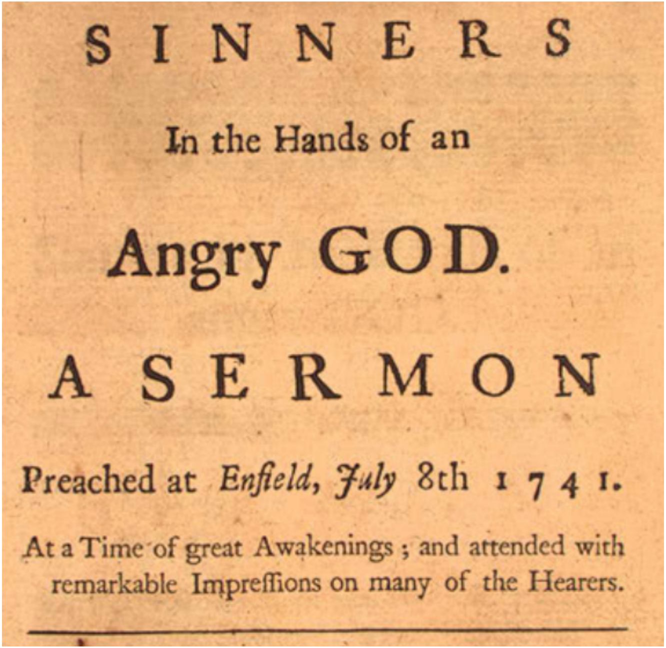
TBA

Frank Thorne

thornef.github.io/sermon-2024.pdf

University of South Carolina



SINNERS

In the Hands of an

Angry GOD.

A SERMON

Preached at *Enfield*, *July* 8th 1741.

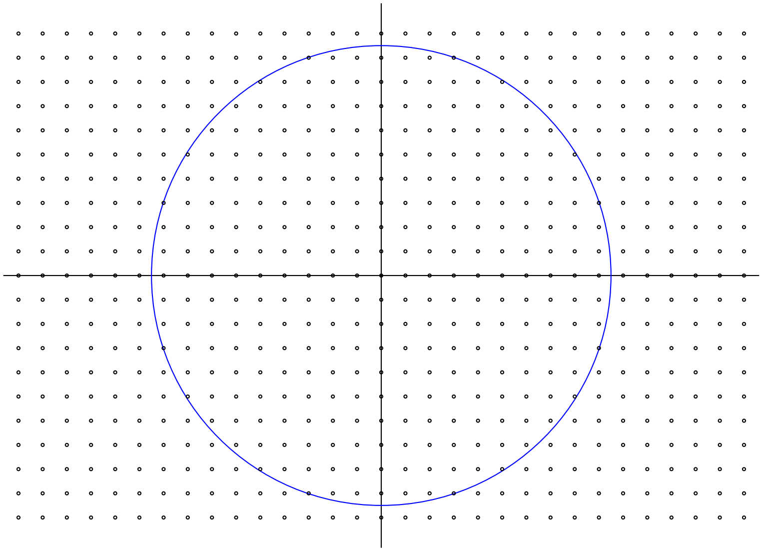
At a Time of great Awakenings; and attended with remarkable Impreſſions on many of the Hearers.

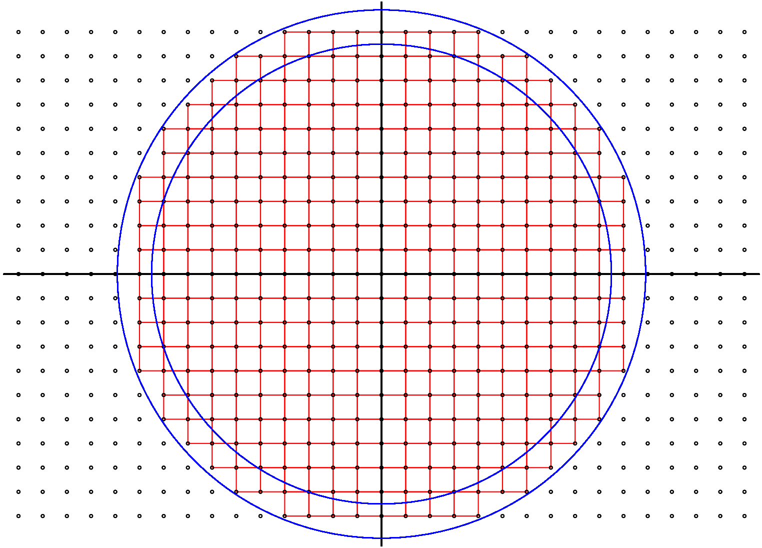
An Exponential Sum Associated to Binary Quartic Forms

