Tools for Fermat's Last Theorem

1. An overview of the proof of Fermat's Last Theorem.

We will sketch the proof of the following assertion:

- **Fermat's Last Theorem.**

For \( n > 2 \), we have

\[
\begin{align*}
\text{FLT}(n): & \quad a^n + b^n = c^n \text{ for } a, b, c \in \mathbb{Z} \\
\Rightarrow & \quad abc = 0.
\end{align*}
\]

**History of the proof.**

1) Fermat (~1640) proved FLT(4).

2) Euler (1758-1770) proved FLT(3).

- **Note:** since FLT(d) \( \Rightarrow \) FLT(n) whenever d|n, it suffices to prove FLT(p) for all primes \( p \geq 5 \).

- The proof uses the rich arithmetic theory of elliptic curves, modular forms, and Galois representations. We emphasise the contributions of:

3) Gerhard Frey (1985), who suggested that the existence of a solution of the Fermat equation might contradict the Modularity Conjecture of Taniyama, Shimura and Weil.

4) Jean-Pierre Serre (1985-6), who formulated a conjecture about modular forms and Galois representations mod \( p \) and showed how a small part of this conjecture (the epsilon conjecture) plus the Modularity Conjecture would imply Fermat's last Theorem.
5) Ken Ribet (1986), who proved Serre's epsilon conjecture.

6) Andrew Wiles (1994), who identified the numerical criterion from which the Modularity Conjecture would follow, and proved it.

7) Richard Taylor (1994), who collaborated with Wiles on the proof of the numerical criterion in the minimal case.

Outline of the proof

The proof we'll sketch follows a program outlined by Serre:

1) Fix a prime $p \geq 5$ and suppose $a, b, c \in \mathbb{Z}$ satisfy $a^p + b^p + c^p = 0$, but $abc \neq 0$. We call $(a^p, b^p, c^p)$ a "remarkable" triple.

2) To this triple, we associate a semistable elliptic curve $E_{a^p, b^p, c^p}$ over $\mathbb{Q}$ (due to Frey and, independently, Hellegouarch).

3) By Wiles's semistable Modularity Theorem, we deduce the existence of a modular form $f_{a^p, b^p, c^p}$ associated to $E_{a^p, b^p, c^p}$ by the Eichler-Shimura correspondence.

4) To $f_{a^p, b^p, c^p}$ we associate a Galois representation mod $p$:

$$\overline{\rho}_{a^p, b^p, c^p} : G \to GL_2(\mathbb{F}_p).$$

Frey and Serre noted that $\overline{\rho}_{a^p, b^p, c^p}$ can only ramify at 2 and (rather mildly) at $p$.

But we don't expect to have large Galois representations with so little ramification. In fact, Serre conjectured and Ribet proved that $\overline{\rho}_{a^p, b^p, c^p}$ cannot exist.
A remarkable Elliptic Curve.

For any triple \((A, B, C)\) of coprime integers satisfying \(A + B + C = 0\), Frey considered the elliptic curve \(E_{A,B,C}\) with Weierstrass equation:

\[
E_{A,B,C} : y^2 = x(x - A)(x + B).
\]

We just need to consider the case where \((A, B, C) = (a^p, b^p, c^p)\) corresponds to a hypothetical solution of Fermat's equation. Without loss of generality, assume \(a \equiv -1 \pmod{4}\) and \(21b\).

**Proposition 1.**

Let \(p \geq 5\) be prime and let \(a, b, c\) be coprime integers satisfying \(a^p + b^p + c^p = 0\), \(abc \neq 0\), \(a \equiv -1 \pmod{4}\) and \(21b\). Then \(E_{a^p, b^p, c^p}\) is a semistable elliptic curve with:

(a) Minimal discriminant \(\Delta_{a^p, b^p, c^p} = 2^{-8} (abc)^{2p}\), and

(b) Conductor \(N_{a^p, b^p, c^p} = \prod \ell labc\).

**Remark.** Szpiro's conjecture says, loosely speaking, that the minimal discriminant and the conductor of an elliptic curve \(E/\mathbb{Q}\) should be close to one another. However, Proposition 1 shows that a counterexample to FLT(p) for big enough \(p\) would produce an elliptic curve contradicting this conjecture.
Galois Representations.

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and endow $G_{\overline{\mathbb{Q}}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with the profinite topology.

**Definition.**

A two-dimensional Galois representation over a topological ring $A$ is a continuous group homomorphism

$$\rho : G_{\overline{\mathbb{Q}}} \rightarrow \text{GL}_2(A).$$

**Example.**

Let $E/\mathbb{Q}$ be an elliptic curve. Then for each $n \geq 0$, $G_{\overline{\mathbb{Q}}}$ acts on the group $E[p^n] \sim \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ of $p^n$-torsion points on $E$.

Since this action commutes with multiplication by $p$ on $E$, $G_{\overline{\mathbb{Q}}}$ acts naturally on the Tate module

$$T_p(E) := \lim_{\leftarrow} E[p^n] \sim \mathbb{Z}_p^2,$$

and we obtain the $p$-adic Galois representation associated to $E$:

$$\rho_{E,p} : G_{\overline{\mathbb{Q}}} \rightarrow \text{GL}_2(\mathbb{Z}_p^2).$$

The residual representation $\overline{\rho}_{E,p} : G_{\overline{\mathbb{Q}}} \rightarrow \text{GL}_2(F_p)$ describes the action of $G_{\overline{\mathbb{Q}}}$ on $E[p] \sim F_p^2$.

