Exponential sums, hypersurfaces with many symmetries and Galois representations

Gabriel Chênevert

McGill University Ph.D. thesis oral defense

August 22, 2008

Equidistribution of exponential sums

Equidistribution of exponential sums

Given $q = p^r$ a prime power, consider the additive character

$$\psi_q : (\mathbb{F}_q, +) \longrightarrow (\mathbb{C}, \times), \qquad \psi_q(x) := \exp\left(\frac{2\pi i}{p}\,\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right).$$

Equidistribution of exponential sums

Given $q = p^r$ a prime power, consider the additive character

$$\psi_q : (\mathbb{F}_q, +) \longrightarrow (\mathbb{C}, \times), \qquad \psi_q(x) := \exp\left(\frac{2\pi i}{p}\operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right).$$

For $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \neq 0$ and ℓ a prime number, define

$$B_\ell(q; \alpha, \beta) := \sum_{x \in \mathbb{F}_q} \psi_q\big(\alpha x^{\ell+1} + \beta x\big) \in \mathbb{C}.$$

Equidistribution of exponential sums

Given $q = p^r$ a prime power, consider the additive character

$$\psi_q : (\mathbb{F}_q, +) \longrightarrow (\mathbb{C}, \times), \qquad \psi_q(x) := \exp\left(\frac{2\pi i}{p}\,\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right).$$

For $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \neq 0$ and ℓ a prime number, define

$$B_\ell(q; \alpha, \beta) := \sum_{x \in \mathbb{F}_q} \psi_q\big(\alpha x^{\ell+1} + \beta x\big) \in \mathbb{C}.$$

Weil estimate: $|B_\ell(q; \alpha, \beta)| \leq \ell\sqrt{q}$ provided $p > \ell + 1$.

Equidistribution of exponential sums

Given $q = p^r$ a prime power, consider the additive character

$$\psi_q : (\mathbb{F}_q, +) \longrightarrow (\mathbb{C}, \times), \qquad \psi_q(x) := \exp\left(\frac{2\pi i}{p} \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right).$$

For $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \neq 0$ and ℓ a prime number, define

$$B_\ell(q; \alpha, \beta) := \sum_{x \in \mathbb{F}_q} \psi_q\big(\alpha x^{\ell+1} + \beta x\big) \in \mathbb{C}.$$

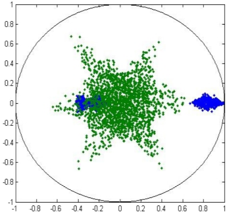
Weil estimate: $|B_\ell(q; \alpha, \beta)| \leq \ell\sqrt{q}$ provided $p > \ell + 1$.

We want to understand how the normalized exponential sums

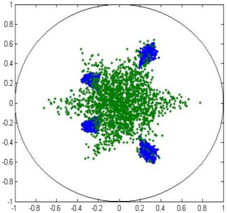
$$b_\ell(q; \alpha, \beta) := \frac{B_\ell(q; \alpha, \beta)}{\ell\sqrt{q}} \in \mathbb{D}$$

are distributed, on average, as $q \to \infty$.

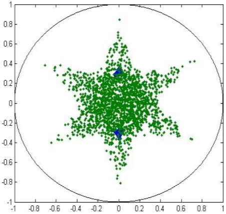
Example: Some of the multisets $\{b_3(p;\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_p, \alpha \neq 0\}$.



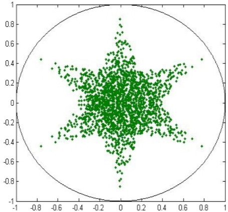
p = 1993



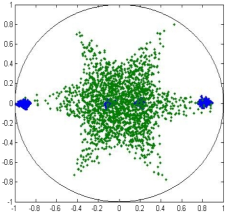
p = 1997



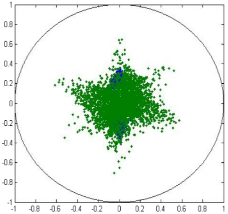
p = 1999



p = 2011



p = 2017



p = 2999

Precise meaning:

Precise meaning:

Let $\mu_\ell(q)$ denote the counting probability measure on $\mathbb{D}$ associated to the multiset

$$\{b_\ell(q; \alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_q, \alpha \neq 0\}.$$

Precise meaning:

Let $\mu_\ell(q)$ denote the counting probability measure on $\mathbb{D}$ associated to the multiset

$$\{b_\ell(q;\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_q, \alpha \neq 0\}.$$

We want to understand the behaviour as $q \to \infty$ of $\mu_\ell(q)$.

