Serre's Conjecture On Imaginary Quadratic Fields

A Survey

Mehmet Haluk Şengün

1 Introduction

Let

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$$

be a continuous representation over a finite field $\mathbb{F}$ of characteristic $l > 0$. Such a representation is called a mod l Galois representation.

Let $f \in S_k(N, \epsilon)$ be a normalised cuspform which is a simultaneous eigenform for the Hecke operators.

We say that ρ and f are **associated** (or "ρ is *modular by f*", or "ρ *comes from f*") if

$$Tr(\rho(Frob_p)) = \overline{a_p(f)} \quad and \quad det(\rho(Frob_p)) = \overline{\epsilon(p).p^{k-1}} \quad \forall p \not| Nl$$

where $a_p(f)$ is the p-th Fourier coefficient of f and the map $z \to \overline{z}$ is a ring homomorphism from the ring of integers of $\mathbb{Q}(a_2(f), a_3(f), ...)$ to $\mathbb{F}$.

2 Conjecture

- **(Weak-Qualitative)** In 1975 Serre ([1]) conjectured that an odd absolutely irreducible mod l Galois representation is modular.
- **(Strong-Refined)** In 1987 Serre ([2]) formulated a stronger version which predicts the level, weight and character of the eigenform that the representation is conjectured to be associated to.
- Let $f \in S_k(N, \epsilon)$ be a normalised cuspidal eigenform. One can show that $E = \mathbb{Q}(a_2(f), a_3(f), ...)$ is a number field. Take a prime λ of the ring of integers O of E lying above l. Let E_λ be the completion of E at λ and let O_λ be its ring of integers. By a construction of Deligne ([3]) (building on a construction of Eichler-Shimura for weight 2), one gets an irreducible l-adic Galois representation

$$\rho_f : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(O_\lambda)$$

that is unramified at every prime $p \not| Nl$ and such that

$$Tr(\rho_f(Frob_p)) = a_p(f) \quad and \quad det(\rho_f(Frob_p)) = \epsilon(p).p^{k-1} \quad \forall p \not| Nl$$

Now one takes reduction of O_λ by λ and gets a mod l Galois representation

$$\overline{\rho}_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_{l^n})$$

with

$$Tr(\overline{\rho}_f(Frob_p)) = \overline{a_p(f)} \quad and \quad det(\overline{\rho}_f(Frob_p)) = \overline{\epsilon(p).p^{k-1}} \quad \forall p \not| Nl$$

Since $\overline{\rho}_f$ is not necessarily irreducible, we take its semisimplification (doesn't change trace and determinant). So Serre's conjecture says that all odd absolutely irreducible mod l Galois representations are isomorphic to a $\overline{\rho}_f$ for some normalised cuspidal eigenform f with prescribed level, weight and character.

3 Notes

- For $l = 2, 3$, the Strong Conjecture has to be modified ([4]).
- (**ϵ-conjecture**) It is conjectured that the WEAK conjecture implies the STRONG one. For $l > 2$, this has been proved by works of many including Boston, Carayol, Coleman, Diamond, Edixhoven, Faltings, Fontaine, Gross, Jordan, Lenstra, Livne, Mazur, Ribet, Serre, Taylor, Tilouine, Voloch and Wiles. See ([5]).
- Because of the congruences between modular forms, a modular Galois representation may be attached to infinitely many modular forms.

4 Known Cases

- Mod l Galois representations coming from elliptic curves are modular. This was proven for semistable elliptic curves over $\mathbb{Q}$ by A.Wiles and then for all elliptic curves over $\mathbb{Q}$ by Breuil-Conrad-Diamond-Taylor ([6]). (Shimura-Taniyama Conjecture mod l version)
- If the image is in $GL(\mathbb{F}_3)$, the conjecture holds. This was proven by Serre ([2]), using results of Langlands and Tunnell.
- If the image is dihedral and characteristic is odd, the conjecture holds. This is work of Hecke ([7]).

