From Fermat’s Last Theorem to some Generalized Fermat Equations

Nuno Freitas

Universitat de Barcelona

January 2012
A **number field** is a finite extension $K/\mathbb{Q}$

$L$ is a finite extension of $\mathbb{Q}_l$

$\mathbb{F}_{p^r}$ is the finite field of $p^r$ elements.

$\mathcal{O}_k :=$ Ring of integers of the field $k$

$\bar{k}$ is the algebraic closure of $k$

$\bar{\mathbb{Z}}$ ring of integers of $\bar{\mathbb{Q}}$ and $G_{\mathbb{Q}} := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

**A Galois Representation** is a continuous (to the Krull topology) homomorphism $\rho : G_{\mathbb{Q}} \rightarrow GL_2(L)$ or $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_{p^r})$.

$K_\lambda$ is the localization of $K$ at the prime $\lambda$
The Modular Approach:

**OBJECTIVE**

Show that there are no solutions to equations with form:

(I) \( x^p + 2^\alpha y^p = z^p, \quad \alpha \geq 0 \)

(II) \( x^5 + y^5 = dz^p, \quad d = 2, 3 \)

The core of the approach was given by Frey, Hellegouarch, Serre, Ribet, Wiles:

(1) Construction of an elliptic Frey-Hellegouarch curve \( E \),
(2*) Modularity results for \( p \)-adic representations \( \rho_{E,p} \), attached to \( E \)
(3) Irreducibility of the mod \( p \) representations \( \bar{\rho}_{E,p} \) attached to \( E \),
(4*) Lowering the level results for representations attached to newforms \( \rho_{f,p} \)
(5) Contradicting the congruence \( \rho_{E,p} \equiv \rho_{f,p} \pmod{\mathfrak{P}} \)

(2)+(4) Serre Conjecture over \( \mathbb{Q} \)
The Modular Approach:

**OBJECTIVE**

Show that there are no solutions to equations with form:

(I) \( x^p + 2^\alpha y^p = z^p, \quad \alpha \geq 0 \)

(II) \( x^5 + y^5 = dz^p, \quad d = 2, 3 \)

The core of the approach was given by Frey, Hellegouarch, Serre, Ribet, Wiles:

(1) Construction of an elliptic Frey-Hellegouarch curve \( E \),
(2\*) Modularity results for \( p \)-adic representations \( \rho_{E,p} \), attached to \( E \),
(3) Irreducibility of the mod \( p \) representations \( \bar{\rho}_{E,p} \) attached to \( E \),
(4\*) Lowering the level results for representations attached to newforms \( \rho_{f,p} \),
(5) Contradicting the congruence \( \rho_{E,p} \equiv \rho_{f,p} \pmod{p^3} \)

(2)+(4) Serre Conjecture over \( \mathbb{Q} \)
The Modular Approach:

OBJECTIVE
Show that there are no solutions to equations with form:

(I) \( x^p + 2^\alpha y^p = z^p, \quad \alpha \geq 0 \)

(II) \( x^5 + y^5 = dz^p, \quad d = 2, 3 \)

The core of the approach was given by Frey, Hellegouarch, Serre, Ribet, Wiles:

(1) Construction of an elliptic Frey-Hellegouarch curve \( E \),
(2*) Modularity results for \( p \)-adic representations \( \rho_{E,p} \), attached to \( E \)
(3) Irreducibility of the mod \( p \) representations \( \bar{\rho}_{E,p} \) attached to \( E \),
(4*) Lowering the level results for representations attached to newforms \( \rho_{f,p} \)
(5) Contradicting the congruence \( \rho_{E,p} \equiv \rho_{f,p} \pmod{\mathfrak{M}} \)

(2)+(4) Serre Conjecture over \( \mathbb{Q} \)
The Modular Approach:

**OBJECTIVE**

Show that there are no solutions to equations with form:

(I) \( x^p + 2^\alpha y^p = z^p \), \( \alpha \geq 0 \)

(II) \( x^5 + y^5 = dz^p \), \( d = 2, 3 \)

The core of the approach was given by Frey, Hellegouarch, Serre, Ribet, Wiles:

1. Construction of an elliptic Frey-Hellegouarch curve \( E \),
2. Modularity results for \( p \)-adic representations \( \rho_{E,p} \), attached to \( E \)
3. Irreducibility of the mod \( p \) representations \( \bar{\rho}_{E,p} \) attached to \( E \),
4. Lowering the level results for representations attached to newforms \( \rho_{f,p} \)
5. Contradicting the congruence \( \rho_{E,p} \equiv \rho_{f,p} \pmod{\mathfrak{p}} \)

(2)+(4) Serre Conjecture over \( \mathbb{Q} \)
Elliptic Curves

Definition

Let $k$ be a field and $\bar{k}$ an algebraic closure of $k$. A **Weierstrass equation over** $k$ is any cubic equation of the form

$$E : y^2 + a_1 y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

where all $a_i \in k$. If $\text{char}(k) \neq 2, 3$ it can be written

$$y^2 = x^3 + Ax + B, \quad A, B \in k$$

and has discriminant $\Delta(E) = 4A^3 + 27B^2$. If $\Delta(E) \neq 0$ then $E$ is **nonsingular** and the set

$$E = \{(x, y) \in \bar{k}^2 \text{ satisfying } E(x, y)\} \cup \{\infty\}$$

is an **elliptic curve over** $k$. 

