

ON THE GENERALIZED FERMAT EQUATION

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

Samuele Anni
joint work with Samir Siksek

University of Warwick

SEMINARI DE TEORIA DE NOMBRES DE BARCELONA,
Barcelona Fall Workshop on NUMBER THEORY,
25 – 27 November 2015

1 GENERALIZED FERMAT EQUATION

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

3 THE PROOF

GENERALIZED FERMAT EQUATION

Let $(p, q, r) \in \mathbb{Z}_{\geq 2}^3$. The equation

$$x^p + y^q = z^r$$

is a **Generalized Fermat Equation** of signature (p, q, r) .

GENERALIZED FERMAT EQUATION

Let $(p, q, r) \in \mathbb{Z}_{\geq 2}^3$. The equation

$$x^p + y^q = z^r$$

is a **Generalized Fermat Equation** of signature (p, q, r) .

A solution $(x, y, z) \in \mathbb{Z}^3$ is called

GENERALIZED FERMAT EQUATION

Let $(p, q, r) \in \mathbb{Z}_{\geq 2}^3$. The equation

$$x^p + y^q = z^r$$

is a **Generalized Fermat Equation** of signature (p, q, r) .

A solution $(x, y, z) \in \mathbb{Z}^3$ is called

- **non-trivial** if $xyz \neq 0$,

GENERALIZED FERMAT EQUATION

Let $(p, q, r) \in \mathbb{Z}_{\geq 2}^3$. The equation

$$x^p + y^q = z^r$$

is a **Generalized Fermat Equation** of signature (p, q, r) .

A solution $(x, y, z) \in \mathbb{Z}^3$ is called

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

CONJECTURE (DARMON & GRANVILLE, TIJDEMAN, ZAGIER, BEAL)

Suppose

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

The only non-trivial primitive solutions to $x^p + y^q = z^r$ are

$$1 + 2^3 = 3^2,$$

$$7^3 + 13^2 = 2^9,$$

$$3^5 + 11^4 = 122^2,$$

$$1414^3 + 2213459^2 = 65^7,$$

$$43^8 + 96222^3 = 30042907^2,$$

$$2^5 + 7^2 = 3^4,$$

$$2^7 + 17^3 = 71^2,$$

$$17^7 + 76271^3 = 21063928^2,$$

$$9262^3 + 15312283^2 = 113^7,$$

$$33^8 + 1549034^2 = 15613^3.$$

CONJECTURE (DARMON & GRANVILLE, TIJDEMAN, ZAGIER, BEAL)

Suppose

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

The only non-trivial primitive solutions to $x^p + y^q = z^r$ are

$$\begin{array}{ll} 1 + 2^3 = 3^2, & 2^5 + 7^2 = 3^4, \\ 7^3 + 13^2 = 2^9, & 2^7 + 17^3 = 71^2, \\ 3^5 + 11^4 = 122^2, & 17^7 + 76271^3 = 21063928^2, \\ 1414^3 + 2213459^2 = 65^7, & 9262^3 + 15312283^2 = 113^7, \\ 43^8 + 96222^3 = 30042907^2, & 33^8 + 1549034^2 = 15613^3. \end{array}$$

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 . . .

Infinite Families of Exponents:

- Wiles: (p, p, p) .
- Darmon and Merel: $(p, p, 2)$, $(p, p, 3)$.
- Many other infinite families by many people . . .

The study of infinite families uses Frey curves, modularity and level-lowering over \mathbb{Q} (or \mathbb{Q} -curves).

Infinite Families of Exponents:

- Wiles: (p, p, p) .
- Darmon and Merel: $(p, p, 2)$, $(p, p, 3)$.
- Many other infinite families by many people . . .

The study of infinite families uses Frey curves, modularity and level-lowering over \mathbb{Q} (or \mathbb{Q} -curves).

Let us look at $x^p + y^p = z^\ell$ for p and ℓ primes.

