The distribution of the cokernel of a random integral symmetric matrix modulo a prime power

Rohan Das
BASIS Independent Silicon Valley

Christopher Qiu
Bridgewater Raritan High School

Shiqiao Zhang
Phillips Exeter Academy

MIT PRIMES Research
Boston, Massachusetts

Under the direction of
Prof. Nathan Kaplan
Prof. Gilyoung Cheong
University of California, Irvine

The distribution of the cokernel of a random integral symmetric matrix modulo a prime power

Rohan Das   Christopher Qiu   Shiqiao Zhang

Abstract

Given a prime p and positive integers n and k, consider the ring $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ of $n \times n$ matrices over $\mathbb{Z}/p^k\mathbb{Z}$. Friedman and Washington computed the number of matrices in $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ with a given residue modulo p and a given cokernel G subject to the condition $p^{k-1}G = 0$. Cheong, Liang, and Strand generalized this result by removing the condition $p^{k-1}G = 0$, completing the description of the distribution of the cokernel of a random matrix uniformly selected from $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$. In this paper, we investigate the distribution of the cokernel of a random symmetric matrix uniformly selected from $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$. We prove a symmetric analogue of the result of Cheong, Liang, and Strand by adapting their methods. Our result leads to a refined version of a result of Clancy, Kaplan, Leake, Payne, and Wood.

Contents

1 Introduction

Throughout the paper, let p be a prime and k and n be positive integers. We adopt the following notation.

Definition 1.1. For any nonnegative integer m and positive integer q, we write

$$\phi_m(q) = \prod_{j=1}^{m}(1 - q^{-j}) \qquad \text{and} \qquad \psi_m(q) = \prod_{j=1}^{\lfloor m/2 \rfloor}(1 - q^{-2j}).$$

In [7], Friedman and Washington studied the distribution of the cokernel of a random matrix selected from $\mathrm{M}_n(\mathbb{Z}_p)$, the ring of $n \times n$ matrices over the p-adic integers. They showed the following result, where we identify $\mathbb{Z}/p\mathbb{Z}$ with the finite field $\mathbb{F}_p$. We recall an explicit formula for $|\mathrm{Aut}(G)|$, the order of the automorphism group of G, in Lemma 2.24.

Theorem 1.2 ([7, pp. 232–233])**.** *Suppose that G is a finitely generated torsion module over $\mathbb{Z}_p$. For a random matrix X selected from $\mathrm{M}_n(\mathbb{Z}_p)$ with respect to additive Haar measure, the probability that $\mathrm{cok}(X) \simeq G$ is*

$$P_n(G) = \frac{1}{|\mathrm{Aut}(G)|} \frac{\phi_n(p)^2}{\phi_{n-r}(p)},$$

where $r = \dim_{\mathbb{F}_p}(G/pG)$.

Friedman and Washington were motivated by the study of Cohen–Lenstra heuristics for p-parts of ideal class groups of number fields; see the introduction to the paper of Cheong and Huang [3] for additional discussion of the connection between ideal class groups and cokernels of p-adic matrices and the motivation behind the work of Friedman and Washington. In addition, the cokernel of a matrix $X \in \mathrm{M}_n(\mathbb{Z}_p)$ carries the same information as the Smith normal form of X, which has a variety of applications throughout combinatorics and number theory; see, for example, the survey of Stanley [12].

Friedman and Washington also studied the distribution of the cokernel of a random matrix uniformly selected from $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$, which is equivalent to counting the number of matrices in $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ whose cokernel is a given finitely generated module G over $\mathbb{Z}/p^k\mathbb{Z}$. A main idea of their work is to fix some matrix $\bar{X} \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ and count the matrices in $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ with the given cokernel G whose residue modulo p is $\bar{X}$. They showed the following result.[1]

Theorem 1.3 ([7, pp. 235–236])**.** *Suppose that G is a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ satisfying $p^{k-1}G = 0$. For any $\bar{X} \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ such that $\mathrm{cok}(\bar{X}) \simeq G/pG$,*

$$\#\left\{\begin{array}{c} X \in \mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z}) : \\ \mathrm{cok}(X) \simeq G \\ \textit{and } X \equiv \bar{X} \pmod{p} \end{array}\right\} = \frac{p^{(k-1)n^2+r^2}}{|\mathrm{Aut}(G)|}\phi_r(p)^2,$$

where $r = \dim_{\mathbb{F}_p}(G/pG)$.

It is striking that the count in Theorem 1.3 does not depend on the fixed residue $\bar{X}$ as long as $\mathrm{cok}(\bar{X}) \simeq G/pG$. Since $\mathrm{cok}(\bar{X}) \simeq G/pG$ is equivalent to

[1] The original result was stated in terms of $\mathrm{cok}(X - I)$ instead of $\mathrm{cok}(X)$, where I is the $n \times n$ identity matrix. This does not affect counting since the map $X \mapsto X - I$ is bijective.

$\operatorname{rank}(\bar{X}) = n - r$, the number of such residues $\bar{X}$ is well-known; see Lemma 2.22. Multiplying the result of Theorem 1.3 by the number of admissible residues $\bar{X}$ gives the total number of matrices $X \in \mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ satisfying $\operatorname{cok}(X) \simeq G$ subject to the condition $p^{k-1}G = 0$, which is enough to recover Theorem 1.2.

In [4], Cheong, Liang, and Strand refined Theorem 1.3 to cover the case $p^{k-1}G \neq 0$.[2]

Theorem 1.4 ([4, p. 8])**.** *Suppose that G is a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$. For any $\bar{X} \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ such that $\operatorname{cok}(\bar{X}) \simeq G/pG$,*

$$\#\left\{\begin{matrix} X \in \mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z}) : \\ \operatorname{cok}(X) \simeq G \\ \textit{and } X \equiv \bar{X} \pmod p \end{matrix}\right\} = \frac{p^{(k-1)n^2+r^2}}{|\operatorname{Aut}(G)|}\frac{\phi_r(p)^2}{\phi_u(p)},$$

where $r = \dim_{\mathbb{F}_p}(G/pG)$ and $u = \dim_{\mathbb{F}_p}(p^{k-1}G)$.

Combined with Lemma 2.22, Theorem 1.4 fully describes the distribution of the cokernel of a random matrix uniformly selected from $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$.