Nuno Freitas  Generalized Fermat Equations
Theorem

- There is an abelian group structure on the set of points of an elliptic curves.
- (Mordell-Weil) This group is finitely generated when $k$ is a number field.
We denote by $E(\bar{\mathbb{Q}})[n]$ the points of order $n$.

Theorem

- $E(\bar{\mathbb{Q}})[n] \sim \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (think over $\mathbb{C}$!)
- There is an action of $G_{\mathbb{Q}}$ on $E(\bar{\mathbb{Q}})[n]$

Let $P_1, P_2$ be a basis of $E(\bar{\mathbb{Q}})[n]$ and $\sigma \in G_{\mathbb{Q}}$. We can write

$$(\sigma(P_1), \sigma(P_2)) = (P_1, P_2) \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix}.$$}

Theorem

The action of $G_{\mathbb{Q}}$ on $E(\bar{\mathbb{Q}})[n]$ defines a representation

$\overline{\rho}_{E,n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/n\mathbb{Z}),$

with image isomorphic $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. 
Let \( k = \mathbb{Q} \) and \( E/\mathbb{Q} \) be an elliptic curve. There exists an equivalent model of \( E \) with integer coefficients such that \( |\Delta(E)| \) is minimal. For such a model and a prime \( p \) we can consider the reduced curve over \( \mathbb{F}_p \):

\[
\tilde{E} : y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6
\]

and it can be seen that \( \tilde{E} \) has at most one singular point.

**Definition (type of reduction)**

We say that \( E \)

- has **good reduction** at \( p \) if \( \tilde{E} \) is an elliptic curve.
- has **bad multiplicative reduction** at \( p \) if \( \tilde{E} \) admits a double point with two distinct tangents (a node)
- has **bad additive reduction** at \( p \) if \( \tilde{E} \) admits a double point with only one tangent (a cusp)
The Conductor $N_E$

**“Definition”**

The **conductor** $N_E$ of an elliptic curve $E$ over $\mathbb{Q}$ is computed by Tate’s algorithm. It is the product $\prod_p p^{f_p}$ over the primes of bad reduction of $E$ and

$$f_p = \begin{cases} 
1 & \text{if has multiplicative reduction at } p \\
2 + \delta \geq 2 & \text{if } E \text{ has additive reduction at } p, \\
2 & \text{if } E \text{ has additive reduction at } p \text{ and } p \neq 2, 3.
\end{cases}$$

**Definition**

Let $E/\mathbb{Q}$ be an elliptic curve. We say that $E$ is semi-stable if at every prime $p$ the reduction of $E$ at $p$ is good or multiplicative.

**Theorem (Mazur)**

Let $p \geq 5$ be a prime and $E$ a semi-stable elliptic curve over $\mathbb{Q}$. Then, the representation $\bar{\rho}_{E,p}$ is irreducible.
The Conductor $N_E$

“Definition”

The **conductor** $N_E$ of an elliptic curve $E$ over $\mathbb{Q}$ is computed by Tate’s algorithm. It is the product $\prod_p p^{f_p}$ over the primes of bad reduction of $E$ and

$$f_p = \begin{cases} 
1 & \text{if has multiplicative reduction at } p \\
2 + \delta \geq 2 & \text{if } E \text{ has additive reduction at } p, \\
2 & \text{if } E \text{ has additive reduction at } p \text{ and } p \neq 2, 3.
\end{cases}$$

Definition

Let $E/\mathbb{Q}$ be an elliptic curve. We say that $E$ is semi-stable if at every prime $p$ the reduction of $E$ at $p$ is good or multiplicative.

Theorem (Mazur)

Let $p \geq 5$ be a prime and $E$ a semi-stable elliptic curve over $\mathbb{Q}$. Then, the representation $\bar{\rho}_{E,p}$ is irreducible.
We will now attach an $l$-adic representation. Fix a prime $l$ and consider the $l^n$-torsion sequence:

$$E[l] \xleftarrow{[l]} E[l^2] \xleftarrow{} E[l^3] \xleftarrow{} ...$$

taking the inverse limit we have the **Tate Module at $l$**

$$T_l(E) = \lim_{\leftarrow n} \{ E[l^n] \} \cong \mathbb{Z}_l \oplus \mathbb{Z}_l.$$ 

From the compatibility of the action of $G_\mathbb{Q}$ with $[l]$ we have an action on $T_l(E)$. Since $\text{Aut}(E[l^n])$ and $GL_2(\mathbb{Z}/l^n\mathbb{Z})$ are isomorphic we also have

$$\text{Aut}(T_l(E)) \cong GL_2(\mathbb{Z}_l),$$

hence there is a continuous homomorphism

$$\rho_{E,l} : G_\mathbb{Q} \to GL_2(\mathbb{Z}_l) \subset GL_2(\mathbb{Q}_l).$$
We will now attach an $l$-adic representation. Fix a prime $l$ and consider the $l^n$-torsion sequence:

$$E[l] \leftarrow E[l^2] \leftarrow E[l^3] \leftarrow \ldots$$

taking the inverse limit we have the **Tate Module at $l$**

$$T_l(E) = \lim_{\leftarrow n} \{E[l^n]\} \cong \mathbb{Z}_l \oplus \mathbb{Z}_l.$$

