Elliptic Curves over Real Quadratic Fields are Modular

Samir Siksek (Warwick)
joint work with Nuno Freitas (Bayreuth)
and Bao Le Hung (Harvard)

11 March 2014

Motivation

Conjecture

Let E be an elliptic curve over a totally real field K. Then E is modular in the following sense: there is a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 over K such that $\mathrm{L}(E, s) = \mathrm{L}(\mathfrak{f}, s)$.

Motivation

Conjecture

Let E be an elliptic curve over a totally real field K. Then E is modular in the following sense: there is a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 over K such that $\mathrm{L}(E,s) = \mathrm{L}(\mathfrak{f},s)$.

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

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

Motivation

Conjecture

Let E be an elliptic curve over a totally real field K. Then E is modular in the following sense: there is a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 over K such that $\mathrm{L}(E, s) = \mathrm{L}(\mathfrak{f}, s)$.

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

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

Theorem (Jarvis and Manoharmayum 2004)

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

Prove Your Own Modularity Theorem

- K totally real number field
- $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$
- E/K elliptic curve defined over K

Prove Your Own Modularity Theorem

- K totally real number field
- $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$
- E/K elliptic curve defined over K

If p is a prime, denote by

$$\overline{\rho}_{E,p} \;:\; G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

the representation giving the action of G_K on the p-torsion of E.

Prove Your Own Modularity Theorem

- K totally real number field
- $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$
- E/K elliptic curve defined over K

If p is a prime, denote by

$$\overline{\rho}_{E,p} \ : \ G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

the representation giving the action of G_K on the p-torsion of E.

Definition

We say $\overline{\rho}_{E,p}$ is **modular** if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, and a place $\varpi \mid p$ of $\overline{\mathbb{Q}}$ such that

$$\overline{\rho}^{ss}_{E,p} \sim \overline{\rho}^{ss}_{\mathfrak{f},\varpi}.$$

Prove Your Own Modularity Theorem

- K totally real number field
- $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$
- E/K elliptic curve defined over K

If p is a prime, denote by

$$\overline{\rho}_{E,p} \ : \ G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

the representation giving the action of G_K on the p-torsion of E.

Definition

We say $\overline{\rho}_{E,p}$ is **modular** if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, and a place $\varpi \mid p$ of $\overline{\mathbb{Q}}$ such that

$$\overline{\rho}^{ss}_{E,p} \sim \overline{\rho}^{ss}_{\mathfrak{f},\varpi}.$$

Fact

E modular $\implies$ $\overline{\rho}_{E,p}$ modular.

A Theorem of Breuil and Diamond (2013)

Théorème 3.2.2. — *Supposons* $p > 2$, $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(k_E)$ *modulaire,* $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F(\sqrt[p]{1}))}$ *irréductible et, si* $p = 5$, *l'image de* $\overline{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}/F(\sqrt[p]{1})))$ *dans* $\mathrm{PGL}_2(k_E)$ *non isomorphe à* $\mathrm{PSL}_2(\mathbb{F}_5)$. *Soit* $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to E^\times$ *un caractère qui relève* $\det \overline{\rho}$ *et tel que* $\psi\varepsilon^{-1}$ *est d'ordre fini,* T *un sous-ensemble de l'ensemble des places de* F *divisant* p *et* S *un ensemble fini de places finies de* F *contenant les places divisant* p *et les places où* $\overline{\rho}$ *ou* ψ *sont ramifiés. Pour chaque* $v \in S$, *soit* $[r_v, N_v]$ *un type de Weil-Deligne en* v *et pour chaque* $v \in T \cup \{v \nmid p, N_v \neq 0\}$, *soit* $\overline{\mu}_v : \mathrm{Gal}(\overline{F_v}/F_v) \to k_E^\times$ *un caractère. Supposons que, pour chaque* $v \in S$, $\overline{\rho}|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ *admet un relevé* $\rho_v : \mathrm{Gal}(\overline{F_v}/F_v) \to \mathrm{GL}_2(E)$ *tel que :*

- (i) *si* $v|p$ *alors* ρ_v *est potentiellement semi-stable de poids de Hodge-Tate* $(0, 1)$ *pour tout* $F_v \hookrightarrow \overline{\mathbb{Q}_p}$
- (ii) *si* $v|p$ *alors* ρ_v *est potentiellement ordinaire si et seulement si* $v \in T$
- (iii) ρ_v *est de type de Weil-Deligne* $[r_v, N_v]$ *(*$v \in S$*)*
- (iv) *si* $v \in T \cup \{v \nmid p, N_v \neq 0\}$ *alors* ρ_v *a une sous-représentation* σ_v *de dimension* 1 *telle que* σ_v *relève* $\overline{\mu}_v\omega$ *et* $\sigma_v\varepsilon^{-1}|_{I_v}$ *est d'ordre fini*
- (v) $\det \rho_v|_{I_v} = \psi|_{I_v}$ *(*$v \in S$*).*