**Now,** let $E := E_{a,p,b,c,p}$ and consider the Galois representation

$$\overline{\rho}_{a,p,b,c,p} : G_{\overline{\mathbb{Q}}} \rightarrow \text{GL}_2(F_p)$$

defined as $\overline{\rho}_{a,p,b,c,p} := \overline{\rho}_{E,p}$. 
Theorem (Frey-Serre).

Let $p > 5$ be prime and $a, b, c \in \mathbb{Z}$ satisfy $a^p + b^p + c^p = 0$, $abc \neq 0$, $a \equiv -1 \mod 4$ and $2|b$. Then

a) $\overline{\mathbb{F}}_{a^p, b^p, c^p}$ is absolutely irreducible,

b) $\overline{\mathbb{F}}_{a^p, b^p, c^p}$ is odd,

c) $\overline{\mathbb{F}}_{a^p, b^p, c^p}$ is unramified outside $2p$ and flct at $p$.

Remarks.

1) We'll define the above terms during the following lectures.

2) It is believed that there is no Galois representation $\overline{\rho}_a : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ satisfying (a), (b) and (c). Moreover, we know that such a $\overline{\rho}_a$ couldn't come from a modular form (see Ribet's theorem below).

Galois representations associated to newforms.

Fix a prime $p$. Let $f = \sum a_n q^n$ be a weight two normalized newform of conductor $N$ and character $\epsilon$. The theory of Eichler-Shimura associates to $f$ a ring $\mathcal{O}_p$ and an odd Galois representation

$S_f : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_p)$

such that for all large enough primes $\ell$, $S_f$ is unramified at $\ell$, $\text{Trace} (S_f(\text{Frob}_{\ell})) = a_{\ell}$, and

$\text{det} (S_f(\text{Frob}_{\ell})) = \epsilon(\ell) \ell$. 

**Ribet's Theorem (Serre's Epsilon Conjecture).**

Let $f$ be a weight 2 newform of conductor $N \ell$ where $\ell k N$ is a prime. Suppose $\overline{f}$ is absolutely irreducible and that one of the following is true:

- $\overline{f}$ is unramified at $\ell$, or
- $\ell = p$ and $\overline{f}$ is flat at $p$.

Then there is a weight 2 newform $g$ of conductor $N$ such that $\overline{f} \sim \overline{g}$.

**Remark:** This theorem is a special case of Serre's conjectures about modularity of Galois representations over finite fields.

**The Modularity Conjecture and Wiles's Theorem.**

**Definition.**

An elliptic curve $E/\mathbb{Q}$ is **modular** if there is a weight 2 newform of conductor $N E$ and trivial character for which

$$L(f, s) = L(E, s).$$

**Note:** In particular, if $E$ is modular and $f$ corresponds to $E$ as above, then $\overline{f}_{E, p} = \overline{f}_{E, p}$.

**Modularity Conjecture (Shimura, Taniyama, Weil).**

Every elliptic curve over $\mathbb{Q}$ is modular.

**Wiles's Theorem.**

Every semistable elliptic curve over $\mathbb{Q}$ is modular.
• **Remark**: The Modularity Conjecture is now a theorem, thanks to the work of Diamond (1996), Conrad, Diamond and Taylor (1999), and Breuil et al., which completed the proof building on Wiles's work.

**The proof of Fermat's Last Theorem.**

• Fix a prime $p > 5$ and suppose $a, b, c \in \mathbb{Z}$ satisfy $a^p + b^p + c^p = 0$ but $abc \neq 0$. Without loss of generality, assume $a \equiv -1 \pmod{4}$ and $2|b$.

• Let $E_{a^p, b^p, c^p}$ be the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ and let $S_{a^p, b^p, c^p}$ be the associated $p$-adic Galois representation.

• By Proposition 1, $E_{a^p, b^p, c^p}$ is semistable and has conductor

$$N_{a^p, b^p, c^p} = \prod \ell_{a b c}.$$

• Hence, by Wiles's Theorem, $E_{a^p, b^p, c^p}$ is modular and there is a weight 2 newform $f_{a^p, b^p, c^p}$ of conductor $N_{a^p, b^p, c^p}$ associated to $E_{a^p, b^p, c^p}$. In particular, $S_{a^p, b^p, c^p} \sim \overline{S}_{f_{a^p, b^p, c^p}}$.

• By Frey–Serre's Theorem, $\overline{S}_{f_{a^p, b^p, c^p}}$ is absolutely irreducible, unramified outside $2p$, and flat at $p$.

• Therefore, by Ribet's Theorem, there is a weight 2 newform $g$ of conductor 2 such that $\overline{S}_{g} \sim \overline{S}_{f_{a^p, b^p, c^p}}$. But

$$\dim( S_2(\Gamma_0(2))) = \text{genus}(X_0(2)) = 2,$$ so there are no weight 2 newforms of conductor 2.