- The conjecture holds for $\mathbb{F}_4$ and $\mathbb{F}_5$ with some restrictions. This is work of Shepherd-Barron and Taylor ([8]).
- **LATEST NEWS!!!** Khare([9]) proved that the conjecture holds when the Serre level of the representation is 1. He also proves the conjecture for prime Serre level and Serre weight 2 for characteristic > 2. His result builds on his joint work with Winterberger and uses results of Ramakrishna, Böckle, Taylor, Dieulefait and others. See "Suggested Readings" section for suggested readings on this latest work.

5 Some Consequences

- **Fermat's Last Theorem** Assuming FLT gives rise to Frey's elliptic curve which gives an odd irreducible cont. Galois representation of Serre level 2, Serre weight 2 with trivial character. This contradicts Serre's conjecture since there are no nontrivial eigenforms of wight 2 on $\Gamma_0(2)$.
- Other similar Diophantine results. If Serre's conjecture is true then

$$x^p + y^p = z^2, \qquad p \geq 13,\ p \equiv 1\ (mod 4),$$

$$x^p + y^p = z^3, \qquad p \geq 13,\ p \equiv 1\ (mod 3),$$

$$x^4 + y^4 = z^p, \qquad p \geq 13,\ p \equiv 1\ (mod 4),$$

  have no solutions (x, y, z) with $xyz \neq 0$ and $gcd(x, y, z) = 1$.
- If Serre's conjecture is true, then an elliptic curve over $\overline{\mathbb{Q}}$ is modular iff it is a $\mathbb{Q}$-curve (Ribet)([10]).
- **Shimura-Taniyama Conjecture** which says that every elliptic curve over $\mathbb{Q}$ comes from a cusp form of weight 2 (i.e. they have the same L-function) is implied by Serre's conjecture (Serre ([2])).

6 Over Imaginary Quadratic Fields

Let F be a global field. There are different ways to approach generalizing modular forms to F; one can use automorphic forms on $GL_2(A_F)$ following Weil ([11]) or go one more step and replace these with automorphic representations following Langlands where A_F is the ring of adeles of F. These are well developed theories but not very amenable for computations. Fortunately for our case, there are simpler approaches which are suitable for computations.

Let K be an imaginary quadratic field and O_K be its ring of integers. Let H_3 be the hyperbolic 3-space. A model of H_3 is the Poincare upper half-space of $\mathbb{R}^3$,

$$H_3 = \mathbb{C} \times \mathbb{R}_{>0} = \ \{(z,t)|z \in \mathbb{C},\ t \in \mathbb{R}^{>0}\}$$

which plays the same role as the upper half plane plays in the classical situation. When we put the hyperbolic metric $ds^2 = \frac{dx^2+dy^2+dt^2}{t^2}$, $PSL_2(\mathbb{C})$ acts on H_3 as a group of isometries. The action is nicely written using quaternion notation: identifying the point (z,t) with the quaternion $q = z + tj$, the action is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : q \to \frac{a+bq}{c+dq}$$

The subgroup $PSL_2(O_K)$ is a discrete subgroup of $PSL_2(\mathbb{C})$, thus it acts discontinuously on H_3. For an ideal N of O_K, put $\Gamma_0(N)$ for the subgroup of $PSL_2(O_K)$ consisting of matrices which are triangular modulo N. The quotient space $X_0(N) = \Gamma_0(N)\backslash H_3$ is a noncompact Riemannian 3-manifold provided that $\Gamma_0(N)$ has no nontrivial torsion elements. Note that one can always work with a finite index torsion-free normal subgroup of $\Gamma_0(N)$, when $\Gamma_0(N)$ is not torsion-free. Existence of such a subgroup is given by a theorem of Selberg([12]). We obtain a compactification of $X_0(N)$ by adjoining the cusps of $\Gamma_0(N)$; let $X_0^*(N) = \Gamma_0(N)\backslash(H_3 \cup P(K))$.

