Modularity and the Fermat Equation over Totally Real Fields

Samir Siksek (University of Warwick)

9 July 2014

What are the most important problems in number theory?

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.

(ii) Diophantine equations, e.g. $x^n + y^n = z^n$.

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.

(ii) Diophantine equations, e.g. $x^n + y^n = z^n$.

(iii) Number fields, rings of integers, class groups, unit groups.

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.

(ii) Diophantine equations, e.g. $x^n + y^n = z^n$.

(iii) Number fields, rings of integers, class groups, unit groups.

(iii) Understanding $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.

(ii) Diophantine equations, e.g. $x^n + y^n = z^n$.

(iii) Number fields, rings of integers, class groups, unit groups.

(iii) Understanding $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Motivation $G_{\mathbb{Q}}$:

1. Take all the problems in algebraic number theory and Galois theory that we can't solve,

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.
(ii) Diophantine equations, e.g. $x^n + y^n = z^n$.
(iii) Number fields, rings of integers, class groups, unit groups.
(iii) Understanding $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Motivation $G_{\mathbb{Q}}$:

1. Take all the problems in algebraic number theory and Galois theory that we can't solve,
2. put them into one big object,

What are the most important problems in number theory?

Possible answers:

(i) Distribution of primes.

(ii) Diophantine equations, e.g. $x^n + y^n = z^n$.

(iii) Number fields, rings of integers, class groups, unit groups.

(iii) Understanding $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Motivation $G_{\mathbb{Q}}$:

1. Take all the problems in algebraic number theory and Galois theory that we can't solve,
2. put them into one big object,
3. say "I want to understand that".

Algebraic Numbers

Definition

Let $\alpha \in \mathbb{C}$.

- We say that α is an **algebraic number** if there is some non-zero polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.
- We say that α is **algebraic integer** if there is some *monic* polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Example

- $\sqrt{-2}$ is an algebraic integer, because it is a root of $x^2 + 2$.
- $1/\sqrt{-2}$ is an algebraic number, but not an algebraic integer; it is a root of $2x^2 + 1$.
- π, e are not algebraic.

Definition

Field of algebraic numbers: $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic number}\}$.
Ring of algebraic integers: $\mathcal{O}_{\overline{\mathbb{Q}}} = \{\alpha \in \overline{\mathbb{Q}} \ : \ \alpha \text{ is an algebraic integer}\}$.

Definition

A **number field** K is a finite extension of $\mathbb{Q}$. (Note: $K \subset \overline{\mathbb{Q}}$). We define its **ring of integers** by
$\mathcal{O}_K = \{\alpha \in K \ : \ \alpha \text{ is an algebraic integer}\} = K \cap \mathcal{O}_{\overline{\mathbb{Q}}}$.

Example

$\mathbb{Q}$ is a number field, and its ring of integers is $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Example

$K = \mathbb{Q}(\sqrt{5})$ is a number field, and its ring of integers is

$$\mathcal{O}_K = \mathbb{Z} + \left(\frac{1+\sqrt{5}}{2}\right)\mathbb{Z}.$$

$G_{\mathbb{Q}}$

Definition

Let K be a number field (thus $K \subset \overline{\mathbb{Q}}$). Define

$$G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K) = \{\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}) \ : \ \sigma(\alpha) = \alpha \text{ for all } \alpha \in K\}.$$

Fact:

1. $$G_{\mathbb{Q}} = \varprojlim \mathrm{Gal}(L/\mathbb{Q})$$
   where L runs through the finite Galois extensions of $\mathbb{Q}$.
2. If K is a number field, then $G_K \subset G_{\mathbb{Q}}$.
3. If K is a Galois number field, then G_K is normal in $G_{\mathbb{Q}}$ and
   $$G_{\mathbb{Q}}/G_K = \mathrm{Gal}(K/\mathbb{Q}).$$

Ramification

Definition

Let K be a number field, and $\ell \in \mathbb{Z}$ a prime number. We say that ℓ **ramifies in** K if $\ell\mathcal{O}_K$ is **not** squarefree.

