Cohen–Lenstra Flag Universality for Random Matrix Products

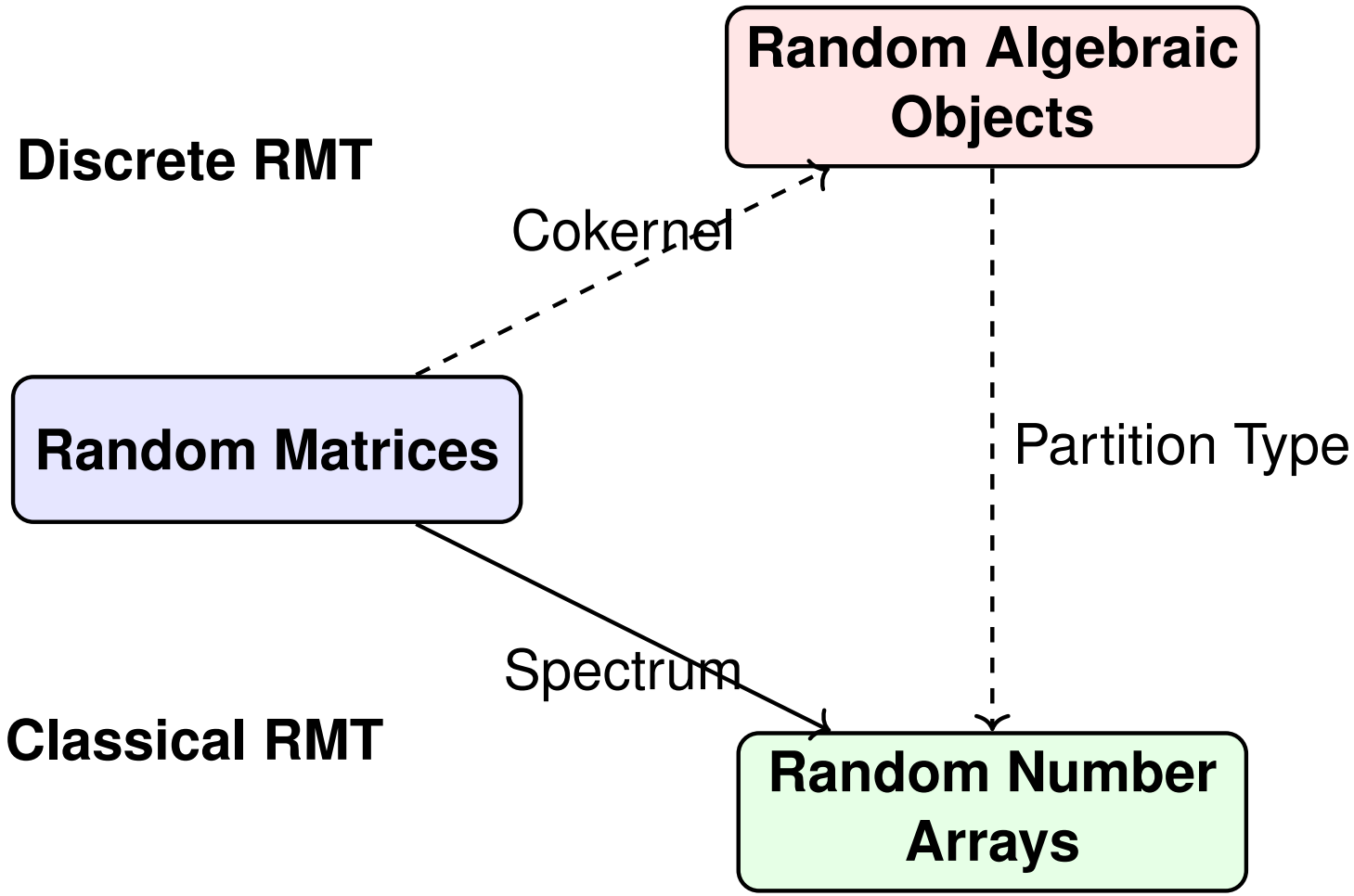
Yifeng Huang

University of Southern California
(Joint work with Hoi H. Nguyen and Roger Van Peski)

May 19, 2026 at OSU

Outline

Overview: Random Matrix Theory



Our Focus

Cokernels of random matrices over $\mathbb{Z}$ or $\mathbb{Z}_p$ (p-adic integers).