SOLVE $x^p + y^p = z^\ell$

SOLVE $x^p + y^p = z^\ell$

NAÏVE IDEA

To solve $x^p + y^p = z^\ell$ factor over $\mathbb{Q}(\zeta)$, where ζ is a p -th root of unity.

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

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

$$\exists \epsilon_j \in \mathbb{Q}(\zeta) \text{ such that } \epsilon_0(x + y) + \epsilon_1(x + \zeta y) + \epsilon_2(x + \zeta^2 y) = 0.$$

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

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

SOLVE $x^p + y^p = z^\ell$

NAÏVE IDEA

To solve $x^p + y^p = z^\ell$ factor over $\mathbb{Q}(\zeta)$, where ζ is a p -th root of unity.

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

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

$$\exists \epsilon_j \in \mathbb{Q}(\zeta) \text{ such that } \epsilon_0(x + y) + \epsilon_1(x + \zeta y) + \epsilon_2(x + \zeta^2 y) = 0.$$

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

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

PROBLEMS

SOLVE $x^p + y^p = z^\ell$

NAÏVE IDEA

To solve $x^p + y^p = z^\ell$ factor over $\mathbb{Q}(\zeta)$, where ζ is a p -th root of unity.

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

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

$$\exists \epsilon_j \in \mathbb{Q}(\zeta) \text{ such that } \epsilon_0(x + y) + \epsilon_1(x + \zeta y) + \epsilon_2(x + \zeta^2 y) = 0.$$

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

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

PROBLEMS

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

SOLVE $x^p + y^p = z^\ell$

NAÏVE IDEA

To solve $x^p + y^p = z^\ell$ factor over $\mathbb{Q}(\zeta)$, where ζ is a p -th root of unity.

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

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

$$\exists \epsilon_j \in \mathbb{Q}(\zeta) \text{ such that } \epsilon_0(x + y) + \epsilon_1(x + \zeta y) + \epsilon_2(x + \zeta^2 y) = 0.$$

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

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

PROBLEMS

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

Problem 2: modularity theorems over non-totally real fields.

IMPROVEMENT: FREITAS

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

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

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

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

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

THEOREM (FREITAS)

Let $\ell > (1 + 3^{18})^2 C$. Then the only primitive solutions to $x^7 + y^7 = 3z^\ell$ are $(\pm 1, \mp 1, 0)$.

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

1 GENERALIZED FERMAT EQUATION

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

3 THE PROOF

THEOREM (ANNI-SIKSEK)

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

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

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

Remark: this is a **bi-infinite** family of equations.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Let $K := \mathbb{Q}(\zeta + \zeta^{-1})$ then

Let $K := \mathbb{Q}(\zeta + \zeta^{-1})$ then

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

Let $K := \mathbb{Q}(\zeta + \zeta^{-1})$ then

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

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

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

Let $K := \mathbb{Q}(\zeta + \zeta^{-1})$ then

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

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

$$\underbrace{(\theta_2 - 2)f_1(a, b)}_u + \underbrace{(2 - \theta_1)f_2(a, b)}_v + \underbrace{4(\theta_1 - \theta_2)a^2}_w = 0.$$

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

Frey curve

Frey curve

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

Frey curve

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

PROBLEMS

Frey curve

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

PROBLEMS

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

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

Frey curve

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

PROBLEMS

Problem 1: ~~trivial solutions $(0, \pm 1, 1)$ become non-trivial.~~

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

Problem 2: ~~modularity theorems over non-totally real fields.~~

$$K := \mathbb{Q}(\zeta + \zeta^{-1})$$

LEMMA

Suppose $p \nmid x$. Let E be the Frey curve (*). The curve E is semistable, with **multiplicative reduction** at all primes above 2 and **good reduction** at \mathfrak{p} . It has minimal discriminant and conductor

$$\mathcal{D}_{E/K} = 2^{4\ell n - 4} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2 \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

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

LEMMA

Suppose $p \nmid x$. Let E be the Frey curve (*). The curve E is semistable, with **multiplicative reduction** at all primes above 2 and **good reduction** at \mathfrak{p} . It has minimal discriminant and conductor

$$\mathcal{D}_{E/K} = 2^{4\ell n - 4} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2 \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