Example

Let $K = \mathbb{Q}(\sqrt{2})$. The $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{2}$. Moreover,

$$2\mathcal{O}_K = (\sqrt{2}\mathcal{O}_K)^2.$$

So 2 ramifies in $\mathbb{Q}(\sqrt{2})$. All other primes are unramified.

For each prime ℓ there is a subgroup $I_\ell \subset G_\mathbb{Q}$ called the ℓ-th **ramification group** whose job is to detect ramification. If K is Galois, then

$$\ell \text{ is ramified in } K \iff \pi_K(I_\ell) \neq 1,$$

where

$$\pi_K \ : \ G_\mathbb{Q} \to G_\mathbb{Q}/G_K \cong \mathrm{Gal}(K/\mathbb{Q}).$$

Linear Representations of G_K

Linear Representations of G_K

Want to understand all continuous linear representations

$$\rho \ : \ G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r}).$$

We say that ρ is **continuous** if the kernel is a subgroup of finite index.

Linear Representations of G_K

Want to understand all continuous linear representations

$$\rho \ : \ G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r}).$$

We say that ρ is **continuous** if the kernel is a subgroup of finite index.

Question: Describe all continuous ρ with a given

1. K, n, p^r,

Linear Representations of G_K

Want to understand all continuous linear representations

$$\rho \ : \ G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r}).$$

We say that ρ is **continuous** if the kernel is a subgroup of finite index.

Question: Describe all continuous ρ with a given

1. K, n, p^r,
2. **ramification data**

$$\mathcal{R} = \{\rho(I_\lambda) \ : \ \lambda \text{ a prime of } K\}.$$

Linear Representations of G_K

Want to understand all continuous linear representations

$$\rho \;:\; G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r}).$$

We say that ρ is **continuous** if the kernel is a subgroup of finite index.

Question: Describe all continuous ρ with a given

1. K, n, p^r,
2. **ramification data**

$$\mathcal{R} = \{\rho(I_\lambda) \;:\; \lambda \text{ a prime of } K\}.$$

$(\rho(I_\lambda) = 1$ for all but finitely many $\lambda)$

Partial Answers

Problem: Given K, n, p^r, describe all continuous $\rho : G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r})$ with a given ramification data $\mathcal{R}$.

Partial Answers

Problem: Given K, n, p^r, describe all continuous $\rho : G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r})$ with a given ramification data $\mathcal{R}$.

Theorem (Minkowski)

If $K = \mathbb{Q}$, and $\mathcal{R} = \{\rho(I_\lambda) = 1 \text{ for all } \lambda\}$ then $\rho = 1$. (Reformulation: The only unramified continuous representation of $G_{\mathbb{Q}}$ is 1.)

Partial Answers

Problem: Given K, n, p^r, describe all continuous $\rho : G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r})$ with a given ramification data $\mathcal{R}$.

Theorem (Minkowski)

If $K = \mathbb{Q}$, and $\mathcal{R} = \{\rho(I_\lambda) = 1$ for all $\lambda\}$ then $\rho = 1$. (Reformulation: The only unramified continuous representation of $G_{\mathbb{Q}}$ is 1.)

If $n = 1$, then class field theory gives an explicit answer, in terms of the class group and unit group of K.

Fermat's Last Theorem

Let $p \geq 3$ be a prime. The Fermat equation of degree p is

$$x^p + y^p + z^p = 0.$$

Let $(a, b, c) \in \mathbb{Z}^3$ be a solution. If $abc = 0$ we say that (a, b, c) is a **trivial solution**, otherwise we say that (a, b, c) is a **non-trivial solution**. If (a, b, c) is a non-trivial solution, we may assume after appropriate scaling that $\gcd(a, b, c) = 1$. Such a solution is called **primitive**.

