Ann. Comb. 23 (2019) 295–315

Published online April 27, 2019
https://doi.org/10.1007/s00026-019-00425-y

Annals of Combinatorics

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.

Mathematics Subject Classification. 15B52, 05E05.

Keywords. Cohen–Lenstra heuristics, Hall–Littlewood polynomial, Probability measure, Random matrices, Random partitions, Finite abelian group.

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 $r \le d$ is chosen with probability

$$P_d(G) = \frac{1}{|\mathrm{Aut}(G)|}\left(\prod_{i=1}^{d}(1-1/p^i)\right)\left(\prod_{i=d-r+1}^{d}(1-1/p^i)\right). \tag{1.1}$$

Let $\lambda = (\lambda_1, \ldots, \lambda_r)$ with $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_r \ge 1$ be a partition. A finite abelian p-group G has *type* λ 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 ν on partitions, we get a corresponding measure ν' 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 λ. We analogously define a measure on partitions given a measure on $\mathcal{L}$. When G is a finite abelian group of type λ, we write $|\mathrm{Aut}(\lambda)|$ for $|\mathrm{Aut}(G)|$, and from Page 181 of [19]

$$|\mathrm{Aut}(\lambda)| = p^{\sum(\lambda_i')^2} \prod_i (1/p)_{m_i(\lambda)}. \tag{1.2}$$

The notation used in (1.2) is standard, and we review it in Sect. 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 λ with $r \le d$ parts with probability

$$P_{d,u}(\lambda) = \frac{u^{|\lambda|}}{p^{\sum(\lambda_i')^2} \prod_i (1/p)_{m_i(\lambda)}} \prod_{i=1}^{d} (1 - u/p^i) \prod_{i=d-r+1}^{d} (1 - 1/p^i). \tag{1.3}$$

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 $P^p_{d,u}(\lambda)$. For clarity, we will suppress this additional notation except in Sect. 3. When p is prime, we can interpret (1.3) as a distribution on $\mathcal{L}$. 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 (1.2) as the definition of $|\mathrm{Aut}(\lambda)|$.

The main goal of this paper is to investigate combinatorial properties of the family of distributions of (1.3). 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

$$\lim_{d\to\infty} P_{d,u}(\lambda) = P_{\infty,u}(\lambda) = \frac{u^{|\lambda|}}{|\mathrm{Aut}(\lambda)|} \prod_{i\ge 1} (1 - u/p^i).$$

  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, taking μ 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 $\mathrm{GL}(N, p)$. See [13] for details.
- Note that

$$P_{\infty,1}(\lambda) = \frac{1}{|\mathrm{Aut}(\lambda)|} \prod_{i\ge 1} (1 - 1/p^i).$$

  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 $\mathrm{GL}(d, p)$ 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 λ a partition. The w-probability of λ, denoted by $P_w(\lambda)$, is the probability that a finite abelian p-group of type λ is obtained by the following three-step random process:

– Choose randomly a p-group H of type μ 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 (1.3):

$$P_w(\lambda) = P_{\infty,1/p^w}(\lambda). \tag{1.4}$$

- 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 λ is given by $P_{\infty,1/p^w}(\lambda)$. See the discussion above Proposition 2.3 of [25].
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 λ [23].
- In Sect. 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 $\mathbb{Q}$ [6].

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, Sect. 9]. Delaunay generalizes these results in Corollary 11 of [7], where he computes the probability that a group drawn from $P_{\infty,u}$ 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 [8].
  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_D^2, the square of the ideal class group of a quadratic field [11].

- Delaunay [7] and Delaunay and Jouhet [8] 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 Sect. 3. In [9], they prove analogues of the results of Fouvry and Klüners [11] for this distribution.

1.1. Outline of the Paper

In Sect. 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 Sect. 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 Sect. 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 Sect. 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 [25], 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 $\mathrm{M}_d(R)$ denote the set of all $d \times d$ matrices with entries in R and let $\mathrm{Sym}_d(R)$ denote the set of all $d \times d$ symmetric matrices with entries in R. For an even integer d, let $\mathrm{Alt}_d(R)$ 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 $\mathrm{Hom}(G,H)$ for the set of homomorphisms from G to H, $\mathrm{Sur}(G,H)$ for the set of surjective homomorphisms from G to H, and $\mathrm{Aut}(G)$ for the set of automorphisms of G. If G is a finite abelian p-group of type λ and H is a finite abelian p-group of type μ, we sometimes write $|\mathrm{Sur}(\lambda,\mu)|$ for $|\mathrm{Sur}(G,H)|$.