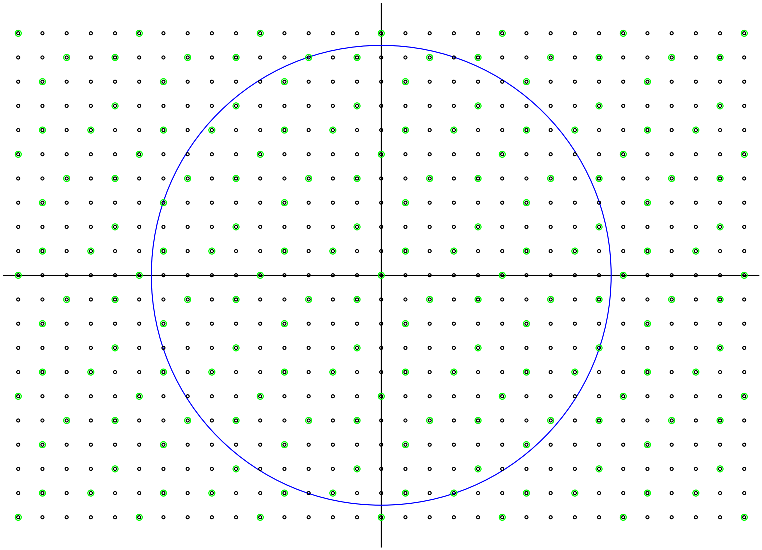
Frank Thorne

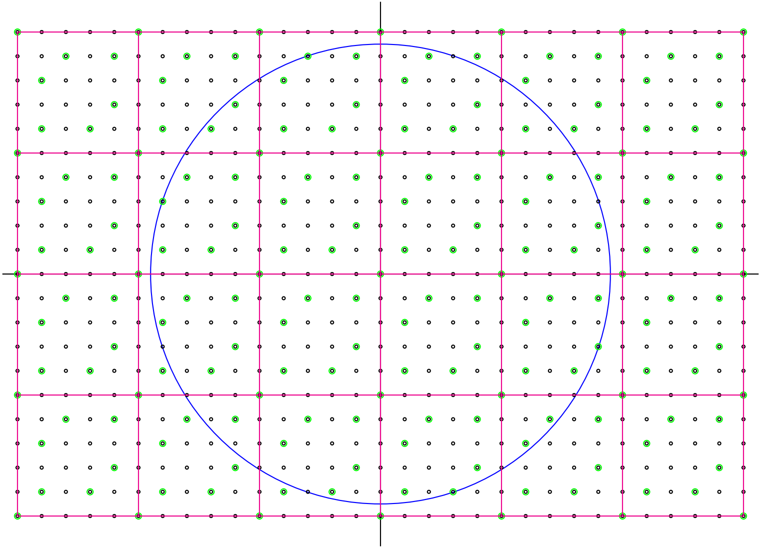
with Yasuhiro Ishitsuka, Takashi Taniguchi, and Stanley Yao Xiao
https://arxiv.org/abs/2404.00541

University of South Carolina









Example: Pólya-Vinogradov

Example: Pólya-Vinogradov

Theorem (Pólya-Vinogradov inequality, special case)

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

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

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.

The standard setup (Bhargava et al.)

We are given:

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary quartic forms);

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary quartic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary quartic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));
- A $G(\mathbb{Z})$-invariant 'discriminant' defined on V;

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary quartic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));
- A $G(\mathbb{Z})$-invariant 'discriminant' defined on V;
- $N(X) :=$ number of $G(\mathbb{Z})$-orbits $v \in V(\mathbb{Z})$ with $0 < |\mathrm{Disc}(v)| < X$;

The standard setup (Bhargava et al.)

