,1/p}$ models the distribution of $p$-parts of class groups of real quadratic fields [5]. Theorem 6.3 in [5] gives the probability that a group chosen from $P_{\infty,1/p^w}$ has given $p$-rank. For any $n$ odd, they show that the average number of elements of order exactly $n$ of a group drawn from $P_{\infty,1}$ is 1, and that this average for a group drawn from $P_{\infty,1/p}$ is $1/n$ [5, Section 9]. Delaunay generalizes these results in Corollary 11 of [9], where he computes the probability that a group drawn from $P_{d,u}$ simultaneously has specified $p^j$-rank for several values of $j$. Delaunay and Jouhet compute averages of
even more complicated functions involving moments of the number of $p^j$-torsion points for varying $j$ in [6].

The distribution of 2-parts of class groups of quadratic fields is not modeled by $P_{\infty, u}$ and several authors have worked to understand these issues. Motivated by work of Gerth [15] [16], Fouvry and Klüners study the conjectural distribution of $p^j$-ranks and moments for the number of torsion points of $C_{2D}^2$, the square of the ideal class group of a quadratic field [11].

• Delaunay [9], and Delaunay and Jouhet [6], prove analogues of the results described in the previous paragraphs for groups drawn from the $n \to \infty$ specialization of the distribution we study in Section 3. In [7], they prove analogues of the results of Fouvry and Klüners [11] for this distribution.

1.1. Outline of the Paper. In Section 2 we interpret $P_{d, u}$ in terms of Hall-Littlewood polynomials and use this interpretation to compute the probability that a partition chosen from $P_{d, u}$ has given size, given number of parts, or given size and number of parts. In Theorem 2.2 we give an algorithm for producing a partition according to the distribution $P_{d, u}$.

In Section 3 we show how a measure studied in [1] that arises from distributions of cokernels of random alternating $p$-adic matrices is given by a specialization of $P_{d, u}$. In Section 4 we briefly study a measure on partitions that arises from distributions of cokernels of random symmetric $p$-adic matrices that is studied in [4, 24]. We give an algorithm for producing a partition according to this distribution.

In Section 5 we combinatorially compute the moments of the distribution $P_{d, u}$ for all $d$ and $u$. These moments were already known for the case $d = \infty, u = 1$, and our method is new even in that special case. We also show that in many cases these moments determine a unique distribution. This is a generalization of a result of Ellenberg, Venkatesh, and Westerland [10], that the moments of the Cohen-Lenstra distribution determine the distribution, and of Wood [26], that the moments of the distribution $P_w$ determine the distribution.

1.2. Notation. Throughout this paper, when $p$ is a prime number we write $\mathbb{Z}_p$ for the ring of $p$-adic integers.

For a ring $R$, let $M_d(R)$ denote the set of all $d \times d$ matrices with entries in $R$ and let $\text{Sym}_d(R)$ denote the set of all $d \times d$ symmetric matrices with entries in $R$. For an even integer $d$, let $\text{Alt}_d(R)$ denote the set of all $d \times d$ alternating matrices with entries in $R$ (that is, matrices $A$ with zeros on the diagonal satisfying that the transpose of $A$ is equal to $-A$).

For groups $G$ and $H$ we write $\text{Hom}(G, H)$ for the set of homomorphisms from $G$ to $H$, $\text{Sur}(G, H)$ for the set of surjective homomorphisms from $G$ to $H$, and $\text{Aut}(G)$ for the set of automorphisms of $G$. If $G$ is a finite abelian $p$-group of type $\lambda$ and $H$ is a finite abelian $p$-group of type $\mu$, we sometimes write $|\text{Sur}(\lambda, \mu)|$ for $|\text{Sur}(G, H)|$. 

For a partition $\lambda$, we let $\lambda_i$ denote the size of the $i^{th}$ part of $\lambda$ and $m_i(\lambda)$ denote the number of parts of $\lambda$ of size $i$. We let $\lambda'_i$ denote the size of the $i^{th}$ column in the diagram of $\lambda$ (so $\lambda'_i = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$). We also let $n(\lambda) = \sum_i \lambda'_i$. We generally use $r$ or $r(\lambda)$ to denote the number of parts of $\lambda$. We use $|\lambda| = n$ to say that $\lambda$ is a partition of $n$, or equivalently $\sum \lambda_i = n$.

We let $n_\lambda(\mu)$ denote the number of subgroups of type $\mu$ of a finite abelian $p$-group of type $\lambda$. For a finite abelian group $G$, the number of subgroups $H \subseteq G$ of type $\mu$ equals the number of subgroups for which $G/H$ has type $\mu$ [19, Equation (1.5), page 181].

We also let $(x)_i = (1 - x)(1 - x/p) \cdots (1 - x/p^{i-1})$. So $(1/p)_i = (1 - 1/p) \cdots (1 - 1/p^i)$. With this notation, (3) is equivalent to

$$P_{d,u}(\lambda) = \frac{u^{\lambda}(u/p)_d}{p^{\sum(\lambda')^2} \prod_i (1/p)^{m_i(\lambda)} (1/p)^{d-r(\lambda)}}.$$

We use some notation related to $q$-binomial coefficients, namely:

$$[n]_q = \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1};$$
$$[n]_q! = [n][n-1]_q \cdots [2]_q;$$
$$\binom{n}{j}_q = \frac{[n]!}{[j]_q! [n-j]_q!}.$$

Finally if $f(u)$ is a power series in $u$, we let Coef. $u^n$ in $f(u)$ denote the coefficient of $u^n$ in $f(u)$.

2. Properties of the measure $P_{d,u}$

To begin we give a formula for $P_{d,u}(\lambda)$ in terms of Hall-Littlewood polynomials. We let $P_\lambda$ denote a Hall-Littlewood polynomial, defined for a partition $\lambda = (\lambda_1, \cdots, \lambda_n)$ of length at most $n$ by

$$P_{\lambda}(x_1, \cdots, x_n; t) = \frac{1}{v_{\lambda}(t)} \sum_{w \in S_n} w \left( x_1^{\lambda_1} \cdots x_n^{\lambda_n} \prod_{i<j} \frac{x_i - tx_j}{x_i - x_j} \right),$$

where

$$v_{\lambda}(t) = \prod_{i \geq 0} \prod_{j=1}^{m_i(\lambda)} \frac{1 - p^i}{1 - t},$$

the permutation $w \in S_n$ permutes the $x$ variables, and we note that some parts of $\lambda$ may have size 0. For background on Hall-Littlewood polynomials, see Chapter 3 of [19].