Alors, quitte à agrandir E, $\overline{\rho}$ *possède un relevé* $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(E)$ *continu non ramifié en dehors de* S *et tel que :*

- (i) *si* $v|p$ *alors* $\rho|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ *est potentiellement semi-stable de poids de Hodge-Tate* $(0, 1)$ *pour tout* $F_v \hookrightarrow \overline{\mathbb{Q}_p}$
- (ii) *si* $v|p$ *alors* $\rho|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ *est potentiellement ordinaire si et seulement si* $v \in T$
- (iii) $\rho|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ *est de type de Weil-Deligne* $[r_v, N_v]$ *(*$v \in S$*)*
- (iv) *si* $v \in T \cup \{v \nmid p, N_v \neq 0\}$ *alors* $\rho|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ *a une sous-représentation* σ'_v *de dimension* 1 *telle que* σ'_v *relève* $\overline{\mu}_v\omega$ *et* $\sigma'_v\varepsilon^{-1}|_{I_v}$ *est d'ordre fini*
- (v) $\det \rho = \psi$.

De plus, un tel relevé ρ *de* $\overline{\rho}$ *provient d'une forme modulaire de Hilbert de poids* $(2, 2, \cdots, 2)$.

Modularity Lifting

Modularity Lifting

Theorem (Langlands–Tunnell)

Suppose $\overline{\rho}_{E,3}$ is irreducible. Then $\overline{\rho}_{E,3}$ is modular.

Modularity Lifting

Theorem (Langlands–Tunnell)

Suppose $\overline{\rho}_{E,3}$ *is irreducible. Then* $\overline{\rho}_{E,3}$ *is modular.*

Theorem (Kisin, Barnet-Lamb–Gee–Geraghty, Breuil–Diamond)

Let $p \geq 3$. *Write* $\overline{\rho} = \overline{\rho}_{E,p}$. *Suppose*

(i) $\overline{\rho}$ *is modular,*

(ii) $\overline{\rho}(G_K) \cap \mathrm{SL}_2(\mathbb{F}_p)$ *is absolutely irreducible.* *("Big Image Condition")*

Then E *is modular.*

Modularity Lifting

Theorem (Langlands–Tunnell)

Suppose $\overline{\rho}_{E,3}$ *is irreducible. Then* $\overline{\rho}_{E,3}$ *is modular.*

Theorem (Kisin, Barnet-Lamb–Gee–Geraghty, Breuil–Diamond)

Let $p \geq 3$*. Write* $\overline{\rho} = \overline{\rho}_{E,p}$*. Suppose*

(i) $\overline{\rho}$ *is modular,*

(ii) $\overline{\rho}(G_K) \cap \mathrm{SL}_2(\mathbb{F}_p)$ *is absolutely irreducible.* *("Big Image Condition")*

Then E *is modular.*

Corollary

If E *satisfies the Big Image Condition mod* 3 *then* E *is modular.*

The Big Image Condition

The Big Image Condition

Fact

If E violates the Big Image Condition mod p, then E gives rise to a K-point on $X_0(p)$, $X_{\mathrm{ns}}(p)$ or $X_{\mathrm{s}}(p)$.

The Big Image Condition

Fact

If E violates the Big Image Condition mod p, then E gives rise to a K-point on $X_0(p)$, $X_{\mathrm{ns}}(p)$ or $X_{\mathrm{s}}(p)$.

Example

The maps $X_0(3) \to X(1)$, $X_{\mathrm{ns}}(3) \to X(1)$ and $X_{\mathrm{s}}(3) \to X(1)$ are given by

$$t \mapsto \frac{(t+27)(t+243)^3}{t^3}, \qquad t \mapsto t^3, \qquad t \mapsto \frac{(t-9)^3(t+3)^3}{t^3}.$$

The Big Image Condition

Fact

If E violates the Big Image Condition mod p, then E gives rise to a K-point on $X_0(p)$, $X_{\mathrm{ns}}(p)$ or $X_{\mathrm{s}}(p)$.