Fermat's Last Theorem

Let $p \geq 3$ be a prime. The Fermat equation of degree p is

$$x^p + y^p + z^p = 0.$$

Let $(a, b, c) \in \mathbb{Z}^3$ be a solution. If $abc = 0$ we say that (a, b, c) is a **trivial solution**, otherwise we say that (a, b, c) is a **non-trivial solution**. If (a, b, c) is a non-trivial solution, we may assume after appropriate scaling that $\gcd(a, b, c) = 1$. Such a solution is called **primitive**.

Fermat's Last Theorem is the claim that the only non-trivial primitive solutions to the Fermat equation are $(1, -1, 0)$ and its permutations.

Fermat's Last Theorem and Kummer

Fermat's Last Theorem and Kummer

Theorem (Kummer)

Let $p \geq 3$ be a prime.

Fermat's Last Theorem and Kummer

Theorem (Kummer)

Let $p \geq 3$ be a prime. Let ζ_p be a primitive p-th root of unity, and write $K = \mathbb{Q}(\zeta_p)$.

Fermat's Last Theorem and Kummer

Theorem (Kummer)

Let $p \geq 3$ *be a prime. Let* ζ_p *be a primitive* p*-th root of unity, and write* $K = \mathbb{Q}(\zeta_p)$*. Let* $(a, b, c) \in \mathbb{Z}^3$ *such that* $a^p + b^p + c^p = 0$*,* $\gcd(a, b, c) = 1$ *and* $abc \neq 0$*.*

Fermat's Last Theorem and Kummer

Theorem (Kummer)

Let $p \geq 3$ be a prime. Let ζ_p be a primitive p-th root of unity, and write $K = \mathbb{Q}(\zeta_p)$. Let $(a, b, c) \in \mathbb{Z}^3$ such that $a^p + b^p + c^p = 0$, $\gcd(a, b, c) = 1$ and $abc \neq 0$. Define

$$\rho \ : \ G_K \to \langle \zeta_p \rangle, \qquad \sigma \mapsto \frac{\sigma(\sqrt[p]{a + b\zeta_p})}{\sqrt[p]{a + b\zeta_p}}.$$

Then ρ is non-trivial, continuous and unramified everywhere (i.e. $\rho(I_\lambda) = 1$ for all primes λ of K).

Fermat's Last Theorem and Kummer

Theorem (Kummer)

Let $p \geq 3$ be a prime. Let ζ_p be a primitive p-th root of unity, and write $K = \mathbb{Q}(\zeta_p)$. Let $(a, b, c) \in \mathbb{Z}^3$ such that $a^p + b^p + c^p = 0$, $\gcd(a, b, c) = 1$ and $abc \neq 0$. Define

$$\rho \ : \ G_K \to \langle \zeta_p \rangle, \qquad \sigma \mapsto \frac{\sigma(\sqrt[p]{a + b\zeta_p})}{\sqrt[p]{a + b\zeta_p}}.$$

Then ρ is non-trivial, continuous and unramified everywhere (i.e. $\rho(I_\lambda) = 1$ for all primes λ of K).

1. $\langle \zeta_p \rangle \leq \mathrm{GL}_1(\mathbb{F}_q)$ if $q \equiv 1 \pmod{p}$.

Fermat's Last Theorem and Kummer

Theorem (Kummer)

Let $p \geq 3$ be a prime. Let ζ_p be a primitive p-th root of unity, and write $K = \mathbb{Q}(\zeta_p)$. Let $(a, b, c) \in \mathbb{Z}^3$ such that $a^p + b^p + c^p = 0$, $\gcd(a, b, c) = 1$ and $abc \neq 0$. Define

$$\rho \ : \ G_K \to \langle \zeta_p \rangle, \qquad \sigma \mapsto \frac{\sigma(\sqrt[p]{a + b\zeta_p})}{\sqrt[p]{a + b\zeta_p}}.$$

Then ρ is non-trivial, continuous and unramified everywhere (i.e. $\rho(I_\lambda) = 1$ for all primes λ of K).

