On the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$

Samir Siksek
joint work with Samuele Anni

University of Warwick

29 June 2015

Generalized Fermat Equation

$x^p + y^q = z^r, \qquad (p,\ q,\ r \in \mathbb{Z}_{\geq 2}).$ Solution (x, y, z) is

1. **non-trivial** if $xyz \neq 0$.
2. **primitive** if $\gcd(x, y, z) = 1$.

Conjecture (Darmon & Granville, Tijdeman, Zagier, Beal)

Suppose $p^{-1} + q^{-1} + r^{-1} < 1$. The only non-trivial primitive solutions to $x^p + y^q = z^r$ are

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7, \qquad 9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2, \qquad 33^8 + 1549034^2 = 15613^3.$$

Poonen–Schaefer–Stoll: $(2, 3, 7)$.
Bruin: $(2, 3, 8)$, $(2, 8, 3)$, $(2, 3, 9)$, $(2, 4, 5)$, $(2, 5, 4)$.
Many others ...

Infinite Families of Exponents

Wiles: (p, p, p).

Darmon and Merel: $(p, p, 2)$, $(p, p, 3)$.

Many other infinite families by many people ...

All infinite families use Frey curves, modularity and level-lowering over $\mathbb{Q}$ (or $\mathbb{Q}$-curves).

Naïve idea

$x^p + y^p = z^\ell$ (solve Fermat and Catalan at the same time).

$$(x+y)(x+\zeta y)\dots(x+\zeta^{p-1}y) = z^\ell\,.$$

$$x+\zeta^j y = \alpha_j \xi_j^\ell, \qquad \alpha_j \in \text{finite set.}$$

$$\exists \epsilon_j \in \mathbb{Q}(\zeta) \qquad : \qquad \epsilon_0\,(x+y) + \epsilon_1\,(x+\zeta y) + \epsilon_2\,(x+\zeta^2 y) = 0\,.$$

$$\therefore \quad \gamma_0\xi_0^\ell + \gamma_1\xi_1^\ell + \gamma_2\xi_2^\ell = 0 \qquad (\gamma_0,\gamma_1,\gamma_2) \in \text{finite set.}$$

Looks like $x^\ell + y^\ell + z^\ell = 0$ solved by Wiles.

Problem 1: trivial solutions $(1,0,1)$ and $(0,1,1)$ become non-trivial.

Problem 2: weak modularity thms over non-totally real fields.

Improvement: Freitas

$x^p + y^p = z^\ell$ factor LHS over $K := \mathbb{Q}(\zeta + \zeta^{-1})$.

$$(x+y) \prod_{j=1}^{(p-1)/2} \left(x^2 + y^2 + \theta_j xy\right) = z^\ell \qquad \theta_j := \zeta^j + \zeta^{-j} \in K.$$

$$x + y = \alpha_0\, \xi_0^\ell, \qquad \underbrace{(x^2 + y^2) + \theta_j xy}_{f_j(x,y)} = \alpha_j \xi_j^\ell, \qquad \alpha_j \in \text{finite set.}$$

$$\exists \epsilon_j \in K \qquad : \qquad \epsilon_0\,(x+y)^2 + \epsilon_1\, f_1(x,y) + \epsilon_2\, f_2(x,y) = 0\,.$$

$$\therefore \quad \gamma_0 \xi_0^{2\ell} + \gamma_1 \xi_1^\ell + \gamma_2 \xi_2^\ell = 0 \qquad (\gamma_0, \gamma_1, \gamma_1) \in \text{finite set.}$$

Looks like $x^\ell + y^\ell + z^\ell = 0$ solved by Wiles.

Problem 1: trivial solutions $(1, 0, 1)$ and $(0, 1, 0)$ become non-trivial.
~~**Problem 2:** weak modularity thms over non-totally real fields.~~

Improvement: Freitas II

$x^p + y^p = z^\ell$ factor LHS over $K := \mathbb{Q}(\zeta + \zeta^{-1})$.

$$(x+y) \prod_{j=1}^{(p-1)/2} \left(x^2 + y^2 + \theta_j xy\right) = z^\ell \qquad \theta_j := \zeta^j + \zeta^{-j} \in K.$$

$$x + y = \alpha_0\, \xi_0^\ell, \qquad \alpha_0 \in \text{finite set.}$$

$$\underbrace{(x^2+y^2) + \theta_j xy}_{f_j(x,y)} = \alpha_j \xi_j^\ell, \qquad \alpha_j \in \text{finite set.}$$

$$\therefore \quad \gamma_0 \xi_0^{2\ell} + \gamma_1 \xi_1^\ell + \gamma_2 \xi_2^\ell = 0 \qquad (\gamma_0, \gamma_1, \gamma_1) \in \text{finite set.}$$

Theorem (Freitas)

Let $\ell > C$. Then the only primitive solutions to $x^7 + y^7 = 3z^\ell$ is $(1, -1, 0)$.