**Proposition 2.1.** For a partition $\lambda$ with $r \leq d$ parts,

$$P_{d,u}(\lambda) = \prod_{i=1}^{d} (1 - u/p^i)^r \cdot \frac{P_\lambda(u/p^2, \cdots, u/p^2; 0, \cdots; 1/p)}{p^{n(\lambda)}}.$$
Proof. From page 213 of [19],
\[
\prod_{i=1}^{d} (1 - u/p^i) \cdot \frac{P_\lambda(u/p^i, u/p^2, \cdots, u/p^r, 0, \cdots ; 1/p)}{p^{n(\lambda)}}
\]
is equal to
\[
u|\lambda| \prod_{i=1}^{d} (1 - u/p^i) \frac{(1/p)_d}{p^{\lambda|\lambda|+2n(\lambda)(1/p)_{d-r}}.}
\]
Since \(|\lambda| + 2n(\lambda) = \sum (\lambda'_i)^2\), this is equal to (3), and the proposition follows. \(\square\)

The fact that \(\sum_{\lambda} P_{d,u}(\lambda) = 1\) follows from Proposition 2.1 and the identity of Example 1 on page 225 of [19]. It is also immediate from Theorem 2.2.

There are two ways to generate random partitions \(\lambda\) according to the distribution \(P_{d,u}\). The first is to run the “Young tableau algorithm” of [13], stopped when coin \(d\) comes up tails. The second method is given by the following theorem.

**Theorem 2.2.** Starting with \(\lambda'_0 = d\), define in succession \(d \geq \lambda'_1 \geq \lambda'_2 \geq \cdots\) according to the rule that if \(\lambda'_i = a\), then \(\lambda'_{i+1} = b\) with probability
\[
K(a, b) = \frac{u^b(1/p)_a(u/p)_a}{p^b(1/p)_{a-b}(1/p)_b(u/p)_b}.
\]
Then the resulting partition is distributed according to \(P_{d,u}\).

**Proof.** One must compute
\[
K(d, \lambda'_1)K(\lambda'_1, \lambda'_2)K(\lambda'_2, \lambda'_3)\cdots.
\]
There is a lot of cancellation, and (recalling that \(\lambda'_1 = a\)), what is left is:
\[
\frac{(u/p)_d(1/p)_d u|\lambda|}{(1/p)_{d-r} p^\sum (\lambda'_i)^2 \prod (1/p)_{m_i(\lambda)}}.
\]
This is equal to \(P_{d,u}(\lambda)\), completing the proof. \(\square\)

The following corollary is immediate from Theorem 2.2.

**Corollary 2.3.** Choose \(\lambda\) from \(P_{d,u}\). Then the chance that \(\lambda\) has \(r \leq d\) parts is equal to
\[
u^r(1/p)_d(u/p)_d
\]
\[
p^r(1/p)_{d-r}(1/p)_r(u/p)_r.
\]

**Proof.** From Theorem 2.2, the sought probability is \(K(d, r)\). \(\square\)

The \(u = 1\) case of this result appears in another form in work of Stanley and Wang [22]. In Theorem 4.14 of [22], the authors compute the probability \(Z_d(p, r)\) that the Smith normal form of a certain model of random integer matrix has at most \(r\) diagonal entries divisible by \(p\). Setting \(u = 1\) in Corollary 2.3 gives \(Z_d(p, r) = Z_d(p, r - 1)\). This expression also appears in [3] where the authors study finite abelian groups arising as \(\mathbb{Z}^d/A\) for random
sublattices \( \Lambda \subset \mathbb{Z}^d \); isolating the prime \( p \) and the \( i = r \) term in Corollary 1.2 of [3] gives the \( u = 1 \) case of Corollary 2.3.

The next result computes the chance that \( \lambda \) chosen from \( P_{d,u} \) has size \( n \).

**Theorem 2.4.** The chance that \( \lambda \) chosen from \( P_{d,u} \) has size \( n \) is equal to

\[
\frac{u^n (u/p)_d (1/p)_{d+n-1}}{p^n (1/p)_{d-1}(1/p)_n}.
\]

**Proof.** By Proposition 2.1, the sought probability is equal to

\[
\sum_{|\lambda|=n} P_{d,u}(\lambda) = (u/p)_d \sum_{|\lambda|=n} \frac{P_{\lambda}(u/p, u/p^2, \ldots, u/p^d, 0, \ldots; 1/p)}{p^n(\lambda)} = (u/p)_d \sum_{|\lambda|=n} u^n \frac{P_{\lambda}(1/p, 1/p^2, \ldots, 1/p^d, 0, \ldots; 1/p)}{p^n(\lambda)} = u^n (u/p)_d \text{Coef.} u^n \text{ in } \sum_{\lambda} \frac{1}{(u/p)_d} \frac{P_{\lambda}(u/p, u/p^2, \ldots, u/p^d, 0, \ldots; 1/p)}{p^n(\lambda)} = \frac{u^n (u/p)_d (1/p)_{d+n-1}}{p^n (1/p)_{d-1}(1/p)_n}.
\]

The fourth equality used Proposition 2.1 and the fact that \( P_{d,u} \) defines a probability distribution, and the final equality used Theorem 349 of [17]. \( \square \)

**Theorem 2.5.** The probability that \( \lambda \) chosen from \( P_{d,u} \) has size \( n \) and \( r \leq \min\{d,n\} \) parts is equal to

\[
\frac{u^n (u/p)_d (1/p)_{d+n-1} (1/p)_{n-1}}{p^n (1/p)_{d-r}(1/p)_r p^{n-r}(1/p)_{r-1}(1/p)_{n-r}}.
\]
Proof. From the definition of $P_{d,u}$, one has that

$$
\sum_{\lambda_i = r, |\lambda| = n} P_{d,u}(\lambda) = \sum_{\lambda_i = r, |\lambda| = n} \frac{u^n(u/p)_d (1/p)_d}{|\text{Aut}(\lambda)|(1/p)_{d-r}}
$$

$$
= u^n(u/p)_d \sum_{\lambda_i = r, |\lambda| = n} \frac{(1/p)_d}{|\text{Aut}(\lambda)|(1/p)_{d-r}}
$$

$$
= u^n(u/p)_d \text{ Coef. } u^n \text{ in } \sum_{\lambda_i = r, |\lambda| = n} \frac{u^{|\lambda|}(1/p)_d}{|\text{Aut}(\lambda)|(1/p)_{d-r}}
$$

$$
= u^n(u/p)_d \text{ Coef. } u^n \text{ in } \frac{1}{(u/p)_d} \sum_{\lambda_i = r, |\lambda| = n} P_{d,u}(\lambda)
$$

$$
= u^n(u/p)_d \text{ Coef. } u^n \text{ in } \frac{1}{(u/p)_d} \frac{u^n(1/p)_d(u/p)_d}{p^{\sum_r (1/p)_{d-r}(1/p)_r (u/p)_r}}
$$

$$
= \frac{u^n(u/p)_d (1/p)_d}{p^{\sum_r (1/p)_{d-r}(1/p)_r}} \text{ Coef. } u^n - r \text{ in } \frac{1}{(u/p)_r}
$$

$$
= \frac{u^n(u/p)_d (1/p)_d}{p^{\sum_r (1/p)_{d-r}(1/p)_r}} \frac{(1/p)_{n-1}}{p^{n-r}(1/p)_{r-1}(1/p)_{n-r}}.
$$

