数理解析研究所講究録
942巻 1996年 164-167

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 avelian 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 $N^{\dim A}$ = conductor of $A/\mathbb{Q}$. The $\mathbb{Q}$-curve E is an elliptic curves over $\bar{\mathbb{Q}}$ which is isogenous to its conjugate E^σ for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ [Gr]. The $\mathbb{Q}$-HBV is an abelian variety A over $\bar{\mathbb{Q}}$ 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^σ for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ [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 variet 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 $M = (\mathrm{End}_{\bar{\mathbb{Q}}}A) \otimes \mathbb{Q}$ 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 $\bar{\mathbb{Q}}$ 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 $\wp$ be a prime of $\mathcal{O}_E$, lying over a rational prime p, $V_\wp(A) = V_p(A) \otimes E_\wp$, and $\rho = \rho_\wp$ the Galois representation of $G = G_\mathbb{Q} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $V_\wp(A)$. Then $\det \rho_\wp = \varepsilon \cdot \theta_p$ for the cyclotomic character θ_p and a character ε 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 $a_l = \mathrm{Tr}\rho_{\wp}(\sigma_l)$ for primes $l \nmid p$-conductor of $A/\mathbb{Q}$ and Frobenius element σ_l of l, and F is generated by $a_l^2\varepsilon^{-1}(l)$ for primes $l \nmid p$-cond.of $A/\mathbb{Q}$ [Mo1][Ri1]. For a Dirichlet character χ, let A_χ be an abelian variety over $\mathbb{Q}$ obtained by the χ-twisting [Sh]. Then A_χ is determined up to isogeny over $\mathbb{Q}$. We note that A is modular if and only if A_χ is modular [Sh].

Now, let $\delta = \delta(E/F(\zeta_{r^2}))$ be the different of E over $F(\zeta_r)$ for $r =$ order of ε and a primitive r-th character ζ_r. Our first result is as follows. We may assume that $\mathcal{O}_E$ of integers of E acts on A over $\mathbb{Q}$. 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 $\wp$.

<u>Th 1</u> Assume that there exists a prime $\wp$ of $\mathcal{O}_E$ which divides δ, $\wp | p \neq 2$, 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 $\mathrm{Ind}_k^{\mathbb{Q}}\chi$ for a character χ of $G_k = \mathrm{Gal}(\bar{k}/k)$.
(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 $\mathbb{Q}$-curve defined over an extension L of $\mathbb{Q}$ of $(2, \cdots, 2)$-type, and $A = \mathrm{Re}_{L/\mathbb{Q}}(E/L)$ is $\mathbb{Q}$-simple . Define the degree $N = N_E$ of E by the l.c.m of the square free degrees of isogenies $\varphi : E \longrightarrow E^\sigma$ for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. The follwing is a partial result for the Ribet's conjecture for $\mathbb{Q}$-curves [Ri3]. This can be extend to $\mathbb{Q}$-HBV.

<u>Th 2</u> If a prime $p \geq 5$ divides N and A has semistable reduction at p, then A is modular.

The $\mathbb{Q}$-curves of degree N corresponds to $\mathbb{Q}$-rational points of the modular curves $X_0{}^*(N) = X_0(N)/ < \{W_l\} >_{l(N)}$ 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 $\mathbb{Q}$ 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 $\mathrm{End}_{\mathbb{Q}}J(C) \neq \mathbb{Z}$. Hashimoto-Murabayashi calculated many examples [H-M].

<u>Th 3</u> 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

[De] Deligne, P., Formes modulaires et représentation l- adiques, sém. Bourbaki, 1968/1969, exposé n° 355, Lecture note in Math., **179**, Springer-Verlag, pp.139-172.

[Di] Diamond, F., On deformation rings and Hecke rings, preprint.

[El] Elkies, N., Remarks on elliptic K-curves, preprint.

[Gr] Gross, B.H., Arithmetic on Elliptic Curves with Complex Multiplication, Lecture note in Math., **776**, Springer-Verlag.

[H-M] Hashimoto, K., Murabayashi, N., Shimura curves as intersections of Humbert surface and defining equations of QM-curves of genus two, Tohoku Math. J., **47**(1995), pp.271-296.

[Mo1] Momose, F., On the l-adic representation s attached to modular forms, J. Facult. of Sci. Univ. of Tokyo, **28**(1981) No.1, pp.89-109.

[Mo2] Momose, F., Galois action on some ideal section points of the abelian variety associated with a modular form and its application, Nagoya Math. J., **91**(1983), pp.19-36.

[Mu] Mumford, D., Abelian varieties, Oxford Univ. Press, 1970.

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

[Ri1] Ribet, K.A., Twists of modular forms and endomorphisms of abelian varieties, Math. Ann., 1980, pp.239-244.

[Ri2] Ribet, K.A., Fielsds of definition of abelian varieties with real multiplication, Conference on Arithmetic Geometly with an Emphasis on Iwasawa Theory , 1993, pp.107-118, Contemp. Math., **174**, AMS, 1994.

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

[Se] Serre, J.P., Sur les représentations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$), Duke Math. J., **54**(1987), pp.179-230.

[Sh] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, no. 11, Princeton Univ. Press, 1971.
[T-W] Taylor, R., Wiles, A., Ring theoretic properties of certain Hecke algebras, Ann. of Math., 141(1995), pp.553-572.
[W] Wiles, A., Modular elliptic curves and Fermat's last theorem, Ann. of Math., 141(1995), pp.443-551.