The Distribution of the Cokernel of a Random Integral Symmetric Matrix Modulo a Prime Power

Rohan Das Christopher Qiu Shiqiao Zhang

Mentors: Gilyoung Cheong Nathan Kaplan

MIT PRIMES October Conference

October 14, 2023

Rings

Definition

A ring is a set R with binary operations $+$ and $\cdot$ such that:

- $(R, +)$ is an abelian group (so addition is commutative, associative, has an identity, and all elements have additive inverses).
- Multiplication is associative and has an identity.
- Multiplication is distributive with respect to addition, namely $(a+b)\cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Rings

Definition

A ring is a set R with binary operations $+$ and $\cdot$ such that:

- $(R, +)$ is an abelian group (so addition is commutative, associative, has an identity, and all elements have additive inverses).
- Multiplication is associative and has an identity.
- Multiplication is distributive with respect to addition, namely $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

R is a commutative ring if multiplication is commutative.

Rings

Definition

A ring is a set R with binary operations $+$ and $\cdot$ such that:

- $(R, +)$ is an abelian group (so addition is commutative, associative, has an identity, and all elements have additive inverses).
- Multiplication is associative and has an identity.
- Multiplication is distributive with respect to addition, namely $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

R is a commutative ring if multiplication is commutative.

Examples

Commutative rings we frequently work with include $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, and $\mathbb{Z}_p$.

Modules

Definition

A module over a commutative ring R is an abelian group $(M, +)$ along with an operation $(\cdot)\colon R \times M \to M$ such that for all $r, s \in R$ and $m, n \in M$,

- $(r + s) \cdot m = r \cdot m + s \cdot m$,
- $r \cdot (m + n) = r \cdot m + r \cdot n$,
- $(rs) \cdot m = r \cdot (s \cdot m)$,
- $1 \cdot m = m$.

Modules

Definition

A module over a commutative ring R is an abelian group $(M, +)$ along with an operation $(\cdot)\colon R \times M \to M$ such that for all $r, s \in R$ and $m, n \in M$,

- $(r + s) \cdot m = r \cdot m + s \cdot m$,
- $r \cdot (m + n) = r \cdot m + r \cdot n$,
- $(rs) \cdot m = r \cdot (s \cdot m)$,
- $1 \cdot m = m$.

Modules generalize vector spaces from fields to arbitrary rings.

Modules

Definition

A module over a commutative ring R is an abelian group $(M, +)$ along with an operation $(\cdot)\colon R \times M \to M$ such that for all $r, s \in R$ and $m, n \in M$,

- $(r + s) \cdot m = r \cdot m + s \cdot m$,
- $r \cdot (m + n) = r \cdot m + r \cdot n$,
- $(rs) \cdot m = r \cdot (s \cdot m)$,
- $1 \cdot m = m$.

Modules generalize vector spaces from fields to arbitrary rings.

Examples

Modules over $\mathbb{Z}$ include $\mathbb{Z}^3$, $(\mathbb{Z}/9\mathbb{Z})^2$, and $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

The image and cokernel of a matrix

Definition

Let M be an $n \times n$ matrix over a commutative ring R. The image of M is the R-module

$$\operatorname{im} M = \{Mv : v \in R^n\}.$$

The image and cokernel of a matrix

Definition

Let M be an $n \times n$ matrix over a commutative ring R. The image of M is the R-module

$$\operatorname{im} M = \{Mv : v \in R^n\}.$$

The cokernel of M is the quotient module

$$\operatorname{cok} M = R^n / \operatorname{im} M.$$

The image and cokernel of a matrix

Example

The matrix

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$$

over the commutative ring $\mathbb{Z}/9\mathbb{Z}$ has image

$$\operatorname{im} M \simeq \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

and cokernel

$$\operatorname{cok} M \simeq \mathbb{Z}/3\mathbb{Z}.$$

Principal ideal domains (PID)

Definition

An ideal of a ring $(R, +, \cdot)$ is a subset $I \subseteq R$ that is closed under addition and under multiplication by elements of R.

Principal ideal domains (PID)

Definition

An ideal of a ring $(R, +, \cdot)$ is a subset $I \subseteq R$ that is closed under addition and under multiplication by elements of R.

Example

Ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some integer n.

Principal ideal domains (PID)

Definition

An ideal of a ring $(R, +, \cdot)$ is a subset $I \subseteq R$ that is closed under addition and under multiplication by elements of R.

Example

Ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some integer n.