For a partition λ, we let λ_i denote the size of the i^{th} part of λ and $m_i(\lambda)$ denote the number of parts of λ of size i. We let λ_i' denote the size of the i^{th} column in the diagram of λ (so $\lambda_i' = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$). We also let $n(\lambda) = \sum_i \binom{\lambda_i'}{2}$. We generally use r or $r(\lambda)$ to denote the number of parts of λ. We use $|\lambda| = n$ to say that λ is a partition of n, or equivalently $\sum \lambda_i = n$.

We let $n_\lambda(\mu)$ denote the number of subgroups of type μ of a finite abelian p-group of type λ. For a finite abelian group G, the number of subgroups $H \subseteq G$ of type μ equals the number of subgroups for which G/H has type μ [19, Eq. (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, (1.3) is equivalent to

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

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

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

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_λ denote a Hall–Littlewood polynomial, defined for a partition $\lambda = (\lambda_1,\ldots,\lambda_n)$ of length at most n by

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

where

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

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

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

$$P_{d,u}(\lambda) = \prod_{i=1}^{d}(1-u/p^i)\cdot\frac{P_\lambda(\frac{u}{p},\frac{u}{p^2},\ldots,\frac{u}{p^d},0,\ldots;\frac{1}{p})}{p^{n(\lambda)}}.$$

Proof. From Page 213 of [19],

$$\prod_{i=1}^{d}(1-u/p^i)\cdot\frac{P_\lambda(\frac{u}{p},\frac{u}{p^2},\ldots,\frac{u}{p^d},0,\ldots;\frac{1}{p})}{p^{n(\lambda)}}$$

is equal to

$$\frac{u^{|\lambda|}\prod_{i=1}^{d}(1-u/p^i)}{\prod_i(1/p)_{m_i(\lambda)}}\frac{(1/p)_d}{p^{|\lambda|+2n(\lambda)}(1/p)_{d-r}}.$$

Since $|\lambda|+2n(\lambda)=\sum(\lambda_i')^2$, this is equal to (1.3), and the proposition follows. □

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 λ 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

$$K(a,b)=\frac{u^b(1/p)_a(u/p)_a}{p^{b^2}(1/p)_{a-b}(1/p)_b(u/p)_b}.$$

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 $\lambda_1'=r$), what is left is:

$$\frac{(u/p)_d(1/p)_d u^{|\lambda|}}{(1/p)_{d-r}p^{\sum(\lambda_i')^2}\prod_i(1/p)_{m_i(\lambda)}}.$$

This is equal to $P_{d,u}(\lambda)$, completing the proof. □

The following corollary is immediate from Theorem 2.2.

Corollary 2.3. *Choose λ from $P_{d,u}$. Then, the chance that λ has $r\leq d$ parts is equal to*

$$\frac{u^r(1/p)_d(u/p)_d}{p^{r^2}(1/p)_{d-r}(1/p)_r(u/p)_r}.$$

Proof. From Theorem 2.2, the sought probability is $K(d,r)$. □

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 $\mathbb{Z}^d/\Lambda$ 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 λ chosen from $P_{d,u}$ has size n.

Theorem 2.4. *The chance that λ chosen from $P_{d,u}$ has size n is equal to*

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

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

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

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]. □

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

$$\frac{u^n (u/p)_d (1/p)_d}{p^{r^2} (1/p)_{d-r} (1/p)_r} \frac{(1/p)_{n-1}}{p^{n-r} (1/p)_{r-1} (1/p)_{n-r}}.$$

Proof. From the definition of $P_{d,u}$, one has that

$$\begin{aligned}
\sum_{\substack{\lambda_1'=r \\ |\lambda|=n}} P_{d,u}(\lambda) &= \sum_{\substack{\lambda_1'=r \\ |\lambda|=n}} \frac{u^n (u/p)_d (1/p)_d}{|\text{Aut}(\lambda)| (1/p)_{d-r}} \\
&= u^n (u/p)_d \sum_{\substack{\lambda_1'=r \\ |\lambda|=n}} \frac{(1/p)_d}{|\text{Aut}(\lambda)| (1/p)_{d-r}}
\end{aligned}$$

$$
\begin{aligned}
&= u^n (u/p)_d \text{ Coef. } u^n \text{ in } \sum_{\lambda'_1=r} \frac{u^{|\lambda|}(1/p)_d}{|\mathrm{Aut}(\lambda)|(1/p)_{d-r}} \\
&= u^n (u/p)_d \text{ Coef. } u^n \text{ in } \frac{1}{(u/p)_d} \sum_{\lambda'_1=r} P_{d,u}(\lambda) \\
&= u^n (u/p)_d \text{ Coef. } u^n \text{ in } \frac{1}{(u/p)_d} \frac{u^r (1/p)_d (u/p)_d}{p^{r^2}(1/p)_{d-r}(1/p)_r (u/p)_r} \\
&= \frac{u^n (u/p)_d (1/p)_d}{p^{r^2}(1/p)_{d-r}(1/p)_r} \text{ Coef. } u^{n-r} \text{ in } \frac{1}{(u/p)_r} \\
&= \frac{u^n (u/p)_d (1/p)_d}{p^{r^2}(1/p)_{d-r}(1/p)_r} \frac{(1/p)_{n-1}}{p^{n-r}(1/p)_{r-1}(1/p)_{n-r}}.
\end{aligned}
$$

