Diophantine equations and semistable elliptic curves over totally real number fields

Samuele Anni
joint work with Samir Siksek

University of Warwick

Algebra, Geometry and Number Theory Seminar,
Universiteit Leiden, 18th April 2016

Generalized Fermat Equation

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

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

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 ...

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

Naïve idea

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

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

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

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

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

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

Problems

Problem 1: trivial solutions $(\pm 1, 0, \pm 1), (0, \pm 1, \pm 1)$ become non-trivial.
Problem 2: modularity theorems over non-totally real fields.

Improvement: Freitas

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

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

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

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

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

Theorem (Freitas)

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

Theorem (Anni-Siksek)

Let $p = 3, 5, 7, 11$ or 13. Let ℓ, $m \geq 5$ be primes, and if $p = 13$ suppose moreover that ℓ, $m \neq 7$. Then the only primitive solutions to

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

are the trivial ones $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

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

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

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

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

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

$$x^\ell = \frac{1}{2}\left((a + bi)^p + (a - bi)^p\right) = a \cdot \prod_{j=1}^{p-1} \left((a + bi) + (a - bi)\zeta^j\right)$$

$$= a \cdot \prod_{j=1}^{(p-1)/2} \left((\theta_j + 2)a^2 + (\theta_j - 2)b^2\right) \qquad \theta_j = \zeta^j + \zeta^{-j} \in \mathbb{Q}\left(\zeta + \zeta^{-1}\right).$$

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

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

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

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

Frey curve

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

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*

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

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*

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

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*

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

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*

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

1. Generalized Fermat Equation
2. $x^{2\ell} + y^{2m} = z^p$
3. The proof
   - Residual irreducibility
   - Modularity

Galois representations and Elliptic curves

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

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

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

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

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 $\rho_{E,\ell} \sim \rho_{\mathfrak{f},\ell}$.*

Hilbert modular forms

Let K be a totally real number field of degree d over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_d$ be the real embeddings of K, therefore we have a map

$$\mathrm{GL}_2(K) \to GL_2(\mathbb{R})^d.$$

Let $\mathcal{O}_K$ be the ring of integers of K.
The group $\mathrm{GL}_2^+(\mathcal{O}_K)$ acts on $\mathcal{H}^d$ component-wise via fractional transformations: for every $\underline{z} = (z_1, \ldots, z_d) \in \mathcal{H}^d$, for ever $\gamma \in \mathrm{GL}_2^+(\mathcal{O}_K)$ we have $\gamma \cdot z = (\sigma_1(\gamma)z_1, \ldots, \sigma_d(\gamma)z_d)$.

Hilbert modular forms

For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ and $z \in \mathcal{H}$ define

$$j(g, z) = \det(g)^{-1/2}(cz + d)$$

Definition

A **Hilbert modular form** f *over* K *of weight* $(k_1, \ldots, k_d)$ *is an analytic function on* $\mathcal{H}^d$ *such that for every* $\gamma \in GL_2^+(\mathcal{O}_K)$

$$f(\gamma z) = \prod_{i=1}^{d} j(\sigma_i(\gamma), z_i)^{k_i} f(z).$$

No extra condition is needed for the cusps (Koecher's principle).
Hilbert modulars forms do have associated Fourier expansions (q-expansions) and Galois representations (Taylor).

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

Goal:

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

Hypotheses:

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

Fact: $\upsilon \nmid \ell, \quad \upsilon$ 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: $\upsilon \mid \ell \quad \Longrightarrow \quad \overline{\rho}_{E,\ell}|_{I_\upsilon} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ 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 $\psi_2|_{I_\upsilon} = \chi|_{I_\upsilon}$.

Let

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

Lemma

Suppose

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

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

Proof.

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

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

□

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.

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

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

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 the places of 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 $\psi|_{I_\upsilon} = 1$ 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–Siksek)

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

Reducible representations

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

Lemma

Suppose $\overline{\rho}_{E,\ell}$ is reducible. Then either E/K has non-trivial ℓ-torsion, or is ℓ-isogenous to an 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 $\overline{\rho}_{E,\ell}$ 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 $\overline{\rho}_{E,\ell}(G_K)$ is 'big' then E is modular.

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

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

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

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 $\zeta_5^\sigma = \zeta_5^{\chi(\sigma)}$.

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

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

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.

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*

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

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 $K(\psi_2^2) = K$.

□

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. □

Corollary

Let K be a real abelian field of conductor $n < 100$ with $5 \nmid n$ and $n \neq 29, 87, 89$. Let E be a semistable elliptic curve over K. Then E is modular.

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

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 $(p-1)/4$.

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	Field $\mathcal{K}$	Frey curve $\mathcal{E}$	Level $\mathcal{N}$	Eigenforms $\mathfrak{f}$	$[\mathbb{Q}_{\mathfrak{f}} : \mathbb{Q}]$
5	$5 \nmid x$	K	E	2_K	–	–
	$5 \mid x$	K	E	$2\mathfrak{p}$	–	–
7	$7 \nmid x$	K	E	2_K	–	–
	$7 \mid x$	K	E	$2\mathfrak{p}$	$\mathfrak{f}_1$	1
11	$11 \nmid x$	K	E	2_K	$\mathfrak{f}_2$	2
	$11 \mid x$	K	E	$2\mathfrak{p}$	$\mathfrak{f}_3, \mathfrak{f}_4$	5
13	$13 \nmid x$	K	E	2_K	$\mathfrak{f}_5, \mathfrak{f}_6$ $\mathfrak{f}_7$ $\mathfrak{f}_8$	1 2 3
	$13 \mid x$	K'	E'	$2\mathfrak{B}$	$\mathfrak{f}_9, \mathfrak{f}_{10}$ $\mathfrak{f}_{11}, \mathfrak{f}_{12}$	1 3

Table : Frey curve and Hilbert eigenform information. Here $\mathfrak{p}$ is the unique prime of K above p, and $\mathfrak{B}$ is the unique prime of K' above p.

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

The only case left is the case $p = 13$ and $\ell = 7$: we strongly suspect that reducibility of $\overline{\rho}_{\mathfrak{f}_{11},\lambda}$ (where λ is the unique prime above 7 of $\mathbb{Q}_{\mathfrak{f}_{11}}$) but we are unable to prove it.

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 ℓ, $m \geq C_p$, the only primitive solutions to $x^{2\ell} + y^{2m} = z^p$ are $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

Diophantine equations and semistable elliptic curves over totally real number fields

Samuele Anni
joint work with Samir Siksek

University of Warwick

Algebra, Geometry and Number Theory Seminar,
Universiteit Leiden, 18th April 2016

Thanks!