Diophantine applications of Serre's modularity conjecture

George Ţurcaş

IMAR, Bucharest

Barcelona Fall Workshop on Number Theory, 2019

Motivation

Theorem (Wiles, Taylor-Wiles 1994)

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

Theorem (Wiles 1994)

The only solutions to the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathbb{Q}, \qquad p \geq 3 \text{ prime}$$

satisfy $abc = 0$.

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

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathbb{Q}(\sqrt{2}), \qquad p \geq 5 \text{ prime}$$

satisfy $abc = 0$.

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

Theoretical Pillars

The proof of Fermat's Last Theorem and more generally, successful proofs of non-existence of solutions over $\mathbb{Q}$ to certain exponential Diophantine equations rest on the following theoretical pillars:

(i) A Frey elliptic curve construction;

(ii) Wiles, Breuil, Conrad, Diamond, Taylor: elliptic curves $/\mathbb{Q}$ are modular;

(iii) Mazur's isogeny theorem;

(iv) Ribet's level lowering theorem.

Can replace (ii) and (iv) with Serre's modularity conjecture $/\mathbb{Q}$ (Khare and Wintenberger).

Frey elliptic curves recipes

- Generalised Fermat equation of signature (p, p, p):

  $Ax^p + By^p + Cy^p = 0$, where A, B, C are fixed and p is prime.

  $\rightarrow E : Y^2 = X(X - Ax^p)(X + By^p)$, $\Delta_E = 2^4(ABC)^2(xyz)^{2p}$.

- Superelliptic equations such as:

  $F(x, y) = z^p$, where F is a given irreducible binary cubic.

$$\rightarrow E : Y^2 = X^3 + 3H(x, y)X + G(x, y),$$

$$\Delta_E = 4(3H(x, y))^3 + 27G(x, y)^2 = -27 \cdot \Delta_F \cdot F(x, y)^2$$

$$\Delta_E = -27 \cdot \Delta_F \cdot z^{2p}.$$

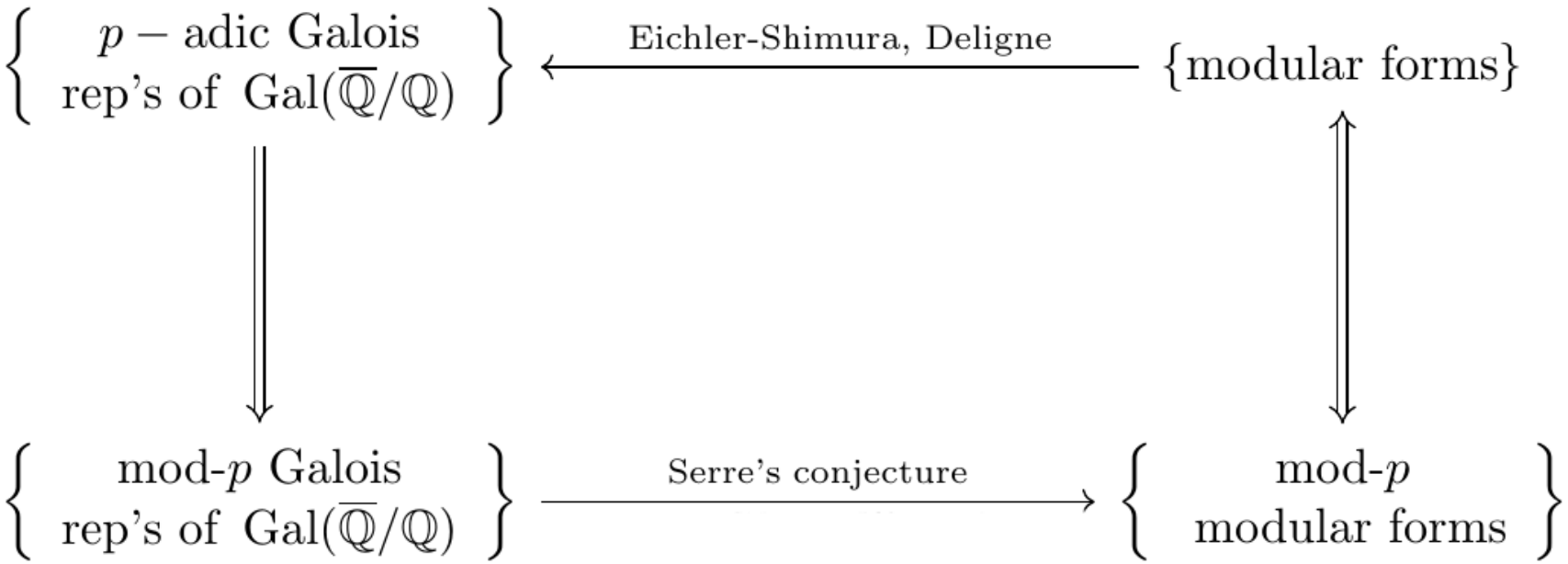
The key properties of a Frey curve E are the following

