Modularity and the Fermat Equation over Totally Real Fields

Samir Siksek (University of Warwick)
joint work with Nuno Freitas (Bayreuth/MPIM)

9 July 2014

Motivation

Theorem (Wiles)

The only solutions to the equation

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

satisfy $abc = 0$.

Motivation

Theorem (Wiles)

The only solutions to the equation

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

satisfy $abc = 0$.

Theorem (Wiles)

Semistable elliptic curves over $\mathbb{Q}$ *are modular.*

Motivation

Theorem (Wiles)

The only solutions to the equation

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

satisfy $abc = 0$.

Theorem (Wiles)

Semistable elliptic curves over $\mathbb{Q}$ *are modular.*

Theorem (Wiles, Breuil, Conrad, Diamond, Taylor)

All elliptic curves over $\mathbb{Q}$ *are modular.*

More Motivation

Theorem (Jarvis and Manoharmayum 2004)

Semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{17})$ *are modular.*

More Motivation

Theorem (Jarvis and Manoharmayum 2004)

Semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{17})$ *are modular.*

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* $abc = 0$.

More Motivation

Theorem (Jarvis and Manoharmayum 2004)

Semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{17})$ *are modular.*

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)*

Modularity over Totally Real Fields

K totally real number field.
After enormous progress with modularity lifting by **Kisin, Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, . . .**

Modularity over Totally Real Fields

K totally real number field.

After enormous progress with modularity lifting by **Kisin, Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, . . .**

Theorem (Calegari, Freitas–Le Hung–S.)

There are at most finitely many j-invariants of elliptic curves over K that are non-modular.

Modularity over Totally Real Fields

K totally real number field.
After enormous progress with modularity lifting by **Kisin, Gee, Barnet-Lamb, Geraghty, Breuil, Diamond, . . .**

Theorem (Calegari, Freitas–Le Hung–S.)

There are at most finitely many j-invariants of elliptic curves over K that are non-modular.

Theorem (Freitas–Le Hung–S.)

If K is real quadratic, then all elliptic curves over K are modular.

Demystifying the proof of FLT: The Tate Curve

- ℓ prime
- $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$
- $q \in \ell \cdot \mathbb{Z}_\ell$
- $E = E_q/\mathbb{Q}_\ell$ Tate curve

Demystifying the proof of FLT: The Tate Curve

- ℓ prime
- $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$
- $q \in \ell \cdot \mathbb{Z}_\ell$
- $E = E_q/\mathbb{Q}_\ell$ Tate curve

Theorem (Tate)

$E(\overline{\mathbb{Q}_\ell}) \cong \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$

Demystifying the proof of FLT: The Tate Curve

- ℓ prime
- $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$
- $q \in \ell \cdot \mathbb{Z}_\ell$
- $E = E_q/\mathbb{Q}_\ell$ Tate curve

Theorem (Tate)

$E(\overline{\mathbb{Q}_\ell}) \cong \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$ as G_ℓ-modules.

Demystifying the proof of FLT: The Tate Curve

- ℓ prime
- $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$
- $q \in \ell \cdot \mathbb{Z}_\ell$
- $E = E_q/\mathbb{Q}_\ell$ Tate curve

Theorem (Tate)

$E(\overline{\mathbb{Q}_\ell}) \cong \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$ as G_ℓ-modules.

- $p \neq \ell$ prime

Demystifying the proof of FLT: The Tate Curve

- ℓ prime
- $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$
- $q \in \ell \cdot \mathbb{Z}_\ell$
- $E = E_q/\mathbb{Q}_\ell$ Tate curve

Theorem (Tate)

$E(\overline{\mathbb{Q}_\ell}) \cong \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$ as G_ℓ-modules.