What is a Cokernel?

Let M be an $n \times n$ matrix with integer entries, $M \in \mathrm{Mat}_n(\mathbb{Z})$. The **cokernel** of M is the finite abelian group:

$$\mathrm{cok}(M) := \mathbb{Z}^n / \mathrm{im}(M)$$

where $\mathrm{im}(M) = M\mathbb{Z}^n$ is the subgroup of $\mathbb{Z}^n$ spanned by the columns of M.

Example

- If $M = [2] \in \mathrm{Mat}_1(\mathbb{Z})$, then $\mathrm{cok}(M) = \mathbb{Z}/2\mathbb{Z}$.
- If $M = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right]$, then $\mathrm{im}(M) = (2\mathbb{Z}) \oplus (3\mathbb{Z})$.

$$\mathrm{cok}(M) = (\mathbb{Z} \oplus \mathbb{Z})/(2\mathbb{Z} \oplus 3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

- If $M = \left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]$, then $\mathrm{cok}(M) \cong \mathbb{Z}/4\mathbb{Z}$.

Question

If we pick a “random“ matrix M, what does “random” cokernel look like?

What is the Partition Type?

Every finite abelian group G has a unique decomposition:

$$G \cong \bigoplus_p G_p = G_2 \oplus G_3 \oplus G_5 \oplus \dots$$

where G_p is the p-Sylow subgroup, or p-**part** of G.

Type

Every finite abelian p-group G is classified by a **partition** $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq 0)$, called the **type** of G, such that

$$G \cong \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\lambda_2}\mathbb{Z} \oplus \mathbb{Z}/p^{\lambda_3}\mathbb{Z} \oplus \dots$$

Example ($p = 2$)

- $\lambda = (2, 1, 1) \longleftrightarrow \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Hall–Littlewood Combinatorics

Hall's Theorem

Given a fixed finite-abelian p-group G of type λ, how many subgroups N have

- type μ, and
- **cotype** ν?

Here, the cotype of N in G is the type of the quotient G/N. The number is given by a specific, well-studied polynomial in p, the **Hall polynomial** $g^{\lambda}_{\mu,\nu}(p)$.

$$g^{\lambda}_{\mu,\nu}(p) = |\{N \leq G_\lambda \mid N \cong G_\mu, G_\lambda/N \cong G_\nu\}|$$

Combinatorial Significance

These polynomials are the structure constants for the **Hall algebra** and (up to renormalization) **Hall-Littlewood symmetric functions**.

What is the most “Random” Group?

The Cohen–Lenstra Heuristics (1984)

Cohen and Lenstra conjectured that in a number-theoretic model of random p-groups (the p-part of the class group of a random imaginary quadratic field, p-odd), a group G should appear with probability proportional to its **inverse automorphism group size**.

$$\mathrm{Prob}(G) = \frac{C_p}{|\mathrm{Aut}(G)|}$$

where $C_p = \prod_{i=1}^{\infty}(1 - p^{-i})$.

This distribution favors smaller and cyclic groups:

- $|\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})| = 4$ (small, so likely)
- $|\mathrm{Aut}(\mathbb{Z}/125\mathbb{Z})| = 100$
- $|\mathrm{Aut}((\mathbb{Z}/5\mathbb{Z})^3)| = 1,488,000$ (large, so unlikely)

Random Groups from Random Matrices

Theorem (Friedman–Washington '87)

Take a "uniformly" random $n \times n$ integer matrix M. (Matrix over $\mathbb{Z}_p$ with i.i.d., Haar-random entries)

As $n \to \infty$, the p-part of its cokernel follows the Cohen–Lenstra distribution:

$$\lim_{n\to\infty} \mathrm{Prob}(\mathrm{cok}(M)_p \cong G) = \frac{1}{|\mathrm{Aut}(G)|} \prod_{i=1}^{\infty}(1 - p^{-i})$$

University Theorem (Wood '19)

The result is **universal** in that the limiting cokernel distribution is independent of the specific entry distribution, as long as it is "reasonable": for $0 < \epsilon < 1$, a random integer matrix M is ϵ, p-**balanced** if $\mathrm{Prob}(M_{ij} \equiv a \pmod p) < 1 - \epsilon$ for any fixed entry i, j and remainder a.

