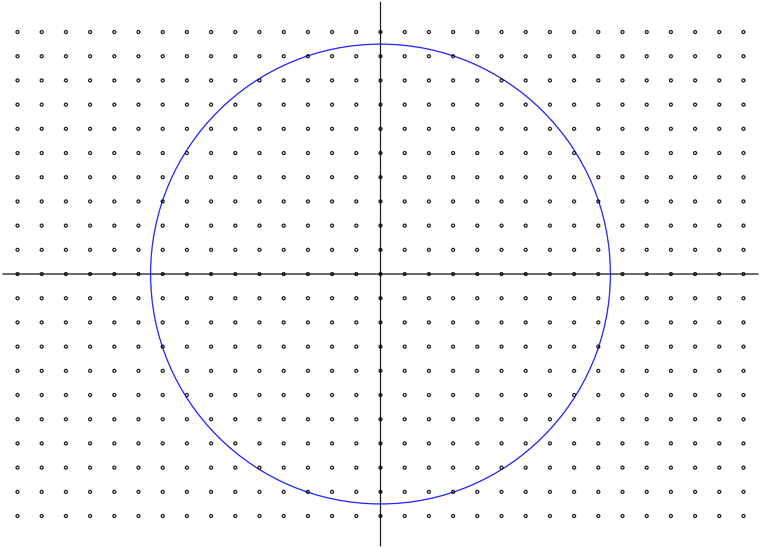
Fourier Analysis in Arithmetic Statistics