LEMMA

Suppose $p \mid x$. Let E be the Frey curve (*). The curve E is semistable, with **multiplicative reduction** at \mathfrak{p} and at all primes above 2. It has minimal discriminant and conductor

$$\mathcal{D}_{E/K} = 2^{4\ell n - 4} \mathfrak{p}^{2\delta} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2\mathfrak{p} \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

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

LEMMA

Suppose $p \nmid x$. Let E be the Frey curve (*). The curve E is semistable, with **multiplicative reduction** at all primes above **2** and **good reduction** at \mathfrak{p} . It has minimal discriminant and conductor

$$\mathcal{D}_{E/K} = 2^{4\ell n - 4} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2 \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

LEMMA

Suppose $p \mid x$. Let E be the Frey curve (*). The curve E is semistable, with **multiplicative reduction** at \mathfrak{p} and at all primes above **2**. It has minimal discriminant and conductor

$$\mathcal{D}_{E/K} = 2^{4\ell n - 4} \mathfrak{p}^{2\delta} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2\mathfrak{p} \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

1 GENERALIZED FERMAT EQUATION

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

3 THE PROOF

- Residual irreducibility
- Modularity

Let ℓ be a prime, and E elliptic curve over totally real field K . The **mod ℓ Galois Representation** attached to E is given by

$$\bar{\rho}_{E,\ell} : G_K \rightarrow \text{Aut}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell) \quad G_K = \text{Gal}(\bar{K}/K).$$

Let ℓ be a prime, and E elliptic curve over totally real field K . The **mod ℓ Galois Representation** attached to E is given by

$$\bar{\rho}_{E,\ell} : G_K \rightarrow \text{Aut}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell) \quad G_K = \text{Gal}(\bar{K}/K).$$

The **ℓ -adic Galois Representation** attached to E is given by

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

where $T_\ell(E) = \varprojlim E[\ell^n]$ is the ℓ -adic Tate module.

Let ℓ be a prime, and E elliptic curve over totally real field K . The **mod ℓ Galois Representation** attached to E is given by

$$\bar{\rho}_{E,\ell} : G_K \rightarrow \text{Aut}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell) \quad G_K = \text{Gal}(\bar{K}/K).$$

The **ℓ -adic Galois Representation** attached to E is given by

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

where $T_\ell(E) = \varprojlim E[\ell^n]$ is the ℓ -adic Tate module.

DEFINITION

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

Proof of Fermat's Last Theorem
uses three big theorems:

Proof of Fermat's Last Theorem
uses three big theorems:

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

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} .

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.

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

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.

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.

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.

REDUCIBLE REPRESENTATIONS

REDUCIBLE REPRESENTATIONS

GOAL:

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

REDUCIBLE REPRESENTATIONS

GOAL:

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

Hypotheses:

REDUCIBLE REPRESENTATIONS

GOAL:

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

Hypotheses:

- 1 E/K **semistable** elliptic curve, over Galois totally real field K .

REDUCIBLE REPRESENTATIONS

GOAL:

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

Hypotheses:

- 1 E/K **semistable** elliptic curve, over Galois totally real field K .
- 2 ℓ rational prime **unramified** in K .

REDUCIBLE REPRESENTATIONS

GOAL:

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

Hypotheses:

- 1 E/K **semistable** elliptic curve, over Galois totally real field K .
- 2 ℓ rational prime **unramified** in K .

