Math. Res. Lett. **14** (2007), *no.* 1, 113–128

SATO-TATE DISTRIBUTION FOR ABELIAN VARIETIES WITH REAL MULTIPLICATION OVER FUNCTION FIELDS

Chung Pang Mok

Abstract. We calculate the monodromy groups of some universal families of abelian varieties with real multiplication by $\mathbf{Q}(\cos\frac{2\pi}{r})$, over certain Hilbert type modular varieties over finite fields. Using Deligne's equidistribution theorem, we obtain the Sato-Tate law for the distribution of Frobenius eigenvalues of these universal families of abelian varieties.

1. Introduction

There is a technique of studying monodromy by using Diophantine considerations over finite fields, *c.f.* [6]. We apply this technique to the one parameter family of curves considered in [11], whose Jacobians have real multiplication by the totally real field $F := \mathbf{Q}(\cos\frac{2\pi}{r})$, with r a prime (see section 4). The condition that the family has real multiplication puts a constraint on the monodromy group. We show that the monodromy is as big as possible; essentially it's g product of SL_2, where $g = \frac{r-1}{2}$ is the degree of F over $\mathbf{Q}$.

Let k be a finite field of cardinality q, with characteristic $\neq 2, r$. Let $\mathcal{M}_{g,3\mathcal{L}} \otimes_{\mathbf{Z}} k$ be the moduli of abelian varieties of dimension g with real multiplication by F, together with a "level $3\mathcal{L}$ structure", base changed to k (a variant of what considered in [8], *c.f.* section 6 below). There is a universal family $\mathcal{A} \otimes_{\mathbf{Z}} k \to \mathcal{M}_{g,3\mathcal{L}} \otimes_{\mathbf{Z}} k$. Once we have shown that there exist some family with geometric monodromy given by g product of SL_2, it then follows that the same is true for the universal family.

Deligne's general equidistribution theorem [3] gives a Sato-Tate distribution law for the eigenvalues of Frobenius on cohomology of a family of varieties, once the geometric monodromy group is known. In our case, we obtained in theorem 7.1 below the Sato-Tate law for the Frobenius eigenvalues of the universal family $\mathcal{A} \otimes_{\mathbf{Z}} k \to \mathcal{M}_{g,3\mathcal{L}} \otimes_{\mathbf{Z}} k$.

The main theorem can be formulated as follows: let k_n/k be a sequence of finite extensions of k inside an algebraic closure $\overline{k}$ of k, with $\#k_n \to \infty$ as $n \to \infty$. We can define a map (see section 7 below)

$$\theta : \mathcal{M}_{g,3\mathcal{L}}(k_n) \longrightarrow \prod_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} [0,\pi]$$

as follows: for each $t \in \mathcal{M}_{g,3\mathcal{L}}(k_n)$, which corresponds to an abelian variety with real multiplication by F and level $3\mathcal{L}$ structure over k_n, we associate the g-tuple of Frobenius angles of the abelian variety, indexed by the set of embeddings of F into

Received by the editors March 21, 2006.
Key words and phrases. étale cohomology, monodromy, Sato-Tate distribution.

$\overline{\mathbf{Q}}$. On the product $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}}[0,\pi]$ with coordinates $(\theta_\tau)_{\tau:F\to\overline{\mathbf{Q}}}$, we have the product Sato-Tate measure:

$$\mu_{ST} = \bigwedge_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \frac{2}{\pi}\sin^2(\theta_\tau)d\theta_\tau.$$

We prove in section 7 the following:

Theorem 1.1. *Let $\delta_{\theta(t)}$ be the delta measure on $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}}[0,\pi]$ associated to $\theta(t)$, then the sequence of measures on $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}}[0,\pi]$ given by*

$$\frac{1}{\#\mathcal{M}_{g,3\mathcal{L}}(k_n)}\sum_{t\in\mathcal{M}_{g,3\mathcal{L}}(k_n)}\delta_{\theta(t)} \tag{1}$$

converges weakly (as $\#k_n\to\infty$) to the product Sato-Tate measure μ_{ST}.