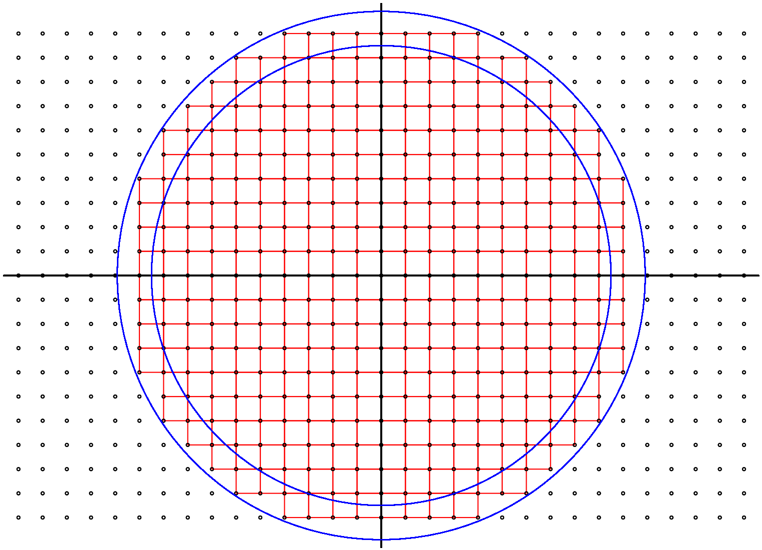
Frank Thorne

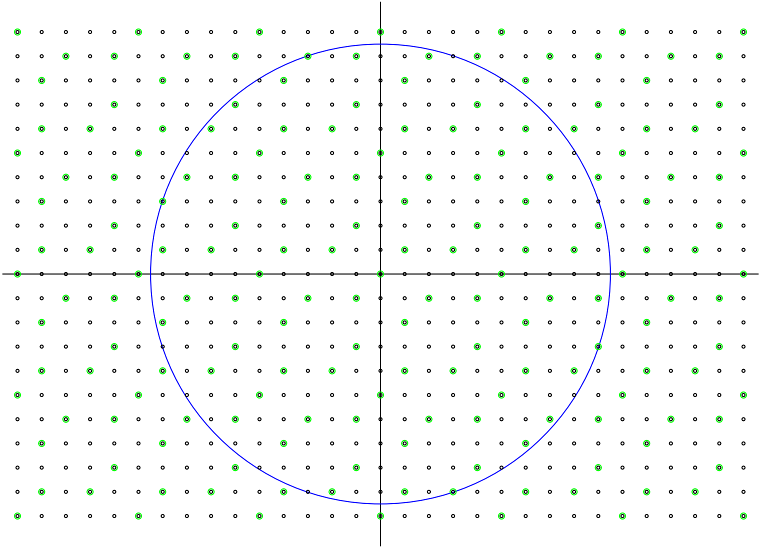
University of South Carolina

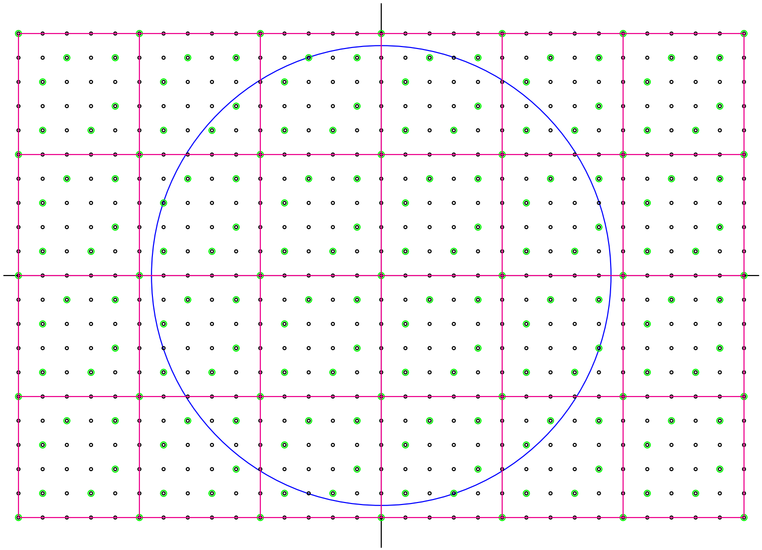
Pittsburgh Number Theory Day, April 18, 2024

thornef.github.io/pitt-2024.pdf









Example: Pólya-Vinogradov

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

Let χ be a primitive Dirichlet character $\pmod{q}$. Then we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < q^{\frac{1}{2}} \log q.$$

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

Let χ be a primitive Dirichlet character $\pmod{q}$. Then we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < q^{\frac{1}{2}} \log q.$$

Proof. By Fourier inversion, we have

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) e^{2\pi i a n/q},$$

with $|\tau(\overline{\chi})| = q^{1/2}$,

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

Let χ be a primitive Dirichlet character $\pmod q$. Then we have

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < q^{\frac{1}{2}} \log q.$$

Proof. By Fourier inversion, we have

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) e^{2\pi i a n / q},$$

with $|\tau(\overline{\chi})| = q^{1/2}$, so that

$$\sum_{n=M+1}^{M+N} \chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q} \overline{\chi}(a) \sum_{n=M+1}^{M+N} e^{2\pi i a n / q},$$

and the innermost sum is a geometric series.

Sample Theorem 1: Counting Cubic Fields

What is "arithmetic statistics"?

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

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

Sample Theorem 2: Counting Quartic and Quintic Fields

Theorem (Bhargava)

We have

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

Theorem (Bhargava)

We have

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

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

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.

Parametrization: The Basic Metatheorem

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.

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* $\pmod{p^2}$*.*

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

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.	$\widetilde{\mathbb{Z}}$	$\mathrm{SL}_1(\mathbb{Z})$	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.

An explicit evaluation

Theorem (Taniguchi-T., 2011)

We have

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

An explicit evaluation

Theorem (Taniguchi-T., 2011)

We have

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

So:

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

Consequence – Improved Davenport-Heilbronn

Theorem (DHBBPBSTTTBTT)

We have

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

Improving the error terms

Theorem (Anderson-Bhargava-T., in progress)

We have

Improving the error terms

Theorem (Anderson-Bhargava-T., in progress)

We have

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

Improving the error terms

Theorem (Anderson-Bhargava-T., in progress)

We have

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

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

Group decomposition (Hough, 2018)

101 / 117 — 100% +

Theorem 2. *The Fourier transform of the maximal set is supported on the mod p orbits $\mathscr{O}_0, \mathscr{O}_{D1^2}, \mathscr{O}_{D11}$ and $\mathscr{O}_{D2}$. It is given explicitly in the following tables.*