- $p \neq \ell$ prime

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle$$

Demystifying the proof of FLT: The Tate Curve

- ℓ prime
- $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$
- $q \in \ell \cdot \mathbb{Z}_\ell$
- $E = E_q/\mathbb{Q}_\ell$ Tate curve

Theorem (Tate)

$E(\overline{\mathbb{Q}_\ell}) \cong \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$ *as* G_ℓ*-modules.*

- $p \neq \ell$ prime

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

If $\sigma \in G_\ell$ then

$$\sigma(\zeta_p) = \zeta_p^a, \qquad \sigma(q^{1/p}) = \zeta_p^b q^{1/p},$$

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

If $\sigma \in G_\ell$ then

$$\sigma(\zeta_p) = \zeta_p^a, \qquad \sigma(q^{1/p}) = \zeta_p^b q^{1/p}, \qquad a, b \in \mathbb{F}_p.$$

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

If $\sigma \in G_\ell$ then

$$\sigma(\zeta_p) = \zeta_p^a, \qquad \sigma(q^{1/p}) = \zeta_p^b q^{1/p}, \qquad a, b \in \mathbb{F}_p.$$

Think of ζ_p and $q^{1/p}$ as an $\mathbb{F}_p$-basis for $E[p]$.

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

If $\sigma \in G_\ell$ then

$$\sigma(\zeta_p) = \zeta_p^a, \qquad \sigma(q^{1/p}) = \zeta_p^b q^{1/p}, \qquad a, b \in \mathbb{F}_p.$$

Think of ζ_p and $q^{1/p}$ as an $\mathbb{F}_p$-basis for $E[p]$. The action of σ is given by

$$\overline{\rho}_p(\sigma) := \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

If $\sigma \in G_\ell$ then

$$\sigma(\zeta_p) = \zeta_p^a, \qquad \sigma(q^{1/p}) = \zeta_p^b q^{1/p}, \qquad a, b \in \mathbb{F}_p.$$

Think of ζ_p and $q^{1/p}$ as an $\mathbb{F}_p$-basis for $E[p]$. The action of σ is given by

$$\overline{\rho}_p(\sigma) := \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

Obtain a representation

$$\overline{\rho}_p : G_\ell \to \mathrm{GL}_2(\mathbb{F}_p).$$

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

As $p \neq \ell$, the extension $\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell$ is unramified, so

$$\sigma(\zeta_p) = \zeta_p, \qquad \text{for all } \sigma \in I_\ell.$$

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

As $p \neq \ell$, the extension $\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell$ is unramified, so

$$\sigma(\zeta_p) = \zeta_p, \qquad \text{for all } \sigma \in I_\ell.$$

So

$$\overline{\rho}_p(I_\ell) \leq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\}$$

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

As $p \neq \ell$, the extension $\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell$ is unramified, so

$$\sigma(\zeta_p) = \zeta_p, \qquad \text{for all } \sigma \in I_\ell.$$

So

$$\overline{\rho}_p(I_\ell) \leq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\} \qquad \text{(cyclic of order } p\text{)}.$$

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

As $p \neq \ell$, the extension $\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell$ is unramified, so

$$\sigma(\zeta_p) = \zeta_p, \qquad \text{for all } \sigma \in I_\ell.$$

So

$$\overline{\rho}_p(I_\ell) \leq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\} \qquad \text{(cyclic of order } p\text{)}.$$

The extension $\mathbb{Q}_\ell(q^{1/p})/\mathbb{Q}_\ell$ is unramified if and only if $p \mid \upsilon_\ell(q)$.

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

As $p \neq \ell$, the extension $\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell$ is unramified, so

$$\sigma(\zeta_p) = \zeta_p, \qquad \text{for all } \sigma \in I_\ell.$$

So

$$\overline{\rho}_p(I_\ell) \leq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\} \qquad \text{(cyclic of order } p\text{)}.$$

The extension $\mathbb{Q}_\ell(q^{1/p})/\mathbb{Q}_\ell$ is unramified if and only if $p \mid \upsilon_\ell(q)$.