Precise meaning:

Let $\mu_\ell(q)$ denote the counting probability measure on $\mathbb{D}$ associated to the multiset

$$\{b_\ell(q;\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_q, \alpha \neq 0\}.$$

We want to understand the behaviour as $q \to \infty$ of $\mu_\ell(q)$.

Convention: $p \to \infty$ as $q \to \infty$.

Precise meaning:

Let $\mu_\ell(q)$ denote the counting probability measure on $\mathbb{D}$ associated to the multiset

$$\{b_\ell(q;\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_q, \alpha \neq 0\}.$$

We want to understand the behaviour as $q \to \infty$ of $\mu_\ell(q)$.

Convention: $p \to \infty$ as $q \to \infty$.

Theorem (Livné) $$\lim_{q\to\infty} \mu_2(q) = \mu_{\mathrm{ST}},$$

where $\mu_{\mathrm{ST}} = \frac{2}{\pi}\sqrt{1-x^2}dx$ *is the Sato-Tate measure on* $[-1,1]$.

Idea (Birch):

Idea (Birch):

Study the distributions $\mu_\ell(q)$ through their moments, which can be related to the number of $\mathbb{F}_q$-rational points on certain algebraic varieties.

Idea (Birch):

Study the distributions $\mu_\ell(q)$ through their moments, which can be related to the number of $\mathbb{F}_q$-rational points on certain algebraic varieties.

In Livné's case ($\ell = 2$):

$$W_m : \quad \sum_{i=1}^{m} x_i = \sum_{i=1}^{m} x_i^3 = 0 \quad \text{in} \quad \mathbb{P}^{m-1}.$$

Idea (Birch):

Study the distributions $\mu_\ell(q)$ through their moments, which can be related to the number of $\mathbb{F}_q$-rational points on certain algebraic varieties.

In Livné's case ($\ell = 2$):

$$W_m : \quad \sum_{i=1}^{m} x_i = \sum_{i=1}^{m} x_i^3 = 0 \quad \text{in} \quad \mathbb{P}^{m-1}.$$

For general ℓ:

$$W_\ell^{m,n} : \quad \sum_{i=1}^{m} x_i - \sum_{j=1}^{n} y_i = \sum_{i=1}^{m} x_i^{\ell+1} - \sum_{j=1}^{n} y_i^{\ell+1} = 0 \quad \text{in} \quad \mathbb{P}^{m+n-1}.$$

Idea (Birch):

Study the distributions $\mu_\ell(q)$ through their moments, which can be related to the number of $\mathbb{F}_q$-rational points on certain algebraic varieties.

In Livné's case ($\ell = 2$):

$$W_m : \quad \sum_{i=1}^{m} x_i = \sum_{i=1}^{m} x_i^3 = 0 \quad \text{in} \quad \mathbb{P}^{m-1}.$$

For general ℓ:

$$W_\ell^{m,n} : \quad \sum_{i=1}^{m} x_i - \sum_{j=1}^{n} y_i = \sum_{i=1}^{m} x_i^{\ell+1} - \sum_{j=1}^{n} y_i^{\ell+1} = 0 \quad \text{in} \quad \mathbb{P}^{m+n-1}.$$

Idea (Birch):

Study the distributions $\mu_\ell(q)$ through their moments, which can be related to the number of $\mathbb{F}_q$-rational points on certain algebraic varieties.