A generalized Fermat equation contrived to fit the method

Let ℓ, m, $p \geq 5$ be primes, $\ell \neq p$, $m \neq p$.

$$x^{2\ell} + y^{2m} = z^p, \qquad \gcd(x, y, z) = 1.$$

A generalized Fermat equation contrived to fit the method

Let ℓ, m, $p \geq 5$ be primes, $\ell \neq p$, $m \neq p$.

$$x^{2\ell} + y^{2m} = z^p, \qquad \gcd(x, y, z) = 1.$$

Modulo 8 we get $2 \nmid z$. WLOG $2 \mid x$. Only expected solution $(0, \pm 1, 1)$.

A generalized Fermat equation contrived to fit the method

Let ℓ, m, $p \geq 5$ be primes, $\ell \neq p$, $m \neq p$.

$$x^{2\ell} + y^{2m} = z^p, \qquad \gcd(x, y, z) = 1.$$

Modulo 8 we get $2 \nmid z$. WLOG $2 \mid x$. Only expected solution $(0, \pm 1, 1)$.

$$\begin{cases} x^\ell + y^m i = (a + bi)^p \\ x^\ell - y^m i = (a - bi)^p \end{cases} \qquad a, b \in \mathbb{Z} \quad \gcd(a, b) = 1.$$

$$\begin{aligned} x^\ell &= \frac{1}{2}\left((a+bi)^p + (a-bi)^p\right) \\ &= a \cdot \prod_{j=1}^{p-1} \left((a+bi) + (a-bi)\zeta^j\right) \\ &= a \cdot \prod_{j=1}^{(p-1)/2} \left((\theta_j + 2)a^2 + (\theta_j - 2)b^2\right) \qquad \theta_j = \zeta^j + \zeta^{-j} \in K. \end{aligned}$$

Frey Curve

$$x^\ell = a \cdot \prod_{j=1}^{(p-1)/2} \underbrace{\left((\theta_j + 2)a^2 + (\theta_j - 2)b^2\right)}_{f_j(a,b)} \qquad \theta_j = \zeta^j + \zeta^{-j} \in K.$$

$$p \nmid x \implies a = \alpha^\ell, \qquad f_j(a,b) \cdot \mathcal{O}_K = \mathfrak{b}_j^\ell$$

$$p \mid x \implies a = p^{\ell-1}\alpha^\ell, \qquad f_j(a,b) \cdot \mathcal{O}_K = \mathfrak{p}\mathfrak{b}_j^\ell \qquad \mathfrak{p} = (\theta_j - 2) \mid p$$

$$\underbrace{(\theta_2 - 2)f_1(a,b)}_{u} + \underbrace{(2 - \theta_1)f_2(a,b)}_{v} + \underbrace{4(\theta_1 - \theta_2)a^2}_{w} = 0\,.$$

Frey curve $\qquad E \,:\, Y^2 = X(X-u)(X+v), \qquad \Delta = 16u^2v^2w^2.$

Scale (u, v, w) to make coprime and make E semistable.

Trivial solution $x = 0 \implies a = 0 \implies w = 0 \implies \Delta = 0.$

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

1. Mazur: irreducibility of mod ℓ representations of elliptic curves over $\mathbb{Q}$ for $\ell > 163$ (i.e. absence of ℓ-isogenies).

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

1. Mazur: irreducibility of mod ℓ representations of elliptic curves over $\mathbb{Q}$ for $\ell > 163$ (i.e. absence of ℓ-isogenies).
2. Wiles (and others): modularity of elliptic curves over $\mathbb{Q}$.

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

1. Mazur: irreducibility of mod ℓ representations of elliptic curves over $\mathbb{Q}$ for $\ell > 163$ (i.e. absence of ℓ-isogenies).
2. Wiles (and others): modularity of elliptic curves over $\mathbb{Q}$.
3. Ribet: level lowering for mod ℓ representations—this requires irreducibility and modularity.