Definition

An integral domain is a nontrivial commutative ring R in which $ab \neq 0$ for any nonzero $a, b \in R$. A principal ideal domain (PID) is an integral domain in which every ideal can be generated by an element.

Principal ideal domains (PID)

Definition

An ideal of a ring $(R, +, \cdot)$ is a subset $I \subseteq R$ that is closed under addition and under multiplication by elements of R.

Example

Ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some integer n.

Definition

An integral domain is a nontrivial commutative ring R in which $ab \neq 0$ for any nonzero $a, b \in R$. A principal ideal domain (PID) is an integral domain in which every ideal can be generated by an element.

Examples

$\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ are PIDs. $\mathbb{Z}/p^2\mathbb{Z}$ is not a PID because it is not an integral domain.

Finitely generated modules over a PID

Theorem (structural theorem)

If M is a finitely generated module over a PID R, then there exist a unique nonnegative integer r and nonzero non-unit elements $a_1, \dots, a_n \in R$ such that $a_1 \mid \cdots \mid a_n$ and

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

The elements $a_1, \dots, a_n$ are unique up to multiplication by a constant. They are called the invariant factors of M.

p-adic integers

Definition

Let p be a prime. 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

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

p-adic integers

Definition

Let p be a prime. 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.

Torsion modules

Definition

A module M is a torsion module if for all $m \in M$, there exists a nonzero element $r \in R$ such that $r \cdot m = 0$.

Torsion modules

Definition

A module M is a torsion module if for all $m \in M$, there exists a nonzero element $r \in R$ such that $r \cdot m = 0$.

In particular, if M is finitely generated and R is a PID, the exponent r of R in the product decomposition of M is zero.

Torsion modules

Definition

A module M is a torsion module if for all $m \in M$, there exists a nonzero element $r \in R$ such that $r \cdot m = 0$.

In particular, if M is finitely generated and R is a PID, the exponent r of R in the product decomposition of M is zero.

Examples

The module $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Z}$ is a torsion module. The module $\mathbb{Z}^3$ over $\mathbb{Z}$ is not a torsion module.

Finitely generated torsion modules over $\mathbb{Z}_p$

Theorem (structural theorem)

Every finitely generated torsion module M over $\mathbb{Z}_p$ admits a product decomposition

$$M \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z},$$

for some and positive integers $e_1 \geq \cdots \geq e_n$.

Finitely generated torsion modules over $\mathbb{Z}_p$

Theorem (structural theorem)

Every finitely generated torsion module M over $\mathbb{Z}_p$ admits a product decomposition

$$M \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z},$$

for some and positive integers $e_1 \geq \cdots \geq e_n$.

A finitely generated module M over $\mathbb{Z}/p^k\mathbb{Z} \simeq \mathbb{Z}_p/p^k\mathbb{Z}_p$ can be viewed as a finitely generated torsion module over $\mathbb{Z}_p$ whose product decomposition satisfies $e_1 \leq k$.

Partitions

Definition

A partition

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

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

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

Partitions

Definition

A partition

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

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

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

We define the type of a finitely generated torsion module

$$M \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}$$

over $\mathbb{Z}_p$ to be the partition $(e_1, \dots, e_n)$, where $e_1 \geq \cdots \geq e_n$.

Additive Haar measure on $\mathbb{Z}_p$

Definition

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 $a + p^k\mathbb{Z}_p$.

Additive Haar measure on $\mathbb{Z}_p$

Definition

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 $a + p^k\mathbb{Z}_p$.

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 $\mathbb{Z}/p^k\mathbb{Z}$.

Notation

From now on, we use

- $\mathrm{M}_n(R)$ to denote the ring of $n \times n$ matrices over the commutative ring R;
- $\mathrm{Sym}_n(R)$ to denote the ring of $n \times n$ symmetric matrices over the commutative ring R; and
- $\mathrm{Alt}_n(R)$ to denote the ring of $n \times n$ alternate matrices over the commutative ring R.

Notation

From now on, we use

- $\mathrm{M}_n(R)$ to denote the ring of $n \times n$ matrices over the commutative ring R;
- $\mathrm{Sym}_n(R)$ to denote the ring of $n \times n$ symmetric matrices over the commutative ring R; and
- $\mathrm{Alt}_n(R)$ to denote the ring of $n \times n$ alternate matrices over the commutative ring R.

For any nonnegative integer m and positive integer q, we write

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

Cokernel distribution of matrices over $\mathbb{Z}_p$

In 1989, Friedman and Washington studied the distribution of the cokernel of a random matrix selected from $\mathrm{M}_n(\mathbb{Z}_p)$.

