Summary of My Research

Arash Rastegar

September 24, 2005

My field of research is arithmetic geometry. I will start by introducing my conceptual background and my research skills, and then I will review my results in four separate sections.

My background in analysis is limited to my research field. The words symmetric spaces, modular forms, L-functions and automorphic representations pretty much classifies the kind of analysis I am most familiar with. I am also familiar with the kind of analysis which is absorbed in geometric formalism. Moduli spaces, deformation theory and dynamical systems introduce a good picture of the most convenient set up for me a geometric object could be studied in. All my geometric concepts could be studied in algebraic language. Any kind of algebraic structure which could be related to number theory is under my focus. Diophantine geometry is my main focus in number theory. I consider my results immature until they contribute to Diophantine geometry.

While performing my research, I try to construct arithmetic versions of every piece of mathematics I encounter. Then, I try to contribute to problems in Diophantine geometry. I lay mostly on geometric imagination rather than analytic calculations. This is my main source of creativity. My background in geometry is a rich toolbox for handling technical difficulties. Any use of analytical techniques is pure imitation for me. Algebraic calculations are successful when I see what I am doing. I have no interest in doing mathematics in the style of Euclid, dealing with axioms and their logical consequences. I don't even like his style of presentation. The process of discovery is very important to me.

1 Modular forms

Let $\mathbf{F}_q$ denote a finite field of characteristic p and let X be a smooth projective absolutely irreducible curve of genus g over $\mathbf{F}_q$. The field of rational functions K of the curve X is an extension of $\mathbf{F}_q$ of transcendence degree one. We fix a place ∞ of K with associated normalized absolute value. The order of the residue field of the ring of integers O_v of the completion K_v is denoted by q_v. In my thesis, I got congruences between $\mathbb{Q}_l$-valued weight two v-old Drinfeld modular forms and v-new Drinfeld modular forms of level vn.

Theorem 1.1 *Let n be a nonzero effective divisor on $X - \{\infty\}$ and let v be a point on $X - \{\infty\}$ which does not intersect n. Let l be a prime not dividing $2q(q_v + 1)$ and not contained in an explicit finite set of places $S_{\Gamma(n)}$. Let f be a Hecke eigen-form of level $\Gamma(n)$ and $T_v f = t_v f$. If $t_v^2 \equiv (q_v + 1)^2$ mod l then f is congruent to a new-form of level $\Gamma_0(v) \cap \Gamma(n)$ mod l.*

In the number field case, the idea of obtaining such a cogruence is due to Ribet [Ri]. In order to do this, we shall first construct a cokernel torsion-free injection from a full lattice in the space of v-old Drinfeld modular forms of level vn into a full lattice in the space of all Drinfeld modular forms of level vn. To get this injection we use ideas introduced by Gekeler and Reversat on uniformization of jacobians of Drinfeld moduli curves [Ge-Re].

In our attempt to generalize this to Siegel modular forms, we introduced a higher dimensional Atkin-Lehner theory for Siegel-parahoric and Borel congruence subgroups of $GSp(2g)$. The philosophy is that, old Siegel forms are induced by geometric correspondences on Siegel moduli spaces which commute with almost all local Hecke algebras. We use elements of the Weyl group of $GSp(2g)$ to construct new congruence subgroups sandwiched between the Siegel-parahoric congruence group

$$\Gamma^P(n) = \{\gamma \in Sp(2g, \mathbb{Z}) | \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, (\text{mod } n)\}$$

and the following congruence group

$$\Gamma^T(n) = \{\gamma \in Sp(2g, \mathbb{Z}) | \gamma \equiv diag(*, ..., *), (\text{mod } n)\}.$$

These groups are all defined in terms of the mod-n reduction of elements in $Sp(2g, \mathbb{Z})$ and thus have moduli interpretations which could be used to define correspondences on the moduli space.

Let ζ_n denote an n-th root of unity for $n \geq 3$. The moduli scheme classifying the principally polarized abelian schemes over $Spec(\mathbb{Z}[\zeta_n, 1/n])$ together with a symplectic principal level-n structure is a scheme over $Spec(\mathbb{Z}[\zeta_n, 1/n])$ and will be denoted by $\mathcal{A}_g(n)$. The symplectic group $Sp(2g, \mathbb{Z}/n\mathbb{Z})$ acts on $\mathcal{A}_g(n)$ as a group of symmetries by acting on level structures. We will recognize these moduli spaces and their etale quotients under the action of subgroups of $Sp(2g, \mathbb{Z}/n\mathbb{Z})$ as Siegel spaces.