3 $\bar{\rho}_{E,\ell}$ is reducible: $\bar{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \quad \psi_i : G_K \rightarrow \mathbb{F}_\ell^\times.$

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

Fact: $v \nmid \ell, v \text{ finite} \implies \bar{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$

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

Fact: $v \nmid \ell, v \text{ finite} \implies \bar{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$

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

Serre: $v \mid \ell \implies \bar{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$

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

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

Serre: $v \mid \ell \quad \implies \quad \bar{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$

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

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

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

Serre: $v \mid \ell \quad \implies \quad \bar{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$

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

Hence, for $v \mid \ell$,

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

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

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

$$\text{Serre: } v \mid \ell \quad \implies \quad \bar{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$$

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

Hence, for $v \mid \ell$,

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

Let

$$S_\ell = \{v : v \mid \ell\}, \quad S = \{v \in S_\ell : \psi_1|_{I_v} = \chi|_{I_v}\}.$$

LEMMA

Suppose

- $h_K^+ = 1$;
- $S = \emptyset$.

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

PROOF.

$S = \emptyset \implies \psi_1 : G_K \rightarrow \mathbb{F}_\ell^\times$ is unramified at all finite places
 $\implies \psi_1 = 1$.

$$\bar{\rho}_{E,\ell} : G_K \rightarrow \text{Aut}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell), \quad \bar{\rho}_{E,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \psi_2 \end{pmatrix}.$$

In this case, can bound ℓ by Merel.

LEMMA

Suppose

- $h_K^+ = 1$;
- $S = S_\ell$.

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

PROOF.

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

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

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- 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 $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Will compute $\psi(\Theta_v(u))$ as v ranges over the places of K .

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Will compute $\psi(\Theta_v(u))$ as v ranges over the places of K .

- Suppose $v \mid \infty$. Then $u > 0$ in K_v . So $\Theta_v(u) = 1$. So $\psi(\Theta_v(u)) = 1$.

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Will compute $\psi(\Theta_v(u))$ as v ranges over the places of K .

- Suppose $v \mid \infty$. Then $u > 0$ in K_v . So $\Theta_v(u) = 1$. So $\psi(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Will compute $\psi(\Theta_v(u))$ as v ranges over the places of K .

- Suppose $v \mid \infty$. Then $u > 0$ in K_v . So $\Theta_v(u) = 1$. So $\psi(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.
 - If $v \notin S$ then $\psi(\Theta_v(u)) = 1$.

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Will compute $\psi(\Theta_v(u))$ as v ranges over the places of K .

- Suppose $v \mid \infty$. Then $u > 0$ in K_v . So $\Theta_v(u) = 1$. So $\psi(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.
 - If $v \notin S$ then $\psi(\Theta_v(u)) = 1$.
 - If $v \in S$ then $\psi(\Theta_v(u)) = \chi(\Theta_v(u)) = \text{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u)^{-1}$.

CLASS FIELD THEORY (MOMOSE?, KRAUS?, DAVID?)

- \exists **non-empty proper** subset $S \subset S_\ell$, and $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : \text{Gal}(L/K) \rightarrow \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \rightarrow \text{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Will compute $\psi(\Theta_v(u))$ as v ranges over the places of K .

- Suppose $v \mid \infty$. Then $u > 0$ in K_v . So $\Theta_v(u) = 1$. So $\psi(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.
 - If $v \notin S$ then $\psi(\Theta_v(u)) = 1$.
 - If $v \in S$ then $\psi(\Theta_v(u)) = \chi(\Theta_v(u)) = \text{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u)^{-1}$.

$$\begin{aligned} \text{Global reciprocity} &\implies \prod \Theta_v(u) = 1 \\ &\implies \prod_{v \in S} \text{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u) = \bar{1} \quad (\bar{1} \in \mathbb{F}_\ell). \end{aligned}$$

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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 $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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.

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

$$\prod_{v \in S} \text{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u) = \bar{1} \quad (\bar{1} \in \mathbb{F}_\ell).$$

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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.

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

$$\prod_{v \in S} \text{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u) = \bar{1} \quad (\bar{1} \in \mathbb{F}_\ell).$$

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

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

Question: Is there a **non-empty proper** subset $S \subset S_\ell$ and a character $\psi : G_K \rightarrow \mathbb{F}_\ell^\times$ 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.

