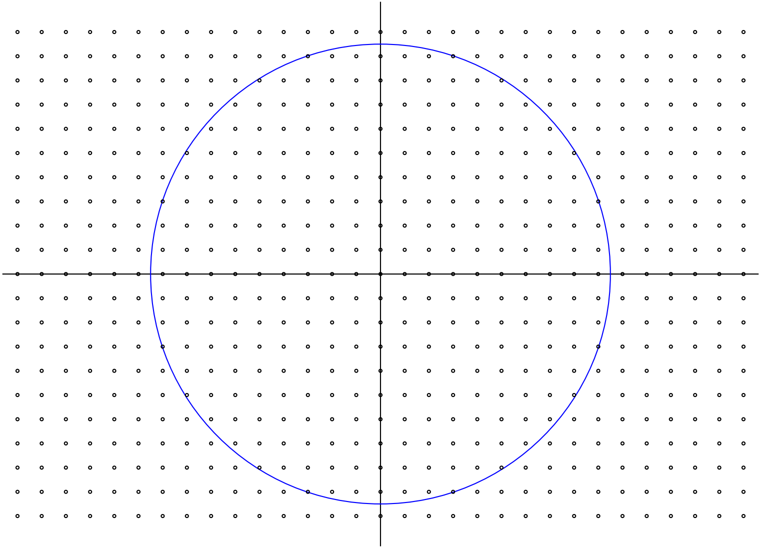
Fourier Analysis in Arithmetic Statistics