A $\Gamma^P(n)$-level structure of type I on (A, λ) is choice of a subgroup $H \subset A[n]$ of order n^g which is totally isotropic with respect to the Weil pairing induced by λ. A $\Gamma^P(n)$-level structure of type II on (A, λ) is choice of a principally polarized isogeny $(A_1, \lambda_1) \to (A_2, \lambda_2)$ of degree n^g. By a principally polarized isogeny, we mean an isogeny $\sigma : A_1 \to A_2$ such that $\sigma \circ \lambda_2 \circ \sigma^t \circ \lambda_1^{-1}$ is multiplication by an integer. For $n \geq 3$ type I and type II $\Gamma^P(n)$-level structures induce isomorphic moduli schemes over $Spec(\mathbb{Z}[1/n])$ [DJ]. We denote this moduli scheme by $\mathcal{A}_g^P(n)$. There exists a natural involution

$$w_n^P : \mathcal{A}_g^P(n) \to \mathcal{A}_g^P(n)$$

taking $(\sigma : (A_1, \lambda_1) \to (A_2, \lambda_2))$ to $(\sigma^t : (A_2, (\lambda_2^t)^{-1}) \to (A_1, (\lambda_1^t)^{-1}))$ which we call the Atkin-Lehner involution.

A $\Gamma^B(n)$-level structure of type I on (A, λ) is choice of g subgroups $H_i \subset A[n]$ of order n^i with $H_1 \subset ... \subset H_g$ where H_g is totally isotropic. A $\Gamma^B(n)$-level structure of type II on (A, λ) is choice of a chain of g isogenies $(A_0, \lambda_0) \xrightarrow{\alpha} ... \xrightarrow{\alpha} (A_g, \lambda_g)$ each of degree n which satisfy $n.id_{A_i} = \alpha^i \circ \lambda_0^{-1} \circ (\alpha^t)^g \circ \lambda_g \circ \alpha^{g-i}$ for all $i = 1, ..., g$. In case $n \geq 3$ type I and type II $\Gamma^B(n)$-level structures induce isomorphic moduli schemes over $Spec(\mathbb{Z}[1/n])$ [DJ]. We denote this moduli scheme by $\mathcal{A}_g^B(n)$. There also exists a natural involution

$$w_n^B : \mathcal{A}_g^B(n) \to \mathcal{A}_g^B(n)$$

taking $((A_0, \lambda_0) \xrightarrow{\alpha} ... \xrightarrow{\alpha} (A_g, \lambda_g))$ to $((A_g, (\lambda_g^t)^{-1}) \xrightarrow{\alpha^t} ... \xrightarrow{\alpha^t} (A_0, (\lambda_0^t)^{-1}))$ which commutes with the Atkin-Lehner involution under the natural projection between the Siegel spaces.

$$\begin{array}{ccc} \mathcal{A}_g^B(n) & \xrightarrow{w_n^B} & \mathcal{A}_g^B(n) \\ \downarrow & & \downarrow \\ \mathcal{A}_g^P(n) & \xrightarrow{w_n^P} & \mathcal{A}_g^P(n) \end{array}$$

