QM-curves and $\mathbb{Q}$-curves

Y. Hasegawa & K. Hashimoto & F. Momose

The Shimura-Taniyama conjecture has been almost solved [W][W-T] [Di]. This is the first report of our work on modular conjecture. Its a special case of the modular conjecture for the abelian variety of $GL(2)$-type(due to Serre[Se]). We give a partial answer to its conjecture for abelian variety of $GL(2)$-type with extra twistings [Sh][Mo1][Ri1]. The abelian variety $A$ over $\mathbb{Q}$ is a $\mathbb{Q}$-simple abelian variety whose ring of endomorphisms over $\mathbb{Q}$ is an order of an algebraic number field of degree equal to $\dim A$. By the congruence relation [Sh][De], we know that any $\mathbb{Q}$-simple factor of the jacobian variety $J_1(N)$ of modular curves $X_1(N)$ is of $GL(2)$-type. The modular conjecture for abelian variety $A$ over $\mathbb{Q}$ of $GL(2)$-type states that $A$ is isogenous over $\mathbb{Q}$ to a $\mathbb{Q}$-simple factor of $J_1(N)$ for the integer $N$ with $N^{\dim A} = \text{conductor of } A/\mathbb{Q}$. The $\mathbb{Q}$-curve $E$ is an elliptic curves over $\overline{\mathbb{Q}}$ which is isogenous to its conjugate $E^\sigma$ for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ [Gr]. The $\mathbb{Q}$-HBV is an abelian variety $A$ over $\overline{\mathbb{Q}}$ whose ring of full endomorphism is an order of totally real algebraic number fields of degree $= \dim A$ and its $F$-isogeny to its conjugate $A^\sigma$ for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ [Ri2]. The $\mathbb{Q}$-curves are special cases of $\mathbb{Q}$-HBV, we know that any $\mathbb{Q}$-HBV is a simple factor of an abelian variety of $GL(2)$-type [Py]. Now, let $A$ be an abelian variety over $\mathbb{Q}$ of $GL(2)$-type and $E$ the field of fractions of the ring of endomorphisms over $\mathbb{Q}$. Then $E$ is totally real or CM-field [Mu]. Let $F$ be the center of the $\mathbb{Q}$-algebra of the ring $M = (\text{End}_{\mathbb{Q}} A) \otimes \mathbb{Q}$ of full ring of endomorphisms of $A$. Then $F$ is totally real algebraic number field or an imaginary quadratic field. In the first case, $M$ is isomorphic to a matrix algebra $M_r(F)$ or $M_r(D)$ for totally indefinite quaternion algebra over $F$. In the latter case, $M$ is isomorphic to $M_r(F)$ and $A$ is isogenous over $\overline{\mathbb{Q}}$ to $r$-tupple of an elliptic curve with complex multiplication by $F$. We call the latter case CM-type. If $A$ is CM-type, then $A$ is modular [Sh]. So, we discuss non CM case. We may assume that the maximal order $\mathcal{O}_E$ of $E$ acts on $A$ over $\mathbb{Q}$ [Sh]. Let $\rho$ be a prime of $\mathcal{O}_E$, lying over a rational prime $p$, $V_p(A) = V_p(A) \otimes E_p$, and $\rho = \rho_p$ the Galois representation of $G = G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $V_p(A)$. Then $\det \rho_p = \varepsilon \cdot \theta_p$ for the cyclotomic character $\theta_p$ and a character $\varepsilon$ of
finite order. By a famous result of Faltings (Tate-Shavarevich conjecture),
A is modular if and only if \( \rho_{\wp} \) associates to a cusp form of \( \Gamma_{1}(N) \) of weight 2. The field \( E \) is generated by \( q_{l} = \text{Tr}_{E_{\wp}}(a_{l}) \) for primes \( l \nmid p \)-conductor of \( A/Q \) and Frobenius element \( a_{l} \) of \( l \), and \( F \) is generated by \( a_{l}^{2}e^{-1}(l) \) for primes \( l \nmid p \)-cond.of \( A/Q \) \([Mo1][Ri1]\). For a Dirichlet character \( \chi \), let \( A_{\chi} \)
be an abelian variety over \( Q \) obtained by the \( \chi \)-twisting \([Sh]\). Then \( A_{\chi} \) is
determined up to isogeny over \( Q \). We note that \( A \) is modular if and only if \( A_{\chi} \) is modular \([Sh]\).