The fifth equality used Corollary 2.3, and the final equality used Theorem 349 of [17]. □

In the rest of this section, we give another view of the distributions given by (1.1) and (1.3). When p is prime, Eq. (19) in [20] implies that

$$
P_d(\lambda) = \frac{1}{p^{|\lambda|d}} \left(\prod_{i=1}^{\lambda_1} p^{\lambda'_{i+1}(d-\lambda'_i)} \binom{d-\lambda'_{i+1}}{\lambda'_i - \lambda'_{i+1}}_p \right) \prod_{i=1}^{d} (1 - 1/p^i). \tag{2.1}
$$

Comparing this to the expression for $P_d(\lambda)$ given in (1.1) shows that

$$
\frac{1}{p^{|\lambda|d}} \left(\prod_{i=1}^{\lambda_1} p^{\lambda'_{i+1}(d-\lambda'_i)} \binom{d-\lambda'_{i+1}}{\lambda'_i - \lambda'_{i+1}}_p \right) = \frac{1}{|\mathrm{Aut}(\lambda)|} \left(\prod_{i=d-r+1}^{d} (1 - 1/p^i) \right). \tag{2.2}
$$

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

$$
P_{d,u}(\lambda) = \frac{u^{|\lambda|}}{p^{|\lambda|d}} \left(\prod_{i=1}^{\lambda_1} p^{\lambda'_{i+1}(d-\lambda'_i)} \binom{d-\lambda'_{i+1}}{\lambda'_i - \lambda'_{i+1}}_p \right) \prod_{i=1}^{d} (1 - u/p^i). \tag{2.3}
$$

We give a combinatorial proof of (2.2) that applies for any real $p > 1$, so (2.3) applies for any $p > 1$ and $0 < u < p$.

Proof of Equation (2.2). It is sufficient to show that for a partition λ with $r \leq d$ parts

$$
|\mathrm{Aut}(\lambda)| \left(\prod_{i=1}^{\lambda_1} p^{\lambda'_{i+1}(d-\lambda'_i)} \binom{d-\lambda'_{i+1}}{\lambda'_i - \lambda'_{i+1}}_p \right) = p^{|\lambda|d} \prod_{j=0}^{r-1} (1 - p^{-d+j}). \tag{2.4}
$$

Clearly

$$\begin{aligned}
&\prod_{i=1}^{\lambda_1} p^{\lambda'_{i+1}(d-\lambda'_i)} \binom{d-\lambda'_{i+1}}{\lambda'_i-\lambda'_{i+1}}_p \\
&\quad = p^{d(|\lambda|-\lambda'_1)-\sum_i \lambda'_i\lambda'_{i+1}} \prod_i \binom{d-\lambda'_{i+1}}{\lambda'_i-\lambda'_{i+1}}_p \\
&\quad = p^{d(|\lambda|-\lambda'_1)-\sum_i \lambda'_i\lambda'_{i+1}} \frac{[d]_p!}{[d-\lambda'_1]_p![\lambda'_1-\lambda'_2]_p![\lambda'_2-\lambda'_3]_p!\cdots} \\
&\quad = p^{d(|\lambda|-\lambda'_1)-\sum_i \lambda'_i\lambda'_{i+1}} \frac{(p-1)^{\lambda'_1}[d]_p!}{[d-\lambda'_1]_p! p^{\sum_i \binom{\lambda'_i-\lambda'_{i+1}+1}{2}} \prod_i (1/p)_{m_i(\lambda)}} \\
&\quad = \frac{p^{d(|\lambda|-\lambda'_1)}(p-1)^{\lambda'_1}[d]_p!}{[d-\lambda'_1]_p! p^{\frac{1}{2}[\sum_i (\lambda'_i)^2+(\lambda'_{i+1})^2+\lambda'_i-\lambda'_{i+1}]} \prod_i (1/p)_{m_i(\lambda)}} \\
&\quad = \frac{p^{d(|\lambda|-\lambda'_1)} p^{(\lambda'_1)^2/2}(p-1)^{\lambda'_1}[d]_p!}{[d-\lambda'_1]_p! p^{\lambda'_1/2}} \cdot \frac{1}{p^{\sum_i (\lambda'_i)^2} \prod_i (1/p)_{m_i(\lambda)}}.
\end{aligned}$$