We are given:

- A vector space V with an integral structure (e.g. binary quartic forms);
- An algebraic group G acting on V, again with an integral structure (e.g. GL(2));
- A $G(\mathbb{Z})$-invariant 'discriminant' defined on V;
- $N(X) :=$ number of $G(\mathbb{Z})$-orbits $v \in V(\mathbb{Z})$ with $0 < |\mathrm{Disc}(v)| < X$;
- $N(X, q) :=$ above, with congruence conditions $\pmod{q}$.

A proof template

A three-step proof template in arithmetic statistics:

A proof template

A three-step proof template in arithmetic statistics:

3. Apply sieves, etc. to obtain arithmetic consequences.

A proof template

A three-step proof template in arithmetic statistics:

2. Prove results of the shape

$$N(X, q) = \omega(q)X^a + O(X^\alpha q^\beta),$$

   where $\alpha < a$ and $\beta \in \mathbb{R}$ are as small as possible.
3. Apply sieves, etc. to obtain arithmetic consequences.

A proof template

A three-step proof template in arithmetic statistics:

1. Bound or evaluate some Fourier transforms.
2. Prove results of the shape

$$N(X, q) = \omega(q)X^a + O(X^\alpha q^\beta),$$

   where $\alpha < a$ and $\beta \in \mathbb{R}$ are as small as possible.
3. Apply sieves, etc. to obtain arithmetic consequences.

A proof template

A three-step proof template in arithmetic statistics:

1. Bound or evaluate some Fourier transforms.
2. Prove results of the shape

$$N(X, q) = \omega(q)X^a + O(X^\alpha q^\beta),$$

   where $\alpha < a$ and $\beta \in \mathbb{R}$ are as small as possible.
3. Apply sieves, etc. to obtain arithmetic consequences.

Today: Investigate Step 1 further.

The Fourier Transform

Let $\Phi_p : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$ be the characteristic function of our congruence conditions,

The Fourier Transform

Let $\Phi_p : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$ be the characteristic function of our congruence conditions,

... or any other $G(\mathbb{Z}/q\mathbb{Z})$-invariant function.

The Fourier Transform

Let $\Phi_p : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$ be the characteristic function of our congruence conditions,

... or any other $G(\mathbb{Z}/q\mathbb{Z})$-invariant function.

Define

$$\widehat{\Phi_q}(y) := q^{-\dim V} \sum_{x \in V(\mathbb{Z}/q\mathbb{Z})} \Phi(x) e^{2\pi i [x,y]/q}.$$

The Million Pound Poisson Hammer

Theorem (Poisson summation)

For a finite dimensional lattice $V(\mathbb{Z})$, we have

$$\sum_{v \in V(\mathbb{Z})} \phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\phi}(w).$$

Theorem (Poisson summation)

For a finite dimensional lattice $V(\mathbb{Z})$, we have

$$\sum_{v \in V(\mathbb{Z})} \phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\phi}(w).$$

(Subject to pesky convergence issues.)

The Million Pound Poisson Hammer

Theorem (Poisson summation)

For a finite dimensional lattice $V(\mathbb{Z})$, we have

$$\sum_{v \in V(\mathbb{Z})} \phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\phi}(w).$$

(Subject to pesky convergence issues.)

Theorem (Poisson summation with local conditions)

For $\Phi_q : V(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{C}$, we have

$$\sum_{v \in V(\mathbb{Z})} \Phi_q(v)\phi(v) = \sum_{w \in \widehat{V(\mathbb{Z})}} \widehat{\Phi_q}(w)\widehat{\phi}(w/q).$$

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

A simple example (I)

On $V = \mathrm{Sym}^3(\mathbb{F}_p^2)$ (binary cubic forms), let Φ_p be the characteristic function of the singular locus:

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

A simple example (II)

Theorem (Mori 2010)

We have

$$\widehat{\Phi_p}(v) = \begin{cases} p^{-1} + p^{-2} - p^{-3} & (v = 0), \\ p^{-2} - p^{-3} & (v \text{ has splitting type } (1^3) \text{ or } (1^2 1)), \\ -p^{-3} & (\text{otherwise}). \end{cases}$$