We will be looking at the space $S_2(N)$ of cuspforms of weight 2 for $\Gamma_0(N)$. Let's assume for simplicity that the class number of K is 1. Following Weil in our case, one defines such a cuspform as a vector valued function

$$F = (F_0, F_1, F_2) : H_3 \to \mathbb{C}^3$$

such that $-F_0\frac{dz}{t} + F_1\frac{dt}{t} + F_2\frac{d\bar{z}}{t}$ is a $\Gamma_0(N)$-invariant harmonic differential on H_3, well behaved at the cusps. Kurcanov ([13]) in late 70's showed that

$$S_2(N) \cong H^1(X_0^*(N), \mathbb{C})$$

Using Generalized Stokes' Theorem, one can integrate a differential form along a chain and get a pairing

$$H_1(X_0^*(N), \mathbb{C}) \ \times \ H^1(X_0^*(N), \mathbb{C}) \to \mathbb{C}$$

De Rham's theorem says that this pairing is an exact duality. The Hecke action on the space of cuspforms can be transfered to the cohomology group too. Fortunately, the duality works at the level of rational (Hecke) structures (as in the classical case), thus it is enough to study $H_1(X_0^*(N), \mathbb{Q})$. A generalization of the Manin-Drinfeld Theorem (by Kurcanov) tells us that the rational homology is generated by the paths between cusps and conversely, any path between two cusps is rational. Now one uses method of modular symbols to compute the rational homology. The method of modular symbols was formalised by Manin and extended to the imaginary quadratic case by Cremona and his students. Cremona and his students focused on the connection between elliptic curves over K and weight 2 cuspforms. An analogue of the correspondance in the classical case does not hold, also there's no analogue of the Shimura-Eichler construction. The difficulty is that unlike the classical case, there's no obvious link to arithmetic geometry. The manifold $X_0^*(N)$ is three dimensional and hence doesn't have a complex structure. A result of Taylor ([14])attaches a system of l-adic Galois representations to a given cuspform under some assumptions.

Now let's look at what has been done on mod l case.

6.1 Work of Figueiredo

In his Ph.D. thesis ([15]) and in ([16]), Figueiredo focuses on a possible analogue of Serre's Conjecture for weight 2 over imaginary quadratic fields.

- He defines mod l the space of cusp forms of weight 2 on $\Gamma_1(N)$ as $H_1(X_1^*(N), \overline{\mathbb{F}}_l)$. Let ϵ be a character,

  $$\epsilon : \Gamma_0(N)/\Gamma_1(N) \to \overline{\mathbb{F}}_l^*$$

  The group $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(O_K/N)^*/O_K^*$. For any $u \in \Gamma_0(N)/\Gamma_1(N)$, let $\gamma_u = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}$. A relation $\gamma_u - \epsilon(u)I_2$ will be called a character relation for ϵ. The space $S_2(\Gamma_1(N), \epsilon)$ cusp form of weight 2 with character ϵ for $\Gamma_1(N)$ is defined as the coinvariant space of $H_1(X_1^*(N), \overline{\mathbb{F}}_l)$ by the character relations for ϵ. In the classical case, mod l cusp forms are defined as the mod l reductions of cusp forms in characteristic 0. This is not the case here as not all classes lift to characteristic 0.

- He formulates an analogue of Serre's Conjecture for weight 2. He uses a result in the classical case as a guide for describing the level of the cusp form.

- The space $S_2(\Gamma_1(N), \epsilon)$ can be computed using modular symbols. He modifies Cremona's program so that it works for $\Gamma_1(N)$ and works over finite fields.

- There's no odd/even representation distinction in our case. He starts with an even Galois representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ (these cannot come from a modular form) and restricts it to $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$. If you start with an odd representation and restrict it, you can take the (conjectural) modular form and make a base change and get a modular form with the same set of eigenvalues. So checking an odd representation will be checking Serre's conjecture for the classical case.