Lemma

- *If $p \mid \upsilon_\ell(q)$ then $\#\overline{\rho}_p(I_\ell) = 1$.*
- *If $p \nmid \upsilon_\ell(q)$ then $\#\overline{\rho}_p(I_\ell) = p$.*

The discriminant Δ of E is given by

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$$

The discriminant Δ of E is given by

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} \qquad \text{(observe } v_\ell(q) = v_\ell(\Delta)\text{).}$$

The discriminant Δ of E is given by

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} \qquad \text{(observe } \upsilon_\ell(q) = \upsilon_\ell(\Delta)\text{)}.$$

Lemma

- *If* $p \mid \upsilon_\ell(\Delta)$ *then* $\#\overline{\rho}_p(I_\ell) = 1$.
- *If* $p \nmid \upsilon_\ell(\Delta)$ *then* $\#\overline{\rho}_p(I_\ell) = p$.

Global Calculations

- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $E/\mathbb{Q}$ an elliptic curve
- Δ minimal discriminant
- N conductor
- $p \neq 2$ prime
- $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Global Calculations

- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $E/\mathbb{Q}$ an elliptic curve
- Δ minimal discriminant
- N conductor
- $p \neq 2$ prime
- $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Question: How do you define the conductor $N(\overline{\rho}_p)$ of $\overline{\rho}_p$?

Global Calculations

- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $E/\mathbb{Q}$ an elliptic curve
- Δ minimal discriminant
- N conductor
- $p \neq 2$ prime
- $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Question: How do you define the conductor $N(\overline{\rho}_p)$ of $\overline{\rho}_p$?
Hint: The conductor measures the action of I_ℓ (and higher ramification subgroups) on $E[p]$ for all primes ℓ.

Global Calculations

- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $E/\mathbb{Q}$ an elliptic curve
- Δ minimal discriminant
- N conductor
- $p \neq 2$ prime
- $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Question: How do you define the conductor $N(\overline{\rho}_p)$ of $\overline{\rho}_p$?
Hint: The conductor measures the action of I_ℓ (and higher ramification subgroups) on $E[p]$ for all primes ℓ.
First Guess: Let $N(\overline{\rho}_p) = N$.

Global Calculations

- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $E/\mathbb{Q}$ an elliptic curve
- Δ minimal discriminant
- N conductor
- $p \neq 2$ prime
- $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Question: How do you define the conductor $N(\overline{\rho}_p)$ of $\overline{\rho}_p$?
Hint: The conductor measures the action of I_ℓ (and higher ramification subgroups) on $E[p]$ for all primes ℓ.
First Guess: Let $N(\overline{\rho}_p) = N$. WRONG

Global Calculations

- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $E/\mathbb{Q}$ an elliptic curve
- Δ minimal discriminant
- N conductor
- $p \neq 2$ prime
- $\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$.

Question: How do you define the conductor $N(\overline{\rho}_p)$ of $\overline{\rho}_p$?
Hint: The conductor measures the action of I_ℓ (and higher ramification subgroups) on $E[p]$ for all primes ℓ.
First Guess: Let $N(\overline{\rho}_p) = N$. WRONG

Better Guess:

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

An Application

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

An Application

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

An Application

$$N(\overline{\rho}_p) = \frac{N}{M_p}\,, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

An Application

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^? \cdot \prod_{\substack{\ell | abc \\ \ell \neq 2}} \ell.$$

An Application

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

$$\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^? \cdot \prod_{\substack{\ell | abc \\ \ell \neq 2}} \ell.$$

Thus $N(\overline{\rho}_p) = 2^?$.