Following the work of Friedman and Washington, many mathematicians have studied distributions of cokernels of families of random matrices over $\mathbb{Z}_p$. For example, Bhargava, Kane, Lenstra, Poonen, and Rains [2] determined the distribution of the cokernel of a random $n \times n$ alternating matrix over $\mathbb{Z}_p$, and Clancy, Kaplan, Leake, Payne, and Wood [5] determined the distribution of the cokernel of a random $n \times n$ symmetric matrix over $\mathbb{Z}_p$. The following symmetric analogue to Theorem 1.2 is a consequence of Theorem 2 in [5, p. 706]. We review partitions and related notation in Section 2.5.

Theorem 1.5 ([8, p. 305])**.** *Suppose that G is a finitely generated torsion module over $\mathbb{Z}_p$ with the product decomposition*

$$G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

as specified in Corollary 2.8 and type $\lambda = (\lambda_1, \ldots, \lambda_r)$ as defined in Definition 2.21. For a random matrix X selected from $\operatorname{Sym}_n(\mathbb{Z}_p)$ with respect to additive Haar measure, the probability that $\operatorname{cok}(X) \simeq G$ is

$$P_n^{\mathrm{Sym}}(\lambda) = p^{-n(\lambda)-|\lambda|}\frac{\phi_n(p)}{\psi_{n-r}(p)}\prod_{i=1}^{s}\frac{1}{\psi_{r_i}(p)}.$$

Theorem 1.5 is enough to determine the total number of matrices $X \in \operatorname{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})$ satisfying $\operatorname{cok}(X) \simeq G$ subject to the condition $p^{k-1}G = 0$.

In this paper, we seek a refinement to Theorem 1.5 analogous to Theorem 1.3 and Theorem 1.4 by counting the matrices in $\operatorname{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})$ with the given cokernel G whose residue modulo p is some fixed matrix $\bar{X} \in \operatorname{Sym}_n(\mathbb{Z}/p\mathbb{Z})$. This is our main result.

[2] The original result was more generally stated in terms of a polynomial pushforward $P(X)$ of the matrix X. We are concerned with the special case $P(t) = t$.

Theorem 1.6 (Main result)**.** *Suppose that G is a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ with the product decomposition*

$$G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

as specified in Corollary 2.8. For any $\bar{X} \in \mathrm{Sym}_n(\mathbb{Z}/p\mathbb{Z})$ such that $\mathrm{cok}(\bar{X}) \simeq G/pG$,

$$\#\left\{ \begin{matrix} X \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z}) : \\ \mathrm{cok}(X) \simeq G \\ \textit{and } X \equiv \bar{X} \pmod{p} \end{matrix} \right\} = \sqrt{\frac{p^{(k-1)n(n+1)+r(r+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_r(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)},$$

where

$$r = \dim_{\mathbb{F}_p}(G/pG) = \sum_{i=1}^{s} r_i$$

and

$$u = \dim_{\mathbb{F}_p}(p^{k-1}G) = \begin{cases} r_1 & \textit{if } e_1 = k, \\ 0 & \textit{if } e_1 < k. \end{cases}$$

Again, since $\mathrm{cok}(\bar{X}) \simeq G/pG$ is equivalent to $\mathrm{rank}(\bar{X}) = n - r$, the number of such residues $\bar{X}$ follows from Lemma 2.23. Multiplying the result of Theorem 1.6 by the number of admissible residues $\bar{X}$ gives the total number of matrices $X \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})$ satisfying $\mathrm{cok}(X) \simeq G$, which is enough to recover Theorem 1.5 as we discuss in Section 4. Our proof of Theorem 1.6, given in Section 3, does not use the method of moments, a major tool in this subject. Instead, we demonstrate that the methodology originally employed by Friedman and Washington in [7] and later refined by Cheong, Liang, and Strand in [4] carries over to the symmetric case.

In Theorem 1.3 on [13, pp. 919–920], Wood showed a strong universality result for the distribution of the cokernel of a random $n \times n$ symmetric matrix as $n \to \infty$, namely that the distribution follows a variant of the Cohen–Lenstra heuristics as long as the random symmetric matrix X comes from choosing each entry X_{ij} $(i \leq j)$ independently from an ϵ-balanced distribution. We show that the cokernel distribution still follows a variant of the Cohen–Lenstra heuristics when we restrict to symmetric matrices with a fixed residue modulo p. Our results fit into a body of literature about cokernels of families of p-adic matrices with algebraic structure and variations of the Cohen–Lenstra heuristics. For example, Cheong and Huang [3] studied the cokernel of a polynomial pushforward of a random matrix, Yan [14] worked with random matrices over a Dedekind domain, and Lee [9] investigated Hermitian matrices.

2 Preliminaries

In this section, we review some preliminary concepts and results.

2.1 p-adic integers and the additive Haar measure on them

Definition 2.1 (p-adic integer)**.** A *p-adic integer* is an infinite sequence $a = (a_1, a_2, a_3, \dots)$ of residues $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ satisfying $a_i \equiv a_j \pmod{p^i}$ for all $i < j$. The set $\mathbb{Z}_p$ of p-adic integers forms a commutative ring under elementwise addition and multiplication over their respective rings $\mathbb{Z}/p^i\mathbb{Z}$. The ring of integers is embedded in $\mathbb{Z}_p$ through the monomorphism

$$n \mapsto (n \bmod p, n \bmod p^2, n \bmod p^3, \dots).$$

We identify the quotient ring $\mathbb{Z}_p/p^k\mathbb{Z}_p$ with $\mathbb{Z}/p^k\mathbb{Z}$ as they are isomorphic.

Definition 2.2 (additive Haar measure on $\mathbb{Z}_p$)**.** Let Σ be the σ-algebra on $\mathbb{Z}_p$ generated by subsets of the form $a + p^k\mathbb{Z}_p$ where k is a positive integer and $a \in \mathbb{Z}_p$. The *additive Haar measure* $\mu\colon \Sigma \to [0, 1]$ is defined by

$$\mu(a + p^k\mathbb{Z}_p) = p^{-k}$$

for all aforementioned subsets $a + p^k\mathbb{Z}_p$.

Remark 2.3. If a is a random p-adic integer selected with respect to additive Haar measure, then its residue $a \bmod p^k$ is uniformly distributed in $\mathbb{Z}/p^k\mathbb{Z}$.

2.2 Principal ideal domains and finitely generated modules over them

Definition 2.4 (principal ideal domain)**.** An *integral domain* is a nontrivial commutative ring in which the product of two nonzero elements is always nonzero. A *principal ideal domain* is an integral domain in which every ideal can be generated by a single element.