From the compatibility of the action of $G_\mathbb{Q}$ with $[l]$ we have an action on $T_l(E)$. Since $\text{Aut}(E[l^n])$ and $GL_2(\mathbb{Z}/l^n\mathbb{Z})$ are isomorphic we also have

$$\text{Aut}(T_l(E)) \xrightarrow{\sim} GL_2(\mathbb{Z}_l),$$

hence there is a continuous homomorphism

$$\rho_{E,l} : G_\mathbb{Q} \rightarrow GL_2(\mathbb{Z}_l) \subset GL_2(\mathbb{Q}_l).$$
Definition

Let $p$ be a prime and $p \subset \mathbb{Z}$ any maximal ideal over $p$. The decomposition and inertia groups at $p$ are defined by

- $D_p = \{ \sigma \in G_{\mathbb{Q}} : p^\sigma = p \}$ then $\sigma \in D_p$ acts on $\overline{\mathbb{Z}}/p = \overline{\mathbb{F}}_p$ as $(x + p)^\sigma = x^\sigma + p$

- $I_p = \{ \sigma \in D_p : x^\sigma \equiv x \pmod{p} \text{ for all } x \in \overline{\mathbb{Z}} \}$ is the kernel of the reduction $D_p \rightarrow G_{\mathbb{F}_p}$.

An absolute Frobenius element over $p$ is any preimage $\text{Frob}_p \in D_p$ of the Frobenious automorphism in $G_{\mathbb{F}_p}$ ($x \mapsto x^p$). $\text{Frob}_p$ are dense in $G_{\mathbb{Q}}$.

Definition

Let $\rho$ be a Galois representation and let $p$ be a prime. Then $\rho$ is said to be unramified at $p$ if the inertia subgroup $I_p$ is contained in $\text{Ker}(\rho)$ for any maximal ideal $p \subset \overline{\mathbb{Z}}$ lying over $p$. 
Definition

Let $p$ be a prime and $\mathfrak{p} \subset \mathbb{Z}$ any maximal ideal over $p$. The decomposition and inertia groups at $\mathfrak{p}$ are defined by

- $D_p = \{ \sigma \in G_{\mathbb{Q}} : p^\sigma = p \}$ then $\sigma \in D_p$ acts on $\mathbb{Z}/p = \overline{F}_p$ as $(x + p)^\sigma = x^\sigma + p$

- $I_p = \{ \sigma \in D_p : x^\sigma \equiv x \pmod{p} \text{ for all } x \in \mathbb{Z} \}$ is the kernel of the reduction $D_p \to G_{\mathbb{F}_p}$.

An absolute Frobenius element over $p$ is any preimage $\text{Frob}_p \in D_p$ of the Frobenious automorphism in $G_{\mathbb{F}_p}$ ($x \mapsto x^p$). $\text{Frob}_p$ are dense in $G_{\mathbb{Q}}$.

Definition

Let $\rho$ be a Galois representation and let $p$ be a prime. Then $\rho$ is said to be unramified at $p$ if the inertia subgroup $I_p$ is contained in $\text{Ker}(\rho)$ for any maximal ideal $\mathfrak{p} \subset \mathbb{Z}$ lying over $p$. 
Let $p \nmid N_E$ be a prime of good reduction for $E$ and define

$$a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p),$$

where $\#\tilde{E}(\mathbb{F}_p)$ is the number of points in the reduced curve $\tilde{E}$.

**Theorem**

The Galois representation $\rho_{E,l}$ is unramified at every prime $p \nmid lN_E$. For any such $p$ let $p \subset \tilde{\mathbb{Z}}$ be any maximal ideal over $p$. Then the characteristic equation of $\rho_{E,l}(\text{Frob}_p)$ is

$$x^2 - a_p(E)x + p = 0.$$

The Galois representation $\rho_{E,l}$ is irreducible.
Let $p \nmid N_E$ be a prime of good reduction for $E$ and define

$$a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p),$$

where $\#\tilde{E}(\mathbb{F}_p)$ is the number of points in the reduced curve $\tilde{E}$.

**Theorem**

The Galois representation $\rho_{E,l}$ is unramified at every prime $p \nmid lN_E$. For any such $p$ let $p \subset \hat{\mathbb{Z}}$ be any maximal ideal over $p$. Then the characteristic equation of $\rho_{E,l}(\text{Frob}_p)$ is

$$x^2 - a_p(E)x + p = 0.$$

The Galois representation $\rho_{E,l}$ is irreducible.
The **modular group** $SL_2(\mathbb{Z})$ is defined by

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

and has the important **congruence subgroups**

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \mod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod N \right\}$$

where “*” means unspecified. Clearly, $\Gamma_1(N) \subset \Gamma_0(N)$.
Let $\Gamma(N) \subset SL_2(\mathbb{Z})$ be a congruence subgroup. An holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is a **modular form of weight $k$ with respect to** $\Gamma(N)$ if

1. For all $\tau \in \mathcal{H}$ and $\alpha \in \Gamma(N)$,

$$f\left(\frac{a \tau + b}{c \tau + d}\right) = (c \tau + d)^k f(\tau)$$

2. For all $\alpha \in SL_2(\mathbb{Z})$, exists a Fourier expansion

$$(c \tau + d)^{-k} f\left(\frac{a \tau + b}{c \tau + d}\right) = \sum_{n=0}^{\infty} c_n q^{n/N}$$

where $q = e^{2\pi i \tau}$.