Beyond the Default Case

The Cohen–Lenstra distribution is the “default”.

Question

What happens if the random matrix M isn’t just i.i.d.? What if it has **internal structure**?

For example:

- M is symmetric ($M = M^T$).
- M is a polynomial of another random matrix ($M = A^2 + I$).
- M has entries with a fixed residue mod p (thus *blatantly* violating ϵ-balancedness).

In all these cases, the limiting distribution **changes**. It is *not* the standard Cohen–Lenstra distribution.

The Key: Extra Structure

Guiding Philosophy

These new distributions are not random. They are explained by identifying **additional algebraic structures** on the cokernel.

The distribution is still of the "Cohen–Lenstra type", but the probability of a group G with extra structure $\mathcal{S}$ is:

$$\mathrm{Prob}(G, \mathcal{S}) \propto \frac{1}{|\mathrm{Aut}(G, \mathcal{S})|}$$

The new distribution is just the "shadow" of this more fundamental, structured distribution.

Examples of Models and Structures

Here are a few examples of this philosophy:

Matrix Model	**Extra Structure**
Symmetric Wood, Clancy, Hodges,...	Group G with a symmetric perfect pairing.
Hermitian Lee, ...	Group G with a Hermitian perfect pairing.
Polynomial $P(M)$ Cheong, H., Yu, ...	A $\mathbb{Z}_p[x]/P(x)$-module.
Matrix with fixed residue Cheong, H., Lee, ...	Group with fixed p-rank

Our Problem: What is the Structure for Products?

This brings us to our problem.
What about a **product** of k independent random matrices?

$$M_1, M_2, \ldots, M_k$$

We have a collection of cokernels:

$$(\mathrm{cok}(M_1)_p, \quad \mathrm{cok}(M_1 M_2)_p, \quad \ldots, \quad \mathrm{cok}(M_1 \cdots M_k)_p)$$

Nguyen, Van Peski '24

Found the joint distribution. It is not the Cohen–Lenstra distribution and the groups are not independent!

Question

What is the "extra structure" that binds this collection of groups together and explains their joint distribution?

The Extra Structure: Flags

There is a natural map $\mathrm{cok}(AB) \to \mathrm{cok}(A)$. Why?

- The image of B is a subgroup: $\mathrm{im}(B) = B\mathbb{Z}^n \subseteq \mathbb{Z}^n$.
- Applying A: $\mathrm{im}(AB) = A(\mathrm{im}(B)) \subseteq A(\mathbb{Z}^n) = \mathrm{im}(A)$.
- This inclusion of subgroups induces a surjection on the quotients:

$$\mathbb{Z}^n / \mathrm{im}(AB) \twoheadrightarrow \mathbb{Z}^n / \mathrm{im}(A)$$

Applying this repeatedly, we get a sequence of surjections:

$$\mathrm{cok}(M_1 \cdots M_k)_p \twoheadrightarrow \mathrm{cok}(M_1 \cdots M_{k-1})_p \twoheadrightarrow \ldots \twoheadrightarrow \mathrm{cok}(M_1)_p$$

Definition

A **surjective** k**-flag** of p-groups is a sequence of k groups connected by surjections:

$$\mathbf{G} = (G_k \twoheadrightarrow G_{k-1} \twoheadrightarrow \ldots \twoheadrightarrow G_1)$$

So, k random matrices give a *random flag* $\mathbf{cok}(M_1, \ldots, M_k)_p$.

What is the most “Random” Flag?

What is the “Cohen–Lenstra” distribution for flags?