An Application

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = 1.$$

Let

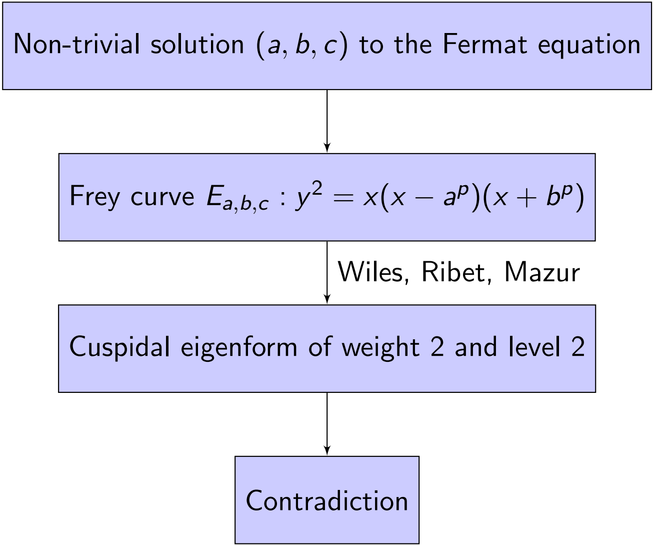
$$E : y^2 = x(x - a^p)(x + b^p).$$

Then

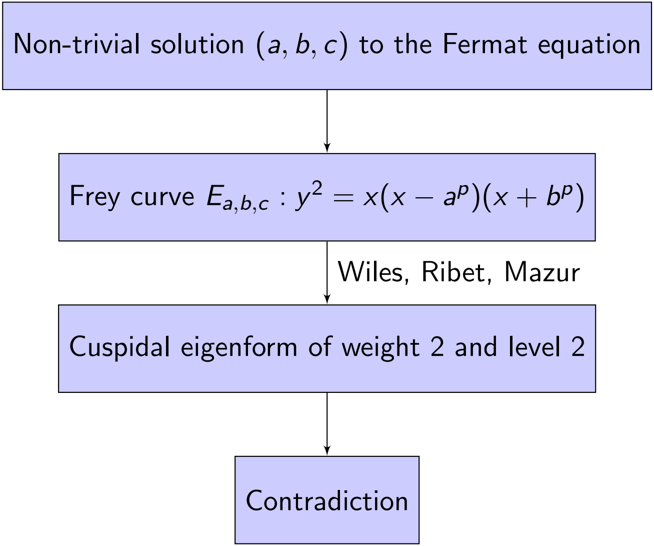
$$\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p}, \qquad N = 2^? \cdot \prod_{\substack{\ell | abc \\ \ell \neq 2}} \ell.$$

Thus $N(\overline{\rho}_p) = 2^?$. With care, $N(\overline{\rho}_p) = 2$.

Fermat equation $a^p + b^p + c^p = 0$ over $\mathbb{Q}$



Fermat equation $a^p + b^p + c^p = 0$ over $\mathbb{Q}$



Accident # 1 : there are no newforms of weight 2 **and level** 2.

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}\,, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = q.$$

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = q.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = q.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then E has additive reduction at q. So $q^2 \mid\mid N$.

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = q.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then E has additive reduction at q. So $q^2 \mid\mid N$. Thus $N(\overline{\rho}_p) = 2q^2$.

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = q.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then E has additive reduction at q. So $q^2 \mid\mid N$. Thus $N(\overline{\rho}_p) = 2q^2$.

Dimension of newspace of weight 2 and level $2q^2$ is roughly $q^2/6$.

A Variant

$$N(\overline{\rho}_p) = \frac{N}{M_p}, \qquad M_p = \prod_{\substack{\ell || N \\ p | \upsilon_\ell(\Delta)}} \ell.$$

Let $q \neq 2$ be a prime. Suppose a, b, $c \in \mathbb{Z}$ satisfy

$$a^p + b^p + c^p = 0, \qquad abc \neq 0, \qquad \gcd(a, b, c) = q.$$

Let

$$E : y^2 = x(x - a^p)(x + b^p).$$

Then E has additive reduction at q. So $q^2 \mid\mid N$. Thus $N(\overline{\rho}_p) = 2q^2$.

Dimension of newspace of weight 2 and level $2q^2$ is roughly $q^2/6$.

Accident # 2: $h(\mathbb{Z}) = 1$.

Fermat $a^p + b^p + c^p = 0$ over a totally real field K

Non-trivial solution (a, b, c) to the Fermat equation

↓

Frey curve $E = E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$

↓ modulo big theorems and conjectures . . .