A $\Gamma^T(n)$-level structure on (A, λ) is choice of $2g$ subgroups $H_i \subset A[n]$ for $i = 1$ to $2g$, each isomorphic to $(\mathbb{Z}/n\mathbb{Z})$ such that $H_1 \oplus ... \oplus H_g$ and $H_{g+1} \oplus ... \oplus H_{2g}$ are totally isotropic subgroups of order n^g which do not intersect with $H_i \oplus H_{g+i}$ hyperbolic for $i = 1$ to g. For A and A' abelian schemes over the schemes S and S' respectively, we define a morphism from $(S, A, \lambda, H_1, ..., H_{2g})$ to $(S', A', \lambda', H_1', ..., H_{2g}')$ to be a pair of morphisms (f, g) where $f : S \to S'$ and $g : A \to A'$ satisfy $g^*(\lambda') = \lambda$ and $g(H_i) = H_i'$ for all $1 \leq i \leq 2g$. Also we want the pair (f, g) to induce an isomorphism $A \simeq S \times_{S'} A'$. Having these morphisms defined, we have formed a category $\mathbf{A}_g^T(n)$. The functor $\pi : \mathbf{A}_g^T(n) \to Sch$ defined by $\pi(S, A, \lambda, H_1, ..., H_{2g}) = S$ makes $\mathbf{A}_g^T(n)$ into a stack in groupoids over S. The 1-morphism of stacks $\pi' : \mathbf{A}_g^T(n) \to \mathbf{A}_g$ defined by $\pi'(S, A, \lambda, H_1, ..., H_{2g}) = (S, A, \lambda)$ is representable and is a proper surjective morphism. For $n \geq 3$ we get a separated scheme of finite type $A_g^T(n)$ which is smooth over $Spec(\mathbb{Z}[1/n])$. The moduli space $\mathcal{A}_g^T(p)$ is the appropriate moduli space to geometrically realize all the endomorphisms

$$v_p^\sigma : \mathcal{A}_g^T(p) \to \mathcal{A}_g^T(p)$$

induced by conjugation via elements σ in the Weyl group W_G.

Theorem 1.2 *The linear subspaces of $H^0(\mathcal{A}_g^{B,P}(p, n), \omega^{\otimes k})$ generated by Atkin-Lehner correspondences $\pi_{n*} C_B^\sigma(p) \pi_n^*$ where $C_B^\sigma(p)$ is defined by $\pi_{T,B*} v_p^{\sigma*} \pi_{T,B}^* w_p^{B*}$*

$$\begin{array}{ccccc} \mathcal{A}_g^{T,P}(p, n) & \xrightarrow{v_p^\sigma} & \mathcal{A}_g^{T,P}(p, n) & & \\ \downarrow & & \downarrow & & \\ \mathcal{A}_g^{B,P}(p, n) & & \mathcal{A}_g^{B,P}(p, n) & \xrightarrow{w_p^B} & \mathcal{A}_g^{B,P}(p, n) \end{array}$$

for σ varying in W_G give several linearly independent copies of $H^0(\mathcal{A}_g^P(n), \omega^{\otimes k})$ inside p-old forms of level pn living on $\mathcal{A}_g^{B,P}(p,n)$.

If one could prove that the number of these copies is $g!2^g$ a geometric formulation for the notion of p-old Siegel modular forms would be available for arbitrary genus. This is what we originally imagined we had proved, but there was some flaws in our arguments.

Using the Atkin-Lehner correspondences, we define a map from four copies of the space of forms of level n to the p-old part of forms of level np which turns out to be injective and generate the whole p-old part. By an Ihara-result we mean cokernel torsion-freeness of the map induced on the specified full lattices in these vector spaces. This is what Ihara proved in the elliptic modular case [Ih]. Injection of this map is an automorphic fact. But cokernel torsion-freeness is proved by getting an injection result in finite characteristic. We generalize a result of G. Pappas to get this injection using density of Hecke orbits. This density result is proved by C. Chai [Ch]. The precise statement of our main result is as follows.

Theorem 1.3 *Let p be a prime which does not divide the square-free integer n. Atkin-Lehner correspondences induce an injection from a full lattice in the space of p-old Siegel modular forms, into a full lattice in the space of all modular forms of level np. The cokernel of this map is free of l-torsions for all primes l not dividing $2np[\Gamma^P(p) : \Gamma^T(p)]$ with $l-1 > k$ where $\Gamma^P(p)$ and $\Gamma^T(p)$ are certain congruence subgroups of $Sp(4,\mathbb{Z})$.*

Using the same ideas one can also prove an Ihara result for Siegel-Jacobi forms of genus two. Let $\mathcal{B}_g^*(n)$ denotes the compactification of the universal abelian variety over the Siegel space $\mathcal{A}_g^B(n)$.

Theorem 1.4 *Let p be a prime which does not divide n. The Atkin-Lehner correspondences induce a cokernel torsion-free injection*

$$H^0(\mathcal{B}_2^{0*}(n)/\mathbb{Z}_l, \omega^{\otimes k} \otimes L^{\otimes m})^{\oplus 4} \to H^0(\mathcal{B}_2^{0*}(np)/\mathbb{Z}_l, \omega^{\otimes k} \otimes L^{\otimes m})$$

for all primes l not dividing $2pn[\Gamma^P(p) : \Gamma^T(p)]$ with $l-1 > k$.