(1) *Case $\mathscr{O}_0$, $\xi = p\xi_0$.*

(6.1)

Orbit	$p^{-12}\widehat{\mathbf{1}_{\max}}(p\xi_0)$	*Orbit size*
$\mathscr{O}_0$	$(p-1)^4 p(p+1)^2(p^5+2p^4+4p^3+4p^2+3p+1)$	1
$\mathscr{O}_{D1^2}$	$-(p-1)^3 p(p+1)^4$	$(p-1)(p+1)(p^2+p+1)$
$\mathscr{O}_{D11}$	$-(p-1)^3 p(2p^3+6p^2+4p+1)$	$(p-1)p(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{D2}$	$(p-1)^2 p(2p^2+3p+1)$	$(p-1)^2 p(p+1)(p^2+p+1)/2$
$\mathscr{O}_{Dns}$	$(p-1)^2 p(2p^2+3p+1)$	$(p-1)^2 p^2(p+1)(p^2+p+1)$
$\mathscr{O}_{Cs}$	$-p^7+5p^5-3p^4-3p^3+p^2+p$	$(p-1)^2 p(p+1)^2(p^2+p+1)$
$\mathscr{O}_{Cns}$	$(p-1)^2 p(2p^2+3p+1)$	$(p-1)^2 p^3(p+1)(p^2+p+1)$
$\mathscr{O}_{B11}$	$(p-1)^2 p(2p^2+3p+1)$	$(p-1)^2 p^2(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{B2}$	$(p-1)^2 p(2p^2+3p+1)$	$(p-1)^3 p^2(p+1)(p^2+p+1)/2$
$\mathscr{O}_{1^4}$	$p(p^3-3p^2+p+1)$	$(p-1)^3 p^2(p+1)^2(p^2+p+1)$
$\mathscr{O}_{1^3 1}$	$p(p^3-3p^2+p+1)$	$(p-1)^3 p^3(p+1)^2(p^2+p+1)$
$\mathscr{O}_{1^2 1^2}$	$(p-1)^2 p(3p+1)$	$(p-1)^2 p^4(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{2^2}$	$-(p-1)p(p+1)^2$	$(p-1)^3 p^4(p+1)(p^2+p+1)/2$
$\mathscr{O}_{1^2 11}$	$p(p^3-3p^2+p+1)$	$(p-1)^3 p^4(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{1^2 2}$	$p(p^3-3p^2+p+1)$	$(p-1)^3 p^4(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{1111}$	$-p^3+p^2+p$	$(p-1)^4 p^4(p+1)^2(p^2+p+1)/24$
$\mathscr{O}_{112}$	$-p^3+p^2+p$	$(p-1)^4 p^4(p+1)^2(p^2+p+1)/4$
$\mathscr{O}_{22}$	$-p^3+p^2+p$	$(p-1)^4 p^4(p+1)^2(p^2+p+1)/8$
$\mathscr{O}_{13}$	$-p^3+p^2+p$	$(p-1)^4 p^4(p+1)^2(p^2+p+1)/3$
$\mathscr{O}_{4}$	$-p^3+p^2+p$	$(p-1)^4 p^4(p+1)^2(p^2+p+1)/4$

The Fouvry-Katz Theorem

Let Y be a (locally closed) subscheme of $\mathbb{A}^n_{\mathbb{Z}}$, of dimension d. Take $V = \mathbb{A}^n$, p prime, and Φ_p the the characteristic function of $Y(\mathbb{F}_p)$.

Theorem (Fouvry-Katz, 2001)

There exists a filtration of subschemes

$$\mathbb{A}^n_{\mathbb{Z}} \supseteq X_1 \supseteq \cdots \supseteq X_j \supseteq \cdots \supseteq X_n$$

with X_j of codimension j, so that

$$|\widehat{\Phi_p}(y)| \leq Cp^{-n+\frac{d}{2}+\frac{j-1}{2}}$$

away from $X_j(\mathbb{F}_p)$.