If in addition, $c_0 = 0$ in all the above Fourier expansions, then $f$ is a said to be a **cusp form**. When $\alpha = \text{Id}$ we denote the Fourier coefficients $c_n$ in (2) by $a_n(f)$. Denoted by $S_k(\Gamma(N))$ the set of the cusp forms of weight $k$ with respect to $\Gamma(N)$. 
Modular Forms

- $S_k(\Gamma(N))$ is a vector space over $\mathbb{C}$ of finite dimension.
- In particular, $S_2(\Gamma_0(2^t)) = \{0\}$ for $t \in \{0, 1, 2, 3, 4\}$ and $S_2(\Gamma_0(32))$ has dimension 1.
- $S_k(\Gamma_1(N)) = \bigoplus S_k(N, \epsilon)$, where the sum is over the Dirichlet characters $\epsilon$ of modulus $N$.
- $f \in S_k(N, \epsilon)$ if
  
  $$f\left(\frac{a\tau + b}{c\tau + d}\right) = \epsilon(d)(c\tau + d)^k f(\tau)$$
  
  for matrices in $\Gamma_0(N)$
- There are Hecke operators $T_n$ ($n \geq 1$) acting on $S_k(\Gamma(N))$.
- There are cuspforms that are eigenvectors for all $T_n$. In that case $T_n(f) = a_n(f)f$. If $f \in S_k(N, \epsilon)$ is such a form we say it is an eigenform of level $N$ and character $\epsilon$. We say $f$ is normalized if $a_1(f) = 1$. 
Denote by $\mathbb{Q}_f = \mathbb{Q}(\{a_p(f)\})$ the coefficient field of $f$.

**Theorem**

Let $f \in S_k(N, \epsilon)$ be a normalized eigenform with number field $\mathbb{Q}_f$. Let $l$ be a prime. For each maximal ideal $\lambda$ of $\mathcal{O}_{\mathbb{Q}_f}$ lying over $l$ there is an irreducible 2-dimensional Galois representation $\rho_{f,\lambda} : G_\mathbb{Q} \to GL_2(\mathbb{Q}_f,\lambda)$.

This representation is unramified at every prime $p \nmid lN$. For any such $p$ let $p \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over $p$. Then $\rho_{f,\lambda}(Frob_p)$ satisfies the polynomial equation

$$x^2 - a_p(f)x + \epsilon(p)p^{k-1} = 0.$$
A representation of $G_\mathbb{Q}$ is **odd** if $\rho(c) = -1$, where $c$ is the complex conjugation. Let $\chi_l$ be the $l$-adic cyclotomic character.

**Definition**

Let $L$ be a finite extension of $\mathbb{Q}_l$ and consider a Galois representation $\rho : G_\mathbb{Q} \to GL_2(L)$. Suppose that $\rho$ is irreducible, odd and that $\det \rho = \epsilon \chi_l^{k-1}$ where $\epsilon$ has finite image. Then $\rho$ is **modular of level** $M_f$ if there exists a newform $f \in S_k(M_f, \epsilon)$ and a prime $\lambda$ above $l$ such that $\mathbb{Q}_{f,\lambda}$ embeds in $L$ and such $\rho_{f,\lambda} \sim \rho$.

**Modularity Theorem**

Let $E/\mathbb{Q}$ be an elliptic curve. $E$ is modular of level $N_E$, i.e. there is a newform $f \in S_2(N_E, \epsilon = 1)$, such that $\rho_{E,l} \sim \rho_{f,l}$ for all $l$. In particular, $a_p(f) = a_p(E)$ for all primes $p \nmid N_E$. 
A representation of $G_Q$ is odd if $\rho(c) = -1$, where $c$ is the complex conjugation. Let $\chi_l$ be the $l$-adic cyclotomic character.

**Definition**

Let $L$ be a finite extension of $\mathbb{Q}_l$ and consider a Galois representation $\rho : G_Q \to GL_2(L)$. Suppose that $\rho$ is irreducible, odd and that $\det \rho = \epsilon \chi_l^{k-1}$ where $\epsilon$ has finite image. Then $\rho$ is **modular of level** $M_f$ if there exists a newform $f \in S_k(M_f, \epsilon)$ and a prime $\lambda$ above $l$ such that $Q_{f,\lambda}$ embeds in $L$ and such $\rho_{f,\lambda} \sim \rho$.

**Modularity Theorem**

Let $E/\mathbb{Q}$ be an elliptic curve. $E$ is modular of level $N_E$, i.e. there is a newform $f \in S_2(N_E, \epsilon = 1)$, such that $\rho_{E,l} \sim \rho_{f,l}$ for all $l$. In particular, $a_p(f) = a_p(E)$ for all primes $p \nmid N_E$. 
Modularity

We are also interested in modularity of mod $p$ representations. For example, those arising from $p$-torsion points of elliptic curves or abelian varieties.

**Definition**

An irreducible representation $\bar{\rho} : G_\mathbb{Q} \rightarrow GL_2(\overline{F}_p)$ is **modular of type** $(N, k, \epsilon)$ if there exists a newform $f \in S_k(N, \epsilon)$ and a maximal ideal $\lambda \subset \mathcal{O}_{Q_f}$ lying over $p$ such that $\bar{\rho}_{f,\lambda} \sim \bar{\rho}$.