Hilbert cuspidal eigenform of weight 2 and one of many levels

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Asymptotic Fermat: $p > C_K$

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Let $\mathfrak{q}$ be a prime of K. Then

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E) \pmod{\varpi}.$$

Asymptotic Fermat: $p > C_K$

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Let $\mathfrak{q}$ be a prime of K. Then

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E) \pmod{\varpi}.$$

So ϖ divides

$$B(\mathfrak{f},\mathfrak{q}) := (a_{\mathfrak{q}}(\mathfrak{f}) - \mathbb{N}(\mathfrak{q}) - 1)(a_{\mathfrak{q}}(\mathfrak{f}) + \mathbb{N}(\mathfrak{q}) + 1) \prod_{|t| \le 2\sqrt{\mathbb{N}(\mathfrak{q})}} (a_{\mathfrak{q}}(\mathfrak{f}) - t)$$

Asymptotic Fermat: $p > C_K$

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Let $\mathfrak{q}$ be a prime of K. Then

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E) \pmod{\varpi}.$$

So ϖ divides

$$B(\mathfrak{f},\mathfrak{q}) := (a_{\mathfrak{q}}(\mathfrak{f}) - \mathbb{N}(\mathfrak{q}) - 1)(a_{\mathfrak{q}}(\mathfrak{f}) + \mathbb{N}(\mathfrak{q}) + 1) \prod_{|t| \le 2\sqrt{\mathbb{N}(\mathfrak{q})}} (a_{\mathfrak{q}}(\mathfrak{f}) - t)$$

Suppose $a_{\mathfrak{q}}(\mathfrak{f}) \notin \mathbb{Q}$.

Asymptotic Fermat: $p > C_K$

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Let $\mathfrak{q}$ be a prime of K. Then

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E) \pmod{\varpi}.$$

So ϖ divides

$$B(\mathfrak{f},\mathfrak{q}) := (a_{\mathfrak{q}}(\mathfrak{f}) - \mathbb{N}(\mathfrak{q}) - 1)(a_{\mathfrak{q}}(\mathfrak{f}) + \mathbb{N}(\mathfrak{q}) + 1) \prod_{|t| \le 2\sqrt{\mathbb{N}(\mathfrak{q})}} (a_{\mathfrak{q}}(\mathfrak{f}) - t)$$

Suppose $a_{\mathfrak{q}}(\mathfrak{f}) \notin \mathbb{Q}$. Then $B(\mathfrak{f},\mathfrak{q}) \neq 0$,

Asymptotic Fermat: $p > C_K$

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Let $\mathfrak{q}$ be a prime of K. Then

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E) \pmod{\varpi}.$$

So ϖ divides

$$B(\mathfrak{f},\mathfrak{q}) := (a_{\mathfrak{q}}(\mathfrak{f}) - \mathbb{N}(\mathfrak{q}) - 1)(a_{\mathfrak{q}}(\mathfrak{f}) + \mathbb{N}(\mathfrak{q}) + 1) \prod_{|t| \le 2\sqrt{\mathbb{N}(\mathfrak{q})}} (a_{\mathfrak{q}}(\mathfrak{f}) - t)$$

Suppose $a_{\mathfrak{q}}(\mathfrak{f}) \notin \mathbb{Q}$. Then $B(\mathfrak{f},\mathfrak{q}) \neq 0$, so p is bounded.

Asymptotic Fermat: $p > C_K$

Conclusion: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ (where $\varpi \mid p$) for some Hilbert eigenform of parallel weight 2 and at one of these levels.

Let $\mathfrak{q}$ be a prime of K. Then

$$a_{\mathfrak{q}}(\mathfrak{f}) \equiv a_{\mathfrak{q}}(E) \pmod{\varpi}.$$

So ϖ divides

$$B(\mathfrak{f},\mathfrak{q}) := (a_{\mathfrak{q}}(\mathfrak{f}) - \mathbb{N}(\mathfrak{q}) - 1)(a_{\mathfrak{q}}(\mathfrak{f}) + \mathbb{N}(\mathfrak{q}) + 1) \prod_{|t| \le 2\sqrt{\mathbb{N}(\mathfrak{q})}} (a_{\mathfrak{q}}(\mathfrak{f}) - t)$$

Suppose $a_{\mathfrak{q}}(\mathfrak{f}) \notin \mathbb{Q}$. Then $B(\mathfrak{f},\mathfrak{q}) \neq 0$, so p is bounded.
CONTRADICTION!
Conclusion: $\mathfrak{f}$ has rational eigenvalues.