Theorem (Friedman–Washington, 1989)

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

Cokernel distribution of matrices over $\mathbb{Z}/p^k\mathbb{Z}$

Friedman and Washington also fixed some matrix $\bar{X} \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ and counted the matrices in $\mathrm{M}_n(\mathbb{Z}/p^k\mathbb{Z})$ with the given cokernel G whose residue modulo p is $\bar{X}$. Cheong, Liang, and Strand refined their result.

Theorem (Cheong–Liang–Strand, 2023)

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 $\mathrm{cok}(\bar{X}) \simeq G/pG$,

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

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

Cokernel distribution of families of matrices over $\mathbb{Z}_p$

In 2015, Clancy, Kaplan, Leake, Payne, and Wood determined the distribution of the cokernel of a random $n \times n$ symmetric matrix over $\mathbb{Z}_p$.
Also in 2015, Bhargava, Kane, Lenstra, Poonen, and Rains determined the distribution of the cokernel of a random $n \times n$ alternating matrix over $\mathbb{Z}_p$.

Cokernel distribution of symmetric matrices over $\mathbb{Z}_p$

The following result follows from the work of Clancy, Kaplan, Leake, Payne, and Wood in 2015.

Theorem (Fulman–Kaplan, 2019)

Suppose that G is a finitely generated torsion module over $\mathbb{Z}_p$ with the product decomposition

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

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

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

Cokernel distribution of symmetric matrices over $\mathbb{Z}/p^k\mathbb{Z}$

We refined the result of Fulman and Kaplan by considering matrices whose residue modulo p is some fixed matrix $\bar{X} \in \mathrm{Sym}_n(\mathbb{Z}/p\mathbb{Z})$.

Theorem (Das–Qiu–Zhang, 2023)

Let $G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$ be a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$. For any $\bar{X} \in \mathrm{Sym}_n(\mathbb{Z}/p\mathbb{Z})$ such that $\mathrm{cok}(\bar{X}) \simeq G/pG$, the number of matrices X over $\mathrm{Sym}_n(\mathbb{Z}/p^k\mathbb{Z})$ such that $\mathrm{cok}(X) \simeq G$ and $X \equiv \bar{X} \pmod{p}$ is

$$\sqrt{\frac{p^{(k-1)n(n+1)+r(r+1)}}{|G||\mathrm{Aut}(G)|}}\frac{\phi_r(p)\psi_u(p)}{\phi_u(p)}\prod_{i=1}^{s}\frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}$$

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

Cokernel distribution of symmetric matrices over $\mathbb{Z}/p^k\mathbb{Z}$

In 2017, 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.

Cokernel distribution of alternate matrices over $\mathbb{Z}/p^k\mathbb{Z}$

Definition

A square matrix A over a commutative ring R is alternate (or skew-symmetric) if $A^\top = -A$ and all diagonal entries of A are zero.

Cokernel distribution of alternate matrices over $\mathbb{Z}/p^k\mathbb{Z}$

Definition

A square matrix A over a commutative ring R is alternate (or skew-symmetric) if $A^\top = -A$ and all diagonal entries of A are zero.

Theorem (Das–Qiu–Zhang, 2023)

Let $G \simeq \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$ be a finitely generated module over $\mathbb{Z}/p^k\mathbb{Z}$ where all r_i are even. For any $\bar{X} \in \mathrm{Alt}_n(\mathbb{Z}/p\mathbb{Z})$ such that $\mathrm{cok}(\bar{X}) \simeq G/pG$, the number of matrices X over $\mathrm{Alt}_n(\mathbb{Z}/p^k\mathbb{Z})$ such that $\mathrm{cok}(X) \simeq G$ and $X \equiv \bar{X} \pmod{p}$ is

$$\sqrt{\frac{p^{(k-1)n(n-1)+r(r-1)}|G|}{|\mathrm{Aut}(G)|}} \frac{\phi_r(p)\psi_u(p)}{\phi_u(p)} \prod_{i=1}^{s} \frac{\sqrt{\phi_{r_i}(p)}}{\psi_{r_i}(p)}$$

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

Acknowledgments

We sincerely thank our mentors Gilyoung Cheong and 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 I

[1] Manjul 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.

[2] Gilyoung Cheong, Yunqi Liang, and Michael 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.

References II

[3] Julien 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.

[4] Eduardo Friedman and Lawrence 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 Jean M. de Koninck and Claude 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.

References III

[5] Jason Fulman and Nathan 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.

[6] Melanie Matchett 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.