Let $\bar{\rho} : G_\mathbb{Q} \rightarrow GL_2(\overline{F}_p)$ be odd and irreducible.

- Serre gives recipes to compute the $N(\bar{\rho})$ (Artin conductor), $k(\bar{\rho})$ and $\epsilon(\bar{\rho})$.
- There exists the notion of $\bar{\rho}$ being **finite** at a prime $l$.
- If $l \neq p$ then $\bar{\rho}$ being finite at $l$ is equivalent to being unramified.
We are also interested in modularity of mod $p$ representations. For example, those arising from $p$-torsion points of elliptic curves or abelian varieties.

**Definition**

An irreducible representation $\bar{\rho} : G_\mathbb{Q} \to GL_2(\overline{\mathbb{F}}_p)$ is **modular of type** $(N, k, \epsilon)$ if there exists a newform $f \in S_k(N, \epsilon)$ and a maximal ideal $\lambda \subset \mathcal{O}_{\mathbb{Q}f}$ lying over $p$ such that $\bar{\rho}_f,\lambda \sim \bar{\rho}$

Let $\bar{\rho} : G_\mathbb{Q} \to GL_2(\overline{\mathbb{F}}_p)$ be odd and irreducible.

- Serre gives recipes compute the $N(\bar{\rho})$ (**Artin conductor**), $k(\bar{\rho})$ and $\epsilon(\bar{\rho})$.
- There exists the notion of $\bar{\rho}$ being **finite** at a prime $l$.
- If $l \neq p$ then $\bar{\rho}$ being finite at $l$ is equivalent to being unramified.
Ex. for \( l = p \): if \( E \) is has multiplicative reduction at \( p \) and \( p | \nu_p(\Delta) \) or \( E \) has good reduction at \( p \) then \( \bar{\rho}_{E,p} \) is finite at \( p \).

\( N(\bar{\rho}) \) is divisible precisely by the primes \( l \) for which \( \bar{\rho} \) is not finite and depends only on \( \bar{\rho} | l \) for those primes.

**Level Lowering Theorem**

Let \( p \geq 3 \) be a prime. Let \( \bar{\rho} : G_\mathbb{Q} \to GL_2(\overline{\mathbb{F}}_p) \) be irreducible over \( \overline{\mathbb{F}}_p \) and modular of type \((N, 2, 1)\). If \( \bar{\rho} \) is finite at \( p \) then it is modular of type \((N(\bar{\rho}), 2, 1)\).

**Serre Conjecture (Khare, Wintenberger)**

Let \( \bar{\rho} : G_\mathbb{Q} \to GL_2(\overline{\mathbb{F}}_p) \) be odd and irreducible. The \( \bar{\rho} \) is modular of type \((N(\bar{\rho}), k(\rho), \epsilon(\rho))\).
Ex. for $l = p$: if $E$ is has multiplicative reduction at $p$ and $p | \nu_p(\Delta)$ or $E$ has good reduction at $p$ then $\bar{\rho}_{E,p}$ is finite at $p$.

$N(\bar{\rho})$ is divisible precisely by the primes $l$ for which $\bar{\rho}$ is not finite and depends only on $\bar{\rho}/l_i$ for those primes.

**Level Lowering Theorem**

Let $p \geq 3$ be a prime. Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_p)$ be irreducible over $\overline{\mathbb{F}}_p$ and modular of type $(N, 2, 1)$. If $\bar{\rho}$ is finite at $p$ then it is modular of type $(N(\bar{\rho}), 2, 1)$.

**Serre Conjecture (Khare, Wintenberger)**

Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_p)$ be odd and irreducible. The $\bar{\rho}$ is modular of type $(N(\bar{\rho}), k(\rho), \epsilon(\rho))$. 
The Generalized Fermat Equation

We will study the solutions of the equation

\[ x^p + 2^\alpha y^p + z^p = 0 \]

in the following order:

- \( \alpha = 0 \) (Fermat’s Last Theorem)
- \( \alpha > 1 \)
- \( \alpha = 1 \)

But first we need to introduce the Frey-Hellegouarch Curves!
Definition (ABC curve)

Let $A$, $B$, $C$ be non-zero coprime integers such that $A + B + C = 0$ and define the elliptic curve over $\mathbb{Q}$ given by

$$E_{A,B,C} : \quad y^2 = x(x - A)(x + B)$$

that has discriminant (not always minimal) of the form $\Delta = 2^4(ABC)^2$.

Theorem

When $A \equiv -1 \mod 4$ and $B \equiv 0 \mod 32$, then $E_{A,B,C}$ is semi-stable and its conductor is $\text{rad}(ABC)$, the product of the primes dividing $ABC$. 
Frey Curves

Definition *(ABC curve)*

Let $A, B, C$ be non-zero coprime integers such that $A + B + C = 0$ and define the elliptic curve over $\mathbb{Q}$ given by

$$E_{A,B,C} : \quad y^2 = x(x - A)(x + B)$$

that has discriminant (not always minimal) of the form $\Delta = 2^4(ABC)^2$.