The fifth equality used Corollary [23] and the final equality used Theorem 349 of [17]. \qed

In the rest of this section we give another view of the distributions given by (11) and (3). When $p$ is prime, equation (19) in [20] implies that

$$
P_d(\lambda) = \frac{1}{p^{\lambda/|d|}} \left( \prod_{i=1}^{\lambda_1} p^{\lambda_i' (d-\lambda_i')} \left( \frac{d - \lambda_i'}{\lambda_i' - \lambda_i'_{i+1}} \right)_p \right) \prod_{i=1}^{d} (1 - 1/p^i).
$$

Comparing this to the expression for $P_d(\lambda)$ given in (11) shows that

$$
\frac{1}{p^{\lambda/|d|}} \left( \prod_{i=1}^{\lambda_1} p^{\lambda_i' (d-\lambda_i')} \left( \frac{d - \lambda_i'}{\lambda_i' - \lambda_i'_{i+1}} \right)_p \right) = \frac{1}{|\text{Aut}(\lambda)|} \left( \prod_{i=d-r+1}^{d} (1 - 1/p^i) \right).
$$

A direct proof is given in Proposition 4.7 of [3]. Therefore, we get a second expression for $P_{d,u}(\lambda)$,

$$
P_{d,u}(\lambda) = \frac{u^{\lambda}}{p^{\lambda/|d|}} \left( \prod_{i=1}^{\lambda_1} p^{\lambda_i' (d-\lambda_i')} \left( \frac{d - \lambda_i'}{\lambda_i' - \lambda_i'_{i+1}} \right)_p \right) \prod_{i=1}^{d} (1 - u/p^i).
$$

We give a combinatorial proof of (6) that applies for any real $p > 1$, so (7) applies for any $p > 1$ and $0 < u < p$. 

Proof of Equation (6). It is sufficient to show that for a partition \( \lambda \) with \( r \leq d \) parts,

\[
|\text{Aut}(\lambda)| \left( \prod_{i=1}^{\lambda_1} p^{\chi_{i+1}(d-\chi_i)} \left( d - \chi_i' + 1 \right) \prod_{j=0}^{r-1} \frac{1}{1 - p^{d+j}} \right) = p^{d|\lambda|} \prod_{j=0}^{r-1} (1 - p^{-d+j}).
\]

Clearly

\[
\prod_{i=1}^{\lambda_1} p^{\chi_{i+1}(d-\chi_i)} \left( d - \chi_i' + 1 \right) \prod_{j=0}^{r-1} \frac{1}{1 - p^{d+j}} = p^{d|\lambda|} \prod_{j=0}^{r-1} (1 - p^{-d+j}).
\]

Since \( \chi_i' = r \), equation (2) implies that the left-hand side of (8) is equal to

\[
p^{d|\lambda| - r^2/2} (p - 1)^r [d]_p! \prod_{j=0}^{r-1} (1 - p^{-d+j}),
\]

which simplifies to the right-hand side of (8). \( \square \)

We now use the alternate expression of (7) to give an additional proof of Theorem 2.4 in the case when \( p \) is prime. The zeta function of \( \mathbb{Z}^d \) is defined by

\[
\zeta_{\mathbb{Z}^d}(s) = \sum_{H \leq \mathbb{Z}^d} [\mathbb{Z}^d : H]^{-s},
\]

where the sum is taken over all finite index subgroups of \( \mathbb{Z}^d \). It is known that

\[
\zeta_{\mathbb{Z}^d}(s) = \zeta(s) \zeta(s-1) \cdots \zeta(s-(d-1))
\]

\[
= \prod_p \left( 1 - p^{-s} \right)^{-1} \left( 1 - p^{-s-1} \right)^{-1} \cdots \left( 1 - p^{-s-(d-1)} \right)^{-1},
\]

with

\[
\chi_{i+1}(d-\chi_i) p^{\sum_{i} (\chi_i' - \chi_i + 1)} \prod_{j=0}^{r-1} (1/p)_{m_i}.
\]

Clearly

\[
\prod_{i=1}^{\lambda_1} p^{\chi_{i+1}(d-\chi_i)} \left( d - \chi_i' + 1 \right) \prod_{j=0}^{r-1} \frac{1}{1 - p^{d+j}} = p^{d|\lambda|} \prod_{j=0}^{r-1} (1 - p^{-d+j}).
\]

Since \( \chi_i' = r \), equation (2) implies that the left-hand side of (8) is equal to

\[
p^{d|\lambda| - r^2/2} (p - 1)^r [d]_p! \prod_{j=0}^{r-1} (1 - p^{-d+j}),
\]

which simplifies to the right-hand side of (8). \( \square \)

We now use the alternate expression of (7) to give an additional proof of Theorem 2.4 in the case when \( p \) is prime. The zeta function of \( \mathbb{Z}^d \) is defined by

\[
\zeta_{\mathbb{Z}^d}(s) = \sum_{H \leq \mathbb{Z}^d} [\mathbb{Z}^d : H]^{-s},
\]

where the sum is taken over all finite index subgroups of \( \mathbb{Z}^d \). It is known that

\[
\zeta_{\mathbb{Z}^d}(s) = \zeta(s) \zeta(s-1) \cdots \zeta(s-(d-1))
\]

\[
= \prod_p \left( 1 - p^{-s} \right)^{-1} \left( 1 - p^{-s-1} \right)^{-1} \cdots \left( 1 - p^{-s-(d-1)} \right)^{-1},
\]

with

\[
\chi_{i+1}(d-\chi_i) p^{\sum_{i} (\chi_i' - \chi_i + 1)} \prod_{j=0}^{r-1} (1/p)_{m_i}.
\]
where $\zeta(s)$ denotes the Riemann zeta function, and the product is taken over all primes. See the book of Lubotzky and Segal for five proofs of this fact [18].

**Second Proof of Theorem [2.4] for p prime.** From (7), we need only prove

$$
\sum_{|\lambda|=n} \frac{u^n}{p^{nd}} \left( \prod_{i=1}^{d-n} p^{\lambda_i+1}(d-\lambda_i) \right) \left( \frac{d-\lambda_i}{d-\lambda_i+1} \right)^p = \frac{u^n}{p^d} \left( \frac{1}{p} \right)^{d+n-1} (1/p)^{d-1} (1/p)^n.
$$

Let $\lambda^* = (\lambda_1, \ldots, \lambda_1)$, where there are $d$ entries in the tuple. The discussion around equation (19) in [20] says that the term in parentheses of the left-hand side of (10) is equal to the number of subgroups of a finite abelian $p$-group of type $\lambda^*$ that have type $\lambda$, $n_{\lambda^*}(\lambda)$, which is also equal to the number of subgroups $\Lambda \subset \mathbb{Z}^d$ such that $\mathbb{Z}^d/\Lambda$ is a finite abelian $p$-group of type $\lambda$.