1. $\langle \zeta_p \rangle \leq \mathrm{GL}_1(\mathbb{F}_q)$ if $q \equiv 1 \pmod{p}$.
2. Class Field Theory:

$$\left\{ \begin{array}{l} \text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p \end{array} \right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Regular Primes

$$\left\{\begin{array}{l}\text{non-trivial, continuous}\\ \text{unramified } \rho : G_K \to C_p\end{array}\right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Regular Primes

$$\left\{ \begin{array}{l} \text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p \end{array} \right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Let $h_p = \# \mathrm{Cl}(\mathbb{Q}(\zeta_p))$. We say that p is **regular prime** if $p \nmid h_p$. Otherwise p is **irregular**.

Regular Primes

$$\left\{\begin{array}{l}\text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p\end{array}\right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Let $h_p = \# \mathrm{Cl}(\mathbb{Q}(\zeta_p))$. We say that p is **regular prime** if $p \nmid h_p$. Otherwise p is **irregular**.

Theorem (Kummer)

Fermat's Last Theorem is true for exponent p, if p is regular.

Regular Primes

$$\left\{ \begin{array}{l} \text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p \end{array} \right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Let $h_p = \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_p))$. We say that p is **regular prime** if $p \nmid h_p$. Otherwise p is **irregular**.

Theorem (Kummer)

Fermat's Last Theorem is true for exponent p, if p is regular.

1. The first few regular primes are 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, $41, \ldots$.

Regular Primes

$$\left\{ \begin{array}{l} \text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p \end{array} \right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Let $h_p = \# \mathrm{Cl}(\mathbb{Q}(\zeta_p))$. We say that p is **regular prime** if $p \nmid h_p$. Otherwise p is **irregular**.

Theorem (Kummer)

Fermat's Last Theorem is true for exponent p, if p is regular.

1. The first few regular primes are 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, ...
2. The first few irregular primes are 37, 59, 67, 101, 103, 131, 149, ...

Regular Primes

$$\left\{ \begin{array}{l} \text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p \end{array} \right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Let $h_p = \# \mathrm{Cl}(\mathbb{Q}(\zeta_p))$. We say that p is **regular prime** if $p \nmid h_p$. Otherwise p is **irregular**.

Theorem (Kummer)

Fermat's Last Theorem is true for exponent p, if p is regular.

1. The first few regular primes are 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, $41, \ldots$.
2. The first few irregular primes are 37, 59, 67, 101, 103, 131, $149, \ldots$.
3. Theorem (Jensen): There are infinitely many irregular primes.

Regular Primes

$$\left\{ \begin{array}{l} \text{non-trivial, continuous} \\ \text{unramified } \rho : G_K \to C_p \end{array} \right\} \longleftrightarrow \{\text{elements of order } p \text{ in } \mathrm{Cl}(K)\}$$

Let $h_p = \# \mathrm{Cl}(\mathbb{Q}(\zeta_p))$. We say that p is **regular prime** if $p \nmid h_p$. Otherwise p is **irregular**.

Theorem (Kummer)

Fermat's Last Theorem is true for exponent p, if p is regular.

1. The first few regular primes are 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, ...
2. The first few irregular primes are 37, 59, 67, 101, 103, 131, 149, ...
3. Theorem (Jensen): There are infinitely many irregular primes.
4. No one knows how to show that there are infinitely many regular primes.

Elliptic Curves

An **elliptic curve** over $\mathbb{Q}$ is an equation of the form

$$E \ : \ y^2 = x^3 + ax^2 + bx + c \qquad \text{(poly on the right must squarefree)}$$

where $a, b, c \in \mathbb{Q}$.