Example

The maps $X_0(3) \to X(1)$, $X_{\mathrm{ns}}(3) \to X(1)$ and $X_{\mathrm{s}}(3) \to X(1)$ are given by

$$t \mapsto \frac{(t+27)(t+243)^3}{t^3}, \qquad t \mapsto t^3, \qquad t \mapsto \frac{(t-9)^3(t+3)^3}{t^3}.$$

Corollary

Let j be the j-invariant of E. If

$$j \neq \frac{(t+27)(t+243)^3}{t^3}, \qquad j \neq t^3, \qquad j \neq \frac{(t-9)^3(t+3)^3}{t^3}$$

the E satisfies the Big Image Condition mod 3.

The Big Image Condition

Fact

If E violates the Big Image Condition mod p, then E gives rise to a K-point on $X_0(p)$, $X_{\mathrm{ns}}(p)$ or $X_{\mathrm{s}}(p)$.

Example

The maps $X_0(3) \to X(1)$, $X_{\mathrm{ns}}(3) \to X(1)$ and $X_{\mathrm{s}}(3) \to X(1)$ are given by

$$t \mapsto \frac{(t+27)(t+243)^3}{t^3}, \qquad t \mapsto t^3, \qquad t \mapsto \frac{(t-9)^3(t+3)^3}{t^3}.$$

Corollary

Let j be the j-invariant of E. If

$$j \neq \frac{(t+27)(t+243)^3}{t^3}, \qquad j \neq t^3, \qquad j \neq \frac{(t-9)^3(t+3)^3}{t^3}$$

the E satisfies the Big Image Condition mod 3. In particular, E is modular.

Corollary

Let j be the j-invariant of E. If

$$j \neq \frac{(t+27)(t+243)^3}{t^3}, \qquad j \neq t^3, \qquad j \neq \frac{(t-9)^3(t+3)^3}{t^3}$$

the E satisfies the Big Image Condition mod 3. In particular, E is modular.

Corollary

Let j be the j-invariant of E. If

$$j \neq \frac{(t+27)(t+243)^3}{t^3}, \qquad j \neq t^3, \qquad j \neq \frac{(t-9)^3(t+3)^3}{t^3}$$

the E satisfies the Big Image Condition mod 3. In particular, E is modular.

Conclusion

There are infinitely many j-invariants $\in K$ for which we cannot yet lift modularity of $\overline{\rho}_{E,3}$.

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

E' satisfies Big Image mod 3

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

$$E' \text{ satisfies Big Image mod } 3 \implies E' \text{ is modular}$$

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

$$\begin{aligned} E' \text{ satisfies Big Image mod } 3 \quad &\implies \quad E' \text{ is modular} \\ &\implies \quad \overline{\rho}_{E',p} \text{ is modular} \end{aligned}$$

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

$$\begin{aligned} E' \text{ satisfies Big Image mod } 3 \quad &\implies \quad E' \text{ is modular} \\ &\implies \quad \overline{\rho}_{E',p} \text{ is modular} \\ &\implies \quad \overline{\rho}_{E,p} \text{ is modular} \end{aligned}$$

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

$$\begin{aligned}
E' \text{ satisfies Big Image mod } 3 \quad &\implies \quad E' \text{ is modular} \\
&\implies \quad \bar{\rho}_{E',p} \text{ is modular} \\
&\implies \quad \bar{\rho}_{E,p} \text{ is modular} \\
&\implies \quad E \text{ is modular (if Big Image Condition mod } p \text{ is satisfied)}
\end{aligned}$$

Modularity Switching (After Wiles)

Let $p \neq 2, 3$. We **TRY** to show

$$E \text{ satisfies Big Image Condition mod } p \implies E \text{ is modular}$$

Fact

A non-cuspidal K-point on $X_E(p)$ represents a pair (E', u) where

- *E' is an elliptic curve $/K$,*
- *$u : E'[p] \to E[p]$ is a symplectic isomorphism of G_K-modules.*

$$\begin{aligned} E' \text{ satisfies Big Image mod } 3 \quad &\implies \quad E' \text{ is modular} \\ &\implies \quad \overline{\rho}_{E',p} \text{ is modular} \\ &\implies \quad \overline{\rho}_{E,p} \text{ is modular} \\ &\implies \quad E \text{ is modular (if Big Image} \\ &\qquad\quad \text{Condition mod } p \text{ is satisfied)} \end{aligned}$$

To make this work, need 'lots' of K-points on $X_E(p)$.

$$\mathrm{genus}(X_E(p)) = \begin{cases} 0 & p = 5 \\ \geq 3 & p \geq 7 \end{cases}.$$

Conclusion: Modularity switching as above works for $p = 5$ but not 7.

$$\mathrm{genus}(X_E(p)) = \begin{cases} 0 & p = 5 \\ \geq 3 & p \geq 7 \end{cases}.$$

Conclusion: Modularity switching as above works for $p = 5$ but not 7.

