Diophantine equations and semistable elliptic curves over totally real fields

Samuele Anni (IWR - Universität Heidelberg)
joint with Samir Siksek (University of Warwick)

Journées Algophantiennes Bordelaises 2017,
Université de Bordeaux, June 2017
1. **Generalized Fermat Equation**

2. \( x^{2\ell} + y^{2m} = z^p \)

3. **The proof**
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

\[
\begin{align*}
1 + 2^3 &= 3^2, \\
7^3 + 13^2 &= 2^9, \\
3^5 + 11^4 &= 122^2, \\
1414^3 + 2213459^2 &= 65^7, \\
43^8 + 96222^3 &= 30042907^2,
\end{align*}
\]

\[
\begin{align*}
2^5 + 7^2 &= 3^4, \\
2^7 + 17^3 &= 71^2, \\
17^7 + 76271^3 &= 21063928^2, \\
9262^3 + 15312283^2 &= 113^7, \\
33^8 + 1549034^2 &= 15613^3.
\end{align*}
\]

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 \(\ell\) primes \(\geq 5\).
**Naïve idea**

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

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

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

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

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

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

**Problems**

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

**Problem 2:** modularity theorems over non-totally real fields.
1 Generalized Fermat Equation

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

3 The proof
Theorem (A.-Siksek)

Let $p = 3, 5, 7, 11$ or $13$. Let $\ell, m \geq 5$ be primes, and if $p = 13$ suppose moreover that $\ell, m \neq 7$. 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, $\ell \neq p$, $m \neq p$.

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

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

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

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

\[
= a \cdot \prod_{j=1}^{(p-1)/2} \left( (\theta_j + 2)a^2 + (\theta_j - 2)b^2 \right) \quad \theta_j = \zeta^j + \zeta^{-j} \in \mathbb{Q}(\zeta + \zeta^{-1}).
\]
Let $K := \mathbb{Q}(\zeta + \zeta^{-1})$ then

\[ x^\ell = a \cdot \prod_{j=1}^{(p-1)/2} ((\theta_j + 2)a^2 + (\theta_j - 2)b^2) \quad \text{with} \quad \theta_j = \zeta^j + \zeta^{-j} \in K. \]

\[ p \nmid x \implies a = \alpha^\ell, \quad f_j(a, b) \cdot \mathcal{O}_K = b_j^\ell, \]

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

\[
\left(\theta_2 - 2\right)f_1(a, b) + (2 - \theta_1)f_2(a, b) + 4(\theta_1 - \theta_2)a^2 = 0.
\]
**Frey curve**

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

**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 ($\ast$). The curve $E$ is \textit{semistable}, with \textbf{multiplicative reduction} at all primes above 2 and \textbf{good reduction} at $\mathfrak{p}$. It has \textit{minimal discriminant} and conductor

$$D_{E/K} = 2^{4\ell n - 4} \alpha^{4\ell} b_j^2 b_k^2, \quad N_{E/K} = 2 \cdot \text{Rad}(\alpha b_j b_k).$$

**Lemma**

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

$$D_{E/K} = 2^{4\ell n - 4} p^{2\delta} \alpha^{4\ell} b_j^2 b_k^2, \quad N_{E/K} = 2p \cdot \text{Rad}(\alpha b_j b_k).$$
**Lemma**

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

$$D_{E/K} = 2^{4\ell n-4} \alpha^{4\ell} b_j b_k^{2\ell}, \quad N_{E/K} = 2 \cdot \text{Rad}(\alpha b_j b_k).$$

**Lemma**

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

$$D_{E/K} = 2^{4\ell n-4} p^{2\delta} \alpha^{4\ell} b_j b_k^{2\ell}, \quad N_{E/K} = 2p \cdot \text{Rad}(\alpha b_j b_k).$$
1 Generalized Fermat Equation

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

3 The proof
   - Residual irreducibility
   - Modularity
Let $\ell$ be a prime, and $E$ elliptic curve over totally real field $K$. The mod $\ell$ Galois Representation attached to $E$ is given by

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

The $\ell$-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 $T_\ell(E) = \lim \leftarrow E[\ell^n]$ is the $\ell$-adic Tate module.