We shall continue this line of research by trying to obtain congruences between Siegel modular forms of arbitrary genus.

2 Arakelov theory

We introduce an admissible pairing of divisors on a Drinfeld moduli space as an analogue of Arakelov's pairing on an arithmetic surface. Such a pairing has been constructed before by S. Zhang by globalizing a pairing which he constructed of divisors on a curve defined over a non-archimedean field [Zh]. In order to define such a pairing, he associated a graph to each finite fiber and defined Green's functions on these metrized graphs. By specializing to Drinfeld moduli spaces we are able to construct a pairing without passage through local theory.

Let k denote the residue class field of $O_\infty \subset K_\infty$ of cardinality q_∞. The set of vertices $V(\tau)$ of the Bruhat-Tits tree consists of the set of similarity classes of O_∞-lattices in K_∞^2. Two vertices are adjacent if and only if they are represented by lattices $\Lambda_1 \subsetneq \Lambda_2$ such that $\Lambda_1 \backslash \Lambda_2$ has length one. This way, we get a connected homogeneous tree τ over which $\mathrm{GL}(2, K_\infty)$ acts by its quotient $\mathrm{PGL}(2, K_\infty)$ [Ge-Re].

There is a canonical map λ from Ω to the realization $\tau(\mathbb{R})$ of τ. Inverse image of vertices of τ under λ are isomorphic as analytic spaces with $P^1(C)$ minus $(q_\infty + 1)$ disjoint open balls, and inverse image of edges of τ (open edges) are isomorphic to an annulus

$$\{z \in C \mid q_\infty^{-1} < |z| < 1\}.$$

The map λ is equivariant with respect to the left action of $\mathrm{GL}(2, K_\infty)$ on Ω and τ. So we get a map $\Gamma\backslash\Omega \to \Gamma\backslash\tau$. The graph $\Gamma\backslash\tau$ is union of on finite graph with finitely many ends. By ends, we mean half lines like this

and λ induces a bijection of the set of ends in $\Gamma\backslash\tau$ with the cusps of the Drinfeld moduli curve $\bar{M}_\Gamma(C) - M_\Gamma(C)$, which are in one-to-one correspondence with the set $\Gamma\backslash P^1(K)$. The genus $g(\bar{M}_\Gamma)$ of $\bar{M}_\Gamma$ equals the first betti number $b_1(\Gamma\backslash\tau)$ of $\Gamma\backslash\tau$ which is also the rank $\dim_{\mathbb{Q}} \Gamma^{ab} \otimes \mathbb{Q}$ of the factor commutator group Γ^{ab} of Γ [De-Hu].

We use Bruhat-Tits tree τ of $\mathrm{PGL}(2, \mathbb{F}_q((t)))$, where $\mathbb{F}_q$ is a finite field of characteristic p, and apply Zhang's version of Green's function to a quotient of τ which is associated to the Drinfeld moduli space, we started with. Our definition has the advantage that it can be naturally generalized to Drinfeld moduli spaces of higher ranks.

S. Bloch suggested to us to use this intersection theory to check Birch and Swinerton-Dyer conjecture in the special case of Drinfeld modular curves.

3 Diophantine geometry

By arithmetic fractals we mean self-similar objects in arithmetic ambient spaces. More precisely, arithmetic fractals are subsets of arithmetic varieties which are finite union of pieces, each similar to the whole object, where these similarity maps are given by algebraic self-maps on the ambient arithmetic variety. For technical reasons, we assume that only finite intersection between these pieces are allowed. This allows us to define a well-defined and well-behaved concept of fractal dimension for these arithmetic objects. This concept is intimately related to the concept of arithmetic height. Examples of arithmetic fractals are the set of rational points on an abelian variety or on a projective space, and the set of torsion points on an abelian variety.

We consider finiteness problems in Diophantine geometry in the context of arithmetic fractals. There are quite a number of statements in Diophantine geometry which are naturally formulated in the context of arithmetic fractals. Indeed, arithmetic fractals provide a common framework in which similar theorems in Diophantine geometry could be united in a single context. We formulate a general conjecture implying and unifying many similar statements.