Since $\lambda'_1 = r$, Eq. (1.2) implies that the left-hand side of (2.4) is equal to

$$\frac{p^{d|\lambda|-dr+r^2/2-r/2}(p-1)^r[d]_p!}{[d-r]_p!} = p^{d|\lambda|-dr+r^2/2-r/2}(p^d-1)\cdots(p^{d-r+1}-1),$$

which simplifies to the right-hand side of (2.4). □

We now use the alternate expression of (2.3) 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

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

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

$$\begin{aligned}
\zeta_{\mathbb{Z}^d}(s) &= \zeta(s)\zeta(s-1)\cdots\zeta(s-(d-1)) \\
&= \prod_p \left((1-p^{-s})^{-1}(1-p^{-(s-1)})^{-1}\cdots(1-p^{-(s-(d-1))})^{-1}\right), \qquad (2.5)
\end{aligned}$$

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 (2.3), we need only prove

$$\sum_{|\lambda|=n} \frac{u^n}{p^{nd}} \left(\prod_{i=1}^{\lambda_1} p^{\lambda'_{i+1}(d-\lambda'_i)} \binom{d-\lambda'_{i+1}}{\lambda'_i-\lambda'_{i+1}}_p\right) = \frac{u^n}{p^n} \frac{(1/p)_{d+n-1}}{(1/p)_{d-1}(1/p)_n}. \qquad (2.6)$$

Let $\lambda^* = (\lambda_1, \ldots, \lambda_1)$, where there are d entries in the tuple. The discussion around Eq. (19) in [20] says that the term in parentheses of the left-hand side of (2.6) is equal to the number of subgroups of a finite abelian p-group of type λ^* that have type λ, $n_{\lambda^*}(\lambda)$, 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 λ.

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 (2.5), this is equal to

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

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. □

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 $P^p_{d,u}$.

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

Lemma 3.1. *Let n be an even positive integer and $A \in \mathrm{Alt}_n(\mathbb{Z}_p)$ be a random matrix chosen with respect to additive Haar measure on $\mathrm{Alt}_n(\mathbb{Z}_p)$. The probability that the cokernel of A is isomorphic to G is given by*

$$P^{Alt}_{n,p}(\lambda) = \frac{\prod_{i=n-2r+1}^{n}(1-1/p^i)\prod_{i=1}^{n/2-r}(1-1/p^{2i-1})}{p^{|\lambda|+4n(\lambda)}\prod_i\prod_{j=1}^{m_i(\lambda)}(1-1/p^{2j})}. \tag{3.1}$$

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

$$\frac{\left|\mathrm{Sur}(\mathbb{Z}_p^n, G)\right|}{|\mathrm{Sp}(G)|}\prod_{i=1}^{n/2-r}(1-1/p^{2i-1})|G|^{1-n}.$$

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

$$|\mathrm{Sur}(\mathbb{Z}_p^n, G)| = p^{2n|\lambda|}\prod_{i=n-2r+1}^{n}(1-1/p^i).$$

An identity on the bottom of Page 538 of [7] says that

$$|\mathrm{Sp}(G)| = p^{|\lambda|} p^{2\sum_i (\lambda_i')^2} \prod_i \prod_{j=1}^{m_i(\lambda)} (1-1/p^{2j})$$
$$= p^{4n(\lambda)+3|\lambda|} \prod_i \prod_{j=1}^{m_i(\lambda)} (1-1/p^{2j}).$$

Putting these results together completes the proof. □

The next theorem shows that (3.1) is a special case of (1.3).

Theorem 3.2. *Let n be an even positive integer. For any partition λ,*

$$P^{p^2}_{n/2,p}(\lambda) = P^{Alt}_{n,p}(\lambda).$$

Proof. Rewrite (1.3) as:

$$\frac{u^{|\lambda|} \prod_{i=1}^{d} (1-u/p^i) \prod_{i=d-r+1}^{d} (1-1/p^i)}{p^{2n(\lambda)+|\lambda|} \prod_i \prod_{j=1}^{m_i(\lambda)} (1-1/p^j)}.$$

Replacing d by $n/2$, u by p, and p by p^2 gives

$$\frac{\prod_{i=1}^{n/2} (1-1/p^{2i-1}) \prod_{i=n/2-r+1}^{n/2} (1-1/p^{2i})}{p^{4n(\lambda)+|\lambda|} \prod_i \prod_{j=1}^{m_i(\lambda)} (1-1/p^{2j})}.$$

On comparing with (3.1), 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 $(1/p)_n$. □

4. Cokernels of Random Symmetric p-Adic Matrices

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

$$P_n^{\mathrm{Sym}}(\lambda) = \frac{\prod_{j=n-r+1}^{n} (1-1/p^j) \prod_{i=1}^{\lceil (n-r)/2 \rceil} (1-1/p^{2i-1})}{p^{n(\lambda)+|\lambda|} \prod_{i\geq 1} \prod_{j=1}^{\lfloor m_i(\lambda)/2 \rfloor} (1-1/p^{2j})}. \tag{4.1}$$