After some obvious cancelation, we need only show that

$$
\sum_{|\lambda|=n} n_{\lambda^*}(\lambda) = \frac{p^n(d-1)(1/p)^{d+n-1}}{(1/p)^{d-1} (1/p)^n}.
$$

The left-hand side is the number of subgroups $\Lambda \subset \mathbb{Z}^d$ such that $\mathbb{Z}^d/\Lambda$ has order $p^n$. This is the $p^{-sn}$ coefficient of $\zeta_{\mathbb{Z}^d}(s)$. Using (9), this is equal to

$$
\text{Coef. } p^{-sn} \text{ in } (1-p^{-s})^{-1}(1-p^{-(s-1)})^{-1} \cdots (1-p^{-(s-(d-1))})^{-1} = \text{Coef. } x^n \text{ in } (1-x)^{-1}(1-px)^{-1}(1-p^2x)^{-1} \cdots (1-p^{d-1}x))^{-1}.
$$

By Theorem 349 of [17], this is equal to

$$
\frac{p^n(d-1)(1/p)^{d+n-1}}{(1/p)^{d-1} (1/p)^n},
$$

and the proof is complete. $\square$

### 3. Cokernels of random alternating $p$-adic matrices

In this section we consider a distribution on finite abelian $p$-groups that arises in the study of cokernels of random $p$-adic alternating matrices. We show that this is a special case of the distributions $P_{d,u}^p$.

Let $n$ be an even positive integer and let $A \in \text{Alt}_n(\mathbb{Z}_p)$ be a random matrix chosen with respect to additive Haar measure on $\text{Alt}_n(\mathbb{Z}_p)$. The cokernel of $A$ is a finite abelian $p$-group of the form $G \cong H \times H$ for some $H$ of type $\lambda$ with at most $n/2$ parts, and is equipped with a nondegenerate alternating pairing $[\ ,\ ] : H \times H \to \mathbb{Q}/\mathbb{Z}$. Let $\text{Sp}(G)$ be the group of automorphisms of $H$ respecting $[\ ,\ ]$. Let $r$ be the number of parts of $\lambda$, and $|\lambda|$, $n(\lambda)$, $m_i(\lambda)$ be as in Section 1.2.
Lemma 3.1. Let \( n \) be an even positive integer and \( A \in \text{Alt}_n(\mathbb{Z}_p) \) be a random matrix chosen with respect to additive Haar measure on \( \text{Alt}_n(\mathbb{Z}_p) \). The probability that the cokernel of \( A \) is isomorphic to \( G \) is given by

\[
P_{\text{Alt}_{n,p}}(\lambda) = \frac{\prod_{i=1}^{n}(1 - 1/p^{i}) \prod_{i=1}^{n/2-1}(1 - 1/p^{2i-1})}{p^{n/2+4n(\lambda)} \prod_{i=1}^{\lambda} \prod_{j=1}^{m_i(\lambda)} (1 - 1/p^{j})}.
\]

Proof. Formula (6) and Lemma 3.6 of [1] imply that the probability that the cokernel of \( A \) is isomorphic to \( G \) is given by

\[
\left| \text{Sur}(\mathbb{Z}_n^p, G) \right| \prod_{i=1}^{n/2-r} (1 - 1/p^{2i-1})|G|^{1-n}.
\]

We can rewrite this expression in terms of the partition \( \lambda \). Clearly \( |G| = p^{2|\lambda|} \). Proposition 3.1 of [5] implies that since \( G \) has rank \( 2r \),

\[
\left| \text{Sur}(\mathbb{Z}_n^p, G) \right| = p^{2n|\lambda|} \prod_{i=n-2r+1}^{n} (1 - 1/p^{i}).
\]

An identity on the bottom of page 538 of [9] says that,

\[
|\text{Sp}(G)| = p^{4n(\lambda)+3|\lambda|} \prod_{i=1}^{\lambda} \prod_{j=1}^{m_i(\lambda)} (1 - 1/p^{2j}).
\]

Putting these results together completes the proof. \( \square \)

The next theorem shows that (11) is a special case of (3).

Theorem 3.2. Let \( n \) be an even positive integer. For any partition \( \lambda \),

\[
P_{n/2,p}^{p^2}(\lambda) = P_{n,p}^{\text{Alt}}(\lambda).
\]

Proof. Rewrite (3) as

\[
u^{|\lambda|} \prod_{i=1}^{d}(1 - u/p^{i}) \prod_{i=d-r+1}^{d}(1 - 1/p^{i})
\]

Replacing \( d \) by \( n/2 \), \( u \) by \( p \), and \( p \) by \( p^{2} \) gives

\[
P_{n/2,p}^{p^2} = \frac{\prod_{i=1}^{n/2}(1 - 1/p^{2i-1}) \prod_{i=n/2-r+1}^{n/2}(1 - 1/p^{2i})}{p^{4n(\lambda)+3|\lambda|} \prod_{i=1}^{\lambda} \prod_{j=1}^{m_i(\lambda)} (1 - 1/p^{2j})}.
\]

Comparing with (11), we see that it suffices to prove

\[
\prod_{i=1}^{n/2}(1 - 1/p^{2i-1}) \prod_{i=n/2-r+1}^{n/2}(1 - 1/p^{2i}) = \prod_{i=n-2r+1}^{n} (1 - 1/p^{i}) \prod_{i=1}^{n/2-r}(1 - 1/p^{2i-1}).
\]
To prove this equality, note that when each side is multiplied by 
\[(1 - 1/p^2)(1 - 1/p^4) \cdots (1 - 1/p^{n-2r}),\]
each side becomes \((1/p)^n\). \(\square\)

4. Cokernels of random symmetric \(p\)-adic matrices

Let \(A \in \text{Sym}_n(Z_p)\) be a random matrix chosen with respect to additive Haar measure on \(\text{Sym}_n(Z_p)\). Let \(r\) be the number of parts of \(\lambda\). Theorem 2 of \([4]\) shows that the probability that the cokernel of \(A\) has type \(\lambda\) is equal to:

\[
P_{n^\text{Sym}}(\lambda) = \prod_{i \geq 1} \frac{p^{\lambda_i} \prod_{j=1}^{\lfloor (n-1)/2 \rfloor} (1 - 1/p^{2i-1})}{p^{\lambda_1+1} \prod_{j=1}^{\lfloor (n-1)/2 \rfloor} (1 - 1/p^{2j})}.
\]

Note that \(P_{n^\text{Sym}}(\lambda) = 0\) if \(\lambda\) has more than \(n\) parts. As in earlier sections, when \(p\) is prime (12) has an interpretation in terms of finite abelian \(p\)-groups, but defines a distribution on partitions for any \(p > 1\). This follows directly from Theorem 4.1 below.