Asymptotic Fermat $a^p + b^p + c^p = 0$ over a totally real field K

Non-trivial solution (a, b, c) to the Fermat equation with p large

↓

Frey curve $E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$

↓ Jarvis, Fujiwarwa, Rajaei, Merel, Momose,.

Hilbert eigenform of weight 2 and level ??, rational eigenvalues

↓ modulo an 'Eichler–Shimura' conjecture

E/K with full 2-torsion, $j(E) \in \mathcal{O}_K[1/2]$, additional properties

Question

What is the 'proportion' of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for which there are such elliptic curves?

Question

What is the 'proportion' of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for which there are such elliptic curves?

Such elliptic curves fall in 5 **parametric families**, and some sporadic ones.

Question

What is the 'proportion' of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for which there are such elliptic curves?

Such elliptic curves fall in 5 **parametric families**, and some sporadic ones. Here is one of them: $y^2 = x(x-1)(x-\lambda)$ where

$$\lambda = \frac{2^{2s} - 2^{2t} + 1 + v_{s,t}\sqrt{d_{s,t}}}{2},$$

where $s > t > 0$ and

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Question

What is the 'proportion' of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for which there are such elliptic curves?

Such elliptic curves fall in 5 **parametric families**, and some sporadic ones. Here is one of them: $y^2 = x(x-1)(x-\lambda)$ where

$$\lambda = \frac{2^{2s} - 2^{2t} + 1 + v_{s,t}\sqrt{d_{s,t}}}{2},$$

where $s > t > 0$ and

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Question

What is the density of such $d_{s,t}$ among the square-free positive integers?

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Let $n > 0$ and $M_n = 2^n - 1$ (the n-th Mersenne number). It is easy to see that

$$\#\{\alpha_{s,t} \mod M_n \,:\, s > t > 0\} \leq n^2.$$

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Let $n > 0$ and $M_n = 2^n - 1$ (the n-th Mersenne number). It is easy to see that

$$\#\{\alpha_{s,t} \mod M_n \ : \ s > t > 0\} \leq n^2.$$

Incorrect assumption: $\gcd(M_n, v_{s,t}) = 1$ for all $s > t > 0$.

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Let $n > 0$ and $M_n = 2^n - 1$ (the n-th Mersenne number). It is easy to see that

$$\#\{\alpha_{s,t} \mod M_n \ : \ s > t > 0\} \leq n^2.$$

Incorrect assumption: $\gcd(M_n, v_{s,t}) = 1$ for all $s > t > 0$.

$$\#\{v_{s,t}^{-2} \mod M_n \ : \ s > t > 0\} \leq \frac{M_n}{2^{\omega(M_n)}}.$$

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Let $n > 0$ and $M_n = 2^n - 1$ (the n-th Mersenne number). It is easy to see that

$$\#\{\alpha_{s,t} \mod M_n \ : \ s > t > 0\} \le n^2.$$

Incorrect assumption: $\gcd(M_n, v_{s,t}) = 1$ for all $s > t > 0$.

$$\#\{v_{s,t}^{-2} \mod M_n \ : \ s > t > 0\} \le \frac{M_n}{2^{\omega(M_n)}}.$$

But $d_{s,t} = \alpha_{s,t} \cdot v_{s,t}^{-2}$,

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Let $n > 0$ and $M_n = 2^n - 1$ (the n-th Mersenne number). It is easy to see that

$$\#\{\alpha_{s,t} \mod M_n \,:\, s > t > 0\} \le n^2.$$

Incorrect assumption: $\gcd(M_n, v_{s,t}) = 1$ for all $s > t > 0$.