**Definition**

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

**Galois representations and Elliptic curves**
The proof

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

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

2. **Wiles** (and others): modularity of elliptic curves over $\mathbb{Q}$.

3. **Ribet**: level lowering for mod $\ell$ 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 $\ell$ representations works exactly as for $\mathbb{Q}$: theorems of Fujiwara, Jarvis and Rajaei. Requires irreducibility and modularity.
Let $E$ be a Frey curve as in $(\ast)$.

**Lemma**

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

**Lemma**

For $p = 5, 7, 11, 13,$ and $\ell \geq 5$, with $\ell \neq p$, the mod $\ell$ 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 $\ell$-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.
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 $\sqrt{5} \not\in K$ 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 $\sqrt{5} \not\in K$. 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:

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

**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.
- $E/K$ semistable elliptic curve,
- $q$ unramified in $K$,
- $\rho_{E,q}$ is reducible:

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

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

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

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

If $K(\psi_1^2) = K$ or $K(\psi_2^2) = K$, then $E$ is modular.
Modularity

Theorem (A.-Siksek)

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

$$\prod_{q \in S} \text{Norm}_{F_q/F_5}(u \mod q) \neq 1.$$ 

Then every semistable elliptic curve $E$ over $K$ is modular.

This theorem builds over results of Thorne and Skinner & Wiles.
Proof.

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

Proposition

Let $K$ be a real abelian field of conductor $n < 100$. Let $E$ be a semistable elliptic curve over $K$. Then $E$ is modular.

This proposition relies on the previous theorem and on a formulation of Thorne’s theorem for $\ell = 7$ for semistable elliptic curves.
**Corollary**

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

**Proof.**

For $p = 7, 11, 13$ apply the previous theorem. 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 \( \mathcal{N}_\ell \), where

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

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.
### The proof

<table>
<thead>
<tr>
<th>$p$</th>
<th>Case</th>
<th>Field $K$</th>
<th>Frey curve $E$</th>
<th>Level $N$</th>
<th>Eigenforms $f$</th>
<th>$[\mathbb{Q}_f : \mathbb{Q}]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$5 \nmid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2K$</td>
<td>$-$</td>
<td>$-$</td>
</tr>
<tr>
<td>5</td>
<td>$5 \mid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2p$</td>
<td>$-$</td>
<td>$-$</td>
</tr>
<tr>
<td>7</td>
<td>$7 \nmid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2K$</td>
<td>$-$</td>
<td>$-$</td>
</tr>
<tr>
<td>7</td>
<td>$7 \mid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2p$</td>
<td>$f_1$</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>$11 \nmid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2K$</td>
<td>$f_2$</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>$11 \mid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2p$</td>
<td>$f_3, f_4$</td>
<td>5</td>
</tr>
<tr>
<td>13</td>
<td>$13 \nmid x$</td>
<td>$K$</td>
<td>$E$</td>
<td>$2K$</td>
<td>$f_5, f_6, f_7, f_8$</td>
<td>1 2 3</td>
</tr>
<tr>
<td>13</td>
<td>$13 \mid x$</td>
<td>$K'$</td>
<td>$E'$</td>
<td>$2\mathfrak{B}$</td>
<td>$f_9, f_{10}, f_{11}, f_{12}$</td>
<td>1 3</td>
</tr>
</tbody>
</table>

**Table**: Frey curve and Hilbert eigenform information. Here $p$ is the unique prime of $K$ above $p$, $K'$ is the unique subfield $K'$ of degree $(p - 1)/4$ and $\mathfrak{B}$ is the unique prime of $K'$ above $p$. The curve $E'$ is a quadratic twist of $E$ over $K'$. 
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 $\overline{\rho}_{f_{11},\lambda}$ (where $\lambda$ is the unique prime above 7 of $\mathbb{Q}_{f_{11}}$) but we are unable to prove it.
Diophantine equations and semistable elliptic curves over totally real fields

Samuele Anni (IWR - Universität Heidelberg)
joint with Samir Siksek (University of Warwick)

Journées Algophantiennes Bordelaises 2017,
Université de Bordeaux, June 2017

Thanks!