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

1. Mazur: irreducibility of mod ℓ representations of elliptic curves over $\mathbb{Q}$ for $\ell > 163$ (i.e. absence of ℓ-isogenies).
2. Wiles (and others): modularity of elliptic curves over $\mathbb{Q}$.
3. Ribet: level lowering for mod ℓ representations—this requires irreducibility and modularity.

Over totally real fields we have

1. Merel's uniform boundedness theorem for **torsion**. No corresponding result for isogenies.

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

1. Mazur: irreducibility of mod ℓ representations of elliptic curves over $\mathbb{Q}$ for $\ell > 163$ (i.e. absence of ℓ-isogenies).
2. Wiles (and others): modularity of elliptic curves over $\mathbb{Q}$.
3. Ribet: level lowering for mod ℓ representations—this requires irreducibility and modularity.

Over totally real fields we have

1. Merel's uniform boundedness theorem for **torsion**. No corresponding result for isogenies.
2. Partial modularity results—no clean statements.

Three Black-Boxes

The proof of Fermat's Last Theorem uses three big theorems:

1. Mazur: irreducibility of mod ℓ representations of elliptic curves over $\mathbb{Q}$ for $\ell > 163$ (i.e. absence of ℓ-isogenies).
2. Wiles (and others): modularity of elliptic curves over $\mathbb{Q}$.
3. Ribet: level lowering for mod ℓ representations—this requires irreducibility and modularity.

Over totally real fields we have

1. Merel's uniform boundedness theorem for **torsion**. No corresponding result for isogenies.
2. Partial modularity results—no clean statements.
3. Level lowering for mod ℓ representations works exactly as for $\mathbb{Q}$—theorems of Fujiwara, Jarvis and Rajaei. Requires irreducibility and modularity.

Representations of Elliptic Curves—Crash Course

Let ℓ be a prime, and E elliptic curve over totally real field K.

$$\overline{\rho}_{E,\ell} \; : \; G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell) \qquad G_K = \mathrm{Gal}(\overline{K}/K).$$

Representations of Elliptic Curves—Crash Course

Let ℓ be a prime, and E elliptic curve over totally real field K.

$$\overline{\rho}_{E,\ell} \;:\; G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell) \qquad G_K = \mathrm{Gal}(\overline{K}/K).$$

$$\rho_{E,\ell} \;:\; G_K \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Representations of Elliptic Curves—Crash Course

Let ℓ be a prime, and E elliptic curve over totally real field K.

$$\overline{\rho}_{E,\ell} \;:\; G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell) \qquad G_K = \mathrm{Gal}(\overline{K}/K).$$

$$\rho_{E,\ell} \;:\; G_K \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

E is **modular** if there exists a cuspidal Hilbert modular eigenform $\mathfrak{f}$ such that $\rho_{E,\ell} \sim \rho_{\mathfrak{f},\ell}$.

Representations of Elliptic Curves—Crash Course

Let ℓ be a prime, and E elliptic curve over totally real field K.

$$\overline{\rho}_{E,\ell} \ : \ G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell) \qquad G_K = \mathrm{Gal}(\overline{K}/K).$$

$$\rho_{E,\ell} \ : \ G_K \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

E is **modular** if there exists a cuspidal Hilbert modular eigenform $\mathfrak{f}$ such that $\rho_{E,\ell} \sim \rho_{\mathfrak{f},\ell}$.

$\overline{\rho}_{E,\ell}$ is **reducible** if

$$\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_\ell^\times.$$

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

1. E/K **semistable** elliptic curve, over Galois totally real field K.
2. ℓ rational prime **unramified** in K.
3. $\overline{\rho}_{E,\ell}$ is reducible: $\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_\ell^\times.$

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

1. E/K **semistable** elliptic curve, over Galois totally real field K.
2. ℓ rational prime **unramified** in K.
3. $\overline{\rho}_{E,\ell}$ is reducible: $\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i : G_K \to \mathbb{F}_\ell^\times.$

Fact: $$\upsilon \nmid \ell, \quad \upsilon \text{ finite} \quad \implies \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

1. E/K **semistable** elliptic curve, over Galois totally real field K.
2. ℓ rational prime **unramified** in K.
3. $\overline{\rho}_{E,\ell}$ is reducible: $\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i : G_K \to \mathbb{F}_\ell^\times.$

Fact: $$\upsilon \nmid \ell, \quad \upsilon \text{ finite} \quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Hence ψ_1, ψ_2 are **unramified** at all finite $\upsilon \nmid \ell$ (i.e. $\psi_i|_{I_\upsilon} = 1$).