In Livné's case ($\ell = 2$):

$$W_m : \quad \sum_{i=1}^m x_i = \sum_{i=1}^m x_i^3 = 0 \quad \text{in} \quad \mathbb{P}^{m-1}.$$

For general ℓ:

$$W_\ell{}^{m,n} : \quad \sum_{i=1}^m x_i - \sum_{j=1}^n y_i = \sum_{i=1}^m x_i^{\ell+1} - \sum_{j=1}^n y_i^{\ell+1} = 0 \quad \text{in} \quad \mathbb{P}^{m+n-1}.$$

Let $M_\ell^{m,n}(q)$ denote the (m,n)-th moment of $\mu_\ell(q)$, i.e.

$$M_\ell^{m,n}(q) = \int_{\mathbb{D}} z^m \bar{z}^n d\mu_\ell(q)$$

Let $M_\ell^{m,n}(q)$ denote the (m,n)-th moment of $\mu_\ell(q)$, i.e.

$$\begin{aligned} M_\ell^{m,n}(q) &= \int_{\mathbb{D}} z^m \bar{z}^n d\mu_\ell(q) \\ &= \frac{1}{q(q-1)} \sum_{\alpha \neq 0, \beta} b_\ell(q;\alpha,\beta)^m \overline{b_\ell(q;\alpha,\beta)}^n . \end{aligned}$$

Let $M_\ell^{m,n}(q)$ denote the (m,n)-th moment of $\mu_\ell(q)$, i.e.

$$\begin{aligned} M_\ell^{m,n}(q) &= \int_{\mathbb{D}} z^m \bar{z}^n d\mu_\ell(q) \\ &= \frac{1}{q(q-1)} \sum_{\alpha \neq 0, \beta} b_\ell(q;\alpha,\beta)^m \overline{b_\ell(q;\alpha,\beta)}^n. \end{aligned}$$

Lemma

$$M_\ell^{m,n}(q) = \frac{1}{\ell^N q^{N/2}} \left(|W_\ell^{m,n}(\mathbb{F}_q)| - \frac{q^{N-2}-1}{q-1} \right), \quad N = m+n.$$

Let $M_\ell^{m,n}(q)$ denote the (m,n)-th moment of $\mu_\ell(q)$, i.e.

$$\begin{aligned} M_\ell^{m,n}(q) &= \int_{\mathbb{D}} z^m \bar{z}^n d\mu_\ell(q) \\ &= \frac{1}{q(q-1)} \sum_{\alpha \neq 0, \beta} b_\ell(q;\alpha,\beta)^m \overline{b_\ell(q;\alpha,\beta)}^n. \end{aligned}$$

Lemma

$$M_\ell^{m,n}(q) = \frac{1}{\ell^N q^{N/2}} \left(|W_\ell^{m,n}(\mathbb{F}_q)| - \frac{q^{N-2}-1}{q-1} \right), \quad N = m+n.$$

Lefschetz trace formula: $|W_\ell^{m,n}(\mathbb{F}_q)|$ can be studied via the action of Frobenius on the étale cohomology groups $H^\bullet(W_\ell^{m,n})$.

The symmetric hypersurfaces $W_\ell^{m,n}$

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$
- dimension $N - 3$

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$
- dimension $N - 3$
- admits a projective action of $S_m \times S_n$.

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$
- dimension $N - 3$
- admits a projective action of $S_m \times S_n$.

Let $p > N$ be a prime which is inert in $\mathbb{Q}(\zeta_\ell)$, i.e. $\mathbb{F}_\ell^\times = \langle p \rangle$.

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$
- dimension $N - 3$
- admits a projective action of $S_m \times S_n$.

Let $p > N$ be a prime which is inert in $\mathbb{Q}(\zeta_\ell)$, i.e. $\mathbb{F}_\ell^\times = \langle p \rangle$.

- $W_\ell^{m,n}$ has good reduction at p whenever $m \not\equiv n \mod \ell$.

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$
- dimension $N - 3$
- admits a projective action of $S_m \times S_n$.

Let $p > N$ be a prime which is inert in $\mathbb{Q}(\zeta_\ell)$, i.e. $\mathbb{F}_\ell^\times = \langle p \rangle$.

- $W_\ell^{m,n}$ has good reduction at p whenever $m \not\equiv n \mod \ell$.
- When $m \equiv n \mod \ell$, the reduction of $W_\ell^{m,n}$ at p acquires ordinary double points (tangent cone is a smooth quadric).

The symmetric hypersurfaces $W_\ell^{m,n}$

$W_\ell^{m,n}$: smooth projective hypersurface over $\mathbb{Q}$

- degree $\ell + 1$
- dimension $N - 3$
- admits a projective action of $S_m \times S_n$.

Let $p > N$ be a prime which is inert in $\mathbb{Q}(\zeta_\ell)$, i.e. $\mathbb{F}_\ell^\times = \langle p \rangle$.