Conjecture 3.1 *Let X be an irreducible variety over a finitely generated field K and let $F \subset X(\bar{K})$ denote an arithmetic fractal on X and let Z be a reduced subscheme of X. The Zariski closure of $Z(\bar{K}) \cap F$ is union of finitely many components B_i for which, either B_i is a point, or $B_i(\bar{K}) \cap F$ is an arithmetic fractal with respect to some induced endomorphisms of B_i.*

Important special cases are proved by Faltings and Raynaud [Fa],[Ra]. Our main theorems are extensions of Siegel's and Falting's theorems on finiteness of integral points, which are special cases of the above general conjecture. Here is our version of Siegel's theorem:

Theorem 3.2 *Let X be an affine irreducible curve defined over a number field K and let $F \subset \mathbb{A}^n(\bar{K})$ denote an affine arithmetic fractal in the affine ambient space of X, which means that self-similarity maps are given by polynomials. If genus of X is ≥ 1, then $X(K) \cap F$ is finite.*

Our version of Faltings' theorem is as follows:

Theorem 3.3 *Let A be an abelian variety defined over a number field. Let W be an affine open subset of A and F be an affine arithmetic fractal contained in $\mathbb{A}^n(\bar{K}) \supset W(\bar{K})$ where K is a number field. Then $F \cap W(K)$ is finite.*

These results are proved using the following strong fractal version of Roth's theorem:

Theorem 3.4 *Fix a number-field K and $\sigma : K \hookrightarrow \mathbb{C}$ a complex embedding. Let V be a smooth projective algebraic variety defined over K and let L be an ample line-bundle on V. Denote the arithmetic height function associated to the line-bundle L by h_L. Suppose $F \subset V(K)$ is a fractal subset with respect to finitely many height-increasing self-endomorphisms $\phi_i : V \to V$ defined over K such that for all i we have*

$$h_L(\phi_i(f)) = m_i h_L(f) + 0(1)$$

where $m_i > 1$. Fix a Riemannian metric on $V_\sigma(\mathbb{C})$ and let d_σ denote the induced metric on $V_\sigma(\mathbb{C})$. Then for every $\delta > 0$ and every choice of an algebraic point $\alpha \in V(\bar{K})$ which is not a critical value of any of the ϕ_i's and all choices of a constant C, there are only finitely many fractal points $\omega \in F$ approximating α in the following manner

$$d_\sigma(\alpha, \omega) \leq C e^{-\delta h_L(\omega)}.$$

We will follow this line of research by trying to connect our conjecture with Vojta's conjectures.

4 Deformation theory

To a hyperbolic smooth curve defined over a number-field one naturally associates an "anabelian" representation of the absolute Galois group of the base field landing in outer automorphism group of the algebraic fundamental group.

$$\rho_X : Gal(\bar{K}/K) \longrightarrow Out(\pi_1(X))$$

Here $Out(\pi_1(X))$ denotes the quotient of the automorphism group $Aut(\pi_1(X))$ by inner automorphisms of the algebraic fundamental group. By a conjecture of Voevodski and Matsumoto the outer Galois representation is injective when topological fundamental group of X is nonabelian. Special cases of this conjecture are proved by Belyi for $\mathbb{P}^1 - \{0, 1, \infty\}$, by Voevodski in cases of genus zero and one [Vo], and by Matsumoto for affine X using Galois action on profinite braid groups [Ma]. The importance of the representation ρ_X is due to the fact that, by a result of Mochizuki, for X and X' hyperbolic curves, the natural map

$$Isom_K(X, X') \longrightarrow Out_{Gal(\bar{K}/K)}(Out(\pi_1(X)), Out(\pi_1(X')))$$

is a one-to-one correspondence [Mo]. Here $Out_{Gal(\bar{K}/K)}$ denotes the set of Galois equivariant isomorphisms between the two profinite groups. In particular, ρ_X determines X completely.