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

1. E/K **semistable** elliptic curve, over Galois totally real field K.
2. ℓ rational prime **unramified** in K.
3. $\overline{\rho}_{E,\ell}$ is reducible: $\quad \overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_\ell^\times.$

Fact: $\quad \upsilon \nmid \ell, \quad \upsilon$ finite $\quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$

Hence ψ_1, ψ_2 are **unramified** at all finite $\upsilon \nmid \ell$ (i.e. $\psi_i|_{I_\upsilon} = 1$).

Serre: $\quad \upsilon \mid \ell \quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

1. E/K **semistable** elliptic curve, over Galois totally real field K.
2. ℓ rational prime **unramified** in K.
3. $\overline{\rho}_{E,\ell}$ is reducible: $\quad \overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_\ell^\times.$

$$\textbf{Fact:} \qquad \upsilon \nmid \ell, \quad \upsilon \text{ finite} \quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Hence ψ_1, ψ_2 are **unramified** at all finite $\upsilon \nmid \ell$ (i.e. $\psi_i|_{I_\upsilon} = 1$).

$$\textbf{Serre:} \qquad \upsilon \mid \ell \quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$$

$\chi : G_K \to \mathbb{F}_\ell^\times$ is the **mod ℓ cyclotomic character:** $\zeta_\ell^\sigma = \zeta_\ell^{\chi(\sigma)}$.

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

1. E/K **semistable** elliptic curve, over Galois totally real field K.
2. ℓ rational prime **unramified** in K.
3. $\overline{\rho}_{E,\ell}$ is reducible: $\quad \overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \; : \; G_K \to \mathbb{F}_\ell^\times.$

Fact: $\quad \upsilon \nmid \ell, \quad \upsilon$ finite $\quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$

Hence ψ_1, ψ_2 are **unramified** at all finite $\upsilon \nmid \ell$ (i.e. $\psi_i|_{I_\upsilon} = 1$).

Serre: $\quad \upsilon \mid \ell \quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$

$\chi : G_K \to \mathbb{F}_\ell^\times$ is the **mod ℓ cyclotomic character:** $\zeta_\ell^\sigma = \zeta_\ell^{\chi(\sigma)}$.

Hence, for $\upsilon \mid \ell$,

- **either** $\psi_1|_{I_\upsilon} = \chi|_{I_\upsilon}$ and $\psi_2|_{I_\upsilon} = 1$;
- **or** $\psi_1|_{I_\upsilon} = 1$ and $\psi_2|_{I_\upsilon} = \chi|_{I_\upsilon}$.

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

Know

- If $\upsilon \nmid \ell$ is finite then, $\psi_i|_{I_\upsilon} = 1$.
- If $\upsilon \mid \ell$ then
  - **either** $\psi_1|_{I_\upsilon} = \chi|_{I_\upsilon}$ and $\psi_2|_{I_\upsilon} = 1$;
  - **or** $\psi_1|_{I_\upsilon} = 1$ and $\psi_2|_{I_\upsilon} = \chi|_{I_\upsilon}$.

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

Know

- If $\upsilon \nmid \ell$ is finite then, $\psi_i|_{I_\upsilon} = 1$.
- If $\upsilon \mid \ell$ then
  - **either** $\psi_1|_{I_\upsilon} = \chi|_{I_\upsilon}$ and $\psi_2|_{I_\upsilon} = 1$;
  - **or** $\psi_1|_{I_\upsilon} = 1$ and $\psi_2|_{I_\upsilon} = \chi|_{I_\upsilon}$.

Let

$$S_\ell = \{\upsilon \ : \ \upsilon \mid \ell\}, \qquad S = \{ \ \upsilon \in S_\ell \ : \ \psi_1|_{I_\upsilon} = \chi|_{I_\upsilon} \ \}.$$

Goal: Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

Know

- If $\upsilon \nmid \ell$ is finite then, $\psi_i|_{I_\upsilon} = 1$.
- If $\upsilon \mid \ell$ then
  - **either** $\psi_1|_{I_\upsilon} = \chi|_{I_\upsilon}$ and $\psi_2|_{I_\upsilon} = 1$;
  - **or** $\psi_1|_{I_\upsilon} = 1$ and $\psi_2|_{I_\upsilon} = \chi|_{I_\upsilon}$.