- $W_\ell^{m,n}$ has good reduction at p whenever $m \not\equiv n \mod \ell$.
- When $m \equiv n \mod \ell$, the reduction of $W_\ell^{m,n}$ at p acquires ordinary double points (tangent cone is a smooth quadric).

In that case, the blow-up $\widetilde{W}_\ell^{m,n}$ along the singularities is smooth.

Cohomology of $\widetilde{W}_\ell^{m,n}$ (Schoen):

Cohomology of $\widetilde{W}_\ell^{m,n}$ (Schoen):

- primitive cohomology in middle degree $(N-3)$;

Cohomology of $\widetilde{W}_\ell^{m,n}$ (Schoen):

- primitive cohomology in middle degree $(N-3)$;
- "subprimitive cohomology" in next-to-middle degrees coming from the primitive cohomology of the exceptional fibers (smooth quadrics).

Cohomology of $\widetilde{W}_\ell^{m,n}$ (Schoen):

- primitive cohomology in middle degree $(N-3)$;
- "subprimitive cohomology" in next-to-middle degrees coming from the primitive cohomology of the exceptional fibers (smooth quadrics).

Theorem

If $q = p^r$ with p inert in $\mathbb{Q}(\zeta_\ell)$,

$$M_\ell^{m,n}(q) = \pm \frac{1}{\ell^N} \dim H_{sub}^{N-4}(\widetilde{W}_\ell^{m,n}) + O\left(\frac{1}{\sqrt{q}}\right).$$

Cohomology of $\widetilde{W}_\ell^{m,n}$ (Schoen):

- primitive cohomology in middle degree $(N-3)$;
- "subprimitive cohomology" in next-to-middle degrees coming from the primitive cohomology of the exceptional fibers (smooth quadrics).

Theorem

If $q = p^r$ with p inert in $\mathbb{Q}(\zeta_\ell)$,

$$M_\ell^{m,n}(q) = \pm \frac{1}{\ell^N} \dim H_{sub}^{N-4}(\widetilde{W}_\ell^{m,n}) + O\left(\frac{1}{\sqrt{q}}\right).$$

Remark: The subprimitive cohomology vanishes unless

$$n \equiv m \bmod \ell \quad \text{and} \quad n \equiv m \bmod 2.$$

Formula for the primitive character:

Formula for the primitive character:

In the smooth case, the character χ_{pr} of the action of $S_m \times S_n$ on $H^{N-3}_{\mathrm{pr}}(W^{m,n}_{\ell})$ can be computed using the Lefschetz fixed point formula.

Formula for the primitive character:

In the smooth case, the character χ_{pr} of the action of $S_m \times S_n$ on $H^{N-3}_{\mathrm{pr}}(W^{m,n}_{\ell})$ can be computed using the Lefschetz fixed point formula.

For $\sigma \in S_N$, $d \geq 1$, let $m_d(\sigma)$ denote the number of cycles in the cycle decomposition of σ whose length is divisible by d.

Formula for the primitive character:

In the smooth case, the character χ_{pr} of the action of $S_m \times S_n$ on $H^{N-3}_{\mathrm{pr}}(W^{m,n}_\ell)$ can be computed using the Lefschetz fixed point formula.

For $\sigma \in S_N$, $d \geq 1$, let $m_d(\sigma)$ denote the number of cycles in the cycle decomposition of σ whose length is divisible by d.

Theorem

Suppose $m \not\equiv n \bmod \ell$. For $\sigma \in S_m \times S_n \hookrightarrow S_N$, we have

$$\chi_{\mathrm{pr}}(\sigma) = (-1)^{N+1} \frac{(1-\ell)^{m_1(\sigma)-1} - (1-\ell)^{m_\ell(\sigma)+1}}{\ell}.$$

Formula for the primitive character:

In the smooth case, the character χ_{pr} of the action of $S_m \times S_n$ on $H^{N-3}_{\mathrm{pr}}(W^{m,n}_\ell)$ can be computed using the Lefschetz fixed point formula.

For $\sigma \in S_N$, $d \geq 1$, let $m_d(\sigma)$ denote the number of cycles in the cycle decomposition of σ whose length is divisible by d.