1. the coefficients of E depend on the putative solution to our Diophantine equation;
2. $\Delta_{E,min} = C \cdot D^p$, where C **does not depend on the putative solution**, but just on the equation itself.
3. E has multiplicative reduction at primes dividing D.

The big picture in the classical case

$$a^p + b^p + c^p = 0 \to E_{p,a,b,c} : Y^2 = X(X - a^p)(X + b^p)$$

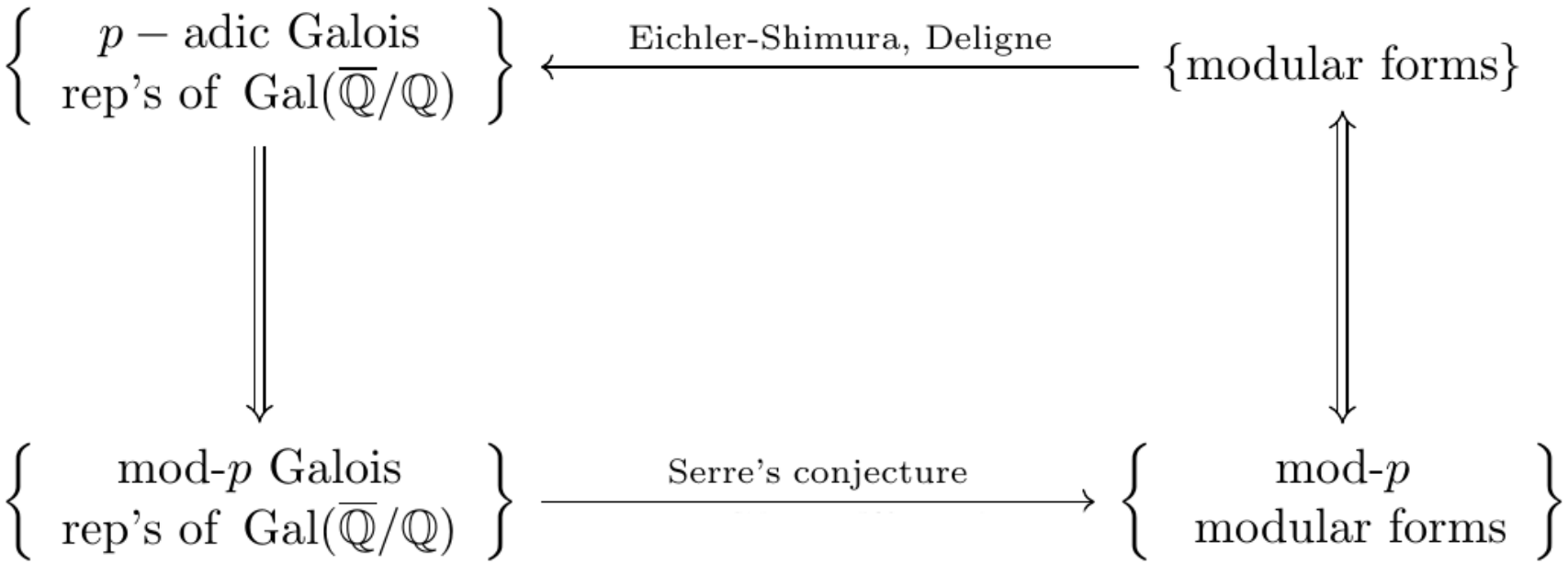
Figure 1: Source: M. H. Şengün's PhD Thesis



The big picture in the classical case

$$a^p + b^p + c^p = 0 \to E_{p,a,b,c} : Y^2 = X(X - a^p)(X + b^p)$$

Figure 1: Source: M. H. Şengün's PhD Thesis



Arrows on the RHS go both ways because, in the classical case, for $p > 3$ mod p modular forms are just reductions of modular forms.

Understanding of modularity (or automorphy) in the setting of general number fields is highly conjectural. In recent work, assuming two conjectures, Şengün and Siksek manage to replicate to some extent the aforementioned successes for Fermat's equation over general number fields.