Definition 2.5 (torsion)**.** Let M be a module over the ring R. A *torsion element* of M is an element that becomes zero when multiplied by some nonzero element of R. The *torsion submodule* of M is the submodule consisting of the torsion elements of M. The module M is a *torsion module* if it equals its torsion submodule.

The following theorem is known as the invariant factor form of the structure theorem for finitely generated modules over a principal ideal domain.

Theorem 2.6 ([6, pp. 462–463])**.** *Let M be a finitely generated module over a principal ideal domain R. Then, M has a product decomposition*

$$M \simeq R^r \oplus \bigoplus_{i=1}^{m} R/a_iR$$

for some nonnegative integer r and nonzero non-unit elements $a_i \in R$ satisfying

$$a_1 \mid \cdots \mid a_m.$$

This product decomposition is unique up to multiplication of a_i by units. The module M is a torsion module if and only if $r = 0$.

Definition 2.7 (invariant factor of a module)**.** In the product decomposition specified in Theorem 2.6, the *invariant factors* of the module M are the elements a_i with multiplicity. Invariant factors are defined up to multiplication by a unit.

For a finitely generated module G over the principal ideal domain $\mathbb{Z}_p$, we may assume that every invariant factor of G is normalized to a power of p via multiplication by an appropriate unit. We arrive at the following corollary of Theorem 2.6.

Corollary 2.8. *Every finitely generated torsion module G over $\mathbb{Z}_p$ has a unique product decomposition*

$$G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

where e_i and r_i are positive integers such that $e_1 > \cdots > e_s$. Each p^{e_i} is an invariant factor of G with multiplicity r_i.

Remark 2.9. Every finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ can be viewed as a finitely generated torsion module over $\mathbb{Z}_p$ via the identification $\mathbb{Z}/p^k\mathbb{Z} \simeq \mathbb{Z}_p/p^k\mathbb{Z}_p$. Thus, Corollary 2.8 also applies to such modules with $e_1 \leq k$.

2.3 Cokernels and the Smith normal form

Definition 2.10 (cokernel)**.** Let $\mathrm{M}_n(R)$ be the ring of $n \times n$ matrices over a commutative ring R. Each matrix $X \in \mathrm{M}_n(R)$ represents an endomorphism $v \mapsto Xv$ of the module R^n over R. The *image* $\mathrm{im}(X)$ of the matrix X is defined as the image of this endomorphism, and the *cokernel* of the matrix X is defined as the quotient module

$$\mathrm{cok}(X) = R^n / \mathrm{im}(X).$$

Definition 2.11 (invariant factor of a matrix)**.** Suppose that R is a principal ideal domain. The *invariant factors* of a matrix in $\mathrm{M}_n(R)$ are the invariant factors of its cokernel.

We use $\mathrm{diag}(a_1, \ldots, a_n)$ to denote the diagonal matrix or diagonal block matrix with entries $a_1, \ldots, a_n$ on the diagonal.

Theorem 2.12 (Smith normal form)**.** *Suppose that R is a principal ideal domain and $X \in \mathrm{M}_n(R)$ has rank r. For any nonnegative integer $i \leq n$, let d_i be the greatest common divisor of all $i \times i$ minors of X, defined up to multiplication by a unit. In particular, d_0 is a unit. Then, $d_0, \ldots, d_r$ are nonzero and satisfy*

$$d_0 \mid \cdots \mid d_r$$

while $d_{r+1} = \cdots = d_n = 0$.

For any positive integer $i \leq r$, there is an element $\alpha_i \in R$ such that $d_i = \alpha_i d_{i-1}$. Again, α_i is defined up to multiplication by a unit. Then,

$$\alpha_1 \mid \cdots \mid \alpha_r,$$

and there are matrices $S, T \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that

$$SXT = \mathrm{diag}(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0).$$

This diagonal matrix is the Smith normal form *of X.*

Remark 2.13. The nonzero diagonal entries of the Smith normal form of X comprise the invariant factors of X, which uniquely describe $\mathrm{cok}(X)$ up to isomorphism. Thus, $\mathrm{cok}(X)$ carries the same information as the Smith normal form of X.

The p-adic integers form a principal ideal domain. For any matrix $X \in \mathrm{M}_n(\mathbb{Z}_p)$, we may assume that every invariant factor of X is normalized to a power of p via multiplication by an appropriate unit. The same applies to nonzero entries in the Smith normal form of X.

Given a matrix $X \in \mathrm{M}_n(\mathbb{Z}_p)$, the following lemma translates a constraint on the smallest invariant factor of $\mathrm{cok}(X)$ and its multiplicity to an equivalent condition on the expansion of X in terms of powers of p.

Lemma 2.14. *Suppose that the nonzero matrix $X \in \mathrm{M}_n(\mathbb{Z}_p)$ can be expressed as*

$$X = \sum_{i=0}^{k-1} p^i X_i$$

for some positive integer k, where each X_i takes entries in $\{0, 1, \ldots, p-1\}$. For any nonnegative integer $e \leq k$ and positive integer $r \leq n$, the smallest invariant factor of X is p^e with multiplicity r if and only if $X_0 = \cdots = X_{e-1} = 0$ and $\mathrm{rank}(X_e) = r$ over $\mathbb{F}_p$.

Proof. Let $\mathrm{diag}(\alpha_1, \ldots, \alpha_m, 0, \ldots, 0)$ be the Smith normal form of X. The smallest invariant factor of X is p^e with multiplicity r if and only if $\alpha_1 = \ldots = \alpha_r = p^e \neq \alpha_{r+1}$.

Let $d_i(X)$ denote the greatest common divisor of all $i \times i$ minors of X, normalized to a power of p. In particular, $d_0(X) = 1$ and $d_i(X) = 0$ for all $i > n$.

($\Longleftarrow$) Suppose that $X_0 = \cdots = X_{e-1} = 0$ and $\mathrm{rank}(X_e) = r$ over $\mathbb{F}_p$. Then, $X = p^e X'$ where

$$X' = \sum_{i=0}^{k-e-1} p^i X_i$$

has rank r, so $d_i(X') = 1$ for all $0 \leq i \leq r$ while $d_{r+1}(X') \neq 1$. Since

$$d_i(X) = d_i(p^e X') = p^{ei} d_i(X'),$$

we have

$$\alpha_i = \frac{d_i(X)}{d_{i-1}(X)} = p^e \frac{d_i(X')}{d_{i-1}(X')},$$

so $\alpha_1 = \cdots = \alpha_r = p^e \neq \alpha_{r+1}$.