Taking \(n \to \infty\) gives a distribution on partitions where \(\lambda\) is chosen with probability

\[
P_{\infty^\text{Sym}}(\lambda) = \frac{\prod_{i \text{ odd}} (1 - 1/p^i)}{p^{\lambda} \prod_{i \geq 1} \prod_{j=1}^{\lfloor m_i(\lambda)/2 \rfloor} (1 - 1/p^{2j})}.
\]

The distribution of (13) is studied in [24], where Wood shows that it arises as the distribution of \(p\)-parts of sandpile groups of large Erdős-Rényi random graphs. Combinatorial properties of this distribution are considered in [14], where it is shown that this distribution is a specialization of a two parameter family of distributions. It is unclear whether the distribution of (12) also sits within a larger family.

The following theorem allows one to generate partitions from the measure (12), and is a minor variation on Theorem 3.1 of [14].

**Theorem 4.1.** Starting with \(\lambda_0' = n\), define in succession \(n \geq \lambda_1' \geq \lambda_2' \geq \cdots\) according to the rule that if \(\lambda_i' = a\), then \(\lambda_{i+1}' = b\) with probability

\[
K(a, b) = \frac{\prod_{i=1}^{b+1} (1 - 1/p^i)}{p^{(b+1)/2} \prod_{i=1}^{b} (1 - 1/p^i) \prod_{j=1}^{\lfloor (a-b)/2 \rfloor} (1 - 1/p^{2j})}.
\]

Then the resulting partition with at most \(n\) parts is distributed according to (12).

**Proof.** It is necessary to compute

\[
K(n, \lambda_1')K(\lambda_1', \lambda_2')K(\lambda_2', \lambda_3') \cdots
\]

There is a lot of cancelation, and (recalling that \(\lambda_1' = r\)), what is left is:

\[
\frac{\prod_{j=1}^{n} (1 - 1/p^j)}{\prod_{j=1}^{\lfloor (n-r)/2 \rfloor} (1 - 1/p^{2j})} \frac{1}{p^{r(\lambda) + |\lambda|} \prod_{i \geq 1} \prod_{j=1}^{\lfloor m_i(\lambda)/2 \rfloor} (1 - 1/p^{2j})}.
\]
So to complete the proof, it is necessary to check that
\[
\prod_{j=1}^{n} \left(1 - \frac{1}{p^j}\right) = \prod_{j=n-r+1}^{n} \left(1 - \frac{1}{p^{\frac{(n-r)/2}}}ight) \prod_{i=1}^{\left\lfloor \frac{(n-r)}{2} \right\rfloor} \left(1 - \frac{1}{p^{2i-1}}\right).
\]
This equation is easily verified by breaking it into cases based on whether \(n - r\) is even or odd. \(\square\)

The following corollary is immediate.

**Corollary 4.2.** Let \(\lambda\) be chosen from \([12]\). Then the chance that \(\lambda\) has \(r \leq n\) parts is equal to
\[
\prod_{j=r+1}^{n} \left(1 - \frac{1}{p^j}\right) \frac{p^{(r+1)}}{\prod_{j=1}^{\left\lfloor \frac{(n-r)}{2} \right\rfloor} \left(1 - \frac{1}{p^{2j}}\right)}.
\]

**Proof.** By Theorem 4.1, the sought probability is equal to \(K(n, r)\). \(\square\)

Taking \(n \to \infty\) in this result recovers Theorem 2.2 of [14], which is also Corollary 9.4 of [24].

### 5. Computation of H-moments

We recall that \(\mathcal{L}\) denotes the set of isomorphism classes of finite abelian \(p\)-groups and that a probability distribution \(\nu\) on \(\mathcal{L}\) gives a probability distribution on the set of partitions in an obvious way. Similarly, a measure on partitions gives a measure on \(\mathcal{L}\), setting \(\nu(G) = \nu(\lambda)\) when \(G\) is a finite abelian \(p\)-group of type \(\lambda\). When \(G, H \in \mathcal{L}\) we write \(|\text{Sur}(G, H)|\) for the number of surjections from any representative of the isomorphism class \(G\) to any representative of the isomorphism class \(H\).

Let \(\nu\) be a probability measure on \(\mathcal{L}\). For \(H \in \mathcal{L}\), the \(H\)-moment of \(\nu\) is defined as
\[
\sum_{G \in \mathcal{L}} \nu(G)|\text{Sur}(G, H)|.
\]
When \(H\) is a finite abelian \(p\)-group of type \(\mu\) this is
\[
\sum_{\lambda} \nu(\lambda)|\text{Sur}(\lambda, \mu)|.
\]

The distribution \(\nu\) gives a measure on partitions and we refer to this quantity as the \(\mu\)-moment of the measure. For an explanation of why these are called the moments of the distribution, see Section 3.3 of [4].

The Cohen-Lenstra distribution is the probability distribution on \(\mathcal{L}\) for which a finite abelian group \(G\) of type \(\lambda\) is chosen with probability \(P_{\infty,1}(\lambda)\). One of the most striking properties of the Cohen-Lenstra distribution is that the \(H\)-moment of \(P_{\infty,1}\) is 1 for every \(H\), or equivalently, for any finite abelian \(p\)-group \(H\) of type \(\mu\),
\[
\sum_{\lambda} P_{\infty,1}(\lambda)|\text{Sur}(\lambda, \mu)| = 1.
\]
There is a nice algebraic explanation of this fact using the interpretation of $P_{\infty,1}$ as a limit of the $P_{d,1}$ distributions given by (1) (see for example [21]).

Lemma 8.2 of [10] shows that the Cohen-Lenstra distribution is determined by its moments.

**Lemma 5.1.** Let $p$ be an odd prime. If $\nu$ is any probability measure on $\mathcal{L}$ for which

$$\sum_{G \in \mathcal{L}} \nu(G)|\text{Sur}(G, H)| = 1$$

for any $H \in \mathcal{L}$, then $\nu = P_{\infty,1}$.

Our next goal is to compute the moments for the measure $P_{d,u}$; see Theorem 5.3 below. Our method is new even in the case $P_{\infty,1}$.

There has been much recent interest in studying moments of distributions related to the Cohen-Lenstra distribution, and showing that these moments determine a unique distribution [2, 24, 26]. At the end of this section, we add to this discussion by proving a version of Lemma 5.1 for the distribution $P_{d,u}$.

The following lemma counts the number of surjections from $G$ to $H$. Recall that $n_{\lambda}(\mu)$ is the number of subgroups of type $\mu$ of a finite abelian $p$-group.

**Lemma 5.2.** Let $G, H$ be finite abelian $p$-groups of types $\lambda$ and $\mu$ respectively. Then

$$|\text{Sur}(G, H)| = |\text{Sur}(\lambda, \mu)| = n_{\lambda}(\mu)|\text{Aut}(\mu)|.$$

For a proof, see page 28 of [27]. The main idea is that $|\text{Sur}(G, H)|$ is the number of injective homomorphisms from $\hat{H}$ to $\hat{G}$, where these are the dual groups of $H$ and $G$, respectively. The image of such a homomorphism is a subgroup of $\hat{G}$ of type $\mu$.