Natural Guess

A random flag **G** should appear with probability:

$$\mathrm{Prob}(\mathbf{G}) \propto \frac{1}{|\mathrm{Aut}(\mathbf{G})|}$$

where $\mathrm{Aut}(\mathbf{G})$ are automorphisms that respect the flag structure.

$$\begin{array}{ccccccc} G_k & \longrightarrow & G_{k-1} & \longrightarrow & \cdots & \longrightarrow & G_1 \\ \downarrow{\scriptstyle \alpha_k} & & \downarrow{\scriptstyle \alpha_{k-1}} & & & & \downarrow{\scriptstyle \alpha_1} \\ G_k & \longrightarrow & G_{k-1} & \longrightarrow & \cdots & \longrightarrow & G_1 \end{array}$$

State of the Art

- Nguyen & Van Peski '24 conjectured that $\mathbf{cok}M_1, \ldots, M_k$ follows the flag Cohen–Lenstra distribution, and verified its consistency with their joint distribution of $\mathrm{cok}(M_1 \cdots M_i)$.
- This conjecture was confirmed by H. '25 when $M_1, \ldots, M_k$ are Haar random.

Main Theorem (H., Nguyen, Van Peski '25+)

The flag Cohen–Lenstra distribution is **universal** and **independent across finitely many primes**.

Main Result: Precise Statement

Theorem (H., Nguyen, Van Peski '25+)

Let $0 < \epsilon < 1$, P be a finite collection of primes, and $M_1, \ldots, M_k$ be independent $n \times n$ random integer matrices that are ϵ, p-balanced for any $p \in P$.
As $n \to \infty$, the random flag $\mathbf{cok}(M_1, \ldots, M_k)_P$ converges in distribution to the **flag Cohen–Lenstra distribution**: for any surjective k-flag $\mathbf{G}$ of finite abelian P-groups,

$$\lim_{n\to\infty} \mathrm{Prob}(\mathbf{cok}(M_1, \ldots, M_k)_P \cong \mathbf{G}) = \frac{C_{k,P}}{|\mathrm{Aut}_{\mathrm{flag}}(\mathbf{G})|}$$

where $C_{k,P} = (\prod_{p\in P} \prod_{i=1}^{\infty} (1 - p^{-i}))^k$.

Consequences for $k = 2$ Case?

Let's look at the simplest non-trivial case: $k = 2$.
We have two independent random matrices M_1, M_2. The random object is the flag:

$$\operatorname{cok}(M_1 M_2)_p \twoheadrightarrow \operatorname{cok}(M_1)_p$$

Let $H = \operatorname{cok}(M_1)_p$ and $K = \operatorname{cok}(M_2)_p$. These are independent Cohen–Lenstra random groups.

Question

What is the distribution of $G = \operatorname{cok}(M_1 M_2)_p$?

It's natural to ask for the distribution of G **conditional on** H and K.

$$\operatorname{Prob}(G \mid H, K) = ?$$

This is a "randomized convolution" of two random groups.

The Conditional Convolution

Corollary (H-N-VP)

Let H, K, G be any finite abelian p-groups. As $n \to \infty$:

$$\begin{aligned}\mathrm{Prob}(\mathrm{cok}(M_1 M_2)_p \cong G \mid \mathrm{cok}(M_1)_p \cong H, \mathrm{cok}(M_2)_p \cong K) \\ = \frac{|\mathrm{Aut}(H)| \cdot |\mathrm{Aut}(K)|}{|\mathrm{Aut}(G)|} \times N(G, H, K)\end{aligned}$$

where $N(G, H, K)$ is the Hall polynomial:

$$N(G, H, K) = |\{N \leq G \mid N \cong K \text{ and } G/N \cong H\}|$$

The new feature is the **universality**: it holds if M_1, M_2 are independent ϵ, p-balanced matrices. Previously, Van Peski proved it when the distribution of M_1, M_2 is $\mathrm{GL}_n(\mathbb{Z}_p)$-invariant.

Connection to Complex Matrices

This result is a deep structural analogue of a famous phenomenon in "free probability".