($\Longrightarrow$) Suppose that $\alpha_1 = \cdots = \alpha_r = p^e \neq \alpha_{r+1}$. Then, $d_1(X) = p^e$, so every entry of X is a multiple of p^e. Hence, $X_0 = \ldots = X_{e-1} = 0$, so $X = p^e X'$ where

$$X' = \sum_{i=0}^{k-e-1} p^i X_i.$$

Reasoning analogously to the previous case, we see that $d_r(X) = p^{er}$ and thus $d_r(X') = 1$, whereas $d_{r+1}(X) \neq p^{e(r+1)}$ and thus $d_{r+1}(X') \neq 1$. It follows that $\operatorname{rank}(X') = r$, so $\operatorname{rank}(X_e) = r$ over $\mathbb{F}_p$. □

The following lemma relates the cokernel of a matrix in $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ to the cokernel of its lift in $\mathrm{M}_n(\mathbb{Z}_p)$ under the identification $\mathbb{Z}_p/p^k\mathbb{Z}_p \simeq \mathbb{Z}/p^k\mathbb{Z}$.

Lemma 2.15. *Suppose that $X \in \mathrm{M}_n(\mathbb{Z}_p)$ is a lift of $\bar{X} \in \mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$. Then*

$$\operatorname{cok}(\bar{X}) \simeq \operatorname{cok}(X)/p^k \operatorname{cok}(X).$$

Proof. We have $\operatorname{cok}(X) = \mathbb{Z}_p^n/\operatorname{im}(X)$ and $\operatorname{cok}(\bar{X}) = (\mathbb{Z}/p^k\mathbb{Z})^n/\operatorname{im}(\bar{X})$. Consider the epimorphism $f\colon \operatorname{cok}(X) \to \operatorname{cok}(\bar{X})$ defined by $f([v]) = [v \bmod p^k]$ for all $v \in \mathbb{Z}_p^n$. Since f factors through the projection $\operatorname{cok}(X) \to \operatorname{cok}(X)/p^k \operatorname{cok}(X)$, we obtain the epimorphism

$$\tilde{f}\colon \operatorname{cok}(X)/p^k \operatorname{cok}(X) \to \operatorname{cok}(\bar{X})$$

defined by $\tilde{f}([v]) = [v \bmod p^k]$ for all $v \in \mathbb{Z}_p^n$.

It remains to show that $\tilde{f}$ is a monomorphism. Suppose that $u, v \in \mathbb{Z}_p^n$ and $\tilde{f}(u) = \tilde{f}(v)$. Then, $(u - v) \bmod p^k \in \operatorname{im}(\bar{X})$, so $(u - v) \bmod p^k = \bar{X}\bar{w}$ for some $\bar{w} \in (\mathbb{Z}/p^k\mathbb{Z})^n$. Fixing a lift $w \in \mathbb{Z}_p^n$ of $\bar{w}$, we have

$$u - v \equiv Xw \pmod{p^k},$$

so $[u] = [v]$ in $\operatorname{cok}(X)/p^k \operatorname{cok}(X)$.

Therefore, $\tilde{f}$ is an isomorphism. □

We can extend Lemma 2.14 to matrices in $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ using Lemma 2.15.

Corollary 2.16. *Suppose that the matrix $X \in \mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ can be expressed as*

$$X = \sum_{i=0}^{k-1} p^i X_i$$

for some positive integer k, where each X_i takes entries in $\{0, 1, \ldots, p-1\}$. For any nonnegative integer $e \leq k$ and positive integer $r \leq n$, the smallest invariant factor of X is p^e with multiplicity r if and only if $X_0 = \cdots = X_{e-1} = 0$ and $\operatorname{rank}(X_e) = r$ over $\mathbb{F}_p$.

2.4 Congruence

Definition 2.17 (congruence)**.** Suppose that A and B are $n \times n$ matrices over a commutative ring R. The matrices A and B are *congruent* if $B = QAQ^\top$ for some matrix $Q \in \mathrm{GL}_n(R)$.

Remark 2.18. Matrix congruence is an equivalence relation on $\mathrm{M}_n(R)$. Given $Q \in \mathrm{GL}_n(R)$, the map $X \mapsto QXQ^\top$ is an automorphism of $\mathrm{M}_n(R)$ that preserves symmetry.

The following corollary of Lemma 7 on [1, p. 391] shows that every symmetric matrix over a field is congruent to a relatively simple matrix.

Lemma 2.19 ([1, p. 391])**.** *Any symmetric matrix over a field* $\mathbb{F}$ *is congruent to some matrix of the form*

$$\mathrm{diag}(0, A)$$

where 0 *is a zero matrix and* A *is an invertible symmetric matrix over* $\mathbb{F}$*.*

2.5 Partitions

Definition 2.20 (partition)**.** A *partition*

$$\lambda = (\lambda_1, \dots, \lambda_r)$$

is a finite sequence of positive integers $\lambda_1 \geq \cdots \geq \lambda_r$. We define

$$|\lambda| = \sum_{i=1}^{r} \lambda_i \qquad \text{and} \qquad n(\lambda) = \sum_{i=1}^{r} (i-1)\lambda_i.$$

Definition 2.21 (type of a finitely generated torsion module over $\mathbb{Z}_p$)**.** Suppose that G is a finitely generated torsion module over $\mathbb{Z}_p$ with the product decomposition

$$G = \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

as specified in Corollary 2.8. The *type* of G is the partition

$$(\underbrace{e_1, \dots, e_1}_{r_1 \text{ copies of } e_1}, \dots, \underbrace{e_s, \dots, e_s}_{r_s \text{ copies of } e_s}).$$

2.6 Useful enumerations

In this section, we review some enumerations used in the proof of Theorem 1.6. We start with a well-known formula for the number of $n \times n$ matrices over a finite field with a given rank.

Lemma 2.22 ([11, p. 6]). *Let $\mathbb{F}_q$ be a finite field and r be an integer such that $0 \le r \le n$. Then*

$$\#\{X \in \mathrm{M}_n(\mathbb{F}_q) : \mathrm{rank}(X) = r\} = \prod_{i=0}^{r-1} \frac{(q^n - q^i)^2}{q^r - q^i} = q^{r(2n-r)} \frac{\phi_n(q)^2}{\phi_r(q)\phi_{n-r}(q)^2}.$$

In particular, setting $r = n$ gives

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i) = q^{n^2}\phi_n(q).$$

The following formula is the analogue of Lemma 2.22 for symmetric matrices.