Corollary

If E satisfies the Big Image Condition mod 3 or mod 5 then E is modular.

$$\mathrm{genus}(X_E(p)) = \begin{cases} 0 & p = 5 \\ \geq 3 & p \geq 7 \end{cases}.$$

Conclusion: Modularity switching as above works for $p = 5$ but not 7.

Corollary

If E satisfies the Big Image Condition mod 3 or mod 5 then E is modular.

Fact

If E violates the Big Image Condition mod 3 and mod 5, then E gives rise to a K-point on one of the curves

$$X_a(3) \times_{X(1)} X_b(5), \qquad a, b \in \{0, \mathrm{ns}, \mathrm{s}\}.$$

$$\mathrm{genus}(X_E(p)) = \begin{cases} 0 & p = 5 \\ \geq 3 & p \geq 7 \end{cases}.$$

Conclusion: Modularity switching as above works for $p = 5$ but not 7.

Corollary

If E satisfies the Big Image Condition mod 3 or mod 5 then E is modular.

Fact

If E violates the Big Image Condition mod 3 and mod 5, then E gives rise to a K-point on one of the curves

$$X_a(3) \times_{X(1)} X_b(5), \qquad a, b \in \{0, \mathrm{ns}, \mathrm{s}\}.$$

Problem: $X_0(3) \times_{X(1)} X_0(5) \cong X_0(15)$ has genus 1, and $X_0(15)(K)$ could be infinite. So there might still be infinitely many non-modular $j \in K$.

Mod. Switching II (Taylor, Ellenberg, Manoharmayum)

IDEA: Look for points on $X_E(p)$ over solvable totally real extensions.

Mod. Switching II (Taylor, Ellenberg, Manoharmayum)

IDEA: Look for points on $X_E(p)$ over solvable totally real extensions.

Theorem (Langlands Solvable Base Change)

Let E be an elliptic curve over a totally real field K. Suppose

- *L/K is solvable and totally real.*
- *E/L is modular.*

Then E/K is modular.

Mod. Switching II (Taylor, Ellenberg, Manoharmayum)

IDEA: Look for points on $X_E(p)$ over solvable totally real extensions.

Theorem (Langlands Solvable Base Change)

Let E be an elliptic curve over a totally real field K. Suppose

- *L/K is solvable and totally real.*
- *E/L is modular.*

Then E/K is modular.

- $X = X_E(7)$ is a plane quartic curve defined over K.

Mod. Switching II (Taylor, Ellenberg, Manoharmayum)

IDEA: Look for points on $X_E(p)$ over solvable totally real extensions.

Theorem (Langlands Solvable Base Change)

Let E be an elliptic curve over a totally real field K. Suppose

- *L/K is solvable and totally real.*
- *E/L is modular.*

Then E/K is modular.

- $X = X_E(7)$ is a plane quartic curve defined over K.
- To generate solvable points, take a line $\ell \in \check{\mathbb{P}}^2(K)$ and look at $\ell \cdot X$.

Mod. Switching II (Taylor, Ellenberg, Manoharmayum)

IDEA: Look for points on $X_E(p)$ over solvable totally real extensions.

Theorem (Langlands Solvable Base Change)

Let E be an elliptic curve over a totally real field K. Suppose

- *L/K is solvable and totally real.*
- *E/L is modular.*

Then E/K is modular.

- $X = X_E(7)$ is a plane quartic curve defined over K.
- To generate solvable points, take a line $\ell \in \check{\mathbb{P}}^2(K)$ and look at $\ell \cdot X$.

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

If E/K satisfies the Big Image Condition mod 7 then E is modular.

Corollary

If E satisfies the Big Image Condition mod 3 or mod 5 then E is modular.

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

If E/K satisfies the Big Image Condition mod 7 then E is modular.

Corollary

If E satisfies the Big Image Condition mod 3 or mod 5 then E is modular.

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

If E/K satisfies the Big Image Condition mod 7 then E is modular.

Fact

If E violates the Big Image Condition mod 3 and mod 5 and mod 7, then E gives rise to a K-point on one of the curves

$$X_a(3) \times_{X(1)} X_b(5) \times_{X(1)} X_c(7), \qquad a, b, c \in \{0, \mathrm{ns}, \mathrm{s}\}.$$

Corollary

If E satisfies the Big Image Condition mod 3 or mod 5 then E is modular.

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

If E/K satisfies the Big Image Condition mod 7 then E is modular.