Classical Random Matrix Theory

- Let A, B be random $n \times n$ *complex* matrices.
- **Addition:** The eigenvalues of $A + B$ are *not* the sum of eigenvalues. Their limiting distribution is the **free additive convolution** $\mu_A \boxplus \mu_B$.
- **Multiplication:** The singular values of AB are *not* the product of singular values. Their limiting distribution is the **free multiplicative convolution** $\mu_A \boxtimes \mu_B$.

Connection

Our result is the discrete analogue of the "multiplicative convolution": cokernel type $\leftrightarrow$ singular values [Van Peski]. Both come from double coset decomposition with respect to the maximal compact subgroup.

How to Prove Universality?

We can't compute $\mathrm{Prob}(\mathbf{cok}(\dots) \cong \mathbf{G})$ directly for a generic, non-Haar matrix distribution.

Recall: Classical Moment

To show $X_n \to X$, we can show their **moments** converge,

$$\lim_{n\to\infty} \mathbb{E}[X_n^k] = \mathbb{E}[X^k] \quad \text{for all } k \geq 1,$$

as long as they are **well-behaved** (e.g., moments don't grow too fast).

Key Question

For a random *algebraic object* **G** (like a group or a flag), what is the "moment"?

The “Sawin–Wood Machine”

Theorem (Sawin-Wood ’22)

There is a general moment method for random objects **G** in a **“diamond category”** $\mathcal{C}$.

- The “moments” are the expected counts of **epimorphisms** onto test objects **H**.

$$M(\mathbf{H}) = \mathbb{E}_{\mathbf{G}}\left[|\mathrm{Epi}_{\mathcal{C}}(\mathbf{G}, \mathbf{H})|\right]$$

- If these limiting moments $M(\mathbf{H})$ exist for all **H**,
- and the moment function M is **“well-behaved”** (a technical growth condition),
- then the moments uniquely determine the distribution of **G**.
- Moreover, limiting distribution corresponds to limiting moment.

Our Problem: What Category to Use?

We need to put our random flags **cok**(...) into a "diamond category" $\mathcal{C}$ where we can:

1. Compute the limiting epimorphism moments $\lim \mathbb{E}[|\mathrm{Epi}_{\mathcal{C}}(\ldots)|]$.
2. Prove that the resulting moment function is "well-behaved".

Attempt 1: The "Obvious" Category $\mathbf{FI}_k$

- Objects: Surjective flags $\mathbf{G} = (G_k \twoheadrightarrow \ldots \twoheadrightarrow G_1)$.
- Each surjective flag gives rise to an **injective flag** $H_1 \subseteq \ldots \subseteq H_k = G_k$, by $H_i = \ker(G_k \twoheadrightarrow G_i)$.
- A morphism $\mathbf{G} \to \mathbf{G}'$ in $\mathbf{FI}_k$ is a group homomorphism $\alpha : G_k \to G'_k$ such that $\alpha(H_i) \subseteq H'_i$ for all i. This is equivalent to the notation defined by the commutative diagram.
- An epimorphism is a morphism such that $\alpha : G_k \to G'_k$ is surjective (and hence so are $G_i \to G'_i$).

Status

- ✓ This *is* a diamond category.
- ✓ We *can* compute the limiting moments.
- × **Problem:** Proving the moments are "well-behaved" is hard. There are no ready-to-use criteria for this category.

Fix: The Right Category $\mathcal{C}$

We use a category with the same objects but fewer morphisms.

- Objects: Same.
- A morphism $\mathbf{G} \to \mathbf{G}'$ in $\mathbf{FI}_k$ is a group homomorphism $\alpha : G_k \to G'_k$ such that $\alpha(H_i) = H'_i$ for all $1 \leq i < k$. The steps must map *onto* each other, not just *into*.
- An epimorphism is a morphism such that $\alpha : G_k \to G'_k$ is surjective; in other words, $\alpha(H_i) = H'_i$ for all $1 \leq i \leq k$..