Conjecture ((1) Serre's modularity conjecture)

This conjecture predicts the existence of a weight 2 mod p eigenform of level $\mathcal{N}$ over K which is associated to every odd, absolutely irreducible continous representation $\overline{\rho} : G_K \to GL_2(\overline{\mathbb{F}}_p)$ of **Serre conductor** *$\mathcal{N}$, such that $\det(\overline{\rho}) = \chi_p$ and is finite flat at every $\mathfrak{p}|p$ of K.*

Conjecture ((2) Eichler-Shimura)

This is a conjecture in the Langlands Programme which says that every weight 2 newform (for GL_2) over K with integer Hecke eigenvalues has an associated elliptic curve over K or a fake elliptic curve over K.

Notation

- $\mathbb{Z}_K$ - the ring of integers of a number field K
- We consider the Fermat equation with prime exponent $p \in \mathbb{Z}$

$$x^p + y^p + z^p = 0, \tag{1}$$

  with $x, y, z \in K$.
- A solution $(a, b, c) \in K^3$ to (1) is called non-trivial if $abc \neq 0$.

Theorem (Şengün, Siksek -2017)

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field where d is a squarefree positive integer satisfying $-d = 2$ or $3 \pmod 4$. Assume that conjectures 1 and 2 hold. Then, there exists a constant B_K such that for $p > B_K$, Fermat's equation

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

does not have non-trivial solutions in K.

Remark

The constant B_K is ineffective.

The strategy of Şengün and Siksek's proof

- Suppose that Fermat's equation has a non-trivial solution $(a, b, c) \in \mathbb{Z}_K^3$. Consider $E := E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p)$.
- Prove that for p large enough, the residual representation $\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p])$ satisfies all the hypothesis of Serre's modularity conjecture, in particular that it is abs. irreducible (uses Merel uniform boundness theorem).
- Apply S.M.C. to obtain a mod p eigenform of trivial weight and level independent on a, b and c.
- Show that for p **large enough** the mod p eigenform lifts to a complex eigenform $\mathfrak{f}$.

The strategy of Ş. & S. cont...

- Use Eichler-Shimura to match the form $\mathfrak{f}$ to an elliptic curve $E_{\mathfrak{f}}$, which does not depend on a, b, c nor on p.
- Using S-unit equations, they show that such an elliptic curve $E_{\mathfrak{f}}$ does not exist.

What can we say about B_K for some simple K?

Theorem (Ţ., 2017)

Assume Conjecture (1) (S.M.C.) holds for $\mathbb{Q}(i)$. Then, Fermat's Last Theorem holds over $\mathbb{Q}(i)$. In other words, for any integer $n \geq 3$, the equation

$$a^n + b^n = c^n$$

has no solutions $a, b, c \in \mathbb{Q}(i) \setminus \{0\}$.

- Let $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7})\}$.

Theorem (Ţ., 2017)

Assume Conjecture (1) (S.M.C.) holds for K. If $p \geq 5$ is a rational prime number, then the equation

$$a^p + b^p + c^p = 0 \tag{2}$$

has no solutions $a, b, c \in K \setminus \{0\}$.

- Let $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7})\}$.

Theorem (Ţ., 2017)

Assume Conjecture (1) (S.M.C.) holds for K. If $p \geq 5$ is a rational prime number, then the equation

$$a^p + b^p + c^p = 0 \tag{2}$$

has no solutions $a, b, c \in K \setminus \{0\}$.

Our techniques prove the result above for $p \geq 19$ when $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})\}$ and $p \geq 17$ when $K = \mathbb{Q}(\sqrt{-7})$ and we rely on previous works on F.L.T. for small p.

Why these restrictions on K?

!!! We had to carry out some explicit computations in the cohomology groups of locally symmetric spaces. These are much simpler when the field has class number 1.

$\Rightarrow$ $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})\}$.

Why these restrictions on K?

!!! We had to carry out some explicit computations in the cohomology groups of locally symmetric spaces. These are much simpler when the field has class number 1.

$\Rightarrow$ $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})\}$.

- To prove that $\overline{\rho}_{E,p}$ is absolutely irreducible, we make use of the fact that K has primes of residue field $\mathbb{F}_2$ above 2.

Why these restrictions on K?

!!! We had to carry out some explicit computations in the cohomology groups of locally symmetric spaces. These are much simpler when the field has class number 1.

$\Rightarrow$ $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})\}$.