Fact

If E violates the Big Image Condition mod 3 and mod 5 and mod 7, then E gives rise to a K-point on one of the curves

$$X_a(3) \times_{X(1)} X_b(5) \times_{X(1)} X_c(7), \qquad a, b, c \in \{0, \mathrm{ns}, \mathrm{s}\}.$$

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

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

Modularity Continued

To prove modularity for all real quadratic fields, it is enough to compute all the non-cuspidal real quadratic points on

$$X_a(3) \times_{X(1)} X_b(5) \times_{X(1)} X_c(7), \qquad a, b, c \in \{0, \mathrm{ns}, \mathrm{s}\}$$

and show that they're modular.

Modularity Continued

To prove modularity for all real quadratic fields, it is enough to compute all the non-cuspidal real quadratic points on

$$X_a(3) \times_{X(1)} X_b(5) \times_{X(1)} X_c(7), \qquad a, b, c \in \{0, \mathrm{ns}, \mathrm{s}\}$$

and show that they're modular.

A much finer analysis shows that it enough to do this for the following seven modular curves:

- $X(\mathrm{b}5, \mathrm{b}7)$ (genus 3);
- $X(\mathrm{b}3, \mathrm{s}5)$ (genus 3);
- $X(\mathrm{s}3, \mathrm{s}5)$ (genus 4);
- $X(\mathrm{b}3, \mathrm{b}5, \mathrm{d}7)$ (genus 97);
- $X(\mathrm{s}3, \mathrm{b}5, \mathrm{d}7)$ (genus 153);
- $X(\mathrm{b}3, \mathrm{b}5, \mathrm{e}7)$ (genus 73);
- $X(\mathrm{s}3, \mathrm{b}5, \mathrm{e}7)$ (genus 113).

Modularity Continued

To prove modularity for all real quadratic fields, it is enough to compute all the non-cuspidal real quadratic points on

$$X_a(3) \times_{X(1)} X_b(5) \times_{X(1)} X_c(7), \qquad a, b, c \in \{0, \mathrm{ns}, \mathrm{s}\}$$

and show that they're modular.

A much finer analysis shows that it enough to do this for the following seven modular curves:

- $X(\mathrm{b}5, \mathrm{b}7)$ (genus 3);
- $X(\mathrm{b}3, \mathrm{s}5)$ (genus 3);
- $X(\mathrm{s}3, \mathrm{s}5)$ (genus 4);
- $X(\mathrm{b}3, \mathrm{b}5, \mathrm{d}7)$ (genus 97);
- $X(\mathrm{s}3, \mathrm{b}5, \mathrm{d}7)$ (genus 153);
- $X(\mathrm{b}3, \mathrm{b}5, \mathrm{e}7)$ (genus 73);
- $X(\mathrm{s}3, \mathrm{b}5, \mathrm{e}7)$ (genus 113).

b=borel.

s=normalizer of split Cartan.

$\mathrm{d}7$ has image $\cong D_3$ in $\mathrm{PGL}_2(\mathbb{F}_7)$.

$\mathrm{e}7$ has image $\cong D_4$ in $\mathrm{PGL}_2(\mathbb{F}_7)$.

$X(\mathrm{b}5, \mathrm{b}7) = X_0(35)$

$$X_0(35)\ :\ y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1).$$

$X(\mathrm{b}5, \mathrm{b}7) = X_0(35)$

$$X_0(35) \ : \ y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1).$$

$$J_0(35)(\mathbb{Q}) \cong \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

$X(\mathrm{b}5, \mathrm{b}7) = X_0(35)$

$$X_0(35)\ :\ y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1).$$

$$J_0(35)(\mathbb{Q}) \cong \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

If P is a quadratic point on $X_0(35)$, then

$$[P + P^\sigma - \infty_+ - \infty_-] \in J_0(35)(\mathbb{Q}).$$

Lemma

All quadratic points on $X_0(35)$ have the form

$$P = (x, \pm\sqrt{f(x)}), \qquad f(x) = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1)$$

with $x \in \mathbb{Q}$ (except for $\left(\frac{-1\pm\sqrt{5}}{2}, 0\right)$).

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Ogg: $\iota = w_{35}$

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Ogg: $\iota = w_{35}$

$$(E^\sigma, C^\sigma) = w_{35}(E, C) = (E/C, E[35]/C)$$

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Ogg: $\iota = w_{35}$

$$(E^\sigma, C^\sigma) = w_{35}(E, C) = (E/C, E[35]/C)$$

Conclusion: E^σ is isogenous to E.