Status

- ✓ **Crucially:** This can be viewed as the category of groups with an "enriched" structure in Sawin–Wood's machinery.
- ✓ This implies that $\mathcal{C}$ is a diamonad category and gives a criterion to check whether a moment function is "well-behaved".
- ✓ Isomorphisms are the same $\mathbf{FI}_k$ and $\mathcal{C}$, so the replacement is valid (does not change the distribution) even though it affects the moments!

The Moment Calculation

So, we use the category $\mathcal{C}$. Recall that epimorphisms in $\mathcal{C}$ are in a very rigid sense.

Main Calculation (H-N-VP '25+)

Let $M_1, \ldots, M_k$ be random matrices as before, then the limit moment is just 1 for any test flag $\mathbf{H}$:

$$\lim_{n\to\infty} \mathbb{E}\left[\left|\mathrm{Epi}_{\mathcal{C}}(\mathbf{cok}(M_1, \ldots, M_k), \mathbf{H})\right|\right] = 1$$

The proof is a manageable induction using combinatorial bounds on "codes" and "non-codes" (different types of vectors in G^n; codes are the more generic vectors).

Finishing the Proof

Our proof is now a clean 3-step argument:

1. **Compute Moments:** We show that the limiting moment is 1 as long as M_i are ϵ-balanced.
2. **Well-behavedness:** We use the general criterion of Sawin–Wood, and a bound of the number of injective flags in a fixed group proved in [N-VP'24] to prove that the moment function 1 (the constant function) is well-behaved.
3. **Identify Limit:** Since the limiting moment determines the limiting distribution, we can extract the limiting distribution from the Haar case proved in [H.'25].

Summary

- We study the rich algebraic structure of cokernels of random matrix *products*.
- This structure is a **flag** of surjective maps.

$$\mathrm{cok}(M_1 \cdots M_k) \twoheadrightarrow \ldots \twoheadrightarrow \mathrm{cok}(M_1)$$

- **Main Result:** We prove a **universality** theorem. For any "reasonable" random matrix, this random flag converges to the Flag Cohen–Lenstra distribution $\mathrm{Prob}(\mathbf{G}) \propto 1/|\mathrm{Aut}(\mathbf{G})|$.
- **Key Corollary:** For $k = 2$, this gives a universal formula for the "conditional convolution" $\mathrm{Prob}(\mathrm{cok}(M_1 M_2) \mid \mathrm{cok}(M_1), \mathrm{cok}(M_2))$.
- This formula is combinatorial, and the probabilities are given by **Hall–Littlewood structure constants**.

Thank you!

Questions?

From fine to coarse: distribution

Concern

If we get the distribution and moment of a fine statistics, can we easily understand a coarser statistics?

Example

While abelian p-groups are classified by partitions, flags of abelian p-groups do not have an elementary classification theory ("wild"). How does one compute the distribution of just the biggest group in a Cohen–Lenstra random flag, recovering the distribution of $\mathrm{cok}(M_1 M_2 \cdots M_k)$?

Short answer

There is a clean **orbit-stabilizer** argument to do it, which absorbs the $|\mathrm{Aut}_{\mathbf{FI}}|$ factor naturally.

From fine to coarse: moments

Observation

Fine moment directly implies the coarse moment, and the moment calculation in the coarse problem informs the fine structure.

$$\mathbb{E}[\#\mathrm{Epi}_{\mathrm{Ab}}(\mathrm{cok}(M_1 \cdots M_k), H)] = \sum_{F \in H^n : \mathrm{span}(F) = H} \mathbb{P}(M_1 \cdots M_k F = 0)$$

$$= \#\{H_1 \leq \cdots \leq H_{k-1} \leq H\}.$$

$$\mathbb{E}[\#\mathrm{Epi}_{\mathcal{C}}(\mathbf{cok}(M_1, \ldots, M_k)), (H_1 \leq \cdots \leq H_{k-1} \leq H)]$$

$$= \sum_{F \in H^n : \mathrm{span}(F) = H} \mathbb{P}(\mathrm{span}(M_k F) = H_{k-1}, \ldots, \mathrm{span}(M_1 \cdots M_k F) = 0)$$

$$= 1.$$