

# Fourier Analysis in Arithmetic Statistics

Frank Thorne

University of South Carolina

IIT Bombay, December 3, 2025

`thornef.github.io/iitb-2025.pdf`



```

Last login: Wed Dec 3 09:31:01 on ttys000
Franks-MacBook-Pro-2:~ frankthorne$ gp
GP/PARI CALCULATOR Version 2.8.0 (development 18205-1c269ec)
i386 running darwin (x86-64 kernel) 64-bit version
compiled: Nov 11 2015, Apple LLVM version 6.0 (clang-600.0.54) (based on LLVM 3.5svn)

          threading engine: single
(readline not compiled in, extended help enabled)

          Copyright (C) 2000-2015 The PARI Group

PARI/GP is free software, covered by the GNU General Public License, and comes
WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?15 for how to get moral (and possibly technical) support.

parisize = 8000000, primelimit = 500000
? default(realprecision, 50)
? exp(Pi*sqrt(163))
%2 = 262537412640768743.9999999999925007259719818568888
? █

```

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

- ▶ **Class numbers** of binary quadratic **or other** forms;

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

- ▶ **Class numbers** of binary quadratic **or other** forms;
- ▶ **Number fields**;

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

- ▶ **Class numbers** of binary quadratic **or other** forms;
- ▶ **Number fields**;
- ▶ **Ideal class groups** in number fields;

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

- ▶ **Class numbers** of binary quadratic **or other** forms;
- ▶ **Number fields**;
- ▶ **Ideal class groups** in number fields;
- ▶ **Elliptic curves**, their **points**, **ranks**, etc.;

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

- ▶ **Class numbers** of binary quadratic **or other** forms;
- ▶ **Number fields**;
- ▶ **Ideal class groups** in number fields;
- ▶ **Elliptic curves**, their **points**, **ranks**, etc.;
- ▶ **Zeroes** of  $\zeta$  and  $L$ -functions;

# What is Arithmetic Statistics?

Want to count **arithmetic objects**, such as

- ▶ **Class numbers** of binary quadratic **or other** forms;
- ▶ **Number fields**;
- ▶ **Ideal class groups** in number fields;
- ▶ **Elliptic curves**, their **points**, **ranks**, etc.;
- ▶ **Zeroes** of  $\zeta$  and  $L$ -functions;
- ▶ .....

# Sample Theorem 1: Counting Cubic Fields

For any integer  $d \geq 1$ , write

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

# Sample Theorem 1: Counting Cubic Fields

For any integer  $d \geq 1$ , write

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

Theorem (Davenport-Heilbronn)

*We have*

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

# Sample Theorem 2: Counting Quartic and Quintic Fields

## Theorem (Bhargava)

*We have*

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

# Sample Theorem 2: Counting Quartic and Quintic Fields

## 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

$$\sum_{|D| < X} \#|\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))[3]| = \frac{10}{\pi^2} X + o(X).$$

# 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.*

# Techniques used in arithmetic statistics

# Techniques used in arithmetic statistics

- ▶ Parametrization and counting theorems involving lattice points;

# Techniques used in arithmetic statistics

- ▶ Parametrization and counting theorems involving lattice points;
- ▶ .....
- ▶ .....
- ▶ .....
- ▶ .....
- ▶ .....
- ▶ .....
- ▶ .....
- ▶ .....
- ▶ .....

# Parametrization: The Basic Metatheorem

## 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  $G$ .*

# Parametrization: The Basic Metatheorem

## 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

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

# 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  $v \leftrightarrow R$ ,

- ▶  $\text{Stab}(v)$  is isomorphic to  $\text{Aut}(R)$ ;