Theorem

Suppose $m \not\equiv n \bmod \ell$. For $\sigma \in S_m \times S_n \hookrightarrow S_N$, we have

$$\chi_{\mathrm{pr}}(\sigma) = (-1)^{N+1} \frac{(1-\ell)^{m_1(\sigma)-1} - (1-\ell)^{m_\ell(\sigma)+1}}{\ell}.$$

Example: $H^4_{\mathrm{pr}}(W_7) \cong 2 \cdot \mathrm{sg} \oplus \theta_6 \oplus \theta_{14}$, where θ_6 and θ_{14} are irreducible representations of S_7 of degree 6 and 14, respectively.

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

- unramified outside $\{3, 5, 7\}$;

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

- unramified outside $\{3, 5, 7\}$;
- $\det \rho = \varepsilon_{35} \otimes \chi_{\mathrm{cycl}}$

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

- unramified outside $\{3, 5, 7\}$;
- $\det \rho = \varepsilon_{35} \otimes \chi_{\mathrm{cycl}}$, ε_{35}: quadratic character of conductor 35.

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

- unramified outside $\{3, 5, 7\}$;
- $\det \rho = \varepsilon_{35} \otimes \chi_{\mathrm{cycl}}$, ε_{35}: quadratic character of conductor 35.

Numerical evidence: We seem to have

$$\mathrm{tr}(Frob_p) = a_p(f), \quad \text{for } p \neq 3, 5, 7,$$

$$f(q) = 1 + q^3 - 5q^5 + 7q^7 + q^9 - 13q^{11} + \cdots \in S_3(35, \varepsilon_{35}).$$

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W^7_2)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

- unramified outside $\{3, 5, 7\}$;
- $\det \rho = \varepsilon_{35} \otimes \chi_{\mathrm{cycl}}$, ε_{35}: quadratic character of conductor 35.

Numerical evidence: We seem to have

$$\mathrm{tr}(Frob_p) = a_p(f), \quad \text{for } p \neq 3, 5, 7,$$

$$f(q) = 1 + q^3 - 5q^5 + 7q^7 + q^9 - 13q^{11} + \cdots \in S_3(35, \varepsilon_{35}).$$

Deligne's construction: $\rho \overset{?}{\sim} \rho_f$

Modularity and the Faltings-Serre method

Let ρ be the 2-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$H^4_{\mathrm{pr}}(W_2^7)_{\mathsf{sg}}(-1).$$

(Actually: compatible system of ℓ-adic Galois representations.)

- unramified outside $\{3, 5, 7\}$;
- $\det \rho = \varepsilon_{35} \otimes \chi_{\mathrm{cycl}}$, ε_{35}: quadratic character of conductor 35.

Numerical evidence: We seem to have

$$\mathrm{tr}(Frob_p) = a_p(f), \quad \text{for } p \neq 3, 5, 7,$$

$$f(q) = 1 + q^3 - 5q^5 + 7q^7 + q^9 - 13q^{11} + \cdots \in S_3(35, \varepsilon_{35}).$$

Deligne's construction: $\rho \overset{?}{\sim} \rho_f$ (up to semi-simplification.)

Let K be a number field, S a finite set of primes of K, and

$$\rho_1, \rho_2 : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

two continuous representations unramified outside S such that

$$\rho_1 \equiv \rho_2 \bmod \ell.$$

Let K be a number field, S a finite set of primes of K, and

$$\rho_1, \rho_2 : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

two continuous representations unramified outside S such that

$$\rho_1 \equiv \rho_2 \bmod \ell.$$

Definition

A subset $\Sigma \subseteq G_K$ is *sufficient* if

$$\left.\begin{array}{r} \operatorname{tr} \rho_1(\sigma) = \operatorname{tr} \rho_2(\sigma) \\ \det \rho_1(\sigma) = \det \rho_2(\sigma) \end{array}\right\} \text{ for all } \sigma \in \Sigma \implies \rho_1 \sim \rho_2.$$

Let K be a number field, S a finite set of primes of K, and

$$\rho_1, \rho_2 : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

two continuous representations unramified outside S such that

$$\rho_1 \equiv \rho_2 \bmod \ell.$$

Definition

A subset $\Sigma \subseteq G_K$ is *sufficient* if

$$\left.\begin{array}{r} \operatorname{tr} \rho_1(\sigma) = \operatorname{tr} \rho_2(\sigma) \\ \det \rho_1(\sigma) = \det \rho_2(\sigma) \end{array}\right\} \text{ for all } \sigma \in \Sigma \implies \rho_1 \sim \rho_2.$$

Faltings-Serre method: There exists a *finite* sufficient set Σ depending only on S, ℓ and $\overline{\rho}_i$.