Note that $P_n^{\mathrm{Sym}}(\lambda) = 0$ if λ has more than n parts. As in earlier sections, when p is prime (4.1) 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 λ is chosen with probability

$$P_\infty^{\mathrm{Sym}}(\lambda) = \frac{\prod_{i \text{ odd}} (1 - 1/p^i)}{p^{n(\lambda)+|\lambda|} \prod_{i \geq 1} \prod_{j=1}^{\lfloor m_i(\lambda)/2 \rfloor} (1 - 1/p^{2j})}. \tag{4.2}$$

The distribution of (4.2) 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 (4.1) also sits within a larger family.

The following theorem allows one to generate partitions from the measure (4.1) 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 $\lambda_l' = a$, then $\lambda_{l+1}' = b$ with probability*

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

Then, the resulting partition with at most n parts is distributed according to (4.1).

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:

$$\frac{\prod_{j=1}^{n}(1 - 1/p^j)}{\prod_{j=1}^{\lfloor (n-r)/2 \rfloor}(1 - 1/p^{2j})} \frac{1}{p^{n(\lambda)+|\lambda|} \prod_{i \geq 1} \prod_{j=1}^{\lfloor m_i(\lambda)/2 \rfloor}(1 - 1/p^{2j})}.$$

So to complete the proof, it is necessary to check that

$$\frac{\prod_{j=1}^{n}(1 - 1/p^j)}{\prod_{j=1}^{\lfloor (n-r)/2 \rfloor}(1 - 1/p^{2j})} = \prod_{j=n-r+1}^{n}(1 - 1/p^j) \prod_{i=1}^{\lceil (n-r)/2 \rceil}(1 - 1/p^{2i-1}).$$

This equation is easily verified by breaking it into cases based on whether $n-r$ is even or odd. □

The following corollary is immediate.

Corollary 4.2. *Let λ be chosen from (4.1). Then, the chance that λ has $r \leq n$ parts is equal to*

$$\frac{\prod_{j=r+1}^{n}(1 - 1/p^j)}{p^{\binom{r+1}{2}} \prod_{j=1}^{\lfloor (n-r)/2 \rfloor}(1 - 1/p^{2j})}.$$

Proof. By Theorem 4.1, the sought probability is equal to $K(n,r)$. □

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 ν 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 λ. When $G, H \in \mathcal{L}$ we write $|\mathrm{Sur}(G,H)|$ for the number of surjections from any representative of the isomorphism class G to any representative of the isomorphism class H.

Let ν be a probability measure on $\mathcal{L}$. For $H \in \mathcal{L}$, the H-moment of ν is defined as:

$$\sum_{G\in\mathcal{L}} \nu(G)|\mathrm{Sur}(G,H)|.$$

When H is a finite abelian p-group of type μ, this is

$$\sum_{\lambda} \nu(\lambda)|\mathrm{Sur}(\lambda,\mu)|.$$

The distribution ν gives a measure on partitions and we refer to this quantity as the μ-moment of the measure. For an explanation of why these are called the moments of the distribution, see Sect. 3.3 of [4].

The Cohen–Lenstra distribution is the probability distribution on $\mathcal{L}$ for which a finite abelian group G of type λ 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 μ,

$$\sum_{\lambda} P_{\infty,1}(\lambda)|\mathrm{Sur}(\lambda,\mu)| = 1.$$

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 (1.1) (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 ν is any probability measure on $\mathcal{L}$ for which*

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

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, 25]. 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 μ of a finite abelian group of type λ.

Lemma 5.2. *Let G, H be finite abelian p-groups of types λ and μ, respectively. Then*

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

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

The distributions $P_{d,u}$ are defined for all $p > 1$. It is not immediately clear what the μ-moment of this distribution should mean when p is not prime, since $|\mathrm{Sur}(\lambda,\mu)|$ is defined in terms of surjective homomorphisms between finite abelian p-groups. In (1.2), we saw how to define $|\mathrm{Aut}(\lambda)|$ in terms of the parts of the partition λ and the parameter p, even in the case where p is not prime. Similarly, Lemma 5.2 gives a way to define $|\mathrm{Sur}(\lambda,\mu)|$ in terms of the parameter p and the partitions λ and μ even when p is not prime. We first define $|\mathrm{Aut}(\mu)|$ using (1.2), and then note that $n_\lambda(\mu)$ is a polynomial in p that we can evaluate for any $p > 1$.

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

$$\begin{cases} \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}, & \text{if } r(\mu) \le d, \\ 0, & \text{otherwise.} \end{cases}$$

Here, as above, $r(\mu)$ denotes the number of parts of μ.