  He provides three mod 3 examples, all representations given by the Galois groups of some polynomials. In each case, the Galois group is $PGL_2(\mathbb{F}_3)$. He studies the necesseray and sufficient conditions on the polynomials so that one can lift the representation to $GL_2(\mathbb{F}_3)$ and the lifting is even. He works over fields $K = \mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7$. In each example, he comes up with cusp forms and checks that the eigenvalues and traces of the Frobenius maps match for more than 150 values. The calculations provide strong evidence that the examples are modular but this is not proven.

6.2 Work of Grunewald,Mennicke,Elstrodt and Helling

They did the first works ([17],[18],[19]) on imaginary quadratic fields in both char. 0 and mod l cases. We will only look at their work on mod l case here. For other aspects, one should check their book "Groups Acting on Hyperbolic Space"([20]).

- Fix an ideal N of O_K. Let $\Gamma = \Gamma_0(N)$. The following is a variation of the Hecke operator construction for congruence subgroups that is given in chapter 3 of Shimura's book ([21]). For an element $\delta \in O_K$, let $\hat{\delta} = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}$. Then one defines a Hecke operator $T_\delta : \Gamma^{ab} \to \Gamma^{ab}$ as the composition of the followings:

$$V : \Gamma^{ab} \to (\Gamma \cap (\hat{\delta}^{-1}\Gamma\hat{\delta}))^{ab}$$

$$\delta^{-1} : (\Gamma \cap (\hat{\delta}^{-1}\Gamma\hat{\delta}))^{ab} \to ((\hat{\delta}\Gamma\hat{\delta}^{-1}) \cap \Gamma)^{ab}$$

$$i : ((\hat{\delta}\Gamma\hat{\delta}^{-1}) \cap \Gamma)^{ab} \to \Gamma^{ab}$$

  where V is the transfer map of group theory, δ^{-1} is induced by conjugation by $\hat{\delta}^{-1}$ map and i is the map that we get from $H \to G \to G^{ab}$ by factoring thru H^{ab}.

- In ([17]), it is shown that $(\Gamma^{ab} \bigotimes \mathbb{Q})^*$ is isomorphic to a certain subspace of $S_2(\Gamma_0(N))$. Accordingly, in mod l case, they work with $Tor(\Gamma^{ab}) \bigotimes \mathbb{F}_l$. The above introduced Hecke operators induce linear endomorphisms on these finite dimensional $\mathbb{F}_l$-vector spaces. One can compute these spaces and the Hecke operators on them concretely for prime N. They come up with examples over $\mathbb{Q}(i)$ suggesting a correspondence similar to Serre's Conjecture.

- Let $N = (6 - 11i)$. Let $P(x) = x^3 - ix - (1 + i)x - (1 - i)$. It is irreducible over $\mathbb{Q}(i)$ and has discriminant $2(6 - 11i)$. Galois group of $P(x)$ is $S_3 \cong GL_2(\mathbb{F}_2)$. They find an eigenvector in $Tor(\Gamma^{ab}) \bigotimes \mathbb{F}_2$ whose eigenvalues match with the traces of images of the Frobenius maps under the representation coming from $P(x)$ for more than 100 values. Again, the matching is not proved.

7 Suggested Readings

The followings are helpful on Galois representations and modularity:

- K.Ribet; Galois Representations and Modular Forms (his website) (check Ribet first for everything, his expositions are the best)
- R.Taylor; Galois Representations (his website)
- H.Darmon; F.Diamond, R.Taylor, Fermat's Last Theorem, in "Elliptic Curves, Modular Forms and Fermat's Last Theorem", edited by J.Coates, S-T.Yau
- J.Buhler; Elliptic Curves, Modular Forms and Applications, in "Arithmetic Algebraic Geometry", edited by B.Conrad, K.Rubin
- N.Boston; Fermat's Last Theorem notes, chapter 4-5 (his website)

The followings are articles on Serre's conjecture in the classical case :

- K.Ribet, W.Stein, Lectures on Serre's Conjecture. (Ribet's website)
- H.Darmon, Serre's Conjectures. (his website)
- D.X.Charles, Serre's Conjecture on 2-dimensional Galois Representations. (his website)
- B.Edixhoven, Introduction to Serre's conjecture. (his website, under "Arithmetic Geometry Intercity Seminar on Khare's work on Serre's conjecture ")