The distributions $P_{d,u}$ are defined for all $p > 1$. It is not immediately clear what the $\mu$-moment of this distribution should mean when $p$ is not prime, since $|\text{Sur}(\lambda, \mu)|$ is defined in terms of surjective homomorphisms between finite abelian $p$-groups. In [2] we saw how to define $|\text{Aut}(\lambda)|$ in terms of the parts of the partition $\lambda$ and the parameter $p$, even in the case where $p$ is not prime. Similarly, Lemma 5.2 gives a way to define $|\text{Sur}(\lambda, \mu)|$ in terms of the parameter $p$ and the partitions $\lambda$ and $\mu$ even when $p$ is not prime. We first define $|\text{Aut}(\mu)|$ using (2), and then note that $n_{\lambda}(\mu)$ is a polynomial in $p$ that we can evaluate for any $p > 1$.

**Theorem 5.3.** The $\mu$-moment of the distribution $P_{d,u}$ is equal to

$$\begin{cases} \frac{n_{\lambda}(\mu)}{(1/p)_{d-r(\mu)}} & \text{if } r(\mu) \leq d \\ 0 & \text{otherwise.} \end{cases}$$

Here, as above, $r(\mu)$ denotes the number of parts of $\mu$. 
Proof. Clearly we can suppose that \( r(\mu) \leq d \). By Lemma 5.2 the \( \mu \)-moment of the distribution \( P_{d,u} \) is equal to

\[
\sum_{\lambda} P_{d,u}(\lambda)|\operatorname{Sur}(\lambda, \mu)| = |\operatorname{Aut}(\mu)| \sum_{\lambda} P_{d,u}(\lambda)n(\mu, \nu).
\]

Let \( n(\mu, \nu) \) be the number of subgroups \( M \) of \( G \) so that \( M \) has type \( \mu \) and \( G/M \) has type \( \nu \). This is a polynomial in \( p \) (see Chapter II Section 4 of \([19]\)). Then by Proposition 2.1, the \( \mu \)-moment becomes

\[
|\operatorname{Aut}(\mu)| \prod_{i=1}^{d} (1 - u/p^i) \cdot \sum_{\nu} \frac{P_{\mu}(\frac{u}{p}, \frac{u}{p^2}, \cdots, \frac{u}{p^d}, 0, \cdots ; \frac{1}{p})}{p^{n(\mu)}} n(\mu, \nu).
\]

Reversing the order of summation, this becomes

\[
|\operatorname{Aut}(\mu)| \prod_{i=1}^{d} (1 - u/p^i) \cdot \sum_{\nu} \frac{P_{\mu}(\frac{u}{p}, \frac{u}{p^2}, \cdots, \frac{u}{p^d}, 0, \cdots ; \frac{1}{p})}{p^{n(\mu)}} n(\mu, \nu).
\]

From Section 3.3 of \([19]\), it follows that for any values of the \( x \) variables,

\[
\sum_{\lambda} n(\mu, \nu) P_{\lambda}(x; \frac{1}{p}) = \frac{P_{\mu}(x; \frac{1}{p})}{p^{n(\mu)}} P_{\nu}(x; \frac{1}{p}) p^{n(\mu)}.
\]

Specializing \( x_i = u/p^i \) for \( i = 1, \cdots, d \) and 0 otherwise, it follows that the \( \mu \)-moment of \( P_{d,u} \) is equal to

\[
|\operatorname{Aut}(\mu)| \prod_{i=1}^{d} (1 - u/p^i) \cdot \sum_{\nu} \frac{P_{\mu}(\frac{u}{p}, \frac{u}{p^2}, \cdots, \frac{u}{p^d}, 0, \cdots ; \frac{1}{p})}{p^{n(\mu)}} \frac{P_{\nu}(\frac{u}{p}, \frac{u}{p^2}, \cdots, \frac{u}{p^d}, 0, \cdots ; \frac{1}{p})}{p^{n(\mu)}}.
\]

By Proposition 2.1, this is equal to

\[
|\operatorname{Aut}(\mu)| \frac{P_{\mu}(\frac{u}{p}, \frac{u}{p^2}, \cdots, \frac{u}{p^d}, 0, \cdots ; \frac{1}{p})}{p^{n(\mu)}}.
\]

By pages 181 and 213 of \([19]\), this simplifies to

\[
\frac{u^{r(\mu)}(1/p_d)}{(1/p_d)^{d-r(\mu)}}.
\]

\[\square\]

Remarks:
Lemma 5.5. Let $e$.

Suppose $H$ and consider the particular generating set for $H$.

The number of elements of $H$ by $T$.

The expected value of $T$.

Theorem 5.4. Let $p$ be a prime, $\ell$ be a positive integer, and $0 < u < p$. The expected value of $T_{\ell}(H)$ for a finite abelian $p$-group $H$ drawn from $P_{d,u}$ is

The expected value of $T_{\ell}(H) - T_{\ell-1}(H)$ is $u^\ell(1 - p^{-d})$.

Remarks:

The exact same argument proves the analogous result for the distribution $P_{\infty,u}$.

Setting $d = \infty$ and $u = 1/p^w$ (with $w$ a positive integer) gives the distribution [1], and in this case Theorem 5.3 recovers Lemma 3.2 of [25].

The argument used in the proof of Theorem 5.3 does not require that $p$ is prime.

We use Theorem 5.3 to determine the expected number of $p^\ell$-torsion elements of a finite abelian group $H$ drawn from $P_{d,u}$. Let $T_{\ell}$ be defined by

$$T_{\ell}(H) = |H[p^\ell]| = |\{x \in H : p^\ell \cdot x = 0\}|.$$

The number of elements of $H$ of order exactly $p^\ell$ is $T_{\ell}(H) - T_{\ell-1}(H)$.

For a finite abelian $p$-group $H$, let $r_{p^\ell}(H)$ denote the $p^\ell$-rank of $H$, that is,

$$r_{p^\ell}(H) = \dim_{\mathbb{Z}/p\mathbb{Z}} \left(\mathbb{Z}/p^{k-1}H/p^kH\right).$$

If $H$ is of type $\lambda$, then $r_{p^\ell}(H) = \lambda'_k$, the number of parts of $\lambda$ of size at least $k$. The number of parts of $\lambda$ of size exactly $k$ is $\lambda'_k - \lambda'_{k+1}$. It is clear that

$$T_{\ell}(H) = p^{r_{p}(H)+r_{p^2}(H)+\cdots+r_{p^\ell}(H)} = p^{\lambda'_1+\lambda'_2+\cdots+\lambda'_\ell}.$$

Theorem 5.4. Let $p$ be a prime, $\ell$ be a positive integer, and $0 < u < p$. The expected value of $T_{\ell}(H)$ for a finite abelian $p$-group $H$ drawn from $P_{d,u}$ is

$$(u^\ell + u^{\ell-1} + \cdots + u)(1 - p^{-d}) + 1.$$

The expected value of $T_{\ell}(H) - T_{\ell-1}(H)$ is $u^\ell(1 - p^{-d})$.