Theorem

When $A \equiv -1 \mod 4$ and $B \equiv 0 \mod 32$, then $E_{A,B,C}$ is semi-stable and its conductor is $rad(ABC)$, the product of the primes dividing $ABC$. 
We need to understand the ramification of $\tilde{\rho}_{E,p}$.

**Theorem (Helllegouarch)**

Let $C/\mathbb{Q}$ be an elliptic curve and $l \neq 2, p$. If $l \mid N_C$ is of multiplicative reduction and $p\mid \nu_l(\Delta(C))$ then $\tilde{\rho}_{E,p}$ is unramified at $l$.

**Néron-Ogg-Shafarevich Criterium**

Let $C/\mathbb{Q}$ be an elliptic curve. $C$ has good reduction at $l$ if and only if $\rho_{C,p}$ is unramified at $l$ for some prime $p \neq l$ if and only if $\rho_{C,p}$ is unramified at $l$ for all primes $p \neq l$. 
Suppose \((a, b, c)\) is a non-trivial \((abc \neq 0)\) primitive (i.e. \(\gcd(a, b, c) = 1\)) solution of \(x^p + y^p = z^p\) and let

\[ A = a^p \quad B = b^p \quad C = c^p. \]

Without loss of generality we can suppose that \(a \equiv -1 \pmod{4}\) and \(b\) to be even.

**Corollary**

Let \(E = E_{a^p,b^p,c^p}\). For \(p \geq 5\), the representation \(\bar{\rho}_{E,p}\) is unramified outside \(2p\).

**Proof:** Let \(l \neq 2, p\).

- \(\Delta(E) = 2^4(ABC)^2 = 2^4(abc)^{2p}\)
- If \(l \nmid abc \Rightarrow l \nmid \Delta \Rightarrow E\) has good reduction at \(l \Rightarrow \rho_{E,p}\) is unramified at \(l\) by N-O-S \(\Rightarrow \bar{\rho}_{E,p}\) also is.
- \(p \geq 5 \Rightarrow B \equiv 0 \pmod{32}\) then \(E\) is semistable. If \(l \mid abc\) then by Hellgouarch theorem \(\bar{\rho}_{E,p}\) is not ramified at \(l\).
Fermat-Wiles Theorem

Let \( p \geq 5 \) be a prime. There are no non-trivial primitive solutions of \( x^p + y^p + z^p = 0 \).

**Proof:** Suppose that \((a, b, c)\) is a non-trivial primitive solution. Recall \( E = E_{a^p,b^p,c^p} \) is semi-stable with \( \Delta = 2^4(abc)^{2p} \).

- Modularity theorem (semi-stable case) \( \Rightarrow \rho_{E,p} \) is modular of level \( N_E \) \( \Rightarrow \bar{\rho}_{E,p} \) is modular of level \( N_E \).
- \( \bar{\rho}_{E,p} \) is irreducible by Mazur theorem.
- \( \bar{\rho}_{E,p} \) is unramified outside \( 2p \)
- \( p|\nu_p(\Delta) \) then \( \bar{\rho}_{E,p} \) is finite at \( p \) \( \Rightarrow N(\bar{\rho}_{E,p}) = 2 \).
- We can take \( N_E \) to be \( N(\bar{\rho}_{E,p}) \) by the LLT.
- \( S_2(\Gamma_0(2)) = \{0\} \Rightarrow \bar{\rho}_{E,p} \) is not modular, contradiction!
Fermat-Wiles Theorem

Let $p \geq 5$ be a prime. There are no non-trivial primitive solutions of $x^p + y^p + z^p = 0$.

**Proof:** Suppose that $(a, b, c)$ is a non-trivial primitive solution. Recall $E = E_{a^p, b^p, c^p}$ is semi-stable with $\Delta = 2^4(abc)^{2p}$.

- Modularity theorem (semi-stable case) $\Rightarrow \rho_{E,p}$ is modular of level $N_E$ $\Rightarrow \bar{\rho}_{E,p}$ is modular of level $N_E$.
- $\bar{\rho}_{E,p}$ is irreducible by Mazur theorem.
- $\bar{\rho}_{E,p}$ is unramified outside 2
- $p | \nu_p(\Delta)$ then $\bar{\rho}_{E,p}$ is finite at $p$ $\Rightarrow N(\bar{\rho}_{E,p}) = 2$.
- We can take $N_E$ to be $N(\bar{\rho}_{E,p})$ by the LLT.
- $S_2(\Gamma_0(2)) = \{0\}$ $\Rightarrow \bar{\rho}_{E,p}$ is not modular, contradiction!
\[ a^p + 2^\alpha b^p + c^p = 0, \quad 1 \leq \alpha \leq p - 1 \]

- Let \((a, b, c)\) be non-trivial and primitive solution
- Observe that for \(\alpha = 1\) there exist the solution \((-1, 1, -1)\)
- Put \(A = a^p, B = 2^\alpha b^p\) and \(C = c^p\)

From Tate’s algorithm we have:

- \(E = E_{A,B,C} : y^2 = x(x - A)(x + B)\) is semistable for \(l \neq 2\).
- \(N_E = 2^t \text{rad}'(ABC)\) with \(t \in \{0, 1, 3, 5\}\)
- \(4\mid B\) if and only if \(t \leq 3\)
- \(t = 5\) if and only if \(\text{ord}_2(B) = 1\)
Theorem

Let $p \geq 5$ be a prime and $\alpha > 1$. The equation $x^p + 2^\alpha y^p + z^p = 0$ has no non-trivial primitive solutions.