The followings are on modularity over imaginary quadratic fields:

- J.E.Cremona, Modular Forms and Elliptic Curves over Imaginary Quadratic Fields. (his website)
- R.Taylor, Representations of Galois Groups Associated to Modular Forms, in "Proceedings of the International Congress of Mathematicians, Zurich, Switzerland 1994"

The followings are on Khare's latest work:

- K.Ribet, Slides for his talk on June 4, 2005 at the summer meeting of the Canadian Mathematical Society, his website
- B.Edixhoven et al; Notes of Arithmetic Geometry Intercity Seminar on Khare's work on Serre's conjecture, Edixhoven's website

8 References

1. J.P.Serre; Valeurs propres es operateurs de Hecke modulo l, Journeees Arithmetique Bordeaux, 1974, Asterisque, 24-25, (1975)

2. J.P.Serre; Sur les representations modulaires de degre 2 de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math.J., 54, (1987)

3. P.Deligne; Formes modulaires et representations l-adiques, Sem. Bourbaki no.335, 1968-69, Springer-Verlag, Lecture Notes in Mathematics, vol.179, (1971)

4. K.Ribet, W.Stein; Lectures on Serre's Conjectures (Ribet's website). It focuses on the ϵ-conjecture.

5. A.Ash, G.Stevens; Modular forms in characteristic l and special values of their L-functions, Duke Math. J. , 53, (1986)

6. C.Breuil, B.Conrad, F.Diamond, R.Taylor; On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, J.Amer.Math.Soc., 14, no.4,(2001)

7. See H.Darmon's notes on Serre's Conjecture, section 3.2.1, listed under "Suggestes Readings"

8. N.I.Shepherd-Barron, R.Taylor; Mod 2 and 5 icosahedral representations, J.Amer.Math.Soc., 10, no.2, (1997)

9. C.Khare; Serre's modularity conjecture: the level one case, preprint, his website

10. K.Ribet; Abelian varieties over $\mathbb{Q}$ and modular forms, Algebra and topology 1992, Taejuon, Korea Adv. Inst. Sci. Tech., (1992)

11. A.Weil; Dirichlet Series and automorphic Forms, Springer-Verlag, Lecture Note Series in Mathematics, 189 (1971)

12. A.Selberg; On discontinuous groups in higher dimensional spaces. Contributions to function theory, International Colloquium on Function Theory, Tata, Institute of Fundamental Research, Bombay

13. P.F.Kurcanov; Cohomology of discrete groups and Dirichlet series connected with Jacquet-Langlands cusp forms, Math.USSR Izvestija, 12(3),(1978)

14. R.Taylor; l-adic representations associated to modular forms over imaginary quadratic fields.II, Invent.Math., 116, (1994)

15. L.M.S.Figueiredo; Serre's conjecture over imaginary quadratic fields, Ph.D. thesis, University of Cambridge, 1995

16. L.M.S.Figueiredo; Serre's conjecture over imaginary quadratic fields, Compositio Math., 118, (1999)

17. F.Grunewald, H.Helling, J.Mennicke; $SL_2(O)$ over complex quadratic numberfields I, Algebra i Logica, 17, (1978)

18. J.Elstrodt, G.Grunewald, J.Mennicke; On the group $PSL_2(\mathbb{Z}[i])$, Journees Arithmetiques 1980 (LMS lecture notes 56), J.V.Armitage (ed.),(1982)

19. J.Elstrodt, G.Grunewald, J.Mennicke; $PSL(2)$ over imaginary quadratic integers, Journees Arithmetiques 1981, Asterique, 94, (1982)

20. J.Elstrodt, G.Grunewald, J.Mennicke; Groups Acting On Hyperbolic Space, Springer Monographs in Mathematics, (1997)

21. G.Shimura; Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press, (1971)