Elliptic Curves

An **elliptic curve** over $\mathbb{Q}$ is an equation of the form

$$E \ : \ y^2 = x^3 + ax^2 + bx + c \qquad \text{(poly on the right must squarefree)}$$

where a, b, $c \in \mathbb{Q}$.
If $K \supset \mathbb{Q}$ is a field, then we define the set of K-points

$$E(K) = \{(x, y) \in K^2 \ : \ y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}.$$

Elliptic Curves

An **elliptic curve** over $\mathbb{Q}$ is an equation of the form

$$E \ : \ y^2 = x^3 + ax^2 + bx + c \qquad \text{(poly on the right must squarefree)}$$

where a, b, $c \in \mathbb{Q}$.
If $K \supset \mathbb{Q}$ is a field, then we define the set of K-points

$$E(K) = \{(x, y) \in K^2 \ : \ y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}.$$

Facts:

1. $E(K)$ is an abelian group.
2. $E(\mathbb{C}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$.
3. Let $E[p]$ be the p-torsion subgroup in $E(\mathbb{C})$. Then
$$E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$
4. $E[p] \subset E(\overline{\mathbb{Q}})$ (the torsion points are alegebraic).
5. $G_{\mathbb{Q}}$ acts on $E[p]$. We obtain a continuous representation
$$\rho \ : \ G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

The Hellegouarch–Frey Curve

Theorem (Frey, 1985)

Let (a, b, c) *be a non-trivial primitive solution to the Fermat equation with exponent* p. *Let*

$$E \;:\; y^2 = x(x - a^p)(x + b^p) \qquad (\textbf{Hellegouarch–Frey curve}).$$

Then $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ *satisfies*

1. $\rho(I_\ell) = 1$ *for* $\ell \neq 2, p$.
2. $\rho(I_p) = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \;:\; a \in \mathbb{F}_p^* \right\}$.
3. $\rho(I_2) \subset \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \;:\; a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\}$.

The Hellegouarch–Frey Curve

Theorem (Frey, 1985)

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent p. Let

$$E \ : \ y^2 = x(x - a^p)(x + b^p) \qquad (\textbf{Hellegouarch–Frey curve}).$$

Then $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ satisfies

1. $\rho(I_\ell) = 1$ *for* $\ell \neq 2, p$.
2. $\rho(I_p) = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \ : \ a \in \mathbb{F}_p^* \right\}$.
3. $\rho(I_2) \subset \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \ : \ a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\}$.

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ *be a continuous, odd, irreducible representation, with given ramification data* $\mathcal{R}$*. Then there is a cuspidal eigenform* f *of level* $N_{\mathcal{R}}$ *and weight* $k_{\mathcal{R}}$ *such that* $\rho \sim \rho_{f,\pi}$*.*

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ *be a continuous, odd, irreducible representation, with given ramification data* $\mathcal{R}$*. Then there is a cuspidal eigenform* f *of level* $N_{\mathcal{R}}$ *and weight* $k_{\mathcal{R}}$ *such that* $\rho \sim \rho_{f,\pi}$*.*

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ *Fermat's Last Theorem.*

Serre's Modularity Conjecture

Theorem (Serre's Modularity Conjecture, 1986 Khare and Wintenberger Theorem, 2008)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ *be a continuous, odd, irreducible representation, with given ramification data* $\mathcal{R}$*. Then there is a cuspidal eigenform* f *of level* $N_{\mathcal{R}}$ *and weight* $k_{\mathcal{R}}$ *such that* $\rho \sim \rho_{f,\pi}$*.*

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ *Fermat's Last Theorem.*

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$.

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ *be a continuous, odd, irreducible representation, with given ramification data* $\mathcal{R}$*. Then there is a cuspidal eigenform* f *of level* $N_{\mathcal{R}}$ *and weight* $k_{\mathcal{R}}$ *such that* $\rho \sim \rho_{f,\pi}$*.*

Theorem (Serre)

Serre's Modularity Conjecture $\Longrightarrow$ *Fermat's Last Theorem.*

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let $E : y^2 = x(x - a^p)(x + b^p)$ (Hellegouarch–Frey curve).

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be a continuous, odd, irreducible representation, with given ramification data $\mathcal{R}$. Then there is a cuspidal eigenform f of level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$ such that $\rho \sim \rho_{f,\pi}$.

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ Fermat's Last Theorem.