Proof: Recall that $N_E = 2^t \text{rad}'(ABC)$ and $\Delta = 2^s(abc)^{2p}$

- Modularity theorem $\Rightarrow \rho_{E,p}$ is modular of level $N_E$ $\Rightarrow \overline{\rho}_{E,p}$ is modular of level $N_E$.
- Suppose $\overline{\rho}_{E,p}$ irreducible for $p \geq 5$ (Mazur do not apply!)
- $\overline{\rho}_{E,p}$ unramified outside $2p$
- $\overline{\rho}_{E,p}$ is finite at $p$ $\Rightarrow N(\overline{\rho}_{E,p}) = 2^t$.
- We can take $N_E$ to be $N(\overline{\rho}_{E,p})$ by LLT
- $S_2(\Gamma_0(2^t)) = \{0\}$ for $t \in \{0, 1, 2, 3, 4\}$ and $S_2(\Gamma_0(32))$ has dimension 1.
- $N(\overline{\rho}_{E,p}) = 2^t \Rightarrow t = 5 \Rightarrow ord_2(B) = ord_2(2^\alpha b^p) = 1$, contradiction with $\alpha > 1$ or $b$ even
**Theorem**

The representation $\overline{\rho}_{E,p}$ is irreducible for $p \geq 5$.

**Proof:** Recall $N_{E} = 2^{t} \text{rad}'(ABC)$ with $t \in \{0, 1, 3, 5\}$

- Suppose $E$ semistable ($t = 0, 1$). Follows from Mazur theorem.
- $E$ not semistable $\Rightarrow$ the 2-part of $N_{E}$ is $2^{2+\delta} \Rightarrow \delta = 1, 3$
- Suppose $\overline{\rho}^{ss}|_{I_{2}} = \epsilon_{1} \oplus \epsilon_{2}$ is reducible
- $\delta = \text{cond}(\epsilon_{1}) + \text{cond}(\epsilon_{2})$
- $\det \overline{\rho} = \overline{\chi}_{\rho} = \epsilon_{1}\epsilon_{2}$ is unramified at 2 $\Rightarrow \epsilon_{2} = \epsilon_{1}^{-1}$
- Then $\delta = 2 \text{cond}(\epsilon_{1})$ is even, contradiction.
- Thus $\overline{\rho}|_{I_{2}}$ is irreducible $\Rightarrow \overline{\rho}$ irreducible.
Observe that $E_0 = E_{(-1,1,-1)}$ by Modularity and LLT must correspond to the eigenform in $S_2(\Gamma_0(32))$. The same is true for any other $E_{(a,b,c)}$.

**Proposition**

If $p \equiv 1 \mod 4$, then the image of $\bar{\rho}_{E_0,p}$ is contained in the normalizer of a Cartan split subgroup of $GL_2(\mathbb{F}_p)$.

**Mazur-Momose Theorem**

Let $p \geq 17$ and $C/\mathbb{Q}$ be an elliptic curve. If the image of $\bar{\rho}_{C,p}$ is contained in the normalizer of a Cartan split subgroup of $GL_2(\mathbb{F}_p)$ then $C$ can not have multiplicative reduction at primes $\mathfrak{l} \neq 2$. 
Theorem

Let $p \geq 17$ and $p \equiv 1 \mod 4$. Let $(a, b, c)$ be non-trivial primitive solution of $x^p + 2y^p + z^p = 0$. Then $(a, b, c) = (-1, 1, -1)$.

Proof:

- We can suppose that $a, b, c$ are all odd.
- $N_E = 2^t \text{rad}'(ABC) \Rightarrow E$ has multiplicative reduction at all odd primes dividing $abc$.
- Since $p \equiv 1 \mod 4$ and $\bar{\rho}_{E,p} \equiv \bar{\rho}_{E_0,p}$ by the proposition $\bar{\rho}_{E,p}$ is under Mazur-Momose hypothesis.
- Then by Mazur-Momose $E$ has no primes of multiplicative reduction hence $abc = \pm 1$
- Thus, the only normalized solution is $(-1,1,-1)$. 
Now we proceed to the generalized equation!

<table>
<thead>
<tr>
<th>Theorem (Billerey and Billerey, Dieulefait)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let $d = 2^\alpha 3^\beta 5^\gamma$ where $\alpha \geq 2$, $\beta, \gamma, \geq 0$, or $d = 7, 13$. Then, for $p &gt; 19$ the equation $x^5 + y^5 = dz^p$ has no non-trivial primitive solution.</td>
</tr>
</tbody>
</table>

Let $\gamma$ be an integer divisible only by primes $l \not\equiv 1 \pmod{5}$.

<table>
<thead>
<tr>
<th>Theorem (Dieulefait, F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>For any $p &gt; 13$ such that $p \equiv 1 \pmod{4}$ and $p \equiv \pm 1 \pmod{5}$, the equation $x^5 + y^5 = 2\gamma z^p$ has no non-trivial primitive solutions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Theorem (Dieulefait, F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>For any $p &gt; 73$ such that $p \equiv 1 \pmod{4}$, the equation $x^5 + y^5 = 3\gamma z^p$ has no non-trivial primitive solutions.</td>
</tr>
</tbody>
</table>
The equation $x^5 + y^5 = dz^p$

Now we proceed to the generalized equation!