$$\#\{v_{s,t}^{-2} \mod M_n \,:\, s > t > 0\} \le \frac{M_n}{2^{\omega(M_n)}}.$$

But $d_{s,t} = \alpha_{s,t} \cdot v_{s,t}^{-2}$, so

$$\#\{d_{s,t} \mod M_n \,:\, s > t > 0\} \le \frac{n^2 \cdot M_n}{2^{\omega(M_n)}}.$$

$s > t > 0$

$$\underbrace{(2^s + 2^t + 1)(2^s + 2^t - 1)(2^s - 2^t + 1)(2^s - 2^t - 1)}_{\alpha_{s,t}} = d_{s,t} \cdot v_{s,t}^2.$$

Let $n > 0$ and $M_n = 2^n - 1$ (the n-th Mersenne number). It is easy to see that

$$\#\{\alpha_{s,t} \mod M_n \ : \ s > t > 0\} \leq n^2.$$

Incorrect assumption: $\gcd(M_n, v_{s,t}) = 1$ for all $s > t > 0$.

$$\#\{v_{s,t}^{-2} \mod M_n \ : \ s > t > 0\} \leq \frac{M_n}{2^{\omega(M_n)}}.$$

But $d_{s,t} = \alpha_{s,t} \cdot v_{s,t}^{-2}$, so

$$\#\{d_{s,t} \mod M_n \ : \ s > t > 0\} \leq \frac{n^2 \cdot M_n}{2^{\omega(M_n)}}.$$

Therefore, the density of $d_{s,t}$

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Density

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Density

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Question

Can I choose n so that $\frac{n^2}{2^{\omega(M_n)}}$ *is arbitrarily small?*

Density

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Question

Can I choose n so that $\frac{n^2}{2^{\omega(M_n)}}$ is arbitrarily small?

Theorem (Bang, 1886)

$$\omega(M_n) \geq 2^{\omega(n)} - 2. \qquad (d \mid n \implies M_d \mid M_n)$$

Density

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Question

Can I choose n so that $\frac{n^2}{2^{\omega(M_n)}}$ *is arbitrarily small?*

Theorem (Bang, 1886)

$$\omega(M_n) \geq 2^{\omega(n)} - 2. \qquad (d \mid n \implies M_d \mid M_n)$$

$$\delta(d_{s,t}) \leq \frac{4n^2}{2^{2^{\omega(n)}}}.$$

Density

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Question

Can I choose n so that $\frac{n^2}{2^{\omega(M_n)}}$ is arbitrarily small?

Theorem (Bang, 1886)

$$\omega(M_n) \geq 2^{\omega(n)} - 2. \qquad (d \mid n \implies M_d \mid M_n)$$

$$\delta(d_{s,t}) \leq \frac{4n^2}{2^{2^{\omega(n)}}}.$$

$$\text{Let } n = \prod_{p \leq y} p \qquad \overset{\Longrightarrow}{PNT} \qquad \omega(n) \sim \frac{y}{\log(y)}, \qquad \log(n) \sim y.$$

Density

$$\delta(d_{s,t}) \leq \frac{n^2}{2^{\omega(M_n)}}.$$

Question

Can I choose n so that $\frac{n^2}{2^{\omega(M_n)}}$ *is arbitrarily small?*

Theorem (Bang, 1886)

$$\omega(M_n) \geq 2^{\omega(n)} - 2. \qquad (d \mid n \implies M_d \mid M_n)$$

$$\delta(d_{s,t}) \leq \frac{4n^2}{2^{2^{\omega(n)}}}.$$

$$\text{Let } n = \prod_{p \leq y} p \qquad \overset{\Longrightarrow}{PNT} \qquad \omega(n) \sim \frac{y}{\log(y)}, \qquad \log(n) \sim y.$$

Answer: $\delta(d_{s,t}) = 0$.

The Asymptotic FLT

Theorem (Freitas–S.)

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

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

The Asymptotic FLT

Theorem (Freitas–S.)

If we assume a suitable "Eichler–Shimura" conjecture, then the asymptotic FLT holds for almost all real quadratic fields.
Unconditionally, *the asymptotic FLT holds for* $5/6$ *of real quadratic fields.*

Thank You!