## 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  $v \leftrightarrow R$ ,

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

## 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  $v \leftrightarrow R$ ,

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

# Some parametrizations

# Some parametrizations

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

# Some parametrizations

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

# Some parametrizations

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

# Some parametrizations

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

# Some parametrizations

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

# More Interesting Parametrizations

56

MANJUL BHARGAVA

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.	$\tilde{\mathbb{Z}}$	$\mathrm{SL}_1(\mathbb{Z})$	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.	$\mathrm{SL}_2$	$\mathrm{Sym}^4(2)$	$(C, L_2)$	2, 3	$A_3^{(2)}$	<b>4.1</b>
2.	$\mathrm{SL}_2^2$	$\mathrm{Sym}^2(2) \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L'_2) \sim (C, L_2, P)$	2, 3, 4	$D_3^{(2)}$	<b>6.1</b>
3.	$\mathrm{SL}_2^4$	$2 \otimes 2 \otimes 2 \otimes 2$	$(C, L_2, L'_2, L''_2) \sim (C, L_2, P, P')$	2, 4, 4, 6	$D_4^{(1)}$	<b>6.2</b>
4.	$\mathrm{SL}_2^3$	$2 \otimes 2 \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L'_2) \sim (C, L_2, P)$	2, 4, 6	$E_3^{(1)}$	<b>6.3.1</b>
5.	$\mathrm{SL}_2^2$	$\mathrm{Sym}^2(2) \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L'_2) \sim (C, L_2, P)$	2, 3, 4	$D_3^{(2)}$	<b>6.3.3</b>
6.	$\mathrm{SL}_2^2$	$2 \otimes \mathrm{Sym}^3(2)$	$(C, L_2, P_3)$	2, 6	$G_2^{(1)}$	<b>6.3.2</b>
7.	$\mathrm{SL}_2$	$\mathrm{Sym}^4(2)$	$(C, L_2, P_3)$	2, 3	$A_2^{(2)}$	<b>6.3.4</b>
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	$D_5^{(1)}$	<b>6.6.1</b>
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	$E_6^{(1)}$	<b>6.6.2</b>
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	$E_6^{(2)}$	<b>6.6.3</b>
11.	$\mathrm{SL}_2 \times \mathrm{Spin}_{12}$	$2 \otimes S^+(32)$	$(C \rightarrow \mathbb{P}^1(\mathcal{H}_3(\mathbb{H})), L_2)$	2, 6, 8, 12	$E_7^{(1)}$	<b>6.6.3</b>
12.	$\mathrm{SL}_2 \times E_7$	$2 \otimes 56$	$(C \rightarrow \mathbb{P}^1(\mathcal{H}_3(\mathbb{O})), L_2)$	2, 6, 8, 12	$E_8^{(1)}$	<b>6.6.3</b>
13.	$\mathrm{SL}_3$	$\mathrm{Sym}^3(3)$	$(C, L_3)$	4, 6	$D_4^{(3)}$	<b>4.2</b>
14.	$\mathrm{SL}_3^3$	$3 \otimes 3 \otimes 3$	$(C, L_3, L'_3) \sim (C, L_3, P)$	6, 9, 12	$E_6^{(1)}$	<b>5.1</b>
15.	$\mathrm{SL}_3^2$	$3 \otimes \mathrm{Sym}^2(3)$	$(C, L_3, P_2)$	6, 12	$F_4^{(1)}$	<b>5.2.1</b>
16.	$\mathrm{SL}_3$	$\mathrm{Sym}^3(3)$	$(C, L_3, P_2)$	4, 6	$D_4^{(3)}$	<b>5.2.2</b>
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	$E_7^{(1)}$	<b>5.5</b>
18.	$\mathrm{SL}_3 \times E_6$	$3 \otimes 27$	$(C \hookrightarrow \mathbb{P}^2(\mathbb{O}), L_3)$	6, 12, 18	$E_8^{(1)}$	<b>5.4</b>
19.	$\mathrm{SL}_2 \times \mathrm{SL}_4$	$2 \otimes \mathrm{Sym}^2(4)$	$(C, L_4)$	8, 12	$E_6^{(2)}$	<b>4.3</b>
20.	$\mathrm{SL}_5 \times \mathrm{SL}_5$	$\wedge^2(5) \otimes 5$	$(C, L_5)$	20, 30	$E_8^{(1)}$	<b>4.4</b>

Table 1: Table of coregular representations and their moduli interpretations

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

## Theorem (DHBBPBSTTTBTT\*)

*We have*

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

## Theorem (DHBBPBSTTTBTT\*)

*We have*

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

\*: Davenport-Heilbronn, Belabas, Belabas-Bhargava-Pomerance, Bhargava-Shankar-Tsimerman, Taniguchi-T., Bhargava-Taniguchi-T.