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let $E : y^2 = x(x - a^p)(x + b^p)$ (Hellegouarch–Frey curve). Let $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Serre's Modularity Conjecture

Theorem (Serre's Modularity Conjecture, 1986 Khare and Wintenberger Theorem, 2008)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be a continuous, odd, irreducible representation, with given ramification data $\mathcal{R}$. Then there is a cuspidal eigenform f of level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$ such that $\rho \sim \rho_{f,\pi}$.

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ Fermat's Last Theorem.

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let $E : y^2 = x(x - a^p)(x + b^p)$ (Hellegouarch–Frey curve). Let $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. This is irreducible (Mazur),

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be a continuous, odd, irreducible representation, with given ramification data $\mathcal{R}$. Then there is a cuspidal eigenform f of level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$ such that $\rho \sim \rho_{f,\pi}$.

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ Fermat's Last Theorem.

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let $E : y^2 = x(x - a^p)(x + b^p)$ (Hellegouarch–Frey curve). Let $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. This is irreducible (Mazur), odd and continuous.

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be a continuous, odd, irreducible representation, with given ramification data $\mathcal{R}$. Then there is a cuspidal eigenform f of level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$ such that $\rho \sim \rho_{f,\pi}$.

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ Fermat's Last Theorem.

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let $E : y^2 = x(x - a^p)(x + b^p)$ (Hellegouarch–Frey curve). Let $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. This is irreducible (Mazur), odd and continuous. Let $\mathcal{R}$ be the ramification data (computed by Frey). Then $N_{\mathcal{R}} = 2$ and $k_{\mathcal{R}} = 2$.

Serre's Modularity Conjecture

**Theorem (Serre's Modularity Conjecture, 1986
Khare and Wintenberger Theorem, 2008)**

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be a continuous, odd, irreducible representation, with given ramification data $\mathcal{R}$. Then there is a cuspidal eigenform f of level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$ such that $\rho \sim \rho_{f,\pi}$.

Theorem (Serre)

Serre's Modularity Conjecture $\implies$ Fermat's Last Theorem.

Proof.

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let $E : y^2 = x(x - a^p)(x + b^p)$ (Hellegouarch–Frey curve). Let $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. This is irreducible (Mazur), odd and continuous. Let $\mathcal{R}$ be the ramification data (computed by Frey). Then $N_{\mathcal{R}} = 2$ and $k_{\mathcal{R}} = 2$. There are no cuspidal eigenforms of level 2 and weight 2. Contradiction. $\square$

Ribet and Wiles

Ribet and Wiles

Theorem (Ribet, 1987)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be odd, irreducible, continuous. If $\rho \sim \rho_{g,\pi}$ for some cuspidal eigenform g of any level and weight, then Serre's modularity conjecture holds for ρ.

Ribet and Wiles

Theorem (Ribet, 1987)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be odd, irreducible, continuous. If $\rho \sim \rho_{g,\pi}$ for some cuspidal eigenform g of any level and weight, then Serre's modularity conjecture holds for ρ.

Theorem (Wiles, 1994)

Let E be a semistable elliptic curve over $\mathbb{Q}$. Then E is modular.

Ribet and Wiles

Theorem (Ribet, 1987)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ *be odd, irreducible, continuous. If* $\rho \sim \rho_{g,\pi}$ *for some cuspidal eigenform* g *of any level and weight, then Serre's modularity conjecture holds for* ρ*.*

Theorem (Wiles, 1994)

Let E *be a semistable elliptic curve over* $\mathbb{Q}$*. Then* E *is modular. In particular, if* $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ *then* $\rho \sim \rho_{g,\pi}$ *for some cuspidal eigenform* g*.*

Ribet and Wiles

Theorem (Ribet, 1987)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be odd, irreducible, continuous. If $\rho \sim \rho_{g,\pi}$ for some cuspidal eigenform g of any level and weight, then Serre's modularity conjecture holds for ρ.