Remarks:

The exact same argument proves the analogous result for the distribution $P_{\infty,u}$.

Taking $d = \infty$, $u = p^{-w}$ recovers a result of Delaunay, the first part of Corollary 3 of [9]. Delaunay’s result generalizes work of Cohen and Lenstra for $P_{\infty,1}$ and $P_{\infty,1/p}$ [5].

Theorem 5.3 can likely be used to compute moments of more complicated functions involving $T_{\ell}(H)$ giving results similar to those of Delaunay and Jouhet in [6]. We do not pursue this further here.

Lemma 5.5. Let $H$ be a finite abelian $p$-group of type $\lambda$ and let $\ell \geq 1$. Then

$$\#\text{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z}) = p^{r_{p^\ell}(H)+r_{p^\ell-1}(H)+\cdots+r_p(H)} = p^{\lambda'_1+\lambda'_2+\cdots+\lambda'_\ell} = T_{\ell}(H).$$

Proof. Suppose

$$H \cong \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\lambda_p(H)}\mathbb{Z},$$

and consider the particular generating set for $H$

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_{r_p(H)} = (0, \ldots, 0, 1).$$

Note that $e_i$ has order $p^{\lambda_i}$. 
A homomorphism from $H$ to $\mathbb{Z}/p^\ell\mathbb{Z}$ is uniquely determined by the images of $e_1, \ldots, e_{r(H)}$. When $\lambda_i \geq \ell$, there are $p^\ell$ choices for the image of $e_i$. If $1 \leq \lambda_i \leq \ell$, there are $p^{\lambda_i}$ choices for the image of $e_i$. Therefore, the total number of homomorphisms is
\[
p^{\ell \lambda_1' + (\ell - 1)(\lambda_{e-1} - \lambda_1') + \cdots + 1(\lambda_1' - \lambda_2')}.
\]

**Proof of Theorem 5.4.** We compute the expected value of
\[
\#\text{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z}) - \#\text{Hom}(H, \mathbb{Z}/p^{\ell-1}\mathbb{Z})
\]
and apply Lemma 5.5 to complete the proof.

Let $H$ be a finite abelian $p$-group drawn from $P_{d,u}$. Every element of $\text{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z})$ is either a surjection, or surjects onto a unique proper subgroup of $\mathbb{Z}/p^\ell\mathbb{Z}$. Every proper subgroup of $\mathbb{Z}/p^\ell\mathbb{Z}$ is contained in the unique proper subgroup of $\mathbb{Z}/p^\ell\mathbb{Z}$ that is isomorphic to $\mathbb{Z}/p^{\ell-1}\mathbb{Z}$. Therefore,
\[
\#\text{Sur}(H, \mathbb{Z}/p^\ell\mathbb{Z}) = \#\text{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z}) - \#\text{Hom}(H, \mathbb{Z}/p^{\ell-1}\mathbb{Z}).
\]

Lemma 5.5 implies $T_\ell(H) - T_{\ell-1}(H) = \#\text{Sur}(H, \mathbb{Z}/p^\ell\mathbb{Z})$. Applying Theorem 5.3, noting that $T_0(H) = 1$ for any $H$, completes the proof.

We close this section by proving a version of Lemma 5.1 for the distribution $P_{d,u}$. The proof of Lemma 8.2 from [10] carries over almost exactly to this more general setting.

**Theorem 5.6.** Suppose that $p > 1$ and $0 < u < p$ are such that
\[
\frac{1}{(u/p)_d} = \prod_{i=1}^d (1 - u/p^i)^{-1} < 2.
\]

If $\nu$ is any probability measure on the set of partitions for which
\[
\sum_\lambda \nu(\lambda) |\text{Sur}(\lambda, \mu)| = \begin{cases} \frac{u^{w}|(1/p)_\mu|}{(1/p)_{d-r(\mu)}} & \text{if } r(\mu) \leq d, \\ 0 & \text{otherwise,} \end{cases}
\]

then $\nu = P_{d,u}$.

**Remarks:**

- When $p$ is prime this result has an interpretation in terms of probability measures on $\mathcal{L}$.
- The exact same argument proves the analogous result for the distribution $P_{\infty,u}$.
- The expression on the left-hand side of (14) is decreasing in $p$ and in $u$. Setting $d = \infty$, $u = 1$ and noting that this inequality holds for all $p \geq 3$ gives Lemma 5.1.
- Similarly, setting $d = \infty$, $u = 1/p^w$ (with $p$ prime and $w$ a positive integer) gives Proposition 2.3 of [26].
• Theorem 5.6 only applies when \( 1/(u/p)_d < 2 \). Results of Wood imply that the moments determine the distribution in additional cases where \( p \) is prime, for example when \( p = 2, \ d = \infty \), and \( u = 1 \). See Theorem 3.1 in [25] and Theorem 8.3 in [24].

Proof. The assumption gives, for every \( \mu \)

\[
\text{(16) } |\text{Aut}(\mu)|\nu(\mu) + \sum_{\lambda \neq \mu} |\text{Sur}(\lambda, \mu)|\nu(\lambda) = \begin{cases} \frac{u|\mu|((1/p)_d^{(1/p)_{d-r(\mu)}}) \quad \text{if } r(\mu) \leq d \\ 0 \quad \text{otherwise.} \end{cases}
\]

Since the second term in the left-hand side of (16) is non-negative, for \( r(\mu) > d \) we have \( |\text{Aut}(\mu)|\nu(\mu) = 0 \), so \( \nu(\mu) = 0 \).

Now suppose that \( r(\mu) \leq d \). Our goal is to show that \( \nu(\mu) = \frac{u|\mu|((u/p)_d^{(1/p)_{d-r(\mu)}})}{|\text{Aut}(\mu)|} \).

By Theorem 5.3 in the particular case \( \nu = P_{d,u} \), (16) is equal to

\[
\frac{u|\mu|((u/p)_d^{(1/p)_{d-r(\mu)}})}{(1/p)_{d-r(\mu)}} + \sum_{\lambda \neq \mu, r(\lambda) \leq d} \frac{u|\lambda|((u/p)_d^{(1/p)_{d-r(\lambda)}})}{|\text{Aut}(\lambda)|((1/p)_{d-r(\lambda)})} = \frac{u|\mu|((1/p)_d^{(1/p)_{d-r(\mu)}})}{(1/p)_{d-r(\mu)}}.
\]

This gives

\[
\sum_{\lambda \neq \mu, r(\lambda) \leq d} \frac{u|\lambda|}{|\text{Aut}(\lambda)|((1/p)_{d-r(\lambda)})} = \frac{u|\mu|}{(1/p)_{d-r(\mu)}} \left( \frac{1}{(u/p)_d} - 1 \right).
\]