Let

$$S_\ell = \{\upsilon \;:\; \upsilon \mid \ell\}, \qquad S = \{\, \upsilon \in S_\ell \;:\; \psi_1|_{I_\upsilon} = \chi|_{I_\upsilon} \,\}.$$

Lemma

Suppose

- $h_K^+ = 1$ *(i.e. the maximal abelian extension of K unramified away for ∞ is K).*
- $S = \emptyset$.

Then $E(K)[\ell] \neq 0$.

Proof.

$S = \emptyset \implies \psi_1 : G_K \to \mathbb{F}_\ell^\times$ is unramified at all finite places ... □

Lemma

Suppose

- $h_K^+ = 1$ *(i.e. the maximal abelian extension of K unramified away for ∞ is K).*
- $S = \emptyset$.

Then $E(K)[\ell] \neq 0$.

Proof.

$$\begin{aligned} S = \emptyset \quad &\Longrightarrow \quad \psi_1 \ : G_K \to \mathbb{F}_\ell^\times \text{ is unramified at all finite places} \\ &\Longrightarrow \quad \psi_1 = 1. \end{aligned}$$

$$\overline{\rho}_{E,\ell} : G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell), \qquad \overline{\rho}_{E,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \psi_2 \end{pmatrix}.$$

$\square$

In this case, can bound ℓ by Merel.

- If $\upsilon \nmid \ell$ is finite then, $\psi_i|_{I_\upsilon} = 1$.
- If $\upsilon \mid \ell$ then $\begin{cases} \textbf{either } \psi_1|_{I_\upsilon} = \chi|_{I_\upsilon}, & \psi_2|_{I_\upsilon} = 1; \\ \textbf{or } \psi_1|_{I_\upsilon} = 1, & \psi_2|_{I_\upsilon} = \chi|_{I_\upsilon}. \end{cases}$

$$S_\ell = \{\upsilon \ : \ \upsilon \mid \ell\}, \qquad S = \{\, \upsilon \in S_\ell \ : \ \psi_1|_{I_\upsilon} = \chi|_{I_\upsilon} \,\}.$$

Lemma

Suppose

- $h_K^+ = 1$ *(i.e. the maximal abelian extension of K unramified away from ∞ is K).*
- $S = S_\ell$.

Then $E'(K)[\ell] \neq 0$, where E' is ℓ-isogenous to K.

Proof.

$$\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \overline{\rho}_{E',\ell} \sim \begin{pmatrix} \psi_2 & * \\ 0 & \psi_1 \end{pmatrix}.$$

$S = S_\ell \implies \psi_2 : G_K \to \mathbb{F}_\ell^\times$ is unramified at all finite places ... $\square$

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \to \mathbb{F}_\ell^\times$ such that $\psi|_{I_v} = 1$ for (finite) $v \notin S$, and $\psi|_{I_v} = \chi|_{I_v}$ for $v \in S$?

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_v} = 1$ for (finite) $v \notin S$, and
  - $\psi|_{I_v} = \chi|_{I_v}$ for $v \in S$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_v} = 1$ for (finite) $v \notin S$, and
  - $\psi|_{I_v} = \chi|_{I_v}$ for $v \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_v} = 1$ for (finite) $v \notin S$, and
  - $\psi|_{I_v} = \chi|_{I_v}$ for $v \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_\upsilon : K_\upsilon^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.
- Will compute $\psi(\Theta_\upsilon(u))$ as υ ranges over M_K.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_\upsilon : K_\upsilon^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.
- Will compute $\psi(\Theta_\upsilon(u))$ as υ ranges over M_K.
- Suppose $\upsilon \mid \infty$. Then $u > 0$ in K_υ. So $\Theta_\upsilon(u) = 1$. So $\psi(\Theta_\upsilon(u)) = 1$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_\upsilon : K_\upsilon^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.
- Will compute $\psi(\Theta_\upsilon(u))$ as υ ranges over M_K.
- Suppose $\upsilon \mid \infty$. Then $u > 0$ in K_υ. So $\Theta_\upsilon(u) = 1$. So $\psi(\Theta_\upsilon(u)) = 1$.
- Suppose $\upsilon \nmid \infty$. By local reciprocity $\Theta_\upsilon(u) \in I_\upsilon$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_\upsilon : K_\upsilon^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.
- Will compute $\psi(\Theta_\upsilon(u))$ as υ ranges over M_K.
- Suppose $\upsilon \mid \infty$. Then $u > 0$ in K_υ. So $\Theta_\upsilon(u) = 1$. So $\psi(\Theta_\upsilon(u)) = 1$.
- Suppose $\upsilon \nmid \infty$. By local reciprocity $\Theta_\upsilon(u) \in I_\upsilon$.
  - If $\upsilon \notin S$ then $\psi(\Theta_\upsilon(u)) = 1$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_\upsilon : K_\upsilon^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.
- Will compute $\psi(\Theta_\upsilon(u))$ as υ ranges over M_K.
- Suppose $\upsilon \mid \infty$. Then $u > 0$ in K_υ. So $\Theta_\upsilon(u) = 1$. So $\psi(\Theta_\upsilon(u)) = 1$.
- Suppose $\upsilon \nmid \infty$. By local reciprocity $\Theta_\upsilon(u) \in I_\upsilon$.
  - If $\upsilon \notin S$ then $\psi(\Theta_\upsilon(u)) = 1$.
  - If $\upsilon \in S$ then $\psi(\Theta_\upsilon(u)) = \chi(\Theta_\upsilon(u)) = \mathrm{Norm}_{\mathbb{F}_\upsilon/\mathbb{F}_\ell}(u)^{-1}$.