Theorem (Wiles, 1994)

Let E be a semistable elliptic curve over $\mathbb{Q}$. Then E is modular. In particular, if $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ then $\rho \sim \rho_{g,\pi}$ for some cuspidal eigenform g. (Extended to all elliptic curves by Breuil, Conrad, Diamond and Taylor.)

Ribet and Wiles

Theorem (Ribet, 1987)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ be odd, irreducible, continuous. If $\rho \sim \rho_{g,\pi}$ for some cuspidal eigenform g of any level and weight, then Serre's modularity conjecture holds for ρ.

Theorem (Wiles, 1994)

Let E be a semistable elliptic curve over $\mathbb{Q}$. Then E is modular. In particular, if $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ then $\rho \sim \rho_{g,\pi}$ for some cuspidal eigenform g. (Extended to all elliptic curves by Breuil, Conrad, Diamond and Taylor.)

Ribet+Wiles $\implies$ Serre's Modularity Conjecture for ρ coming from elliptic curves.

Ribet and Wiles

Theorem (Ribet, 1987)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ *be odd, irreducible, continuous. If* $\rho \sim \rho_{g,\pi}$ *for some cuspidal eigenform* g *of any level and weight, then Serre's modularity conjecture holds for* ρ*.*

Theorem (Wiles, 1994)

Let E *be a semistable elliptic curve over* $\mathbb{Q}$*. Then* E *is modular. In particular, if* $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ *then* $\rho \sim \rho_{g,\pi}$ *for some cuspidal eigenform* g*. (Extended to all elliptic curves by Breuil, Conrad, Diamond and Taylor.)*

Ribet+Wiles $\implies$ Serre's Modularity Conjecture for ρ coming from elliptic curves.

Theorem (Wiles, Fermat's Last Theorem, 1994)

If $n \geq 3$*, then the only integer solutions to* $x^n + y^n = z^n$ *satisfy* $xyz = 0$*.*

Modularity over totally real fields

Definition

A number field $K = \mathbb{Q}(\theta)$ is totally real, if θ is a root of a non-zero polynomial $f \in \mathbb{Q}[x]$, where all the roots of f are real.

Modularity over totally real fields

Definition

A number field $K = \mathbb{Q}(\theta)$ is totally real, if θ is a root of a non-zero polynomial $f \in \mathbb{Q}[x]$, where all the roots of f are real.

Example

Let $d > 1$ be a squarefree integer. Then $\mathbb{Q}(\sqrt{d})$ is totally real. In fact, it is a real quadratic field.

Modularity over totally real fields

Definition

A number field $K = \mathbb{Q}(\theta)$ is totally real, if θ is a root of a non-zero polynomial $f \in \mathbb{Q}[x]$, where all the roots of f are real.

Example

Let $d > 1$ be a squarefree integer. Then $\mathbb{Q}(\sqrt{d})$ is totally real. In fact, it is a real quadratic field.
$\mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field.

Modularity over totally real fields

Definition

A number field $K = \mathbb{Q}(\theta)$ is totally real, if θ is a root of a non-zero polynomial $f \in \mathbb{Q}[x]$, where all the roots of f are real.

Example

Let $d > 1$ be a squarefree integer. Then $\mathbb{Q}(\sqrt{d})$ is totally real. In fact, it is a real quadratic field.
$\mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field.

Great progress on modularity over totally real fields over past 5 years, due to Kisin, Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, ...

Theorem (Freitas–Le Hung–S., 2013)

Let K be a real quadratic field. Let E be an elliptic curve over K. Then E is modular.

Can we prove Fermat's Last Theorem over Real Quadratic Fields?

Theorem (Jarvis and Meekin, 2004)

The only solutions to the equation

$$a^p + b^p + c^p = 0, \qquad p \geq 5 \text{ prime}$$

with $a, b, c \in \mathbb{Q}(\sqrt{2})$ *satisfy* $abc = 0$.

Can we prove Fermat's Last Theorem over Real Quadratic Fields?

Theorem (Jarvis and Meekin, 2004)

The only solutions to the equation

$$a^p + b^p + c^p = 0, \qquad p \geq 5 \text{ prime}$$

with $a, b, c \in \mathbb{Q}(\sqrt{2})$ *satisfy* $abc = 0$.