Lemma 2.23 ([10, pp. 154–155]). *Let $\mathbb{F}_q$ be a finite field and r be an integer such that $0 \le r \le n$. Then*

$$\begin{aligned}\#\{X \in \mathrm{Sym}_n(\mathbb{F}_q) : \mathrm{rank}(X) = r\} &= \prod_{i=1}^{\lfloor r/2 \rfloor} \frac{q^{2i}}{q^{2i} - 1} \prod_{i=0}^{r-1}(q^{n-i} - 1) \\ &= q^{r(2n-r+1)/2} \frac{\phi_n(q)}{\phi_{n-r}(q)\psi_r(q)}.\end{aligned}$$

The following formula calculates $|\mathrm{Aut}(G)|$ in terms of the product decomposition of a finitely generated module G over $\mathbb{Z}/p^k\mathbb{Z}$.

Lemma 2.24 ([7, p. 236]). *Suppose that G is a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ with the product decomposition*

$$G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

as specified in Corollary 2.8. Then

$$\begin{aligned}|\mathrm{Aut}(G)| &= \prod_{i=1}^{s} q^{-r_i^2} |\mathrm{GL}_{r_i}(\mathbb{F}_q)| \prod_{i=1}^{s}\prod_{j=1}^{s} q^{\min(e_i,e_j)r_ir_j} \\ &= \prod_{i=1}^{s} \phi_{r_i}(q) \prod_{i=1}^{s}\prod_{j=1}^{s} q^{\min(e_i,e_j)r_ir_j}.\end{aligned}$$

3 Proof of Theorem 1.6

A major step toward proving Theorem 1.6 is to consider the special case where $n = r = \dim_{\mathbb{F}_p}(G/pG)$. Let $X \in \mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ and let $\bar{X} \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ satisfy $X \equiv \bar{X} \pmod{p}$. Suppose $\mathrm{cok}(X) \simeq G$. Since $\dim_{\mathbb{F}_p}(G/pG) = n - \mathrm{rank}(\bar{X})$, we see that $n = \dim_{\mathbb{F}_p}(G/pG)$ if and only if $\bar{X}$ is the zero matrix.

Lemma 3.1. *Suppose that G is a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ with the product decomposition*

$$G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

as specified in Corollary 2.8. Then,

$$\begin{aligned}&\#\{X \in \mathrm{Sym}_r(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X) \simeq G\}\\ &= \sqrt{\frac{p^{kr(r+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_r(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)},\end{aligned}$$

where

$$r = \dim_{\mathbb{F}_p}(G/pG) = \sum_{i=1}^{s} r_i$$

and

$$u = \dim_{\mathbb{F}_p}(p^{k-1}G) = \begin{cases} r_1 & \text{if } e_1 = k, \\ 0 & \text{if } e_1 < k. \end{cases}$$

Proof. We use induction on s. We consider two base cases.

The first base case is when G is trivial, so $r = s = u = 0$ and $|G| = |\mathrm{Aut}(G)| = 1$. We have

$$\begin{aligned}&\#\{X \in \mathrm{Sym}_r(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X) \simeq G\}\\ &= \sqrt{\frac{p^{kr(r+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_r(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)} = 1\end{aligned}$$

in this case.

The second base case is when $G \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$, so $s = 1$, $e_1 = k$, and $u = r$. For any $X \in \mathrm{Sym}_r(\mathbb{Z}/p^k\mathbb{Z})$, we have $\mathrm{cok}(X) \simeq G$ if and only if $X = 0$, so

$$\#\{X \in \mathrm{Sym}_r(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X) \simeq G\} = 1.$$

On the other hand,

$$\begin{aligned}&\sqrt{\frac{p^{kr(r+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_r(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}\\ &= \sqrt{\frac{p^{kr(r+1)}}{p^{kr+kr^2}\phi_r(p)}} \frac{\phi_r(p)\psi_r(p)}{\phi_r(p)} \frac{\sqrt{\phi_r(p)}}{\psi_r(p)} = 1\end{aligned}$$

by Lemmas 2.22 and 2.24, concluding the proof for this case.

Now, we provide a proof of the inductive step. Suppose that the result holds for $G \simeq \bigoplus_{i=1}^{s}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$ and consider the finitely generated module

$$G' \simeq G \oplus (\mathbb{Z}/p^{e_{s+1}}\mathbb{Z})^{r_{s+1}} = \bigoplus_{i=1}^{s+1} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

over $\mathbb{Z}/p^k\mathbb{Z}$, where e_i and r_i are positive integers such that $k \geq e_1 > \cdots > e_{s+1}$. Let $r = \dim_{\mathbb{F}_p}(G/pG) = \sum_{i=1}^{s} r_i$ and $r' = \dim_{\mathbb{F}_p}(G'/pG') = r + r_{s+1}$. Our choice of base cases allow us to assume that $e_{s+1} < k$, so we may write $u = \dim_{\mathbb{F}_p}(p^{k-1}G) = \dim_{\mathbb{F}_p}(p^{k-1}G')$. We would like to show that

$$\begin{aligned}&\#\{X' \in \mathrm{Sym}_{r'}(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X') \simeq G'\} \\ &= \sqrt{\frac{p^{kr'(r'+1)}}{|G'||\mathrm{Aut}(G')|}} \frac{\phi_{r'}(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s+1} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}.\end{aligned}$$

To this end, consider an arbitrary matrix $X' \in \mathrm{Sym}_{r'}(\mathbb{Z}/p^k\mathbb{Z})$ satisfying $\mathrm{cok}(X') \simeq G'$. It follows from Corollary 2.16 that $X' = p^{e_{s+1}}X_0 + p^{e_{s+1}+1}X_1$ for some symmetric X_0 taking entries in $\{0, 1, \ldots, p-1\}$ and symmetric X_1 taking entries in $\{0, 1, \ldots, p^{k-e_{s+1}-1} - 1\}$ such that $\mathrm{rank}(X_0) = r_{s+1}$ over $\mathbb{F}_p$. There are

$$p^{r_{s+1}(2r'-r_{s+1}+1)/2} \frac{\phi_{r'}(p)}{\phi_r(p)\psi_{r_{s+1}}(p)} = p^{r_{s+1}(2r+r_{s+1}+1)/2} \frac{\phi_{r'}(p)}{\phi_r(p)\psi_{r_{s+1}}(p)}$$

choices for X_0 by Lemma 2.23.