A less simple example (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*
$\mathscr{O}_0$	$(p-1)^4p(p+1)^2(p^5+2p^4+4p^3+4p^2+3p+1)$	1
$\mathscr{O}_{D1^2}$	$-(p-1)^3p(p+1)^4$	$(p-1)(p+1)(p^2+p+1)$
$\mathscr{O}_{D11}$	$-(p-1)^3p(2p^3+6p^2+4p+1)$	$(p-1)p(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{D2}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p(p+1)(p^2+p+1)/2$
$\mathscr{O}_{Dns}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p^2(p+1)(p^2+p+1)$
$\mathscr{O}_{Cs}$	$-p^7+5p^5-3p^4-3p^3+p^2+p$	$(p-1)^2p(p+1)^2(p^2+p+1)$
$\mathscr{O}_{Cns}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p^3(p+1)(p^2+p+1)$
$\mathscr{O}_{B11}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^2p^2(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{B2}$	$(p-1)^2p(2p^2+3p+1)$	$(p-1)^3p^2(p+1)(p^2+p+1)/2$
$\mathscr{O}_{1^4}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^2(p+1)^2(p^2+p+1)$
$\mathscr{O}_{1^31}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^3(p+1)^2(p^2+p+1)$
$\mathscr{O}_{1^21^2}$	$(p-1)^2p(3p+1)$	$(p-1)^2p^4(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{2^2}$	$-(p-1)p(p+1)^2$	$(p-1)^3p^4(p+1)(p^2+p+1)/2$
$\mathscr{O}_{1^211}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^4(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{1^22}$	$p(p^3-3p^2+p+1)$	$(p-1)^3p^4(p+1)^2(p^2+p+1)/2$
$\mathscr{O}_{1111}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/24$
$\mathscr{O}_{112}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/4$
$\mathscr{O}_{22}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/8$
$\mathscr{O}_{13}$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/3$
$\mathscr{O}_4$	$-p^3+p^2+p$	$(p-1)^4p^4(p+1)^2(p^2+p+1)/4$

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

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

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

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

Let Φ_p be the characteristic function of the singular locus:

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

Main Theorem for Quartic Forms

Theorem (Ishitsuka, Taniguchi, T., Xiao)

For a prime $p > 3$, we have

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

Here E_v' is the elliptic curve defined by

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

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

Proof of ITTX: 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

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

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

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

Theorem

We have

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

An application

Theorem

We have

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

Moreover, we obtain only squarefree discriminants $\mathrm{disc}(E)$ in the above.

An application

Theorem

We have

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

Moreover, we obtain only squarefree discriminants $\mathrm{disc}(E)$ in the above.

Main ingredient: Bhargava-Shankar parametrization of $\mathrm{Sel}_2(E)$ in terms of $\mathrm{PGL}_2(\mathbb{Q})$-orbits on integral binary quartic forms.

An application (2)

More ingredients:

An application (2)

More ingredients:

- Bounds for $\sum |\widehat{\Phi_q}(v)|$ over boxes of side length smaller than q.

An application (2)

More ingredients:

- Bounds for $\sum |\widehat{\Phi_q}(v)|$ over boxes of side length smaller than q.
- A tail estimate due to Shankar, Shankar, and Wang for when $\mathrm{disc}(E)$ has a large prime square factor.

An application (2)

More ingredients:

- Bounds for $\sum |\widehat{\Phi_q}(v)|$ over boxes of side length smaller than q.
- A tail estimate due to Shankar, Shankar, and Wang for when $\mathrm{disc}(E)$ has a large prime square factor.
- Control the difference between $\mathrm{GL}_2(\mathbb{Z})$ and $\mathrm{PGL}_2(\mathbb{Q})$.

An application (2)

More ingredients:

- Bounds for $\sum |\widehat{\Phi_q}(v)|$ over boxes of side length smaller than q.
- A tail estimate due to Shankar, Shankar, and Wang for when $\mathrm{disc}(E)$ has a large prime square factor.
- Control the difference between $\mathrm{GL}_2(\mathbb{Z})$ and $\mathrm{PGL}_2(\mathbb{Q})$.
- Some 2- and 3-adic conditions to avoid some technicalities.

Thank you!