"...the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$*... there are no other real quadratic fields for which this is true ..."(Jarvis and Meekin)*

Can we prove Fermat's Last Theorem over Real Quadratic Fields?

Theorem (Jarvis and Meekin, 2004)

The only solutions to the equation

$$a^p + b^p + c^p = 0, \qquad p \geq 5 \text{ prime}$$

with a, b, $c \in \mathbb{Q}(\sqrt{2})$ satisfy $abc = 0$.

> *"...the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$... there are no other real quadratic fields for which this is true ..."(Jarvis and Meekin)*

Explanation: Over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$, there are no eigenforms of the predicted level and weight. For all other real quadratic fields this is not true!

Can we prove Fermat's Last Theorem over Real Quadratic Fields?

Theorem (Jarvis and Meekin, 2004)

The only solutions to the equation

$$a^p + b^p + c^p = 0, \qquad p \geq 5 \text{ prime}$$

with a, b, $c \in \mathbb{Q}(\sqrt{2})$ satisfy $abc = 0$.

> *"...the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$... there are no other real quadratic fields for which this is true ..."(Jarvis and Meekin)*

Explanation: Over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$, there are no eigenforms of the predicted level and weight. For all other real quadratic fields this is not true! This is similar to the irregular primes.

Fermat Over Real Quadratic Fields

Theorem (Freitas–S., 2014)

If we assume a suitable "Eichler–Shimura" conjecture, then the asymptotic FLT holds for almost all real quadratic fields:

Fermat Over Real Quadratic Fields

Theorem (Freitas–S., 2014)

If we assume a suitable "Eichler–Shimura" conjecture, then the asymptotic FLT holds for almost all real quadratic fields: for almost all squarefree $d > 1$, there is some constant B_d such that if $p > B_d$, then the only solutions to the Fermat equation $x^p + y^p + z^p = 0$ satisfy $xyz = 0$.

Fermat Over Real Quadratic Fields

Theorem (Freitas–S., 2014)

If we assume a suitable "Eichler–Shimura" conjecture, then the asymptotic FLT holds for almost all real quadratic fields: for almost all squarefree $d > 1$, there is some constant B_d such that if $p > B_d$, then the only solutions to the Fermat equation $x^p + y^p + z^p = 0$ satisfy $xyz = 0$.
Unconditionally, *the asymptotic FLT holds for $5/6$ of real quadratic fields.*

Fermat Over Real Quadratic Fields

Theorem (Freitas–S., 2014)

If we assume a suitable "Eichler–Shimura" conjecture, then the asymptotic FLT holds for almost all real quadratic fields: for almost all squarefree $d > 1$, there is some constant B_d such that if $p > B_d$, then the only solutions to the Fermat equation $x^p + y^p + z^p = 0$ satisfy $xyz = 0$.
Unconditionally, *the asymptotic FLT holds for* $5/6$ *of real quadratic fields.*

Explanation: Many different sets of ramification data $\mathcal{R}$ lead to the same level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$. To make the proof work, throw away all the eigenforms giving the wrong ramification data. If nothing is left, we have a contradiction.

Fermat Over Real Quadratic Fields

Theorem (Freitas–S., 2014)

If we assume a suitable "Eichler–Shimura" conjecture, then the asymptotic FLT holds for almost all real quadratic fields: for almost all squarefree $d > 1$, there is some constant B_d such that if $p > B_d$, then the only solutions to the Fermat equation $x^p + y^p + z^p = 0$ satisfy $xyz = 0$.

Unconditionally, *the asymptotic FLT holds for $5/6$ of real quadratic fields.*

Explanation: Many different sets of ramification data $\mathcal{R}$ lead to the same level $N_{\mathcal{R}}$ and weight $k_{\mathcal{R}}$. To make the proof work, throw away all the eigenforms giving the wrong ramification data. If nothing is left, we have a contradiction.

Thank You!