Fix some choice of X_0. It follows from Lemma 2.19 that there is some $\bar{Q} \in \mathrm{GL}_{r'}(\mathbb{F}_p)$ such that

$$\bar{Q}X_0\bar{Q}^\top = \mathrm{diag}(0, \Sigma)$$

where $\Sigma \in \mathrm{Sym}_{r_{s+1}}(\mathbb{F}_p)$ is invertible. Pick an arbitrary lift $Q \in \mathrm{GL}_{r'}(\mathbb{Z}/p^k\mathbb{Z})$ of $\bar{Q}$. The map $X' \mapsto QX'Q^\top$ is an automorphism on $\mathrm{Sym}_{r'}(\mathbb{Z}/p^k\mathbb{Z})$, and $\mathrm{cok}(X') \simeq \mathrm{cok}(QX'Q^\top)$. Hence, we may assume $X_0 = \mathrm{diag}(0, \Sigma)$ without loss of generality.

Write

$$X_1 = \begin{bmatrix} A & B \\ B^\top & C \end{bmatrix}$$

where A, B, and C are $r \times r$, $r \times r_{s+1}$, and $r_{s+1} \times r_{s+1}$ matrices respectively, all taking entries in $\{0, 1, \ldots, p^{k-e_{s+1}-1} - 1\}$. Note that A and C are symmetric. Leaving A unchosen, there are $p^{(k-e_{s+1}-1)rr_{s+1}}$ choices for B and $p^{(k-e_{s+1}-1)r_{s+1}(r_{s+1}+1)/2}$ choices for C.

Fix some choice of B and some choice of C. It is straightforward to verify that

$$PX'P^\top = \begin{bmatrix} p^{e_{s+1}+1}(A - pB(\Sigma + pC)^{-1}B^\top) & 0 \\ 0 & p^{e_{s+1}}(\Sigma + pC) \end{bmatrix}$$

where

$$P = \begin{bmatrix} I_r & -pB(\Sigma + pC)^{-1} \\ 0 & I_{r_{s+1}} \end{bmatrix} \in \mathrm{GL}_{r'}(\mathbb{Z}/p^k\mathbb{Z})$$

and I_m denotes the $m \times m$ identity matrix. Corollary 2.16 shows that the $r_{s+1} \times r_{s+1}$ matrix $p^{e_{s+1}}(\Sigma + pC)$ has an invariant factor $p^{e_{s+1}}$ with multiplicity r_{s+1}, so

$$\mathrm{cok}(p^{e_{s+1}}(\Sigma + pC)) \simeq (\mathbb{Z}/p^{e_{s+1}}\mathbb{Z})^{r_{s+1}}.$$

Since

$$\begin{aligned}\operatorname{cok}(X') &\simeq \operatorname{cok}(PX'P^\top)\\ &\simeq \operatorname{cok}(p^{e_{s+1}+1}(A - pB(\Sigma + pC)^{-1}B^\top)) \oplus \operatorname{cok}(p^{e_{s+1}}(\Sigma + pC))\\ &\simeq \operatorname{cok}(p^{e_{s+1}+1}(A - pB(\Sigma + pC)^{-1}B^\top)) \oplus (\mathbb{Z}/p^{e_{s+1}}\mathbb{Z})^{r_{s+1}},\end{aligned}$$

it remains to count the number of choices for A such that

$$\operatorname{cok}(p^{e_{s+1}+1}(A - pB(\Sigma + pC)^{-1}B^\top)) \simeq G.$$

The inductive hypothesis shows that

$$\begin{aligned}&\#\{X \in \operatorname{Sym}_r(\mathbb{Z}/p^k\mathbb{Z}) : \operatorname{cok}(X) \simeq G\}\\ &= \sqrt{\frac{p^{kr(r+1)}}{|G||\operatorname{Aut}(G)|}}\frac{\phi_r(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}.\end{aligned}$$

Corollary 2.16 shows that any such X satisfies $X \equiv 0 \pmod{p^{e_s}}$. Since $e_s \geq e_{s+1} + 1$, there is a unique A such that

$$X = p^{e_{s+1}+1}(A - pB(\Sigma + pC)^{-1}B^\top).$$

The choice of A concludes the determination of X'.

Multiplying the quantities involved in this process, we have

$$\begin{aligned}&\#\{X' \in \operatorname{Sym}_{r'}(\mathbb{Z}/p^k\mathbb{Z}) : \operatorname{cok}(X') \simeq G'\}\\ &= p^{r_{s+1}(2r+r_{s+1}+1)/2}\frac{\phi_{r'}(p)}{\psi_{r_{s+1}}(p)\phi_r(p)}p^{(k-e_{s+1}-1)r_{s+1}(2r+r_{s+1}+1)/2}\\ &\quad\cdot\sqrt{\frac{p^{kr(r+1)}}{|G||\operatorname{Aut}(G)|}}\frac{\phi_r(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}\\ &= \sqrt{\frac{p^{kr(r+1)+(k-e_{s+1})r_{s+1}(2r+r_{s+1}+1)}}{\phi_{r_{s+1}}(p)|G||\operatorname{Aut}(G)|}}\frac{\phi_{r'}(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s+1}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}\\ &= \sqrt{\frac{p^{kr'(r'+1)-e_{s+1}r_{s+1}(2r+r_{s+1}+1)}}{\phi_{r_{s+1}}(p)|G||\operatorname{Aut}(G)|}}\frac{\phi_{r'}(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s+1}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}.\end{aligned}$$

Note that

$$\frac{|G'|}{|G|} = p^{e_{s+1}r_{s+1}}$$

and

$$\frac{|\operatorname{Aut}(G')|}{|\operatorname{Aut}(G)|} = p^{e_{s+1}r_{s+1}(2r+r_{s+1})}\phi_{r_{s+1}}(p)$$

by Lemmas 2.22 and 2.24. Therefore,

$$\begin{aligned}&\#\{X' \in \operatorname{Sym}_{r'}(\mathbb{Z}/p^k\mathbb{Z}) : \operatorname{cok}(X') \simeq G'\}\\ &= \sqrt{\frac{p^{kr'(r'+1)}}{|G'||\operatorname{Aut}(G')|}}\frac{\phi_{r'}(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s+1}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}.\end{aligned}$$

This concludes the induction. □

Now, we are ready to prove Theorem 1.6 in the general case.

Proof of Theorem 1.6. As in the proof of Lemma 3.1, we may assume $\bar{X} = \mathrm{diag}(0, \Sigma)$ without loss of generality.

Write

$$X = \begin{bmatrix} A & B \\ B^\top & C \end{bmatrix}$$

where A, B, and C are $r \times r$, $r \times (n-r)$, and $(n-r) \times (n-r)$ matrices respectively, all taking entries in $\{0, 1, \ldots, p^{k-1}-1\}$. Note that A and C are symmetric. Leaving A unchosen, there are $p^{(k-1)r(n-r)}$ choices for B and $p^{(k-1)(n-r)(n-r+1)/2}$ choices for C.