Example: Fouvry-Katz

Corollary (Fouvry-Katz, 2001)

There exist $\gg \frac{X}{\log X}$ *primes* $p \leq X$ *with*

$$\#\mathrm{Cl}(\mathbb{Q}(\sqrt{p+4}))[3] = 1.$$

Example: Fouvry-Katz

Corollary (Fouvry-Katz, 2001)

There exist $\gg \frac{X}{\log X}$ *primes* $p \leq X$ *with*

$$\#\mathrm{Cl}(\mathbb{Q}(\sqrt{p+4}))[3] = 1.$$

(Here $p + 4 \equiv 1 \pmod 4$ and squarefree.)

Binary quartic forms

Let V be the space of binary quartic forms, where $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts by

$$\left(\alpha, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \cdot f(x, y) = \alpha f(ax + cy, bx + dy).$$

Binary quartic forms

Let V be the space of binary quartic forms, where $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts by

$$\left(\alpha, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot f(x, y) = \alpha f(ax + cy, bx + dy).$$

Associate to $f = a_0 x^4 + a_1 x^3 y + a_2 x^2 y^2 + a_3 x y^3 + a_4 y^4$:

$$\begin{aligned} I(f) &= 12 a_0 a_4 - 3 a_1 a_3 + a_2^2, \\ J(f) &= 72 a_0 a_2 a_4 + 9 a_1 a_2 a_3 - 27(a_0 a_3^2 + a_1^2 a_4) - 2 a_2^3. \end{aligned}$$

Binary quartic forms

Let V be the space of binary quartic forms, where $\mathrm{GL}(1) \times \mathrm{GL}(2)$ acts by

$$\left(\alpha, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot f(x, y) = \alpha f(ax + cy, bx + dy).$$

Associate to $f = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$:

$$I(f) = 12a_0a_4 - 3a_1a_3 + a_2^2,$$
$$J(f) = 72a_0a_2a_4 + 9a_1a_2a_3 - 27(a_0a_3^2 + a_1^2a_4) - 2a_2^3.$$

Let Φ_p be the characteristic function of the singular locus:

$$\Phi_p(v) := \begin{cases} 1 & \text{if } \mathrm{Disc}(v) = 0 \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

Theorem (Ishitsuka, Taniguchi, T., Xiao)

For a prime $p > 3$, we have

$$\widehat{\Phi_p}(v) = \begin{cases} p^{-1} + p^{-2} - p^{-3} & (v = 0), \\ p^{-2} - p^{-3} & (v \textit{ has splitting type } (1^4) \textit{ or } (1^3 1)), \\ \chi_{12}(p)(p^{-4} - p^{-3}) & (v \textit{ has splitting type } (1^2 1^2)), \\ \chi_{12}(p)(p^{-4} + p^{-3}) & (v \textit{ has splitting type } (2^2)), \\ \chi_{12}(p) p^{-4} & (v \textit{ has splitting type } (1^2 11) \textit{ or } (1^2 2)), \\ \chi_3(p) \left(\frac{I(v)}{p}\right) \cdot p^{-4} & (J(v) = 0, I(v) \neq 0), \\ a(E_v') p^{-4} & (J(v) \neq 0, \mathrm{Disc}(v) \neq 0). \end{cases}$$

Here E'_v is the elliptic curve defined by

$$y^2 = x^3 - 3I(v)x^2 + J(v)^2,$$

with $a(E'_v) := p + 1 - \#E'_v(\mathbb{F}_p)$.

Main Application for Quartic Forms

Theorem (Ishitsuka, Taniguchi, T., Xiao)

We have

$$\sum_{\substack{E:\ \text{elliptic curve } /\mathbb{Q} \\ H(E)<X \\ \Omega(\mathrm{disc}(E))\leq 4 \\ \mathrm{disc}(E):\ \text{squarefree}}} (|\mathrm{Sel}_2(E)| - 1) \gg \frac{X^{5/6}}{\log X}. \tag{1}$$