- To prove that $\overline{\rho}_{E,p}$ is absolutely irreducible, we make use of the fact that K has primes of residue field $\mathbb{F}_2$ above 2.
- Be aware of

$$\boxed{1^p + \varepsilon^p + (\varepsilon^2)^p = 0}, \text{ where } \varepsilon^3 = 1, \varepsilon \neq 1.$$

Asumme K is quadratic imaginary of class number 1

Let $(a, b, c) \in K^3$ be a non-trivial solution to the Fermat equation. We can scale (a, b, c) such that the triple is integral and a, b, c are coprime.
Let

$$E = E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p).$$

Denote by $\overline{\rho} = \overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$, the representation induced by the action of G_K on the p-torsion $E[p]$.

Asumme K is quadratic imaginary of class number 1

Let $(a, b, c) \in K^3$ be a non-trivial solution to the Fermat equation. We can scale (a, b, c) such that the triple is integral and a, b, c are coprime.
Let

$$E = E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p).$$

Denote by $\overline{\rho} = \overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$, the representation induced by the action of G_K on the p-torsion $E[p]$.

Plan

Prove that $\overline{\rho}$ satisfies the hypothesis required for Serre's modularity conjecture. Get an weight 2 eigenform for K at a level that does not depend on p or a, b, c. Compute the space of those eigenforms and hope for a contradiction. This will prove that $(a, b, c) \in K^3$ does not exist.

$$E : Y^2 = X(X - a^p)(X + b^p)$$

- $c_4 = 2^4(b^{2p} - a^p c^p)$ and $\Delta = 2^4(abc)^{2p}$;
- The determinant of $\overline{\rho}$ is the mod p cyclotomic character;
- $\overline{\rho}$ is unramified at any prime that does not lie above 2 and p;
- By the above, the Serre conductor $\mathcal{N}$ of $\overline{\rho}$ belongs to a finite set that depends only on the field K.
- $\overline{\rho}$ is finite flat at $\mathfrak{p}$ for all $\mathfrak{p}|p$ (if $p > 2$).

Abs. irreducibility of $\overline{\rho}$

To apply S.M.C. to the mod p representation $\overline{\rho}$ of the Frey curve E, we need to prove that $\overline{\rho}$ is absolutely irreducible.

Theorem

For $\boxed{p > B_K}$, $\overline{\rho}$ *is irreducible.*

Sketch of proof. Suppose that p does not ramify in K. If $\overline{\rho}$ is reducible, then

$$\overline{\rho} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix},$$

where $\theta, \theta' : G_K \to \mathbb{F}_p^*$ are characters, such that $\theta\theta' = \chi_p$. Let $\mathcal{N}$ be the conductor of $\overline{\rho}$.
It is easy to show that if $\mathfrak{q} \nmid p$ is a prime of additive reduction, then

$$v_{\mathfrak{q}}(\mathcal{N}_\theta) = v_{\mathfrak{q}}(\mathcal{N}_{\theta'}) = \frac{1}{2} v_{\mathfrak{q}}(\mathcal{N}).$$

i) Suppose that p is coprime to $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$. By replacing E with a p isogenous curve if necessary we can assume that p is coprime to $\mathcal{N}_\theta$.

- finitely many choices for $\mathcal{N}_\theta$;
- θ is the character of a ray class group for which we have finitely many candidates;
- we use MAGMA to compute these gps. $\Rightarrow$ bound $\mathrm{ord}(\theta)$;
- this gives a p torsion point for E defined over a filed of absolute degree $\boxed{2 \cdot \mathrm{ord}(\theta)}$;

ii) If p is not coprime with N_θ nor with $N_{\theta'}$, we use CFT and ideas of A. David to bound p. $\square$

- When E has potentially multiplicative reduction at $\mathfrak{a} \subset \mathbb{Z}_K$, a prime above 2, the image of $\overline{\rho}$ contains an element of order p;
- any irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that has elements of order p contains $\mathrm{SL}_2(\mathbb{F}_p)$;
- $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, therefore $\det(\overline{\rho}) = \chi_p$ is surjective, which implies that $\overline{\rho}$ is surjective.