Fix some choice of B and some choice of C. It is straightforward to verify that

$$PXP^\top = \begin{bmatrix} A - pB(\Sigma + pC)^{-1}B^\top & 0 \\ 0 & \Sigma + pC \end{bmatrix}$$

where

$$P = \begin{bmatrix} I_r & -pB(\Sigma + pC)^{-1} \\ 0 & I_{n-r} \end{bmatrix} \in \mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})$$

and I_m denotes the $m \times m$ identity matrix. Since $\Sigma + pC$ is invertible, we have

$$\begin{aligned} \mathrm{cok}(X) &\simeq \mathrm{cok}(PXP^\top) \\ &\simeq \mathrm{cok}(A - pB(\Sigma + pC)^{-1}B^\top) \oplus \mathrm{cok}(\Sigma + pC) \\ &\simeq \mathrm{cok}(A - pB(\Sigma + pC)^{-1}B^\top), \end{aligned}$$

so it remains to count the number of choices for A such that $\mathrm{cok}(A - pB(\Sigma + pC)^{-1}B^\top) \simeq G$.

Lemma 3.1 shows that

$$\begin{aligned} &\#\{A' \in \mathrm{Sym}_r(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(A) \simeq G\} \\ &= \sqrt{\frac{p^{kr(r+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_r(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}. \end{aligned}$$

For any such A', there is a unique A such that

$$A' = A - pB(\Sigma + pC)^{-1}B^\top.$$

The choice of A concludes the determination of X.

Multiplying the quantities involved in this process, we have

$$\begin{aligned}
&\#\left\{\begin{matrix} X \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z}) : \\ \mathrm{cok}(X) \simeq G \\ \text{and } X \equiv \bar{X} \pmod{p} \end{matrix}\right\} \\
&= p^{(k-1)(n-r)(n+r+1)/2}\sqrt{\frac{p^{kr(r+1)}}{|G||\mathrm{Aut}(G)|}}\,\frac{\phi_r(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)} \\
&= \sqrt{\frac{p^{kr(r+1)+(k-1)(n-r)(n+r+1)}}{|G||\mathrm{Aut}(G)|}}\,\frac{\phi_r(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)} \\
&= \sqrt{\frac{p^{(k-1)n(n+1)+r(r+1)}}{|G||\mathrm{Aut}(G)|}}\,\frac{\phi_r(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}.
\end{aligned}$$

□

4 Theorem 1.6 implies Theorem 1.5

In order to count the total number of matrices $X \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})$ such that $\mathrm{cok}(X) \simeq G$, we multiply the result of Theorem 1.6 by the number of residue $\bar{X} \in \mathrm{Sym}_n(\mathbb{Z}/p\mathbb{Z})$ satisfying $\bar{X} \simeq G/pG$.

Lemma 4.1. *Suppose that G is a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ with the product decomposition*

$$G \simeq \bigoplus_{i=1}^{s}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$$

as specified in Corollary 2.8. Then

$$\begin{aligned}
&\#\{X \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X) \simeq G\} \\
&= \sqrt{\frac{p^{kn(n+1)}}{|G||\mathrm{Aut}(G)|}}\,\frac{\phi_n(p)\psi_u(p)}{\phi_u(p)\psi_{n-r}(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)},
\end{aligned}$$

where

$$r = \dim_{\mathbb{F}_p}(G/pG) = \sum_{i=1}^{s} r_i$$

and

$$u = \dim_{\mathbb{F}_p}(p^{k-1}G) = \begin{cases} r_1 & \text{if } e_1 = k, \\ 0 & \text{if } e_1 < k. \end{cases}$$

Proof. For any residue $\bar{X} \in \mathrm{Sym}_n(\mathbb{Z}/p\mathbb{Z})$, the condition $\mathrm{cok}(\bar{X}) \simeq G/pG$ is equivalent to $\mathrm{rank}(\bar{X}) = n - r$. Hence,

$$\#\{\bar{X} \in \mathrm{Sym}_n(\mathbb{Z}/p\mathbb{Z}) : \mathrm{cok}(\bar{X}) \simeq G/pG\} = p^{(n-r)(n+r+1)/2}\frac{\phi_n(p)}{\phi_r(p)\psi_{n-r}(p)}$$

by Lemma 2.23. Multiplying this count by the result of Theorem 1.6, we see that

$$\begin{aligned}
&\#\{X \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X) \simeq G\} \\
&= p^{(n-r)(n+r+1)/2} \sqrt{\frac{p^{(k-1)n(n+1)+r(r+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_n(p)\psi_u(p)}{\phi_u(p)\psi_{n-r}(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)} \\
&= \sqrt{\frac{p^{kn(n+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_n(p)\psi_u(p)}{\phi_u(p)\psi_{n-r}(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}. \qquad \square
\end{aligned}$$

Now we apply Lemma 4.1 to prove Theorem 1.5. We emphasize that this argument is different than the one appearing in [5].

Proof of Theorem 1.5. Pick any $k > e_1$, so $p^k G = 0$. For a random matrix X selected from $\mathrm{Sym}_n(\mathbb{Z}_p)$ with respect to additive Haar measure, its residue X' modulo p^k is uniformly distributed in $\mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})$, and $\mathrm{cok}(X) \simeq G$ if and only if $\mathrm{cok}(X') \simeq G$. Therefore, we see that

$$\begin{aligned}
P_n^{\mathrm{Sym}}(\lambda) &= \frac{\#\{X' \in \mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{cok}(X') \simeq G\}}{|\mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})|} \\
&= p^{-kn(n+1)/2} \sqrt{\frac{p^{kn(n+1)}}{|G||\mathrm{Aut}(G)|}} \frac{\phi_n(p)\psi_u(p)}{\phi_u(p)\psi_{n-r}(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)} \\
&= \frac{1}{\sqrt{|G||\mathrm{Aut}(G)|}} \frac{\phi_n(p)}{\psi_{n-r}(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}
\end{aligned}$$

by Lemma 4.1 (note that $u = 0$). Since

$$|G| = \prod_{i=1}^{s} p^{e_i r_i} = p^{|\lambda|}$$

and

$$\begin{aligned}
|\mathrm{Aut}(G)| &= \prod_{i=1}^{s} \phi_{r_i}(p) \prod_{i=1}^{s} \prod_{j=1}^{s} p^{\min(e_i, e_j) r_i r_j} \\
&= \prod_{i=1}^{s} \phi_{r_i}(p) \prod_{i=1}^{r} \prod_{j=1}^{r} p^{\min(\lambda_i, \lambda_j)} \\
&= \prod_{i=1}^{s} \phi_{r_i}(p) \prod_{i=1}^{r} p^{\lambda_i (2i-1)} \\
&= p^{2n(\lambda)+|\lambda|} \prod_{i=1}^{s} \phi_{r_i}(p)
\end{aligned}$$

by Lemma 2.24, we have

$$P_n^{\mathrm{Sym}}(\lambda) = p^{-n(\lambda)-|\lambda|} \frac{\phi_n(p)}{\psi_{n-r}(p)} \prod_{i=1}^{s} \frac{1}{\psi_{r_i}(p)}. \qquad \square$$