Class Field Theory (Momose?, Kraus?, David?)

- $\exists$ **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \to \mathbb{F}_\ell^\times$ such that
  - $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and
  - $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$.
- Let $L = K(\psi)$. View $\psi : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_\upsilon : K_\upsilon^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.
- Will compute $\psi(\Theta_\upsilon(u))$ as υ ranges over M_K.
- Suppose $\upsilon \mid \infty$. Then $u > 0$ in K_υ. So $\Theta_\upsilon(u) = 1$. So $\psi(\Theta_\upsilon(u)) = 1$.
- Suppose $\upsilon \nmid \infty$. By local reciprocity $\Theta_\upsilon(u) \in I_\upsilon$.
  - If $\upsilon \notin S$ then $\psi(\Theta_\upsilon(u)) = 1$.
  - If $\upsilon \in S$ then $\psi(\Theta_\upsilon(u)) = \chi(\Theta_\upsilon(u)) = \mathrm{Norm}_{\mathbb{F}_\upsilon/\mathbb{F}_\ell}(u)^{-1}$.

$$\text{Global reciprocity} \implies \prod \Theta_\upsilon(u) = 1$$
$$\implies \prod_{\upsilon \in S} \mathrm{Norm}_{\mathbb{F}_\upsilon/\mathbb{F}_\ell}(u) = \overline{1} \qquad (\overline{1} \in \mathbb{F}_\ell).$$

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \to \mathbb{F}_\ell^\times$ such that $\psi|_{I_v} = 1$ for (finite) $v \notin S$, and $\psi|_{I_v} = \chi|_{I_v}$ for $v \in S$?

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \to \mathbb{F}_\ell^\times$ such that $\psi|_{I_v} = 1$ for (finite) $v \notin S$, and $\psi|_{I_v} = \chi|_{I_v}$ for $v \in S$?

If answer is no then can bound ℓ by Merel.

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \to \mathbb{F}_\ell^\times$ such that $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$?

If answer is no then can bound ℓ by Merel.

Suppose answer is YES. Let u be a totally positive unit. Then

$$\prod_{\upsilon \in S} \mathrm{Norm}_{\mathbb{F}_\upsilon/\mathbb{F}_\ell}(u) = \overline{1} \qquad (\overline{1} \in \mathbb{F}_\ell).$$

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \to \mathbb{F}_\ell^\times$ such that $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$?

If answer is no then can bound ℓ by Merel.

Suppose answer is YES. Let u be a totally positive unit. Then

$$\prod_{\upsilon \in S} \mathrm{Norm}_{\mathbb{F}_\upsilon/\mathbb{F}_\ell}(u) = \overline{1} \qquad (\overline{1} \in \mathbb{F}_\ell).$$

Therefore, there is a **non-empty proper** subset $T \subset \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\ell \mid B_T(u) \qquad B_T(u) := \mathrm{Norm}\left(\left(\prod_{\sigma \in T} u^\sigma\right) - 1\right).$$

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \to \mathbb{F}_\ell^\times$ such that $\psi|_{I_\upsilon} = 1$ for (finite) $\upsilon \notin S$, and $\psi|_{I_\upsilon} = \chi|_{I_\upsilon}$ for $\upsilon \in S$?