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Ogg: $\iota = w_{35}$

$$(E^\sigma, C^\sigma) = w_{35}(E, C) = (E/C, E[35]/C)$$

Conclusion: E^σ is isogenous to E. Therefore E is a $\mathbb{Q}$-curve.

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Ogg: $\iota = w_{35}$

$$(E^\sigma, C^\sigma) = w_{35}(E, C) = (E/C, E[35]/C)$$

Conclusion: E^σ is isogenous to E. Therefore E is a $\mathbb{Q}$-curve. Therefore, E is modular (by Ribet and Khare–Wintenberger).

Modular Interpretation of Real Quadratic P

$$P = \left(x, \sqrt{f(x)}\right) = (E, C), \qquad x \in \mathbb{Q}, \qquad K = \mathbb{Q}(\sqrt{f(x)})$$

where E/K is an elliptic curve and C is a cyclic subgroup of order 35.

$$(E^\sigma, C^\sigma) = P^\sigma = (x, -\sqrt{f(x)}) = \iota(P), \qquad \begin{cases} \sigma : K \to K \text{ conjugation} \\ \iota = \text{hyperelliptic involution} \end{cases}$$

Ogg: $\iota = w_{35}$

$$(E^\sigma, C^\sigma) = w_{35}(E, C) = (E/C, E[35]/C)$$

Conclusion: E^σ is isogenous to E. Therefore E is a $\mathbb{Q}$-curve. Therefore, E is modular (by Ribet and Khare–Wintenberger).
Moral: If you want to prove modularity of quadratic points on a modular curve X, use Mordell–Weil information (over $\mathbb{Q}$) to prove that Galois conjugation is a geometric involution on X.

A Big Example

Let $X = X(\mathrm{s}3, \mathrm{b}5, \mathrm{d}7)$ (genus 153).

A Big Example

Let $X = X(\mathrm{s3}, \mathrm{b5}, \mathrm{d7})$ (genus 153). Then $X = X(\mathrm{s3}, \mathrm{b5}) \times_{X(1)} X(\mathrm{d7})$.

A Big Example

Let $X = X(\mathrm{s3}, \mathrm{b5}, \mathrm{d7})$ (genus 153). Then $X = X(\mathrm{s3}, \mathrm{b5}) \times_{X(1)} X(\mathrm{d7})$.

$$\begin{tikzcd} & X \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ X(\mathrm{s3}, \mathrm{b5}) \arrow[dr, "j"'] & & X(\mathrm{d7}) \arrow[dl, "j"] \\ & X(1) & \end{tikzcd}$$

A Big Example

Let $X = X(\mathrm{s3}, \mathrm{b5}, \mathrm{d7})$ (genus 153). Then $X = X(\mathrm{s3}, \mathrm{b5}) \times_{X(1)} X(\mathrm{d7})$.

$$\begin{tikzcd}
 & X \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
X(\mathrm{s3}, \mathrm{b5}) \arrow[dr, "j"'] & & X(\mathrm{d7}) \arrow[dl, "j"] \\
 & X(1) &
\end{tikzcd}$$

Representing points on X: Roughly speaking, if $\mathbb{F}$ is a field, then $P \in X(\mathbb{F})$ is a pair (P_1, P_2) where $P_1 \in X(\mathrm{s3}, \mathrm{b5})(\mathbb{F})$ and $P_2 \in X(\mathrm{d7})(\mathbb{F})$ with $j(P_1) = j(P_2)$.

A Big Example

Let $X = X(\mathrm{s3}, \mathrm{b5}, \mathrm{d7})$ (genus 153). Then $X = X(\mathrm{s3}, \mathrm{b5}) \times_{X(1)} X(\mathrm{d7})$.

$$\begin{tikzcd}
 & X \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
X(\mathrm{s3}, \mathrm{b5}) \arrow[dr, "j"'] & & X(\mathrm{d7}) \arrow[dl, "j"] \\
 & X(1) &
\end{tikzcd}$$

Representing points on X: Roughly speaking, if $\mathbb{F}$ is a field, then $P \in X(\mathbb{F})$ is a pair (P_1, P_2) where $P_1 \in X(\mathrm{s3}, \mathrm{b5})(\mathbb{F})$ and $P_2 \in X(\mathrm{d7})(\mathbb{F})$ with $j(P_1) = j(P_2)$.