Theorem

Suppose $\ell = 2$*, and let* H *denote the common image of* $\overline{\rho}_i$ *in* $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

Theorem

Suppose $\ell = 2$*, and let* H *denote the common image of* $\overline{\rho}_i$ *in* $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$*. Let* Σ *be a subset of* G_K *which surjects onto* $\overline{G}$*, and in addition,*

Theorem

Suppose $\ell = 2$, *and let* H *denote the common image of* $\overline{\rho}_i$ *in* $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. *Let* Σ *be a subset of* G_K *which surjects onto* $\overline{G}$, *and in addition,*

- *if* $|H| \leq 2$*: onto the greatest quotient of exponent 2 of* G *(Faltings-Serre-Livné)*

Theorem

Suppose $\ell = 2$*, and let* H *denote the common image of* $\overline{\rho}_i$ *in* $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$*. Let* Σ *be a subset of* G_K *which surjects onto* $\overline{G}$*, and in addition,*

- *if* $|H| \leq 2$*: onto the greatest quotient of exponent 2 of* G *(Faltings-Serre-Livné)*
- *if* $|H| = 3$*: an element of order 6 in every intermediate quotient* $\mathbb{Z}/2\mathbb{Z} \times H \cong \mathbb{Z}/6\mathbb{Z}$*;*

Theorem

Suppose $\ell = 2$, and let H denote the common image of $\overline{\rho}_i$ in $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. Let Σ be a subset of G_K which surjects onto $\overline{G}$, and in addition,

- *if $|H| \leq 2$: onto the greatest quotient of exponent 2 of G (Faltings-Serre-Livné)*
- *if $|H| = 3$: an element of order 6 in every intermediate quotient $\mathbb{Z}/2\mathbb{Z} \times H \cong \mathbb{Z}/6\mathbb{Z}$;*
- *if $H \cong S_3$: an element of order ≥ 3 in every intermediate quotient Q of the form $H \times \mathbb{Z}/2\mathbb{Z}$ or*

$$1 \longrightarrow V_4 \longrightarrow Q \longrightarrow \overline{G} \longrightarrow 1.$$

Theorem

Suppose $\ell = 2$, and let H denote the common image of $\overline{\rho}_i$ in $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. Let Σ be a subset of G_K which surjects onto $\overline{G}$, and in addition,

- *if $|H| \leq 2$: onto the greatest quotient of exponent 2 of G (Faltings-Serre-Livné)*
- *if $|H| = 3$: an element of order 6 in every intermediate quotient $\mathbb{Z}/2\mathbb{Z} \times H \cong \mathbb{Z}/6\mathbb{Z}$;*
- *if $H \cong S_3$: an element of order ≥ 3 in every intermediate quotient Q of the form $H \times \mathbb{Z}/2\mathbb{Z}$ or*

$$1 \longrightarrow V_4 \longrightarrow Q \longrightarrow \overline{G} \longrightarrow 1.$$

Then Σ is sufficient.

Theorem

Suppose $\ell = 2$, and let H denote the common image of $\overline{\rho}_i$ in $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. Let Σ be a subset of G_K which surjects onto $\overline{G}$, and in addition,

- *if $|H| \leq 2$: onto the greatest quotient of exponent 2 of G (Faltings-Serre-Livné)*
- *if $|H| = 3$: an element of order 6 in every intermediate quotient $\mathbb{Z}/2\mathbb{Z} \times H \cong \mathbb{Z}/6\mathbb{Z}$;*
- *if $H \cong S_3$: an element of order ≥ 3 in every intermediate quotient Q of the form $H \times \mathbb{Z}/2\mathbb{Z}$ or*

$$1 \longrightarrow V_4 \longrightarrow Q \longrightarrow \overline{G} \longrightarrow 1.$$

Then Σ is sufficient.