Proof of IITTX: Projectivization

If $w \neq 0$, we have

$$\sum_{\substack{w \in \overline{w} \\ w \neq 0}} \langle [w, v] \rangle = \begin{cases} p - 1 & ([w, v] = 0) \\ -1 & ([w, v] \neq 0), \end{cases}$$

where $\overline{w}$ is the line through w and 0. So,

$$\begin{aligned} \widehat{\Phi_p}(v) &= 1 + (p-1) \sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] = 0} \Phi_p(\overline{w}) - \sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] \neq 0} \Phi_p(\overline{w}) \\ &= 1 + p \# X_v(\mathbb{F}_p) - \# X(\mathbb{F}_p), \end{aligned}$$

where

$$\begin{aligned} X &:= \{ w \in \mathbb{P}(V) \mid \mathrm{Disc}(w) = 0 \}, \\ X_v &:= \{ w \in \mathbb{P}(V) \mid \mathrm{Disc}(w) = [w, v] = 0 \}. \end{aligned}$$

Three morphisms

Consider projective morphisms

$$\psi_1 \colon \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathrm{Sym}^2 \mathbb{F}_p^2) \to \mathbb{P}(\mathrm{Sym}^4 \mathbb{F}_p^2) = \mathbb{P}(V)$$
$$(s_0 x + s_1 y, t_0 x^2 + t_1 xy + t_2 y^2) \mapsto (s_0 x + s_1 y)^2 (t_0 x^2 + t_1 xy + t_2 y^2).$$

$$\psi_2 \colon \mathbb{P}(\mathrm{Sym}^2 \mathbb{F}_p^2) \to \mathbb{P}(\mathrm{Sym}^4 \mathbb{F}_p^2) = \mathbb{P}(V)$$
$$t_0 x^2 + t_1 xy + t_2 y^2 \mapsto (t_0 x^2 + t_1 xy + t_2 y^2)^2$$

$$\psi_3 \colon \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathbb{F}_p^2) \to \mathbb{P}(\mathrm{Sym}^4 \mathbb{F}_p^2) = \mathbb{P}(V)$$
$$(s_0 x + s_1 y, t_0 x + t_1 y) \mapsto (s_0 x + s_1 y)^2 (t_0 x + t_1 y)^2.$$

Three morphisms – inverse images

Then, the cardinalities of each $\psi_i(v)$ are:

Spitting type	$\#\psi_1^{-1}$	$\#\psi_2^{-1}$	$\#\psi_3^{-1}$
non-degenerate	0	0	0
(1^4)	1	1	1
$(1^3 1)$	1	0	0
$(1^2 1^2)$	2	1	2
(2^2)	0	1	0
$(1^2 11)$	1	0	0
$(1^2 2)$	1	0	0

Three morphisms – inverse images

Then, the cardinalities of each $\psi_i(v)$ are:

Spitting type	$\#\psi_1^{-1}$	$\#\psi_2^{-1}$	$\#\psi_3^{-1}$
non-degenerate	0	0	0
(1^4)	1	1	1
$(1^3 1)$	1	0	0
$(1^2 1^2)$	2	1	2
(2^2)	0	1	0
$(1^2 1 1)$	1	0	0
$(1^2 2)$	1	0	0

So,

$$\Phi_p(\overline{w}) = \#\psi_1^{-1}(\overline{w}) + \#\psi_2^{-1}(\overline{w}) - \#\psi_3^{-1}(\overline{w}).$$

The elliptic curve

We have

$$\sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] = 0} \# \psi_3^{-1}(\overline{w}) = \# C_3(v),$$

where

$$C_3(v) = \left\{ (l_1, l_2) \in \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathbb{F}_p^2) \mid [l_1^2 l_2^2, v] = 0 \right\}.$$

The elliptic curve

We have

$$\sum_{\overline{w} \in \mathbb{P}(V), [\overline{w}, v] = 0} \# \psi_3^{-1}(\overline{w}) = \# C_3(v),$$

where

$$C_3(v) = \left\{ (l_1, l_2) \in \mathbb{P}(\mathbb{F}_p^2) \times \mathbb{P}(\mathbb{F}_p^2) \mid [l_1^2 l_2^2, v] = 0 \right\}.$$

Proposition (Bhargava-Ho)

If $\mathrm{Disc}(v) \neq 0$ and $J(v) \neq 0$, then $C_3(v)$ is of genus one, isomorphic to

$$E_v' \ : \ y^2 = x^3 - 3I(v)x^2 + J(v)^2.$$