If answer is no then can bound ℓ by Merel.

Suppose answer is YES. Let u be a totally positive unit. Then

$$\prod_{\upsilon \in S} \mathrm{Norm}_{\mathbb{F}_\upsilon/\mathbb{F}_\ell}(u) = \overline{1} \qquad (\overline{1} \in \mathbb{F}_\ell).$$

Therefore, there is a **non-empty proper** subset $T \subset \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\ell \mid B_T(u) \qquad B_T(u) := \mathrm{Norm}\left(\left(\prod_{\sigma \in T} u^\sigma\right) - 1\right).$$

Lemma (Freitas–S). For each non-empty proper subset $T \subset \mathrm{Gal}(K/\mathbb{Q})$, there exists totally positive unit u such that $B_T(u) \neq 0$.

Frey curve again

Recall

- $p \geq 5$ and $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.
- Frey curve E/K is semistable.

Lemma

For $p = 5, 7, 11, 13$, and $\ell \geq 5$, $\ell \neq p$, the mod ℓ representation $\overline{\rho}_{E,\ell}$ is irreducible.

Proof.

$h_K^+ = 1$ for all these p. Use above and

- Classification of ℓ-torsion over fields of
  - degree 2 by Kamienny,
  - degree 3 by Parent,
  - degrees 4, 5, 6 by Derickx, Kamienny, Stein, and Stoll.
- "A criterion to rule out torsion groups for elliptic curves over number fields", Bruin and Najman.
- Computations of K-points on modular curves.

□

Is it modular?

Let q be a prime, and E elliptic curve over totally real field K.

$$\overline{\rho}_{E,q} \; : \; G_K \to \mathrm{Aut}(E[q]) \cong \mathrm{GL}_2(\mathbb{F}_q) \qquad G_K = \mathrm{Gal}(\overline{K}/K).$$

$$\rho_{E,q} \; : \; G_K \to \mathrm{Aut}(T_q(E)) \cong \mathrm{GL}_2(\mathbb{Z}_q).$$

E is **modular** if there exists a cuspidal Hilbert modular eigenform $\mathfrak{f}$ such that $\rho_{E,q} \sim \rho_{\mathfrak{f},q}$.

Three kinds of modularity theorems:

Kisin, Gee, Breuil, . . . : if $q = 3$, 5 or 7 and $\overline{\rho}(G_K)$ is 'big' then E is modular.

Thorne: if $q = 5$, and $\sqrt{5} \notin K$ and $\mathbb{P}\overline{\rho}(G_K)$ is dihedral then E is modular.

Skinner & Wiles: if $\overline{\rho}(G_K)$ is reducible (and other conditions) then E is modular.

Fix $q = 5$ and suppose $\sqrt{5} \notin K$. Remaining case $\overline{\rho}(G_K)$ reducible.

Skinner & Wiles

- K totally real field,
- E/K semistable elliptic curve,
- 5 unramified in K,
- $\overline{\rho}_{E,5}$ is reducible:

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_5^\times .$$

Theorem (Skinner & Wiles)

Suppose $K(\psi_1/\psi_2)$ is an abelian extension of $\mathbb{Q}$. Then E is modular.

Plan: Start with K abelian over $\mathbb{Q}$. Find sufficient conditions so that $K(\psi_1/\psi_2) \subseteq K(\zeta_5)$. Then (assuming these conditions) E is modular.

Reducible Representations of Elliptic Curves (again)

K real abelian field.

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_5^\times .$$

Reducible Representations of Elliptic Curves (again)

K real abelian field.

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_5^\times.$$

Fact: $\psi_1 \psi_2 = \chi$

Reducible Representations of Elliptic Curves (again)

K real abelian field.

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_5^\times.$$

Fact: $\psi_1 \psi_2 = \chi$ where $\chi \ : \ G_K \to \mathbb{F}_5^\times$ satisfies $\zeta_5^\sigma = \zeta_5^{\chi(\sigma)}$.

Reducible Representations of Elliptic Curves (again)

K real abelian field.

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \;:\; G_K \to \mathbb{F}_5^\times.$$

Fact: $\psi_1 \psi_2 = \chi$ where $\chi \;:\; G_K \to \mathbb{F}_5^\times$ satisfies $\zeta_5^\sigma = \zeta_5^{\chi(\sigma)}$.

$$\frac{\psi_1}{\psi_2} = \frac{\chi}{\psi_2^2} = \frac{\psi_1^2}{\chi}\,.$$

Reducible Representations of Elliptic Curves (again)

K real abelian field.