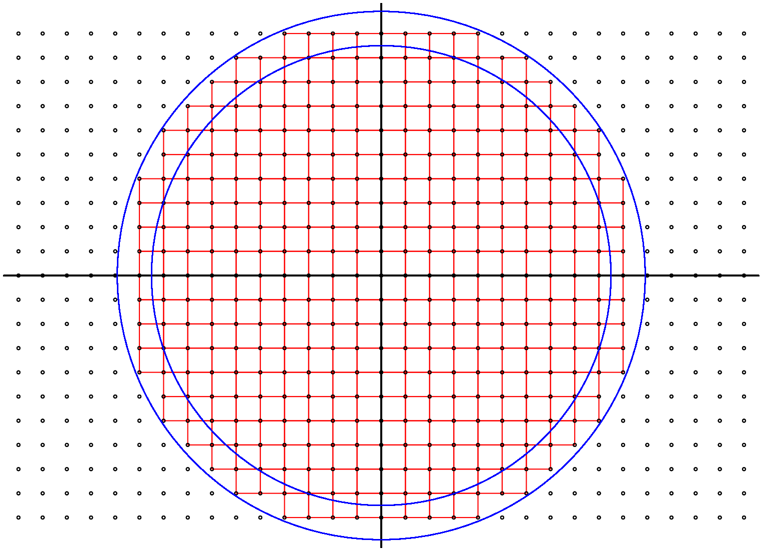
Frank Thorne

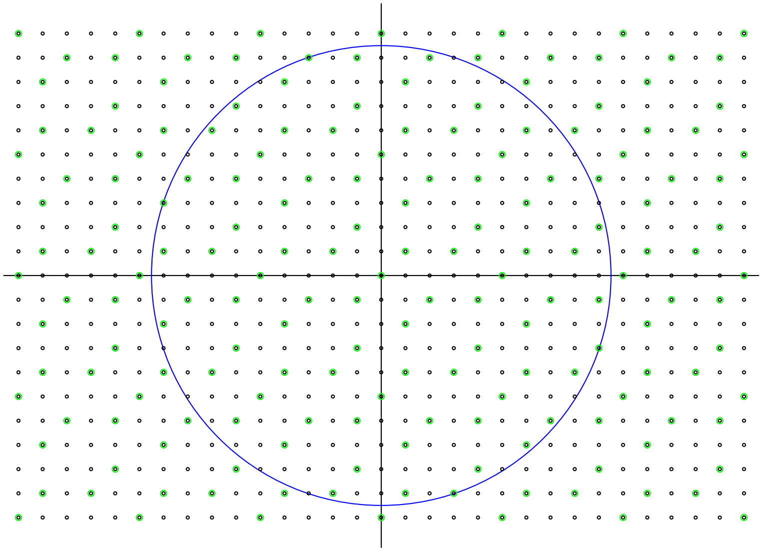
University of South Carolina

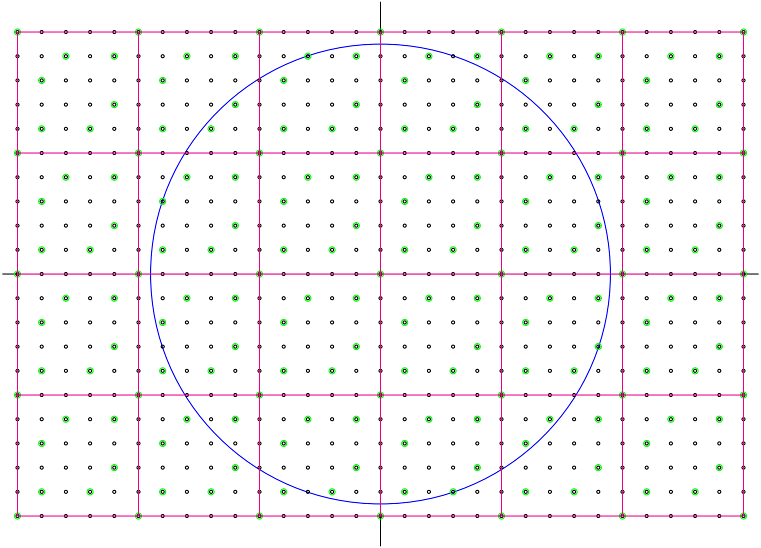
Kobe University, June 6, 2025

thornef.github.io/japan-fourier-2025.pdf









Sample Theorem 1: Counting Cubic Fields

What is “arithmetic statistics”?

Sample Theorem 1: Counting Cubic Fields

What is "arithmetic statistics"?

For any integer $d \geq 1$, write

$$N_d(X) := \#\{K \ : \ [K : \mathbb{Q}] = d, \ |\mathrm{Disc}(K)| < X\}.$$

Sample Theorem 1: Counting Cubic Fields

What is "arithmetic statistics"?

For any integer $d \geq 1$, write

$$N_d(X) := \#\{K \ : \ [K : \mathbb{Q}] = d, \ |\mathrm{Disc}(K)| < X\}.$$

Theorem (Davenport-Heilbronn)

We have

$$N_3(X) = \frac{1}{3\zeta(3)} X + o(X).$$

Theorem (Bhargava)

We have

$$N_4(X, S_4) \sim \frac{5}{24} \prod_p (1 + p^{-2} - p^{-3} - p^{-4}) X,$$

Theorem (Bhargava)

We have

$$N_4(X, S_4) \sim \frac{5}{24} \prod_p (1 + p^{-2} - p^{-3} - p^{-4}) X,$$

$$N_5(X) \sim \frac{13}{130} \prod_p (1 + p^{-2} - p^{-4} - p^{-5}) X.$$

Sample Theorem 3: 3-torsion in Quadratic Class Groups

Theorem (Davenport-Heilbronn)

We have

$$\sum_{|D|<X} \#|\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))[3]| = \frac{3+3+1+3}{\pi^2} X + o(X).$$

Sample Theorem 4: 2-Selmer Groups in Elliptic Curves

Theorem (Bhargava-Shankar)

When elliptic curves E are ordered by height, the average size of their 2-Selmer groups is 3.

Sample Theorem 4: 2-Selmer Groups in Elliptic Curves

Theorem (Bhargava-Shankar)

When elliptic curves E are ordered by height, the average size of their 2-Selmer groups is 3.

Corollary

Their average rank is at most 1.5.

Theorem

There exists an explicit, "nice" bijection

$$\{\ \textit{Something nice}\ \} \longleftrightarrow G(\mathbb{Z})\backslash V(\mathbb{Z})$$

where V is a f.d. representation of an algebraic group G.

Theorem

There exists an explicit, "nice" bijection

$$\{ \text{ Something nice } \} \longleftrightarrow G(\mathbb{Z})\backslash V(\mathbb{Z})$$

where V is a f.d. representation of an algebraic group G.

Moreover, certain arithmetic properties on the left correspond to congruence conditions on the right.