Proof. Clearly, we can suppose that $r(\mu) \le d$. By Lemma 5.2, the μ-moment of the distribution $P_{d,u}$ is equal to

$$\sum_\lambda P_{d,u}(\lambda)|\mathrm{Sur}(\lambda,\mu)| = |\mathrm{Aut}(\mu)| \sum_\lambda P_{d,u}(\lambda) n_\lambda(\mu).$$

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

$$|\mathrm{Aut}(\mu)| \prod_{i=1}^d (1 - u/p^i) \cdot \sum_\lambda \frac{P_\lambda(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p})}{p^{n(\lambda)}} \sum_\nu n_\lambda(\mu,\nu).$$

Reversing the order of summation, this becomes

$$|\mathrm{Aut}(\mu)| \prod_{i=1}^d (1 - u/p^i) \cdot \sum_\nu \sum_\lambda \frac{P_\lambda(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p})}{p^{n(\lambda)}} n_\lambda(\mu,\nu).$$

From Sect. 3.3 of [19], it follows that for any values of the x variables

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

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

$$|\mathrm{Aut}(\mu)| \prod_{i=1}^{d} \left(1 - \frac{u}{p^i}\right) \cdot \sum_{\nu} \frac{P_\mu(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p}) P_\nu(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p})}{p^{n(\mu)} p^{n(\nu)}}$$

$$= |\mathrm{Aut}(\mu)| \frac{P_\mu(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p})}{p^{n(\mu)}} \sum_{\nu} \prod_{i=1}^{d} \left(1 - \frac{u}{p^i}\right) \frac{P_\nu(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p})}{p^{n(\nu)}}.$$

By Proposition 2.1, this is equal to

$$|\mathrm{Aut}(\mu)| \frac{P_\mu(\frac{u}{p}, \frac{u}{p^2}, \ldots, \frac{u}{p^d}, 0, \ldots; \frac{1}{p})}{p^{n(\mu)}}.$$

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

$$\frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}.$$

□

Remark.
- 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 (1.4), and in this case Theorem 5.3 recovers Lemma 3.2 of [26].
- 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^ℓ-torsion elements of a finite abelian group H drawn from $P_{d,u}$. Let T_ℓ 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^ℓ is $T_\ell(H) - T_{\ell-1}(H)$.

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

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

If H is of type λ, then $r_{p^k}(H) = \lambda'_k$, the number of parts of λ of size at least k. The number of parts of λ 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, ℓ 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 $u^\ell(1 - p^{-d})$.

Remark.
- 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 [7]. 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 [8]. We do not pursue this further here.

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

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

Proof. Suppose

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

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^{λ_i}.

A homomorphism from H to $\mathbb{Z}/p^\ell\mathbb{Z}$ is uniquely determined by the images of $e_1, \ldots, e_{r_p(H)}$. When $\lambda_i \geq \ell$ there are p^ℓ choices for the image of e_i. If $1 \leq \lambda_i \leq \ell$, there are p^{λ_i} choices for the image of e_i. Therefore, the total number of homomorphisms is

$$p^{\ell\lambda'_\ell+(\ell-1)(\lambda'_{\ell-1}-\lambda'_\ell)+\cdots+1\cdot(\lambda'_1-\lambda'_2)}.$$

□

Proof of Theorem 5.4. We compute the expected value of

$$\#\mathrm{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z}) - \#\mathrm{Hom}(H, \mathbb{Z}/p^{\ell-1}\mathbb{Z})$$

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 $\mathrm{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z})$ 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

$$\#\mathrm{Sur}(H, \mathbb{Z}/p^\ell\mathbb{Z}) = \#\mathrm{Hom}(H, \mathbb{Z}/p^\ell\mathbb{Z}) - \#\mathrm{Hom}(H, \mathbb{Z}/p^{\ell-1}\mathbb{Z}).$$

Lemma 5.5 implies $T_\ell(H) - T_{\ell-1}(H) = \#\mathrm{Sur}(H, \mathbb{Z}/p^\ell\mathbb{Z})$. 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*

$$\frac{1}{(u/p)_d} = \prod_{i=1}^{d}(1 - u/p^i)^{-1} < 2. \tag{5.1}$$

If ν is any probability measure on the set of partitions for which

$$\sum_\lambda \nu(\lambda)|\mathrm{Sur}(\lambda, \mu)| = \begin{cases} \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}, & \text{if } r(\mu) \leq d, \\ 0, & \text{otherwise,} \end{cases} \tag{5.2}$$

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

Remark.

- 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 (5.1) decreases 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 [25].
- 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 [26] and Theorem 8.3 in [24].