Conclusions

- In the proof of Fermat's Last Theorem over $\mathbb{Q}$, Serre's modularity conjecture predicts that the representation $\overline{\rho}$ comes from an eigenform of weight 2 and level 2.
- over quad. imag. K, after applying S.M.C. we obtain a Hecke eigenform in $H^1(Y_0(\mathcal{N}), \mathbb{F}_p)$.

$$0 \longrightarrow \mathbb{Z}_{(p)} \xrightarrow{\times p} \mathbb{Z}_{(p)} \longrightarrow \mathbb{F}_p \longrightarrow 0 \ .$$

This gives rise to a long exact sequence on cohomology

$$\ldots H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \xrightarrow{\times p} H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \longrightarrow H^1(Y_0(\mathfrak{N}), \mathbb{F}_p) \xrightarrow{\delta} H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \longrightarrow \ldots$$

from which we can extract the short exact sequence

$$0 \longrightarrow H^1(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)}) \otimes \mathbb{F}_p \longrightarrow H^1(Y_0(\mathfrak{N}), \mathbb{F}_p) \xrightarrow{\delta} H^2(Y_0(\mathfrak{N}), \mathbb{Z}_{(p)})[p] \longrightarrow 0 \ .$$

• We can show that for $p \geq 17$, mod p eigenforms lift to complex ones. The latter are called Bianchi modular forms.

• The predicted complex eigenforms are cuspidal and using the **MAGMA** implementation of an algorithm of Gunnels we can compute the space of this forms (level $\mathcal{N}$ is fixed).

• For $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-7})$ these spaces are empty, so we are done. For $\mathbb{Q}(\sqrt{-2})$, there's more work to do. Namely, we find some eigenforms, we prove that they correspond to some **specific** ell. curves (and not fake ell. curves). We conclude using some congruences mod p involving traces of Frobenia.

What about $d = 3, 11, 19, 43, 67$ or 163?

Theorem (Ţ, 2018)

Let $K = \mathbb{Q}(\sqrt{-d})$, when $d \in \{3, 11, 19, 43, 67, 163\}$. Assume Serre's modularity conjecture holds for K. For any prime $p \geq 19$, the Fermat equation

$$a^p + b^p + c^p = 0,$$

does not have solutions in coprime $a, b, c \in \mathcal{O}_K \setminus \{0\}$ such that $2 \mid abc$.

Affirmative answer to Serre's uniformity question implies ...

If one assumes an affirmative answer to Serre's uniformity question, which enquires whether if given a number field K, there exists a constant B_K such that for every elliptic curve E/K without CM and every $p > B_K$, the mod p representation $\overline{\rho}_{E,p}$ is surjective, then one can show the following.

Theorem

Let $K = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary number field of class number 1 and suppose that Serre's modularity and Serre's uniformity hold over K. There is an absolute constant $C(K) > 0$ such that the only solutions to the Fermat equation $a^p + b^p + c^p = 0$ satisfy $abc = 0$ or $a + b + c = 0$.

Question(s)

Let K be a fixed quadratic imaginary field and fix S, a finite set of prime ideals in K. Denote by
$\mathcal{E}_S = \{E$ defined over $K : E$ is semistable away from $S\}$. Is there a constant $B_{K,S}$ such that for every prime $p > B_{K,S}$ the implication

$$\boxed{\text{For } E \in \mathcal{E}_S \text{ with } \overline{\rho}_{E,p} \textit{ is absolutely reducible } \Rightarrow j(E) \text{ is integral}}$$

holds?
Does anybody know if this is substantially easier than Serre's uniformity question?

Thank you very much for listening!

It is time to give a more precise statement of Conjecture (1)

It is time to give a more precise statement of Conjecture (1)

Conjecture (1)

Let $\overline{\rho} : G_K \to GL_2(\overline{\mathbb{F}}_p)$ be an odd, irreducible, continuous representation with Serre conductor $\mathfrak{N}$ (prime-to-p part of its Artin conductor) and trivial character (prime-to-p part of $\det(\overline{\rho})$). Assume that p is unramified in K and that $\overline{\rho}\,|_{G_{K_\mathfrak{p}}}$ arises from a finite-flat group scheme over $\mathbb{Z}_{K_\mathfrak{p}}$ for every prime $\mathfrak{p}|p$. Then there is a (weight 2) mod p eigenform θ over K of level $\mathfrak{N}$ such that for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have

$$Tr(\overline{\rho}(Frob_\mathfrak{q})) = \theta(T_\mathfrak{q}).$$

It is time to give a more precise statement of Conjecture (1)

Conjecture (1)