Example: Binary Cubic Forms

Let V be the space of binary cubic forms:

$$V := \{x(u, v) = au^3 + bu^2v + cuv^2 + dv^3\}.$$

Example: Binary Cubic Forms

Let V be the space of binary cubic forms:

$$V := \{x(u,v) = au^3 + bu^2v + cuv^2 + dv^3\}.$$

$G = \mathrm{GL}_2$ acts on V by

$$(gx)(u,v) = \frac{1}{\det g} x((u,v)g).$$

Example: Binary Cubic Forms

Let V be the space of binary cubic forms:

$$V := \{x(u,v) = au^3 + bu^2v + cuv^2 + dv^3\}.$$

$G = \mathrm{GL}_2$ acts on V by

$$(gx)(u,v) = \frac{1}{\det g} x((u,v)g).$$

We have

$$\mathrm{Disc}(x) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd,$$

for which we have

Example: Binary Cubic Forms

Let V be the space of binary cubic forms:

$$V := \{x(u,v) = au^3 + bu^2v + cuv^2 + dv^3\}.$$

$G = \mathrm{GL}_2$ acts on V by

$$(gx)(u,v) = \frac{1}{\det g} x((u,v)g).$$

We have

$$\mathrm{Disc}(x) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd,$$

for which we have

- $\mathrm{Disc}(gx) = (\det g)^2 \mathrm{Disc}(x)$;

Example: Binary Cubic Forms

Let V be the space of binary cubic forms:

$$V := \{x(u,v) = au^3 + bu^2v + cuv^2 + dv^3\}.$$

$G = \mathrm{GL}_2$ acts on V by

$$(gx)(u,v) = \frac{1}{\det g} x((u,v)g).$$

We have

$$\mathrm{Disc}(x) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd,$$

for which we have

- $\mathrm{Disc}(gx) = (\det g)^2 \mathrm{Disc}(x)$;
- $\mathrm{Disc}(x) = 0$ if and only if $x(u,v)$ has a repeated root.

Example: Binary Cubic Forms (2)

Theorem (Levi, Delone-Faddeev, Gan-Gross-Savin)

$G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ parametrize cubic rings. Further, if $v \leftrightarrow R$,

Example: Binary Cubic Forms (2)

Theorem (Levi, Delone-Faddeev, Gan-Gross-Savin)

$G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ parametrize cubic rings. Further, if $v \leftrightarrow R$,

- Stab(v) *is isomorphic to* $\mathrm{Aut}(R)$*;*

Example: Binary Cubic Forms (2)

Theorem (Levi, Delone-Faddeev, Gan-Gross-Savin)

$G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ parametrize cubic rings. Further, if $v \leftrightarrow R$,

- $\mathrm{Stab}(v)$ *is isomorphic to* $\mathrm{Aut}(R)$;
- $\mathrm{Disc}(v) = \mathrm{Disc}(R)$;

Example: Binary Cubic Forms (2)

Theorem (Levi, Delone-Faddeev, Gan-Gross-Savin)

$G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ parametrize cubic rings. Further, if $v \leftrightarrow R$,

- Stab(v) *is isomorphic to* $\mathrm{Aut}(R)$*;*
- $\mathrm{Disc}(v) = \mathrm{Disc}(R)$*;*
- *(Davenport-Heilbronn) R is maximal iff, for all primes p, v satisfies a certain congruence condition $\pmod{p^2}$.*

Theorem (DHBBPBSTTTBTT)

We have

$$N_3(X) = \frac{1}{3\zeta(3)}X + \frac{4(1+\sqrt{3})\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{\frac{2}{3}}(\log X)^3).$$

Some parametrizations

Some parametrizations

- $V = \mathrm{Sym}^3(2)$, $G = \mathrm{GL}_2$: cubic rings; 3-torsion in class groups (Levi, Delone-Faddeev, Davenport-Heilbronn)

Some parametrizations

- $V = \mathrm{Sym}^3(2)$, $G = \mathrm{GL}_2$: cubic rings; 3-torsion in class groups (Levi, Delone-Faddeev, Davenport-Heilbronn)
- $V = 2 \otimes \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_3$. quartic rings; 2-torsion in class groups of cubic fields (Wright-Yukie; Bhargava)

Some parametrizations

- $V = \mathrm{Sym}^3(2)$, $G = \mathrm{GL}_2$: cubic rings; 3-torsion in class groups (Levi, Delone-Faddeev, Davenport-Heilbronn)
- $V = 2 \otimes \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_3$.
  quartic rings; 2-torsion in class groups of cubic fields (Wright-Yukie; Bhargava)
- $V = 4 \otimes \wedge^2(5)$, $G = \mathrm{GL}_4 \times \mathrm{SL}_5$
  quintic rings (Wright-Yukie; Bhargava)