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

$$\prod_{v \in S} \text{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u) = \bar{1} \quad (\bar{1} \in \mathbb{F}_\ell).$$

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

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

LEMMA (FREITAS-SIKSEK)

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

REDUCIBLE REPRESENTATIONS

Let E be a Frey curve as in (*).

LEMMA

Suppose $\bar{\rho}_{E,\ell}$ is reducible. Then either E/K has non-trivial ℓ -torsion, or is ℓ -isogenous to an elliptic curve over K that has non-trivial ℓ -torsion.

REDUCIBLE REPRESENTATIONS

Let E be a Frey curve as in (*).

LEMMA

Suppose $\bar{\rho}_{E,\ell}$ is reducible. Then either E/K has non-trivial ℓ -torsion, or is ℓ -isogenous to an elliptic curve over K that has non-trivial ℓ -torsion.

LEMMA

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

Sketch of the proof: use $h_K^+ = 1$ for all these p , class field theory and

- Classification of ℓ -torsion over fields of degree 2 (Kamienny), degree 3 (Parent), degrees 4, 5, 6 (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.

MODULARITY

Three kinds of modularity theorems:

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

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

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

Fix $\ell = 5$ and suppose $\sqrt{5} \notin K$. Remaining case $\bar{\rho}_{E,\ell}(G_K)$ reducible.

SKINNER & WILES

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

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

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

K real abelian field.

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

REDUCIBLE REPRESENTATIONS

K real abelian field.

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

Fact: $\psi_1\psi_2 = \chi$

REDUCIBLE REPRESENTATIONS

K real abelian field.

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

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

REDUCIBLE REPRESENTATIONS

K real abelian field.

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

Fact: $\psi_1\psi_2 = \chi$ where $\chi : G_K \rightarrow \mathbb{F}_5^\times$ 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

K real abelian field.

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

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

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

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

REDUCIBLE REPRESENTATIONS

K real abelian field.

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

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

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

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

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.

MODULARITY

MODULARITY

THEOREM (ANNI-SIKSEK)

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

$$\prod_{\mathfrak{q} \in S} \text{Norm}_{\mathbb{F}_q/\mathbb{F}_5}(u \bmod \mathfrak{q}) \neq \bar{1}.$$

Then every semistable elliptic curve E over K is modular.

PROOF.

- By Kisin, . . . and Thorne, can suppose that $\bar{\rho}_{E,5}$ 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 $K(\psi_2^2) = K$.



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 & Siksek. □

Let E/K be the Frey curve (*), then $\bar{\rho}_{E,\ell}$ is modular and irreducible. Then $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{f,\lambda}$ for some Hilbert cuspidal eigenform f over K of parallel weight 2 that is new at level \mathcal{N}_ℓ , where

$$\mathcal{N}_\ell = \begin{cases} 2\mathcal{O}_K & \text{if } p \nmid x \\ 2\mathfrak{p} & \text{if } p \mid x. \end{cases}$$

Here $\lambda \mid \ell$ is a prime of \mathbb{Q}_f , the field generated over \mathbb{Q} by the eigenvalues of f .

Let E/K be the Frey curve $(*)$, then $\bar{\rho}_{E,\ell}$ is modular and irreducible. Then $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{f,\lambda}$ for some Hilbert cuspidal eigenform f over K of parallel weight 2 that is new at level \mathcal{N}_ℓ , where

$$\mathcal{N}_\ell = \begin{cases} 2\mathcal{O}_K & \text{if } p \nmid x \\ 2\mathfrak{p} & \text{if } p \mid x. \end{cases}$$

Here $\lambda \mid \ell$ is a prime of \mathbb{Q}_f , the field generated over \mathbb{Q} by the eigenvalues of f .

For $p = 3$ the modular forms to consider are classical newform of weight 2 and level 6: there is no such newform and so we conclude.

If $p \equiv 1 \pmod{4}$, the field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ has a unique subfield K' of degree $(p-1)/4$.

If $p \equiv 1 \pmod{4}$, the field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ has a unique subfield K' of degree $(p-1)/4$.