Let

\[
\beta = \frac{(1/p)_{d-r(\mu)}}{u|\mu|} \sum_{\lambda \neq \mu, r(\lambda) \leq d} \frac{|\text{Sur}(\lambda, \mu)|}{|\text{Aut}(\lambda)|((1/p)_{d-r(\lambda)})} = \frac{1}{(u/p)_d} - 1.
\]

It is enough to show that

\[
\text{(17) } |\text{Aut}(\mu)|\nu(\mu) = \frac{u|\mu|((1/p)_d^{(1/p)_{d-r(\mu)}})}{(1/p)_{d-r(\mu)}} \frac{1}{\beta + 1}.
\]

By assumption, \( |\beta| < 1 \), so we verify (17) by showing that \( |\text{Aut}(\mu)|\nu(\mu) \) is bounded by the alternating partial sums of the series

\[
\frac{u|\mu|((1/p)_d^{(1/p)_{d-r(\mu)}})}{(1/p)_{d-r(\mu)}} \frac{1}{\beta + 1} = u|\mu|((1/p)_d^{(1/p)_{d-r(\mu)}})(1 - \beta + \beta^2 - \cdots).
\]

Equation (16) implies that

\[
|\text{Aut}(\mu)|\nu(\mu) \leq \frac{u|\mu|((1/p)_d^{(1/p)_{d-r(\mu)}})}{(1/p)_{d-r(\mu)}}.
\]
For any $\lambda$ with $r(\lambda) \leq d$ this gives

$$\nu(\lambda) \leq \frac{u|\lambda|(1/p)d}{|\text{Aut}(\lambda)|(1/p)d-r(\lambda)}.$$  

Using this bound in (16) gives

$$|\text{Aut}(\mu)|\nu(\mu) = u|\mu|(1/p)d - \sum_{\lambda \neq \mu, r(\lambda) \leq d} |\text{Sur}(\lambda, \mu)|\nu(\lambda)$$

$$\geq u|\mu|(1/p)d - \sum_{\lambda \neq \mu, r(\lambda) \leq d} u|\lambda| \frac{|\text{Sur}(\lambda, \mu)|}{|\text{Aut}(\lambda)|} (1/p)d-r(\lambda)$$

$$= u|\mu|(1/p)d - \sum_{\lambda \neq \mu, r(\lambda) \leq d} u|\lambda| (1/p)d-r(\mu) \beta = u|\mu|(1/p)d (1-\beta).$$

Similarly, for any $\lambda$ with $r(\lambda) \leq d$, this gives

$$\nu(\lambda) \geq \frac{u|\lambda|}{|\text{Aut}(\lambda)|(1/p)d-r(\lambda)} (1-\beta).$$  

Using this bound in (16) gives

$$|\text{Aut}(\mu)|\nu(\mu) = u|\mu|(1/p)d - \sum_{\lambda \neq \mu, r(\lambda) \leq d} |\text{Sur}(\lambda, \mu)|\nu(\lambda)$$

$$\leq u|\mu|(1/p)d - \sum_{\lambda \neq \mu, r(\lambda) \leq d} u|\lambda| \frac{|\text{Sur}(\lambda, \mu)|}{|\text{Aut}(\lambda)|} (1/p)d-r(\lambda) (1-\beta)$$

which implies

$$|\text{Aut}(\mu)|\nu(\mu) \leq u|\mu|(1/p)d - u|\mu|(1/p)d-r(\mu) \beta(1-\beta)$$

$$= u|\mu|(1/p)d (1-\beta + \beta^2).$$

Continuing in this way completes the proof. \qed

REFERENCES

[1] Bhargava, M., Kane, D., Lenstra, H., Poonen, B., and Rains, E., Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves, *Camb. J. Math.* 3 (2015), 275-321.

[2] Boston, N. and Wood, M. M., Non-abelian Cohen-Lenstra heuristics over function fields. *Compos. Math.* 153 (2017), 1372-1390.

[3] Chinta, G., Kaplan, N., and Koplewitz, S., The cotype zeta function of $\mathbb{Z}^d$. Preprint (2017). [https://arxiv.org/abs/1708.08547v1](https://arxiv.org/abs/1708.08547v1)

[4] Clancy, J., Kaplan, N., Leake, T., Payne, S., and Wood, M., On a Cohen-Lenstra heuristic for Jacobians of random graphs, *J. Algebraic Combin.* 42 (2015), 701-723.
[5] Cohen, H., and Lenstra, H. W., Heuristics on class groups of number fields, In *Number Theory Noordwijkhout 1983 (Noordwijkhout,1983)*, pages 33–62. Springer, Berlin, 1984.

[6] Delaunay, C., and Jouhet, F., $p^i$-torsion points in finite abelian groups and combinatorial identities. *Adv. Math.* **258** (2014), 13–45.

[7] Delaunay, C., and Jouhet, F., The Cohen-Lenstra heuristics, moments and $p^i$-ranks of some groups. *Acta Arith.* **164** (2014), no 3, 245–263.

[8] Delaunay, C., Heuristics of Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$, *Experiment. Math.* **10** (2001), 191-196.

[9] Delaunay, C., Averages of groups involving $p^i$-rank and combinatorial identities, *J. Number Theory* **131** (2011), 536-551.

[10] Ellenberg, J., Venkatesh, A., and Westerland, C., Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, *Ann. of Math. (2)* **183** (2016), 729-786.

[11] Fouvry, E., and Klüners, J., Cohen-Lenstra heuristics of quadratic number fields. *Algorithmic number theory*, 40–55, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.

[12] Friedman, E., and Washington, L., On the distribution of divisor class groups of curves over a finite field. In *Theorie des nombres (Quebec, PQ, 1987)*, pages 227-239. de Gruyter, Berlin, 1989.

[13] Gerth III, F., The 4-class ranks of quadratic fields. *Invent. Math* **77** (1984), no. 3, 489–515.

[14] Macdonald, I., Symmetric functions and Hall polynomials, Second edition, Oxford University Press, 1995.

[15] Petrogradsky, V., Multiple zeta functions and asymptotic structure of free abelian groups of finite rank. *J. Pure Appl. Algebra* **208** (2007), 1137-1158.

[16] Speyer, D., An expectation of Cohen-Lenstra measure (answer). MathOverflow. [https://mathoverflow.net/questions/9950](https://mathoverflow.net/questions/9950) (visited on 01/19/2019).

[17] Stanley, R. and Wang, Y., The Smith normal form distribution of a random integer matrix, *SIAM J. Discrete Math.* **31** (2017), 2247–2268.

[18] Tse, L-S., Distribution of cokernels of $(n+u) \times n$ matrices over $\mathbb{Z}_p$, [arXiv:1608.01714](https://arxiv.org/abs/1608.01714) 2016.

[19] Wright, D. J., Distribution of discriminants of abelian extensions, *Proc. London Math. Soc.* **58** (1989), 17–50.
Department of Mathematics, University of Southern California, Los Angeles, CA 90089
E-mail address: fulman@usc.edu

Department of Mathematics, University of California, Irvine, CA 92697-3875
E-mail address: nckaplan@math.uci.edu