Mordell–Weil Information

$$X(\mathrm{s3}, \mathrm{b5}) = 15A3, \qquad X(\mathrm{d7}) = 49A3.$$

A Big Example

Let $X = X(\mathrm{s3}, \mathrm{b5}, \mathrm{d7})$ (genus 153). Then $X = X(\mathrm{s3}, \mathrm{b5}) \times_{X(1)} X(\mathrm{d7})$.

$$\begin{tikzcd}
 & X \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
X(\mathrm{s3}, \mathrm{b5}) \arrow[dr, "j"'] & & X(\mathrm{d7}) \arrow[dl, "j"] \\
 & X(1) &
\end{tikzcd}$$

Representing points on X: Roughly speaking, if $\mathbb{F}$ is a field, then $P \in X(\mathbb{F})$ is a pair (P_1, P_2) where $P_1 \in X(\mathrm{s3}, \mathrm{b5})(\mathbb{F})$ and $P_2 \in X(\mathrm{d7})(\mathbb{F})$ with $j(P_1) = j(P_2)$.

Mordell–Weil Information

$$X(\mathrm{s3}, \mathrm{b5}) = 15A3, \qquad X(\mathrm{d7}) = 49A3.$$

Moreover, $\quad X(\mathrm{s3}, \mathrm{b5})(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad X(\mathrm{d7})(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$

$P \in X(K)$

$$P \in X(K) \quad \Longrightarrow \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K)$$

$$
\begin{aligned}
P \in X(K) \quad &\Longrightarrow \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\
&\Longrightarrow \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}.
\end{aligned}
$$

$$
\begin{aligned}
P \in X(K) \quad &\implies \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\
&\implies \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}.
\end{aligned}
$$

Suppose $Q + Q^\sigma = \mathcal{O}$. Then $Q^\sigma = -Q$.

$$\begin{aligned} P \in X(K) \quad &\implies \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\ &\implies \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}. \end{aligned}$$

Suppose $Q + Q^\sigma = \mathcal{O}$. Then $Q^\sigma = -Q$. But $X(\mathrm{d}7)/\langle -1 \rangle = X(\mathrm{s}7)$.

$$
\begin{aligned}
P \in X(K) \quad &\Longrightarrow \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\
&\Longrightarrow \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}.
\end{aligned}
$$

Suppose $Q + Q^\sigma = \mathcal{O}$. Then $Q^\sigma = -Q$. But $X(\mathrm{d}7)/\langle -1 \rangle = X(\mathrm{s}7)$.

$$
Q + Q^\sigma = \mathcal{O} \quad \Longrightarrow \quad Q \text{ maps to a point in } X(\mathrm{s}7)(\mathbb{Q})
$$

$$
\begin{aligned}
P \in X(K) \quad &\Longrightarrow \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\
&\Longrightarrow \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}.
\end{aligned}
$$

Suppose $Q + Q^\sigma = \mathcal{O}$. Then $Q^\sigma = -Q$. But $X(\mathrm{d}7)/\langle -1 \rangle = X(\mathrm{s}7)$.

$$
\begin{aligned}
Q + Q^\sigma = \mathcal{O} \quad &\Longrightarrow \quad Q \text{ maps to a point in } X(\mathrm{s}7)(\mathbb{Q}) \\
&\Longrightarrow \quad \text{the point } Q \in X(\mathrm{d}7)(K) \text{ is modular}
\end{aligned}
$$

$$
\begin{aligned}
P \in X(K) \quad &\implies \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\
&\implies \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}.
\end{aligned}
$$

Suppose $Q + Q^\sigma = \mathcal{O}$. Then $Q^\sigma = -Q$. But $X(\mathrm{d}7)/\langle -1 \rangle = X(\mathrm{s}7)$.

$$
\begin{aligned}
Q + Q^\sigma = \mathcal{O} \quad &\implies \quad Q \text{ maps to a point in } X(\mathrm{s}7)(\mathbb{Q}) \\
&\implies \quad \text{the point } Q \in X(\mathrm{d}7)(K) \text{ is modular} \\
&\implies \quad \text{the point } P \in X(K) \text{ is modular}
\end{aligned}
$$

$$
\begin{aligned}
P \in X(K) \quad &\Longrightarrow \quad Q := \pi_2(P) \in X(\mathrm{d}7)(K) \\
&\Longrightarrow \quad Q + Q^\sigma \in X(\mathrm{d}7)(\mathbb{Q}) = \{\mathcal{O}, T\}.
\end{aligned}
$$

Suppose $Q + Q^\sigma = \mathcal{O}$. Then $Q^\sigma = -Q$. But $X(\mathrm{d}7)/\langle -1 \rangle = X(\mathrm{s}7)$.

$$
\begin{aligned}
Q + Q^\sigma = \mathcal{O} \quad &\Longrightarrow \quad Q \text{ maps to a point in } X(\mathrm{s}7)(\mathbb{Q}) \\
&\Longrightarrow \quad \text{the point } Q \in X(\mathrm{d}7)(K) \text{ is modular} \\
&\Longrightarrow \quad \text{the point } P \in X(K) \text{ is modular}
\end{aligned}
$$

Objective: Show that this is true for all $P \in X(K)$ for all quadratic K.