Some parametrizations

- $V = \mathrm{Sym}^3(2)$, $G = \mathrm{GL}_2$: cubic rings; 3-torsion in class groups (Levi, Delone-Faddeev, Davenport-Heilbronn)
- $V = 2 \otimes \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_3$.
  quartic rings; 2-torsion in class groups of cubic fields
  (Wright-Yukie; Bhargava)
- $V = 4 \otimes \wedge^2(5)$, $G = \mathrm{GL}_4 \times \mathrm{SL}_5$
  quintic rings (Wright-Yukie; Bhargava)
- $V = \mathrm{Sym}^4(2)$, $G = \mathrm{PGL}_2$
  2-Selmer elements of elliptic curves
  (Birch–Swinnerton-Dyer, Bhargava-Shankar)

Some parametrizations

- $V = \mathrm{Sym}^3(2)$, $G = \mathrm{GL}_2$: cubic rings; 3-torsion in class groups (Levi, Delone-Faddeev, Davenport-Heilbronn)
- $V = 2 \otimes \mathrm{Sym}^2(3)$, $G = \mathrm{GL}_2 \times \mathrm{GL}_3$.
  quartic rings; 2-torsion in class groups of cubic fields
  (Wright-Yukie; Bhargava)
- $V = 4 \otimes \wedge^2(5)$, $G = \mathrm{GL}_4 \times \mathrm{SL}_5$
  quintic rings (Wright-Yukie; Bhargava)
- $V = \mathrm{Sym}^4(2)$, $G = \mathrm{PGL}_2$
  2-Selmer elements of elliptic curves
  (Birch–Swinnerton-Dyer, Bhargava-Shankar)
- ... and more!
  (Bhargava, Ho, Shankar, Varma, X. Wang, Wood, ...)

More Interesting Parametrizations

Table 1: Summary of Higher Composition Laws

#	Lattice ($V_{\mathbb{Z}}$)	Group acting ($G_{\mathbb{Z}}$)	Parametrizes ($\mathcal{C}$)	(k)	(n)	(H)
1.	$\{0\}$	-	Linear rings	0	0	A_0
2.	$\widetilde{\mathbb{Z}}$	$\mathrm{SL}_1(\mathbb{Z})$	Quadratic rings	1	1	A_1
3.	$(\mathrm{Sym}^2\mathbb{Z}^2)^*$ (GAUSS'S LAW)	$\mathrm{SL}_2(\mathbb{Z})$	Ideal classes in quadratic rings	2	3	B_2
4.	$\mathrm{Sym}^3\mathbb{Z}^2$	$\mathrm{SL}_2(\mathbb{Z})$	Order 3 ideal classes in quadratic rings	4	4	G_2
5.	$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$	$\mathrm{SL}_2(\mathbb{Z})^2$	Ideal classes in quadratic rings	4	6	B_3
6.	$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$	$\mathrm{SL}_2(\mathbb{Z})^3$	Pairs of ideal classes in quadratic rings	4	8	D_4
7.	$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$	$\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$	Ideal classes in quadratic rings	4	12	D_5
8.	$\wedge^3\mathbb{Z}^6$	$\mathrm{SL}_6(\mathbb{Z})$	Quadratic rings	4	20	E_6
9.	$(\mathrm{Sym}^3\mathbb{Z}^2)^*$	$\mathrm{GL}_2(\mathbb{Z})$	Cubic rings	4	4	G_2
10.	$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$	Order 2 ideal classes in cubic rings	12	12	F_4
11.	$\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})^2$	Ideal classes in cubic rings	12	18	E_6
12.	$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$	Cubic rings	12	30	E_7
13.	$(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3)^*$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$	Quartic rings	12	12	F_4
14.	$\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$	$\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$	Quintic rings	40	40	E_8