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \; : \; G_K \to \mathbb{F}_5^\times.$$

Fact: $\psi_1 \psi_2 = \chi$ where $\chi \; : \; G_K \to \mathbb{F}_5^\times$ satisfies $\zeta_5^\sigma = \zeta_5^{\chi(\sigma)}$.

$$\frac{\psi_1}{\psi_2} = \frac{\chi}{\psi_2^2} = \frac{\psi_1^2}{\chi} .$$

$$\therefore \quad K(\psi_1/\psi_2) \subseteq K(\zeta_5) K(\psi_2^2), \qquad K(\psi_1/\psi_2) \subseteq K(\zeta_5) K(\psi_1^2).$$

Reducible Representations of Elliptic Curves (again)

K real abelian field.

$$\overline{\rho}_{E,5} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \psi_i \ : \ G_K \to \mathbb{F}_5^\times.$$

Fact: $\psi_1 \psi_2 = \chi$ where $\chi \ : \ G_K \to \mathbb{F}_5^\times$ satisfies $\zeta_5^\sigma = \zeta_5^{\chi(\sigma)}$.

$$\frac{\psi_1}{\psi_2} = \frac{\chi}{\psi_2^2} = \frac{\psi_1^2}{\chi}.$$

$$\therefore \quad K(\psi_1/\psi_2) \subseteq K(\zeta_5)K(\psi_2^2), \qquad K(\psi_1/\psi_2) \subseteq K(\zeta_5)K(\psi_1^2).$$

Plan: If $K(\psi_1^2) = K$ or $K(\psi_2^2) = K$ then $K(\psi_1/\psi_2) \subseteq K(\zeta_5)$. Then E is modular.

Theorem (Anni–S)

Let K be a real abelian number field. Write $S_5 = \{\mathfrak{q} \mid 5\}$. Suppose

(a) *5 is unramified in K;*

(b) *the class number of K is odd;*

(c) *for each non-empty proper subset S of S_5, there is some totally positive unit u of $\mathcal{O}_K$ such that*

$$\prod_{\mathfrak{q} \in S} \mathrm{Norm}_{\mathbb{F}_\mathfrak{q}/\mathbb{F}_5}(u \bmod \mathfrak{q}) \neq \overline{1}\,.$$

Then every semistable elliptic curve E over K is modular.

Proof.

- By Kisin, ...and Thorne, can suppose that $\overline{\rho}_{E,5}$ is reducible.
- By (c), ψ_1 or ψ_2 is unramified at all finite places.
- So ψ_1^2 or ψ_2^2 is unramified at all places.
- By (b), $K(\psi_1^2) = K$ or $K(\psi_2^2) = K$.

□

Modularity of the Frey Curve

Recall

- $p \geq 5$ and $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.
- Frey curve E/K is semistable.

Corollary

For $p = 5, 7, 11, 13$, the Frey curve E is modular.

Proof.

For $p = 7, 11, 13$ apply the above. For $p = 5$ we have $K = \mathbb{Q}(\sqrt{5})$. Modularity of elliptic curves over quadratic fields was proved by Freitas, Le Hung & S. □

Theorem (Anni–S)

Let $p = 3, 5, 7, 11$ or 13. Let ℓ, $m \geq 5$ be primes. The only primitive solutions to

$$x^{2\ell} + y^{2m} = z^p$$

bi-infinite!

are $(\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

Theorem (Anni–S)

Let $p = 3$, 5, 7, 11 or 13. Let ℓ, $m \geq 5$ be primes. The only primitive solutions to

$$x^{2\ell} + y^{2m} = z^p \qquad \textit{bi-infinite!}$$

are $(\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

Proof makes use of level-lowering and `Magma` computations of Hilbert modular forms (based on algorithms of Dembélé, Donnelly, Voight and Greenberg).

Theorem (Anni–S)

Let $p = 3, 5, 7, 11$ or 13. Let ℓ, $m \geq 5$ be primes. The only primitive solutions to

$$x^{2\ell} + y^{2m} = z^p \qquad \text{bi-infinite!}$$

are $(\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

Proof makes use of level-lowering and `Magma` computations of Hilbert modular forms (based on algorithms of Dembélé, Donnelly, Voight and Greenberg).

Thank You!