Proof. The assumption gives, for every μ

$$|\mathrm{Aut}(\mu)|\nu(\mu) + \sum_{\lambda \neq \mu} |\mathrm{Sur}(\lambda, \mu)|\nu(\lambda) = \begin{cases} \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}, & \text{if } r(\mu) \leq d, \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$

Since the second term on the left-hand side of (5.3) is non-negative, for $r(\mu) > d$ we have $|\mathrm{Aut}(\mu)|\nu(\mu) = 0$, so $\nu(\mu) = 0$.

Now suppose that $r(\mu) \leq d$. Our goal is to show that

$$\nu(\mu) = \frac{u^{|\mu|}(u/p)_d}{|\mathrm{Aut}(\mu)|} \frac{(1/p)_d}{(1/p)_{d-r(\mu)}}.$$

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

$$\frac{u^{|\mu|}(u/p)_d(1/p)_d}{(1/p)_{d-r(\mu)}} + \sum_{\substack{\lambda \neq \mu \\ r(\lambda) \leq d}} u^{|\lambda|}(u/p)_d \frac{|\mathrm{Sur}(\lambda, \mu)|}{|\mathrm{Aut}(\lambda)|} \frac{(1/p)_d}{(1/p)_{d-r(\lambda)}} = \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}.$$

This gives

$$\sum_{\substack{\lambda \neq \mu \\ r(\lambda) \leq d}} u^{|\lambda|} \frac{|\mathrm{Sur}(\lambda, \mu)|}{|\mathrm{Aut}(\lambda)|(1/p)_{d-r(\lambda)}} = \frac{u^{|\mu|}}{(1/p)_{d-r(\mu)}} \left(\frac{1}{(u/p)_d} - 1 \right).$$

Let

$$\beta = \frac{(1/p)_{d-r(\mu)}}{u^{|\mu|}} \sum_{\substack{\lambda \neq \mu \\ r(\lambda) \leq d}} u^{|\lambda|} \frac{|\mathrm{Sur}(\lambda, \mu)|}{|\mathrm{Aut}(\lambda)|(1/p)_{d-r(\lambda)}} = \frac{1}{(u/p)_d} - 1.$$

It is enough to show that

$$|\mathrm{Aut}(\mu)|\nu(\mu) = u^{|\mu|} \frac{(1/p)_d}{(1/p)_{d-r(\mu)}} \frac{1}{\beta + 1}. \tag{5.4}$$

By assumption, $|\beta| < 1$, so we verify (5.4) by showing that $|\mathrm{Aut}(\mu)|\nu(\mu)$ is bounded by the alternating partial sums of the series

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

Equation (5.3) implies that

$$|\mathrm{Aut}(\mu)|\nu(\mu) \le \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}.$$

For any λ with $r(\lambda) \le d$, this gives

$$\nu(\lambda) \le \frac{u^{|\lambda|}(1/p)_d}{|\mathrm{Aut}(\lambda)|(1/p)_{d-r(\lambda)}}.$$

Using this bound in (5.3) gives

$$\begin{aligned}
|\mathrm{Aut}(\mu)|\nu(\mu) &= u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}} - \sum_{\substack{\lambda\neq\mu \\ r(\lambda)\le d}} |\mathrm{Sur}(\lambda,\mu)|\nu(\lambda) \\
&\ge u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}} - \sum_{\substack{\lambda\neq\mu \\ r(\lambda)\le d}} u^{|\lambda|}\frac{|\mathrm{Sur}(\lambda,\mu)|}{|\mathrm{Aut}(\lambda)|}\frac{(1/p)_d}{(1/p)_{d-r(\lambda)}} \\
&= \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}} - \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}\beta \\
&= \frac{u^{|\mu|}(1/p)_d}{(1/p)_{d-r(\mu)}}(1-\beta).
\end{aligned}$$

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

$$\nu(\lambda) \ge \frac{u^{|\lambda|}}{|\mathrm{Aut}(\lambda)|}\frac{(1/p)_d}{(1/p)_{d-r(\lambda)}}(1-\beta).$$

Using this bound in (5.3) gives

$$\begin{aligned}
|\mathrm{Aut}(\mu)|\nu(\mu) &= u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}} - \sum_{\substack{\lambda\neq\mu \\ r(\lambda)\le d}} |\mathrm{Sur}(\lambda,\mu)|\nu(\lambda) \\
&\le u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}} - \sum_{\substack{\lambda\neq\mu \\ r(\lambda)\le d}} u^{|\lambda|}\frac{|\mathrm{Sur}(\lambda,\mu)|}{|\mathrm{Aut}(\lambda)|}\frac{(1/p)_d}{(1/p)_{d-r(\lambda)}}(1-\beta),
\end{aligned}$$

which implies

$$\begin{aligned}
|\mathrm{Aut}(\mu)|\nu(\mu) &\le u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}} - u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}}\beta(1-\beta) \\
&= u^{|\mu|}\frac{(1/p)_d}{(1/p)_{d-r(\mu)}}(1-\beta+\beta^2).
\end{aligned}$$

Continuing in this way completes the proof. □

Acknowledgements

Fulman is supported by Simons Foundation Grant 400528. Kaplan is supported by NSA Young Investigator Grant H98230-16-10305, NSF Grant DMS 1802281 and by an AMS-Simons Travel Grant. The authors thank the referees, Gilyoung Cheong, and Melanie Matchett Wood for helpful comments.