Bhargava, *Higher composition laws IV*, Ann. Math., 2008

Still More Interesting Parametrizations

	Group (s.s.)	Representation	Geometric Data	Invariants	Dynkin	§
1.	SL_2	$\mathrm{Sym}^4(2)$	(C, L_2)	$2, 3$	$A_2^{(2)}$	4.1
2.	SL_2^2	$\mathrm{Sym}^2(2) \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L_2') \sim (C, L_2, P)$	$2, 3, 4$	$D_3^{(2)}$	6.1
3.	SL_2^4	$2 \otimes 2 \otimes 2 \otimes 2$	$(C, L_2, L_2', L_2'') \sim (C, L_2, P, P')$	$2, 4, 4, 6$	$D_4^{(1)}$	6.2
4.	SL_2^3	$2 \otimes 2 \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L_2') \sim (C, L_2, P)$	$2, 4, 6$	$B_3^{(1)}$	6.3.1
5.	SL_2^2	$\mathrm{Sym}^2(2) \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L_2') \sim (C, L_2, P)$	$2, 3, 4$	$D_3^{(2)}$	6.3.3
6.	SL_2^2	$2 \otimes \mathrm{Sym}^3(2)$	(C, L_2, P_3)	$2, 6$	$G_2^{(1)}$	6.3.2
7.	SL_2	$\mathrm{Sym}^4(2)$	(C, L_2, P_3)	$2, 3$	$A_2^{(2)}$	6.3.4
8.	$\mathrm{SL}_2^2 \times \mathrm{GL}_4$	$2 \otimes 2 \otimes \wedge^2(4)$	$(C, L_2, M_{2,6})$	$2, 4, 6, 8$	$D_5^{(1)}$	6.6.1
9.	$\mathrm{SL}_2 \times \mathrm{SL}_6$	$2 \otimes \wedge^3(6)$	$(C, L_2, M_{3,6})$ with $L^{\otimes 3} \cong \det M$	$2, 6, 8, 12$	$E_6^{(1)}$	6.6.2
10.	$\mathrm{SL}_2 \times \mathrm{Sp}_6$	$2 \otimes \wedge_0^3(6)$	$(C, L_2, (M_{3,6}, \varphi))$ with $L^{\otimes 3} \cong \det M$	$2, 6, 8, 12$	$E_6^{(2)}$	6.6.3
11.	$\mathrm{SL}_2 \times \mathrm{Spin}_{12}$	$2 \otimes S^+(32)$	$(C \to \mathbb{P}^1(\mathscr{H}_3(\mathbb{H})), L_2)$	$2, 6, 8, 12$	$E_7^{(1)}$	6.6.3
12.	$\mathrm{SL}_2 \times E_7$	$2 \otimes 56$	$(C \to \mathbb{P}^1(\mathscr{H}_3(\mathbb{O})), L_2)$	$2, 6, 8, 12$	$E_8^{(1)}$	6.6.3
13.	SL_3	$\mathrm{Sym}^3(3)$	(C, L_3)	$4, 6$	$D_4^{(3)}$	4.2
14.	SL_3^3	$3 \otimes 3 \otimes 3$	$(C, L_3, L_3') \sim (C, L_3, P)$	$6, 9, 12$	$E_6^{(1)}$	5.1
15.	SL_3^2	$3 \otimes \mathrm{Sym}^2(3)$	(C, L_3, P_2)	$6, 12$	$F_4^{(1)}$	5.2.1
16.	SL_3	$\mathrm{Sym}^3(3)$	(C, L_3, P_2)	$4, 6$	$D_4^{(3)}$	5.2.2
17.	$\mathrm{SL}_3 \times \mathrm{SL}_6$	$3 \otimes \wedge^2(6)$	$(C, L_3, M_{2,6})$ with $L^{\otimes 2} \cong \det M$	$6, 12, 18$	$E_7^{(1)}$	5.5
18.	$\mathrm{SL}_3 \times E_6$	$3 \otimes 27$	$(C \hookrightarrow \mathbb{P}^2(\mathbb{O}), L_3)$	$6, 12, 18$	$E_8^{(1)}$	5.4
19.	$\mathrm{SL}_2 \times \mathrm{SL}_4$	$2 \otimes \mathrm{Sym}^2(4)$	(C, L_4)	$8, 12$	$E_6^{(2)}$	4.3
20.	$\mathrm{SL}_5 \times \mathrm{SL}_5$	$\wedge^2(5) \otimes 5$	(C, L_5)	$20, 30$	$E_8^{(1)}$	4.4

Table 1: Table of coregular representations and their moduli interpretations

Bhargava and Ho, *Coregular spaces and genus one curves*, Camb. J. Math.

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;
- We might impose congruence conditions as well.

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;
- We might impose congruence conditions as well.

To do this, use:

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;
- We might impose congruence conditions as well.

To do this, use:

- Elementary methods (choose a fundamental domain);

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;
- We might impose congruence conditions as well.

To do this, use:

- Elementary methods (choose a fundamental domain);
- Bhargava's averaging method;

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;
- We might impose congruence conditions as well.

To do this, use:

- Elementary methods (choose a fundamental domain);
- Bhargava's averaging method;
- Sato-Shintani zeta functions;

Counting methods

Problem: Want to count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where:

- (G, V) is a "nice" f.d. representation of an algebraic group;
- We require $|\mathrm{Disc}(v)| < X$ for $v \in V(\mathbb{Z})$;
- We might impose congruence conditions as well.

To do this, use:

- Elementary methods (choose a fundamental domain);
- Bhargava's averaging method;
- Sato-Shintani zeta functions;
- (New!) Bhargava's method with Fourier analysis.