Now, let \( \delta = \delta(E/F(\zeta_{r^{2}})) \) be the different of \( E \) over \( F(\zeta_{r}) \) for \( r = \text{order of } \epsilon \) and a primitive \( r \)-th character \( \zeta_{r} \). Our first result is as follows. We may assume that \( \mathcal{O}_{E} \) of integers of \( E \) acts on \( A \) over \( Q \). For a prime \( \wp \) of \( \mathcal{O}_{E} \),
let \( \rho = \rho_{\wp} \) be the \( \wp \)-adic representation on the \( \wp \)-divisible points on \( A \), and \( \bar{\rho} \) its reduction mod \( \wp \).

**Th 1** Assume that there exists a prime \( \wp \) of \( \mathcal{O}_{E} \) which divides \( \delta \), \( \wp \nmid p \neq 2 \),
and \( A \) has semistable reduction at \( p \). Then,
(1) There exists a quadratic field \( k \) such that \( \bar{\rho} \) is isomorphic to the induced representation \( \text{Ind}_{k}^{Q} \chi \) for a character \( \chi \) of \( G_{k} = \text{Gal}(\bar{k}/k) \).
(2) If \( p \geq 5 \) or \( p = 3 \) and \( k \) is imaginary or \( A \) has super singular reduction at \( p \), then \( A \) is modular.

For its proof, see \([Mo2]\). It has many corollaries. Let \( E \) be a non-CM \( Q \)-curve defined over an extension \( L \) of \( Q \) of \((2, \cdots, 2)\)-type, and \( A = \text{Re}_{L/Q}(E/L) \) is \( Q \)-simple . Define the degree \( N = N_{E} \) of \( E \) by the l.c.m of
the square free degrees of isogenies \( \varphi : E \to E^{\sigma} \) for \( \sigma \in \text{Gal}(L/Q) \). The
following is a partial result for the Ribet's conjecture for \( Q \)-curves \([Ri3]\). This
can be extend to \( Q \)-HBV.

**Th 2** If a prime \( p \geq 5 \) divides \( N \) and \( A \) has semistable reduction at \( p \), then \( A \) is modular.

The \( Q \)-curves of degree \( N \) corresponds to \( Q \)-rational points of the modular curves \( X_{0}^{*}(N) = X_{0}(N)/\langle \{W_{l}\} \rangle_{N} \) for Atkin involutions \( W_{l} \) \([El]\). We get many examples, if \( X_{0}^{*}(N) = \mathbb{P}^{1} \). cf \([Py]\).

For other examples, we explain the QM-curves. The QM-curve is a curve \( C \) over \( Q \) of genus 2 such that the ring of full endomorphisms of its jacobian variety \( J(C) \) is an order of indefinite quaternion algebra \( D \) and \( \text{End}_{Q}J(C) \neq \mathbb{Z} \). Hashimoto-Murabayashi calculated many examples \([H-M]\).
Th 3 If a prime \( p \neq 2 \) ramifies in \( D \), and \( C \) has good reduction at \( p \), then \( J(C) \) is modular.

The above results can be extend to more general cases. Using Pyle's [Py] results, we have many examples of modular QM-curves over number fields [H-M]. Further, the condition on reduction at \( p \) can be improved in some cases. Especially, if the abelian variety \( A \) of \( GL(2) \)-type has potentially ordinary reduction at \( p \), the we have a criterion for modular conjecture.

References


[Py] Pyle, E.E., Abelian varieties over \( \mathbb{Q} \) with large endomorphism algebras and their simple components over \( \overline{\mathbb{Q}} \), Thesis, Univ. of California at Barkley.


[Ri3] Ribet, K.A., Abelian varieties over \( \mathbb{Q} \) and modular forms, Proceeding of KAIST Math. Workshop, pp.53-79.