The induced pro-l representation

$$\rho_X^l : Gal(\bar{K}/K) \longrightarrow Out(\pi_1^l(X))$$

after abelianization of the pro-l fundamental group induces the standard Galois representation associated to Tate module of the Jacobian variety of X. Curves with abelian fundamental group are not interesting here, because the outer representation does not give any new information. After dividing $\pi_1^l(X)$ by its Frattini subgroup, or by mod-l reduction of the abelianized representation, one obtains a mod-l representation

$$\bar{\rho}_X^l : Gal(\bar{K}/K) \longrightarrow GSp(2g, \bar{\mathbb{F}}_l).$$

We are interested in the space of deformations of the representation ρ_X^l fixing the mod-l reduction $\bar{\rho}_X^l$. In order to make sense of deforming a representation landing in $Out(\pi_1^l(X))$ we will translate the outer representation of the Galois group to the language of graded Lie-algebras.

If all of the points in the complement $\bar{X} - X$ are K-rational, then the pro-l outer representation of the Galois group lands in the braid type outer automorphism group

$$\tilde{\rho}_X^l : Gal(\bar{K}/K) \longrightarrow \widetilde{Out}(\pi_1^l(X))$$

and the weight filtration on the pro-l outer automorphism group induce a filtration on the absolute Galois group mapping to $\widetilde{Out}(\pi_1^l(X))$ and also an injection between associated Lie algebras over $\mathbb{Z}_l$ defined by each of these filtrations

$$Gr^{\bullet}_{X,l} Gal(\bar{K}/K) \hookrightarrow Gr^{\bullet}_I \widetilde{Out}(\pi_1^l(X)).$$

The classical Schlessinger criteria for deformations of functors on Artin local rings is used for deformation of the Galois action on the abelianization of the pro-l fundamental group which is the same as etale cohomology. Using Schlessinger criteria, we will construct universal deformation rings parameterizing all liftings of the mod-l representation $\bar{\rho}_X^l$ to actions of the Galois group on graded Lie-algebras over $\mathbb{Z}_l$ with finite-dimensional graded components. We also show that this deformation theory is equivalent to deformation of abelian representations of the Galois group. Together with Shimura-Tanyama-Weil conjecture proved by Wiles and his collaborators [Wi] [Ta-Wi] [Br-Co-Di-Ta] we get the following

Theorem 4.1 *Let E be an elliptic curve over $\mathbb{Q}$ together with a rational point $0 \in E$. For each m the Galois representation*

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(gr^m \widetilde{Out}(\pi_1^l(E - \{0\})))$$

appear as direct summand of the Galois representation

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(gr^m \widetilde{Out}(\pi_1^l(Y_0(N))))$$

for some integer N.

To use the full power of outer representations, we deform the corresponding Galois-Lie algebra representation to the graded Lie algebra associated to weight filtration on outer automorphism group of the pro-l fundamental group. We construct a deformation ring parameterizing all deformations fixing the mod-l Lie-algebra representation. Alongside, we develop an arithmetic theory of deformations of Lie-algebras.

More, precisely, we are interested in deforming the following graded representation of the Galois graded Lie algebra

$$\rho : Gr^{\bullet}_{X,l} Gal(\bar{K}/K) \to Gr^{\bullet}_{I} \widetilde{Out}(\pi_1^l(X))$$

among all graded representations which modulo l reduce to the graded representation

$$\bar{\rho} : Gr^{\bullet}_{X,l} Gal(\bar{K}/K) \to \bar{L}$$

where the Lie algebra $\bar{L}$ over $\bar{\mathbb{F}}_l$ is the mod-l reduction of $Gr^{\bullet}_{I} \widetilde{Out}(\pi_1^l(X))$.

The main point we are trying to raise in this paper is that for a hyperbolic curve X the l-adic Lie-algebra representation we associate to a hyperbolic curve X contains more information than the associated abelian l-adic representation.