**Theorem (Billerey and Billerey, Dieulefalt)**

Let $d = 2^\alpha 3^\beta 5^\gamma$ where $\alpha \geq 2$, $\beta, \gamma \geq 0$, or $d = 7, 13$. Then, for $p > 19$ the equation $x^5 + y^5 = dz^p$ has no non-trivial primitive solution.

Let $\gamma$ be an integer divisible only by primes $l \equiv \not 1 \pmod{5}$.

**Theorem (Dieulefait, F)**

For any $p > 13$ such that $p \equiv 1 \pmod{4}$ and $p \equiv \pm 1 \pmod{5}$, the equation $x^5 + y^5 = 2\gamma z^p$ has no non-trivial primitive solutions.

**Theorem (Dieulefait, F)**

For any $p > 73$ such that $p \equiv 1 \pmod{4}$, the equation $x^5 + y^5 = 3\gamma z^p$ has no non-trivial primitive solutions.
Now we proceed to the generalized equation!

**Theorem (Billerey and Billerey, Dieulefait)**

Let \( d = 2^\alpha 3^\beta 5^\gamma \) where \( \alpha \geq 2, \beta, \gamma, \geq 0 \), or \( d = 7, 13 \). Then, for \( p > 19 \) the equation \( x^5 + y^5 = dz^p \) has no non-trivial primitive solution.

Let \( \gamma \) be an integer divisible only by primes \( l \not\equiv 1 \pmod{5} \).

**Theorem (Dieulefait, F)**

For any \( p > 13 \) such that \( p \equiv 1 \pmod{4} \) and \( p \equiv \pm 1 \pmod{5} \), the equation \( x^5 + y^5 = 2^\gamma z^p \) has no non-trivial primitive solutions.

**Theorem (Dieulefait, F)**

For any \( p > 73 \) such that \( p \equiv 1 \pmod{4} \), the equation \( x^5 + y^5 = 3^\gamma z^p \) has no non-trivial primitive solutions.
Let \((a, b, c)\) be a primitive solution to \(x^5 + y^5 = d\gamma z^p\). From

**Key factorization:**

\[
x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4) = (x + y)\phi(x, y)
\]

can be seen that

We need to prove that \(\phi(x, y) = rz^p\) where \(r = 1, 5\) has no non-trivial primitive solutions if \(d \mid a + b\).

Observe that over \(\mathbb{Q}(\sqrt{5})\)

- \(\phi(x, y) = \phi_1(x, y)\phi_2(x, y)\), where
- \(\phi_1(x, y) = x^2 + \omega xy + y^2\) and \(\phi_2(x, y) = x^2 + \bar{\omega} xy + y^2\), with
- \(\omega = \frac{-1+\sqrt{5}}{2}\), \(\bar{\omega} = \frac{-1-\sqrt{5}}{2}\)
Let \((a, b, c)\) be a primitive solution of \(\phi(x, y) = rz^p\).

**Definition (Frey-curve)**

Consider over \(\mathbb{Q}(\sqrt{5})\) the curve given by

\[
E_{(a,b)} : y^2 = x^3 + 2(a + b)x^2 - \bar{\omega}_\phi(a, b)x,
\]

with \(\Delta(E) = 2^6\bar{\omega}_\phi\phi_1\), where

- There are Galois representations \(\rho_{E,l}\) and \(\bar{\rho}_{E,l}\) of \(G_{\mathbb{Q}}(\sqrt{5})\)
- We need to extend them to \(G_{\mathbb{Q}}\) and compute \((N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))\) to apply Serre conjecture
From Serre conjecture there is a newform $f$ of type $(M, 2, \bar{\epsilon})$ with $M = 1600, 800, 400$ or $100$ and a prime $\mathfrak{p}$ in $\mathbb{Q}_f$ above $p$ such that $\bar{\rho} \equiv \bar{\rho}_f,\mathfrak{p} (\text{mod } \mathfrak{p})$

Observe that $\mathbb{Q}(i) = \mathbb{Q}(\bar{\epsilon}) \subseteq \mathbb{Q}_f$ and define the sets:

S1: Newforms with CM (Complex Multiplication),
S2: Newforms without CM and field of coefficients strictly containing $\mathbb{Q}(i)$,
S3: Newforms without CM and field of coefficients $\mathbb{Q}(i)$
From Serre conjecture there is a newform \( f \) of type \((M, 2, \bar{\epsilon})\) with \( M = 1600, 800, 400 \) or 100 and a prime \( \mathfrak{p} \) in \( \Bbb{Q}_f \) above \( p \) such that \( \bar{\rho} \equiv \bar{\rho}_{f, \mathfrak{p}} (\text{mod } \mathfrak{p}) \)

Observe that \( \Bbb{Q}(i) = \Bbb{Q}(\bar{\epsilon}) \subseteq \Bbb{Q}_f \) and define the sets:

\begin{align*}
\text{S1: } & \text{Newforms with CM (Complex Multiplication),} \\
\text{S2: } & \text{Newforms without CM and field of coefficients strictly containing } \Bbb{Q}(i), \\
\text{S3: } & \text{Newforms without CM and field of coefficients } \Bbb{Q}(i)
\end{align*}