In the case $p \nmid x$ the Frey curve E is defined over K' .

If $p \equiv 1 \pmod{4}$, the field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ has a unique subfield K' of degree $(p-1)/4$.

In the case $p \nmid x$ the Frey curve E is defined over K' .

This not true in the case $p \mid x$, but we can take a twist of the Frey curve some that it is defined over K' .

If $p \equiv 1 \pmod{4}$, the field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ has a unique subfield K' of degree $(p-1)/4$.

In the case $p \nmid x$ the Frey curve E is defined over K' .

This not true in the case $p \mid x$, but we can take a twist of the Frey curve some that it is defined over K' .

This way we can work with Hilbert modular cuspforms over a totally real field of lower degree. The conductor of this Frey curve can be computed similarly to the previous case.

p	Case	Level	Eigenforms f	$[\mathbb{Q}_f : \mathbb{Q}]$
5	$5 \nmid x$	$2\mathcal{O}_K$	–	–
	$5 \mid x$	$2p$	–	–
7	$7 \nmid x$	$2\mathcal{O}_K$	–	–
	$7 \mid x$	$2p$	f_1	1
11	$11 \nmid x$	$2\mathcal{O}_K$	f_2	2
	$11 \mid x$	$2p$	f_3, f_4	5
13	$13 \nmid x$	$2\mathfrak{B}^2$	f_5, \dots, f_9	1
			f_{10}, \dots, f_{21}	3
			f_{22}, f_{23}	6
			f_{24}, \dots, f_{27}	9
	$13 \mid x$	$2\mathfrak{B}$	f_{28}, f_{29}	1
		f_{30}, f_{31}	3	

p	Case	Level	Eigenforms f	$[\mathbb{Q}_f : \mathbb{Q}]$
5	$5 \nmid x$	$2\mathcal{O}_K$	–	–
	$5 \mid x$	$2p$	–	–
7	$7 \nmid x$	$2\mathcal{O}_K$	–	–
	$7 \mid x$	$2p$	f_1	1
11	$11 \nmid x$	$2\mathcal{O}_K$	f_2	2
	$11 \mid x$	$2p$	f_3, f_4	5
13	$13 \nmid x$	$2\mathfrak{B}^2$	f_5, \dots, f_9	1
			f_{10}, \dots, f_{21}	3
			f_{22}, f_{23}	6
			f_{24}, \dots, f_{27}	9
	$13 \mid x$	$2\mathfrak{B}$	f_{28}, f_{29}	1
		f_{30}, f_{31}	3	

In each case we deduce a contradiction using the q -expansions of the Hilber modular forms in the table coefficients and the study of the Frey curve described before.

FINAL REMARKS

In order to solve $x^{2\ell} + y^{2m} = z^p$ for $p \geq 17$ we need to be able to compute Hilbert modular cuspforms over totally real field of high degree. Anyway the following theorem hold:

FINAL REMARKS

In order to solve $x^{2\ell} + y^{2m} = z^p$ for $p \geq 17$ we need to be able to compute Hilbert modular cuspforms over totally real field of high degree. Anyway the following theorem hold:

THEOREM (ANNI-SIKSEK)

Let p be an odd prime and let $K = \mathbb{Q}(\zeta + \zeta^{-1})$. Let \mathcal{O}_K be the ring of integers of K and \mathfrak{p} be the unique prime ideal above p . Suppose that there are no elliptic curves E/K with full 2-torsion and conductors $2\mathcal{O}_K$, $2\mathfrak{p}$. Then there is an ineffective constant C_p (depending only on p) such that for all primes $\ell, m \geq C_p$, the only primitive solutions to $x^{2\ell} + y^{2m} = z^p$ are $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

ON THE GENERALIZED FERMAT EQUATION

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

Samuele Anni
joint work with Samir Siksek

University of Warwick

SEMINARI DE TEORIA DE NOMBRES DE BARCELONA,
Barcelona Fall Workshop on NUMBER THEORY,
25 – 27 November 2015

Thanks!