Theorem 4.2 *The cohomology groups $H^i(Gr^{\bullet}_{I} \widetilde{Out}(\pi_1^l(X)), Gr^{\bullet}_{I} \widetilde{Out}(\pi_1^l(X)))(0)$ are finite dimensional for all non-negative integer i.*

Theorem 4.3 $H^1(Gr^{\bullet}_{X,l} Gal(\bar{K}/K), Ad \circ \bar{\rho})(0)$ *is finite dimensional.*

Theorem 4.4 *Suppose $Gr^{\bullet}_{X,l} Gal(\bar{K}/K)$ is a free Lie algebra over $\mathbb{Z}_l$, then the Galois cohomology $H^2(Gr^{\bullet}_{X,l} Gal(\bar{K}/K), Ad \circ \bar{\rho})$ vanishes.*

Theorem 4.5 *Suppose that $Gr^{\bullet}_{X,l}Gal(\bar{K}/K)$ is a free Lie algebra over $\mathbb{Z}_l$. There exists a universal deformation ring $R_{univ} = R(X, K, l)$ and a universal deformation of the representation $\bar{\rho}$*

$$\rho^{univ} : Gr^{\bullet}_{X,l}Gal(\bar{K}/K) \longrightarrow Gr^{\bullet}_{I}\widetilde{Out}(\pi_1^l(X)) \otimes R_{univ}$$

which is unique in the usual sense. If $Gr^{\bullet}_{X,l}Gal(\bar{K}/K)$ is not free, then a mini-versal deformation exists which is universal among infinitesimal deformations of $\bar{\rho}$.

The following conjecture places the above result in the correct perspective.

Conjecture 4.6 *(Deligne) The graded Lie algebra $(Gr^{\bullet}_{\mathbb{P}^1-\{0,1,\infty\},l}Gal(\bar{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l$ is a free graded Lie algebra over $\mathbb{Q}_l$ which is generated by Soule elements and the Lie algebra structure is induced from a Lie algebra over $\mathbb{Z}$ independent of l.*

Remark 4.7 *It is reasonable to expect freeness to hold for $(Gr^{\bullet}_{X,l}Gal(\bar{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l$.*

The main obstacle in generalizing this method is the fact that fundamental groups of curves are one relator groups and therefore very similar to free groups. This makes it possible to mimic many structures which work for free groups in the case of such fundamental groups. This is heavily used in the course of our computations.

References

[Br-Co-Di-Ta] Breuil C., Conrad B., Diamond F., Taylor R.; *On the modularity of elliptic curves over $\mathbb{Q}$: wilde 3-adic excercises,* J. amer. Math. Society 14 no. 4,843-939(2001).

[Ch] Chai C.-L.:*Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Invent. Math. 121 (1995), no. 3, 439–479.

[DJ] De Jong J.: *The moduli space of principally polarized abelian varieties with $\Gamma_0(p)$-level structure.*, J. Algebraic Geom.2(1993). no. 4. 667–688.

[De-Hu] Deligne P., Husemöller D., *Survey of Drinfeld modules*, Contemp. Math. **67** (1987), 25-91.

[Ge-Re] Gekeler E.-U., Reversat M.: *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. 476 (1996), 27-93.

[Fa] Faltings G.; *Diophantine approximation on abelian varieties*, Ann. of Math. (2), 133 (3) 549-576.

[Ih] Ihara Y.:*On modular curves over finite fields; in Discrete subgroups of Lie groups and applications to moduli*, Internat. Colloq., Bombay, 1973 pp. 161–202. Oxford Univ. Press, Bombay, 1975.

[Ma] Matsumoto M.; *On the Galois image in the derivation algebra of* π_1 *of the projective line minus three points*, Contemporary Math. 186,201-213(1995).

[Mo] Mochizuki S.; *The profinite Grothendieck conjecture for closed hyperbolic curves over number fields*, J. Math. Sci. Univ. Tokyo 3,571-627(1996).

[Ra] Raynaud M.; *Sous-variètès d'une variètè abèlienne et points de torsion*, In Arithmetic and Geometry (volume dedicated to Shafarevich), M. Artin, J. Tate, eds., Birkhaüser, 327-352(1983).

[Ri] Ribet K.A.; *Congruence relations between modular forms*, Proceedings on the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 503-514, PWN, Warsaw, 1984.

[Ta-Wi] Taylor R., Wiles A.; *Ring-theoretic properties of certain Hecke algebras,* Ann. of Math. 142,553-572(1995).

[Vo] Voevodski V.A.; *Galois representations connected with hyperbolic curves*, Math. USSR Izvestiya 39,1281-1291 (1992)

[Wi] Wiles A.; *Modular elliptic curves and Fermat's last theorem,* Ann. of Math. 142,443-551(1995).

[Zh] Zhang S.; *Admissible pairing on a curve*, Invent. Math. **112** (1993), 171-193.