Let $\overline{\rho} : G_K \to GL_2(\overline{\mathbb{F}}_p)$ be an odd, irreducible, continuous representation with Serre conductor $\mathfrak{N}$ (prime-to-p part of its Artin conductor) and trivial character (prime-to-p part of $\det(\overline{\rho})$). Assume that p is unramified in K and that $\overline{\rho}\,|_{G_{K_\mathfrak{p}}}$ arises from a finite-flat group scheme over $\mathbb{Z}_{K_\mathfrak{p}}$ for every prime $\mathfrak{p}|p$. Then there is a (weight 2) mod p eigenform θ over K of level $\mathfrak{N}$ such that for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have

$$Tr(\overline{\rho}(Frob_\mathfrak{q})) = \theta(T_\mathfrak{q}).$$

Remark

We say that $\overline{\rho}$ is odd if the determinant of every complex conjugation is -1. In our case, K is totally complex and we regard $\overline{\rho}$ automatically as odd.

$GL_2(K)$ acts on the hyperbolic 3-space $\mathcal{H}_3$ via the embedding $GL_2(K) \hookrightarrow GL_2(K \otimes \mathbb{R}) \simeq GL_2(\mathbb{C})$. Fix an ideal $\mathfrak{N} \subseteq \mathbb{Z}_K$ and define the compact open subgroup

$$U_0(\mathfrak{N}) := \left\{ \gamma \in GL_2(\widehat{\mathbb{Z}_K}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod \mathfrak{N} \right\}.$$

The locally symmetric space

$$Y_0(\mathfrak{N}) = GL_2(K) \backslash \left(\left(GL_2(\mathbb{A}_K^f) / U_0(\mathfrak{N}) \right) \times \mathcal{H}_3 \right)$$

is in this particular case just a Riemannian 3-fold

$$Y_0(\mathfrak{N}) = \Gamma_0(\mathfrak{N}) \backslash \mathcal{H}_3,$$

where $\Gamma_0(\mathfrak{N})$ is the usual congruence subgroup $\Gamma_0(\mathfrak{N})$ of the modular group $GL_2(\mathbb{Z}_K)$.

For $i \in \{1, 2\}$ consider the i-th cohomology group $H^i(Y_0(\mathfrak{N}), \mathbb{C})$. For any prime $\mathfrak{q}$ coprime to the level $\mathfrak{N}$, we can construct a linear endomorphism $T_\mathfrak{q}$ of $H^i(Y_0(\mathfrak{N}), \mathbb{C})$, called a **Hecke operator**. Let $\mathbb{T}_\mathbb{C}^{(i)}(\mathfrak{N})$ be the commutative $\mathbb{Z}$-algebra generated by these Hecke operators inside the endomorphism algebra of $H^i(Y_0(\mathfrak{N}), \mathbb{C})$.
A **complex eigenform** f over K of degree i and level $\mathfrak{N}$ is a ring homomorphism $f : \mathbb{T}_\mathbb{C}^{(i)}(\mathfrak{N}) \to \mathbb{C}$.

- values of f generate a $\#$ field $\mathbb{Q}_f$.
- f is **trivial** if $f(T_\mathfrak{q}) = Norm(\mathfrak{q}) + 1, \forall \mathfrak{q} \nmid \mathfrak{N}$
- f, g are **equivalent** if $f(T_\mathfrak{q}) = g(T_\mathfrak{q})$, for almost all $\mathfrak{q}$. f, g are allowed to have different degrees and levels.
- f is called **new** if it is not equivalent to one whose level is a proper divisor of $\mathfrak{N}$.

If p is a rational prime unramified in K and coprime to the level, $H^i\left(Y_0(\mathfrak{N}), \overline{\mathbb{F}}_p\right)$ also comes equipped ith Hecke operators $T_\mathfrak{q}$ where $\mathfrak{q} \nmid p\mathfrak{N}$. They form an algebra $\mathbb{T}^{(i)}_{\overline{\mathbb{F}}_p}$. A **(weight 2) mod p eigenform** f over K of degree i and level $\mathfrak{N}$ is a ring homomorphism $f : \mathbb{T}^{(i)}_{\overline{\mathbb{F}}_p}(\mathfrak{N}) \to \overline{\mathbb{F}}_p$.

Definition

We say that a mod p eigenform θ, of level $\mathfrak{N}$, lifts to a complex eigenform if there exists a complex eigenform f, of the same degree and level and a prime ideal $\mathfrak{p}$ of $\mathbb{Q}_f$ over p such that for every prime $\mathfrak{q}$ of K coprime to $p\mathfrak{N}$ we have $\theta(T_\mathfrak{q}) = \overline{f(T_\mathfrak{q})} \pmod{\mathfrak{p}}$.