A fundamental task in this subject is to give some quantitative measures of additive structure in a set, and then investigate to what extent these measures are equivalent to each other. For example, one could try to quantify each of the following informal statements as being some version of the assertion “ $A$  has additive structure”:

- $A + A$  is small;
- $A - A$  is small;
- $A - A$  can be covered by a small number of translates of  $A$ ;
- $kA$  is small for any fixed  $k$ ;
- there are many quadruples  $(a_1, a_2, a_3, a_4) \in A \times A \times A \times A$  such that  $a_1 + a_2 = a_3 + a_4$ ;
- there are many quadruples  $(a_1, a_2, a_3, a_4) \in A \times A \times A \times A$  such that  $a_1 - a_2 = a_3 - a_4$ ;
- the convolution  $1_A * 1_A$  is highly concentrated;
- the subset sums  $FS(A) := \{\sum_{a \in B} a : B \subseteq A\}$  have high multiplicity;
- the Fourier transform  $\widehat{1_A}$  is highly concentrated;
- the Fourier transform  $\widehat{1_A}$  is highly concentrated in a cube;
- $A$  has a large intersection with a generalized arithmetic progression, of size comparable to  $A$ ;
- $A$  is contained in a generalized arithmetic progression, of size comparable to  $A$ ;
- $A$  (or perhaps  $A - A$ , or  $2A - 2A$ ) contains a large generalized arithmetic progression.

The reader is invited to investigate to what extent these informal statements are true for sets such as progressions and cubes, and false for sets such as random sets. As it turns out, once one makes the above assertions more quantitative, there are a number of deep and important equivalences between them; indeed, to oversimplify tremendously, all of the above criteria for additive structure are “essentially”

Tao and Vu, *Additive Combinatorics*, Cambridge Univ. Press, 2006

# The overall program

Let  $\Phi_{p^2} : V(\mathbb{Z}/p^2\mathbb{Z}) \rightarrow \mathbb{C}$  be, for example, the characteristic function of nonmaximal cubic rings.

# The overall program

Let  $\Phi_{p^2} : V(\mathbb{Z}/p^2\mathbb{Z}) \rightarrow \mathbb{C}$  be, for example, the characteristic function of nonmaximal cubic rings.

- Show that  $\Phi_{p^2}$  is nice in some way we can quantify;

# The overall program

Let  $\Phi_{p^2} : V(\mathbb{Z}/p^2\mathbb{Z}) \rightarrow \mathbb{C}$  be, for example, the characteristic function of nonmaximal cubic rings.

- ▶ Show that  $\Phi_{p^2}$  is nice in some way we can quantify;
- ▶ Develop lattice point counting methods which use the niceness.

# An explicit evaluation

## Theorem (Taniguchi-T., 2011)

We have

$$\widehat{\Phi_{p^2}}(v) = \begin{cases} p^{-2} + p^{-3} - p^{-5} & v/p : \text{of type } (0), \\ p^{-3} - p^{-5} & v/p : \text{of type } (1^3), (1^2 1), \\ -p^{-5} & v/p : \text{of type } (111), (21), (3). \\ p^{-3} - p^{-5} & v : \text{of type } (1_{**}^3), \\ -p^{-5} & v : \text{of type } (1_*^3), (1_{\max}^3), \\ 0 & \text{otherwise.} \end{cases}$$