Acknowledgments

We sincerely thank our mentors Prof. Gilyoung Cheong and Prof. Nathan Kaplan for guiding us through our research process and always providing timely feedback. We are grateful to the organizers of MIT PRIMES for bringing us together and providing us with a wonderful research opportunity.

References

[1] A. A. Albert. "Symmetric and Alternate Matrices in An Arbitrary Field, I." In: *Transactions of the American Mathematical Society* 43.3 (1938), pp. 386–436. ISSN: 00029947. URL: https://www.jstor.org/stable/1990068 (visited on 07/27/2023).

[2] M. Bhargava et al. "Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves." In: *Cambridge Journal of Mathematics* 3.3 (2015), pp. 275–321. DOI: 10.4310/cjm.2015.v3.n3.a1. URL: https://doi.org/10.4310/cjm.2015.v3.n3.a1.

[3] G. Cheong and Y. Huang. "Cohen–Lenstra distributions via random matrices over complete discrete valuation rings with finite residue fields." In: *Illinois Journal of Mathematics* 65.2 (2021), pp. 385–415. DOI: 10.1215/00192082-8939615. URL: https://doi.org/10.1215/00192082-8939615.

[4] G. Cheong, Y. Liang, and M. Strand. *Polynomial equations for matrices over integers modulo a prime power and the cokernel of a random matrix.* To be published in *Linear Algebra and its Applications.* 2023. DOI: https://doi.org/10.1016/j.laa.2023.07.031. URL: https://www.sciencedirect.com/science/article/pii/S0024379523002975.

[5] J. Clancy et al. "On a Cohen–Lenstra heuristic for Jacobians of random graphs." In: *Journal of Algebraic Combinatorics* 42.3 (May 2015), pp. 701–723. DOI: 10.1007/s10801-015-0598-x. URL: https://doi.org/10.1007/s10801-015-0598-x.

[6] D. S. Dummit and R. M. Foote. *Abstract Algebra.* 3rd ed. John Wiley and Sons, 2004.

[7] E. Friedman and L. C. Washington. "On the distribution of divisor class groups of curves over a finite field." In: *Proceedings of the International Number Theory Conference held at Université Laval, July 5-18, 1987.* Ed. by J. M. de Koninck and C. Levesque. Berlin, New York: De Gruyter, 1989, pp. 227–239. ISBN: 9783110852790. DOI: doi:10.1515/9783110852790.227. URL: https://doi.org/10.1515/9783110852790.227.

[8] J. Fulman and N. Kaplan. "Random Partitions and Cohen–Lenstra Heuristics." In: *Annals of Combinatorics* 23.2 (2019), pp. 295–315. DOI: 10.1007/s00026-019-00425-y. URL: https://doi.org/10.1007/s00026-019-00425-y.

[9] J. Lee. *Universality of the cokernels of random p-adic Hermitian matrices.* 2023. DOI: https://doi.org/10.48550/arXiv.2205.09368. arXiv: 2205.09368.

[10] J. MacWilliams. “Orthogonal Matrices Over Finite Fields.” In: *The American Mathematical Monthly* 76.2 (1969), pp. 152–164. ISSN: 00029890, 19300972. URL: https://www.jstor.org/stable/2317262 (visited on 05/27/2023).

[11] K. E. Morrison. “Integer Sequences and Matrices Over Finite Fields.” In: *Journal of Integer Sequences* 9.2 (2006), pp. 1–25.

[12] R. P. Stanley. “Smith normal form in combinatorics.” In: *Journal of Combinatorial Theory, Series A* 144 (2016). Fifty Years of the Journal of Combinatorial Theory, pp. 476–495. ISSN: 0097-3165. DOI: https://doi.org/10.1016/j.jcta.2016.06.013. URL: https://www.sciencedirect.com/science/article/pii/S0097316516300474.

[13] M. M. Wood. “The distribution of sandpile groups of random graphs.” In: *Journal of the American Mathematical Society* 30.4 (2017), pp. 915–958. DOI: 10.1090/jams/866. URL: https://doi.org/10.1090/jams/866.

[14] E. Yan. *Universality for Cokernels of Dedekind Domain Valued Random Matrices.* 2023. DOI: https://doi.org/10.48550/arXiv.2301.09196. arXiv: 2301.09196.

Commitments on Academic Honesty and Integrity

We hereby declare that we

1. are fully committed to the principle of honesty, integrity and fair play throughout the competition.
2. actually perform the research work ourselves and thus truly understand the content of the work.
3. observe the common standard of academic integrity adopted by most journals and degree theses.
4. have declared all the assistance and contribution we have received from any personnel, agency, institution, etc. for the research work.
5. undertake to avoid getting in touch with assessment panel members in a way that may lead to direct or indirect conflict of interest.
6. undertake to avoid any interaction with assessment panel members that would undermine the neutrality of the panel member and fairness of the assessment process.
7. observe the safety regulations of the laboratory(ies) where we conduct the experiment(s), if applicable.
8. observe all rules and regulations of the competition.
9. agree that the decision of YHSA is final in all matters related to the competition.

We understand and agree that failure to honour the above commitments may lead to disqualification from the competition and/or removal of reward, if applicable; that any unethical deeds, if found, will be disclosed to the school principal of team member(s) and relevant parties if deemed necessary; and that the decision of YHSA is final and no appeal will be accepted.

(Signatures of full team below)

X Rohan Das

Name of team member: Rohan Das

X Christopher Qiu

Name of team member: Christopher Qiu

X Shiqiao Zhang

Name of team member: Shiqiao Zhang

X

Name of supervising teacher: Gilyoung Cheong

X

Name of supervising teacher: Nathan Kaplan