The Mordell–Weil Sieve

$$\begin{tikzcd}
X^{(2)}(\mathbb{Q}) \arrow[r, "\alpha"'] \arrow[d] & X(\mathrm{s7}, \mathrm{b5})(\mathbb{Q}) \times X(\mathrm{d7})(\mathbb{Q}) \arrow[d, "\mu"'] \\
\prod X^{(2)}(\mathbb{F}_p) \arrow[r, "\beta"'] & \prod X(\mathrm{s7}, \mathrm{b5})(\mathbb{F}_p) \times X(\mathrm{d7})(\mathbb{F}_p)
\end{tikzcd}$$

$$\alpha(P) = (\pi_1(P) + \pi_1(P)^\sigma, \pi_2(P) + \pi_2(P)^\sigma)$$

The Mordell–Weil Sieve

$$
\begin{tikzcd}
X^{(2)}(\mathbb{Q}) \arrow[r, "\alpha"'] \arrow[d] & X(\mathrm{s7}, \mathrm{b5})(\mathbb{Q}) \times X(\mathrm{d7})(\mathbb{Q}) \arrow[d, "\mu"'] \\
\prod X^{(2)}(\mathbb{F}_p) \arrow[r, "\beta"'] & \prod X(\mathrm{s7}, \mathrm{b5})(\mathbb{F}_p) \times X(\mathrm{d7})(\mathbb{F}_p)
\end{tikzcd}
$$

$$\alpha(P) = (\pi_1(P) + \pi_1(P)^\sigma, \pi_2(P) + \pi_2(P)^\sigma)$$

Observe $\mathrm{Im}(\alpha) \subseteq \mu^{-1}(\mathrm{Im}(\beta))$.

The Mordell–Weil Sieve

$$\begin{tikzcd}
X^{(2)}(\mathbb{Q}) \arrow[r, "\alpha"'] \arrow[d] & X(\mathrm{s7}, \mathrm{b5})(\mathbb{Q}) \times X(\mathrm{d7})(\mathbb{Q}) \arrow[d, "\mu"'] \\
\prod X^{(2)}(\mathbb{F}_p) \arrow[r, "\beta"'] & \prod X(\mathrm{s7}, \mathrm{b5})(\mathbb{F}_p) \times X(\mathrm{d7})(\mathbb{F}_p)
\end{tikzcd}$$

$$\alpha(P) = (\pi_1(P) + \pi_1(P)^\sigma, \pi_2(P) + \pi_2(P)^\sigma)$$

Observe $\mathrm{Im}(\alpha) \subseteq \mu^{-1}(\mathrm{Im}(\beta))$.

Using $11 \leq p \leq 100$ we find

$$\mathrm{Im}(\alpha) \subseteq \mu^{-1}(\mathrm{Im}(\beta)) = \{(?, \mathcal{O}), (?, \mathcal{O}), (?, \mathcal{O})\}.$$

Note $\pi_2(P) + \pi_2(P)^\sigma = 0$.

The Mordell–Weil Sieve

$$
\begin{tikzcd}
X^{(2)}(\mathbb{Q}) \arrow[rr, "\alpha"'] \arrow[d] & & X(\mathrm{s7},\mathrm{b5})(\mathbb{Q}) \times X(\mathrm{d7})(\mathbb{Q}) \arrow[d, "\mu"'] \\
\prod X^{(2)}(\mathbb{F}_p) \arrow[rr, "\beta"'] & & \prod X(\mathrm{s7},\mathrm{b5})(\mathbb{F}_p) \times X(\mathrm{d7})(\mathbb{F}_p)
\end{tikzcd}
$$

$$\alpha(P) = (\pi_1(P) + \pi_1(P)^\sigma, \pi_2(P) + \pi_2(P)^\sigma)$$

Observe $\mathrm{Im}(\alpha) \subseteq \mu^{-1}(\mathrm{Im}(\beta))$.

Using $11 \leq p \leq 100$ we find

$$\mathrm{Im}(\alpha) \subseteq \mu^{-1}(\mathrm{Im}(\beta)) = \{(?, \mathcal{O}), (?, \mathcal{O}), (?, \mathcal{O})\}.$$

Note $\pi_2(P) + \pi_2(P)^\sigma = 0$. So P is modular!!

Theorem (Freitas–Le Hung–S.)

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

Thank You!