# An explicit evaluation

## Theorem (Taniguchi-T., 2011)

We have

$$\widehat{\Phi_{p^2}}(v) = \begin{cases} p^{-2} + p^{-3} - p^{-5} & v/p : \text{of type } (0), \\ p^{-3} - p^{-5} & v/p : \text{of type } (1^3), (1^2 1), \\ -p^{-5} & v/p : \text{of type } (111), (21), (3). \\ p^{-3} - p^{-5} & v : \text{of type } (1_{**}^3), \\ -p^{-5} & v : \text{of type } (1_*^3), (1_{\max}^3), \\ 0 & \text{otherwise.} \end{cases}$$

So:

$$\frac{1}{p^8} \sum_{v \in V(\mathbb{Z}/p^2\mathbb{Z})} |\widehat{\Phi_{p^2}}(v)| \ll p^{-7}.$$

## Theorem (DHBBPBSTTTBTT)

*We have*

$$N_3(X) = \frac{1}{3\zeta(3)}X + \frac{4(1 + \sqrt{3})\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{\frac{3}{5}+\epsilon}) + O(X^{1-\frac{1}{8-7+2}+\epsilon}).$$

# Methods for proving Fourier transform formulas

# Methods for proving Fourier transform formulas

- ▶ The **group decomposition method** (Mori, Taniguchi-T., Hough);

# Methods for proving Fourier transform formulas

- ▶ The **group decomposition method** (Mori, Taniguchi-T., Hough);
- ▶ The **subspace method** (Taniguchi-T.; Ishimoto);

# Methods for proving Fourier transform formulas

- ▶ The **group decomposition method** (Mori, Taniguchi-T., Hough);
- ▶ The **subspace method** (Taniguchi-T.; Ishimoto);
- ▶ The **morphism method** (Ishitsuka, Taniguchi, T., Xiao).

# Methods for counting lattice points

- ▶ Geometry of Numbers (Gauss, Davenport-Heilbronn, ...)

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)   
General and very widely applicable.   
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)   
Expect best possible results when everything is in place.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)   
General and very widely applicable.   
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)   
Expect best possible results when everything is in place.   
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.
- ▶ **“Simple Harmonic Analysis”** (Belabas-Fouvry, Taniguchi-T., ...)

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.
- ▶ **“Simple Harmonic Analysis”** (Belabas-Fouvry, Taniguchi-T., ...)  
Very effective for lower bound sieves.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.
- ▶ **“Simple Harmonic Analysis”** (Belabas-Fouvry, Taniguchi-T., ...)  
Very effective for lower bound sieves.  
Not designed to produce asymptotics.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.
- ▶ **“Simple Harmonic Analysis”** (Belabas-Fouvry, Taniguchi-T., ...)  
Very effective for lower bound sieves.  
Not designed to produce asymptotics.
- ▶ **Averaging with Fourier analysis** (Anderson-Bhargava-T.)

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.
- ▶ **“Simple Harmonic Analysis”** (Belabas-Fouvry, Taniguchi-T., ...)  
Very effective for lower bound sieves.  
Not designed to produce asymptotics.
- ▶ **Averaging with Fourier analysis** (Anderson-Bhargava-T.)  
Quantitative improvements in Bhargava’s averaging method.

# Methods for counting lattice points

- ▶ **Geometry of Numbers** (Gauss, Davenport-Heilbronn, ...)  
General and very widely applicable.  
Does not deal well with cusps.
- ▶ **Zeta Functions** (Sato-Shintani, Datskovsky-Wright, Yukie, ...)  
Expect best possible results when everything is in place.  
Underlying theory is difficult.
- ▶ **The Averaging Technique** (Bhargava)  
Naturally separates the main body from the cusp.  
Inherits some limitations from the geometry of numbers.
- ▶ **“Simple Harmonic Analysis”** (Belabas-Fouvry, Taniguchi-T., ...)  
Very effective for lower bound sieves.  
Not designed to produce asymptotics.
- ▶ **Averaging with Fourier analysis** (Anderson-Bhargava-T.)  
Quantitative improvements in Bhargava’s averaging method.  
Expect it to work in the same situations.

Thank you!  
धन्यवाद!