Fermat’s Last Theorem - Not Enough Margin!

Philippe Michaud-Rodgers

University of Warwick

Young Researchers in Mathematics, 10th edition
08.06.2021
Statement of Fermat’s Last Theorem

Theorem (Wiles + many others! 1995)

The equation

\[ x^n + y^n = z^n, \]

with \( n \geq 3 \), has no non-trivial solutions for integers \( x, y, z \).

By a non-trivial solution, we mean that \( xyz \neq 0 \).

Aim for today: Overview the proof.

[Slides available on my webpage.]
Fermat’s Little Margin

- Pierre de Fermat:

- His margin:

  “I have discovered a truly remarkable proof of this result which this margin is too small to contain.”
First Observations

• If \( n = p \cdot m \) and \((x, y, z)\) satisfies \(x^n + y^n = z^n\), then

\[(x^m)^p + (y^m)^p = (z^m)^p.\]

• \( n = 3 \) (Euler, 1770) and \( n = 4 \) (Fermat, 1670): elementary.

So enough to prove:

**FLT**

The equation

\[x^p + y^p = z^p,\]

with \( p \geq 5 \), prime, has no non-trivial solutions for integers \( x, y, z \).
Suppose \((x, y, z)\) is a (non-trivial) solution and define the Frey curve

\[ E_{x,y,z,p} : Y^2 = X(X - x^p)(X + y^p). \]

This is an elliptic curve over \(\mathbb{Q}\).

**Definition**

An **elliptic curve over** \(\mathbb{Q}\) **is a curve given by an equation**

\[ E : Y^2 = X^3 + AX^2 + BX + C, \]

where \(A, B, C \in \mathbb{Q}\). It is smooth.
More on Elliptic Curves

They look like this:

\[ y^2 = x^3 - x \]

\[ y^2 = x^3 - x + 1 \]

- **Fact:** \( E(\mathbb{Q}) \) is a group.
- \( E \) has a **minimal discriminant**, \( \Delta_{\text{min}} \).

\[ \Delta_{\text{min}}(E_{x,y,z,p}) = 2^{-8}(xyz)^{2p}. \]

- \( E \) has a **conductor**, \( N \).

\[ N(E_{x,y,z,p}) = 2 \prod_{p \mid xyz, \text{odd}} p, \quad (\text{squarefree}). \]

- \( a_\ell(E) := \ell + 1 - \# \tilde{E}(\mathbb{F}_\ell) \), for \( \ell \) prime with \( \ell \nmid N \).
Let $N' > 0$. There are finitely many newforms at level $N'$.

- A newform is a holomorphic function on the upper half-plane.
- It has a Fourier, or $q$-expansion:

  $$f = \sum_{n=1}^{\infty} a_n q^n, \quad \text{where} \quad q = e^{\frac{2\pi i}{z}}.$$

- Newforms at level 38:
  
  $$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
  
  $$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

- There are no newforms at level 2.
The Key Theorem

Level-Lowering Theorem (Ribet)

Let $E$ be a modular elliptic curve over $\mathbb{Q}$ of conductor $N$ and let $p \geq 5$ be prime. Suppose $E$ has no rational subgroups of size $p$. Then $E$ arises mod $p$ from a newform $f$ at level $N_p$, where

$$N_p = \frac{N}{\prod_{q \mid \text{ord}_q(\Delta_{\text{min}})} q^{|N,p|\text{ord}_q(\Delta_{\text{min}})}}.$$

- $E$ arises mod $p$ from a newform $f = \sum_{n=1}^{\infty} a_n q^n$ at level $N_p$ means

  $$a_\ell(E) \equiv a_\ell(f) \pmod{p}$$

  for all primes $\ell \nmid pNN_p$. 
Condition in level-lowering theorem: \( E \) is modular.

**Definition**

Let \( E / \mathbb{Q} \) be an elliptic curve of conductor \( N \). Then \( E \) is modular if there exists a newform \( f = \sum_{n=1}^{\infty} a_n q^n \) at level \( N \) such that

\[
a_{\ell}(E) = a_{\ell}(f)
\]

for every prime \( \ell \nmid N \).

**Theorem (Wiles)**

If \( N \) is squarefree, then \( E \) is modular.

So \( E_{x,y,z,p} \) is modular.
Mazur’s Theorem

Condition in level-lowering theorem: \(E\) has no rational subgroups of size \(p\).

Mazur’s Theorem

Let \(E : Y^2 = g(X)\) be an elliptic curve over \(\mathbb{Q}\) of conductor \(N\) and let \(p \geq 5\). Suppose \(N\) is squarefree and that \(g\) has 3 rational roots. Then \(E\) has no rational subgroups of size \(p\).

This is true for our Frey curve

\[E_{x,y,z,p} : Y^2 = X(X - x^p)(X + y^p).\]

Conclusion: we can apply the level-lowering theorem to \(E_{x,y,z,p}\).
Apply the level-lowering theorem to the Frey curve $E_{x,y,z,p}$:

- $E_{x,y,z,p}$ arises mod $p$ from a newform $f$ at level $N_p$, where

$$N_p = \frac{N}{\prod_{q\mid N, p\mid \text{ord}_q(\Delta_{\min})} q} = \frac{2 \prod_{p\mid xyz, \text{odd}} p}{\prod_{p\mid xyz, \text{odd}} p} = 2.$$

**Note:** $N_p$ no longer depends on $x, y, z, \text{ or } p$.

**BUT!** There are no newforms at level 2, a contradiction.

**Conclusion:** Fermat’s Last Theorem is true!
FLT over quadratic fields

Theorem (Jarvis and Meekin, \(d = 2\), 2013. Freitas and Siksek, \(d > 2\), 2014)

The equation

\[ x^n + y^n = z^n, \quad x, y, z \in K, \]

has no non-trivial solutions for \(n \geq 4\) and \(K = \mathbb{Q}(\sqrt{d})\), when \(d \in \{2, 3, 6, 7, 10, 11, 13, 14, 15, 19, 21, 22, 23\}\). (No \(d = 5, 17\)).

Theorem (M. 2021)

The equation

\[ x^n + y^n = z^n, \quad x, y, z \in K, \]

has no non-trivial solutions for \(n \geq 4\) and \(K = \mathbb{Q}(\sqrt{d})\), when \(d \in \{26, 29, 30, 31, 35, 37, 38, 42, 43, 46, 47, 51, 53, 58, 59, 61, 62, 65, 66, 67, 69, 71, 73, 74, 77, 79, 82, 83, 85, 86, 87, 91, 93, 94, 97\}\).

Thank you for listening! :)