References

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

[2] Boston, N., Wood, M.M.: Non-abelian Cohen-Lenstra heuristics over function fields. Compos. Math. 153(7), 1372–1390 (2017)

[3] Chinta, G., Kaplan, N., Koplewitz, S.: The cotype zeta function of $\mathbb{Z}^d$. arXiv:1708.08547v1 (2017)

[4] Clancy, J., Kaplan, N., Leake, T., Payne, S., Wood, M.M.: On a Cohen-Lenstra heuristic for Jacobians of random graphs. J. Algebraic Combin. 42(3), 701–723 (2015)

[5] Cohen, H., Lenstra Jr., H.W.: Heuristics on class groups of number fields. In: Jager, H. (ed.) Number Theory, Noordwijkerhout 1983 (Noordwijkerhout,1983), pp. 33–62. Springer, Berlin (1984)

[6] Delaunay, C.: Heuristics of Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. Experiment. Math. 10(2), 191–196 (2001)

[7] Delaunay, C.: Averages of groups involving p^l-rank and combinatorial identities. J. Number Theory 131(3), 536–551 (2011)

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

[9] Delaunay, C., Jouhet, F.: The Cohen-Lenstra heuristics, moments and p^j-ranks of some groups. Acta Arith. 164(3), 245–263 (2014)

[10] Ellenberg, J.S., Venkatesh, A., Westerland, C.: Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. Ann. of Math. (2) 183(3), 729–786 (2016)

[11] Fouvry, E., Klüners, J.: Cohen-Lenstra heuristics of quadratic number fields. In: Hess, F., Pauli, S., Pohst, M. (eds.) Algorithmic Number Theory, Lecture Notes in Comput. Sci., Vol. 4076, pp. 40–55. Springer, Berlin (2006)

[12] Friedman, E., Washington, L.: On the distribution of divisor class groups of curves over a finite field. In: De Koninck, J.-M., Levesque, C. (eds.) Théorie des Nombres (Quebec, PQ, 1987), pp. 227–239. de Gruyer, Berlin (1989)

[13] Fulman, J.: A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups. J. Algebra 212(2), 557–590 (1999)

[14] Fulman, J.: Hall-Littlewood polynomials and Cohen-Lenstra heuristics for Jacobians of random graphs. Ann. Comb. 20(1), 115–124 (2016)

[15] Gerth III, F.: The 4-class ranks of quadratic fields. Invent. Math. 77(3), 489–515 (1984)

[16] Gerth III, F.: Extension of conjecture of Cohen and Lenstra. Exposition. Math. 5(2), 181–184 (1987)

[17] Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Fifth Edition. Oxford University Press, New York (1979)

[18] Lubotzky, A., Segal, D.: Subgroup Growth. Progress in Mathematics, Vol. 212. Birkhäuser Verlag, Basel (2003)

[19] Macdonald, I.G.: Symmetric Functions and Hall Polynomials. Second Edition. Oxford University Press, New York (1995)

[20] Petrogradsky, V.M.: Multiple zeta functions and asymptotic structure of free abelian groups of finite rank. J. Pure Appl. Algebra 208(3), 1137–1158 (2007)

[21] Speyer, D.: An expectation of Cohen-Lenstra measure (answer). MathOverflow. https://mathoverflow.net/questions/9950

[22] Stanley, R.P., Wang, Y.: The Smith normal form distribution of a random integer matrix. SIAM J. Discrete Math. 31(3), 2247–2268 (2017)

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

[24] Wood, M.M.: The distribution of sandpile groups of random graphs. J. Amer. Math. Soc. 30(4), 915–958 (2017)

[25] Wood, M.M.: Cohen-Lenstra heuristics and local conditions. Res. Number Theory 4(4), Art. 41 (2018)

[26] Wood, M.M.: Random integral matrices and the Cohen-Lenstra heuristics. Amer. J. Math. 41(2), 383–398 (2019)

[27] Wright, D.J.: Distribution of discriminants of abelian extensions. Proc. London Math. Soc. (3) 58(1), 17–50 (1989)

Jason Fulman
Department of Mathematics
University of Southern California
Los Angeles
CA 90089
USA
e-mail: fulman@usc.edu

Nathan Kaplan
Department of Mathematics
University of California
Irvine
CA 92697-3875
USA
e-mail: nckaplan@math.uci.edu

Received: 4 March 2018.
Accepted: 30 October 2018.