2. Generalities on monodromy

We review some of the formalism of monodromy. With k a finite field as in the introduction, let S be a scheme of finite type over k; in addition, we assume that S is geometrically connected, i.e. $S_{\overline{k}} := S\otimes\overline{k}$ is connected. We begin by considering principally polarised abelian schemes over S:

$$p:\mathcal{A}\longrightarrow S,\ \varphi:\mathcal{A}\longrightarrow\mathcal{A}^t\,\text{principal polarisation over } S$$

(here $\mathcal{A}^t$ is the dual abelian scheme of $\mathcal{A}$).

Consider the l-adic sheaf $\mathcal{E} = R^1p_*\overline{\mathbf{Q}}_l$ on S; the proper and smooth base change theorems imply that $\mathcal{E}$ is a lisse l-adic sheaf on S. By the Weil conjecture for abelian varieties and the proper base change theorem again, $\mathcal{E}$ is pure of weight one.

Since S is connected, $\mathcal{E}$ is given by a representation of the étale fundamental group of S. We recall some notations for fundamental groups: let s be a point of S, choose a geometric point $\overline{s}$ over s. The arithmetic fundamental group of $(S,\overline{s})$, $\pi_1^{\mathrm{arith}}(S,\overline{s})$, is just the usual étale fundamental group $\pi_1^{\text{ét}}(S,\overline{s})$. In addition, since S is geometrically connected, there is a (closed) normal subgoup, called the geometric fundamental group, $\pi_1^{\mathrm{geom}}(S,\overline{s})$, which is the étale fundamental group $\pi_1^{\text{ét}}(S\otimes\overline{k},\overline{s})$ ("arithmetic" in the former case because it contains various Frobenius conjugacy classes). We will omit the basepoint $\overline{s}$ if the context is clear.

We have the following homotopy short exact sequence:

$$1\longrightarrow\pi_1^{\mathrm{geom}}(S,\overline{s})\longrightarrow\pi_1^{\mathrm{arith}}(S,\overline{s})\xrightarrow{\deg}\mathrm{Gal}(\overline{k}/k)\longrightarrow 1.$$

Returning to our lisse l-adic sheaf $\mathcal{E}$, let $E_l = \mathcal{E}_{\overline{s}}$ be its geometric stalk over $\overline{s}$; then $\mathcal{E}$ corresponds to a representation

$$\rho_l:\pi_1^{\mathrm{arith}}(S,\overline{s})\longrightarrow\mathrm{GL}_{E_l}(\overline{\mathbf{Q}}_l). \tag{2}$$

By abuse of notation, we denote again by ρ_l the representation restricted to $\pi_1^{\mathrm{geom}}(S,\overline{s})$:

$$\rho_l:\pi_1^{\mathrm{geom}}(S,\overline{s})\longrightarrow\pi_1^{\mathrm{arith}}(S,\overline{s})\longrightarrow\mathrm{GL}_{E_l}(\overline{\mathbf{Q}}_l). \tag{3}$$

We will call the Zariski closure of the images of these two representations, the arithmetic and geometric monodromy groups, denoted as G^{arith}, G^{geom}, respectively.

A $\mathbf{Q}_l$-rational form of $\mathcal{E}$ is given by Tate module as follows. Let $\mathcal{V}_l = \mathcal{V}_l\mathcal{A}$ be the $\mathbf{Q}_l$-rational l-adic Tate module of the abelian scheme $\mathcal{A}/S$ given by:

$$\mathcal{V}_l\mathcal{A} := \varprojlim \mathcal{A}[l^n] \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$$

which is a $\mathbf{Q}_l$ rational l-adic sheaf on S. Let $V_l := \mathcal{V}_{l,\overline{s}}$ be the geometric stalk above $\overline{s}$, which is just the usual Tate module $V_l\mathcal{A}_s$ of $\mathcal{A}_s$, the fibre of $\mathcal{A}$ over s. We have representations:

$$r_l : \pi_1^{\text{arith}}(S, \overline{s}) \longrightarrow \mathrm{GL}_{V_l}(\mathbf{Q}_l), \tag{4}$$

and its dual:

$$r_l^* : \pi_1^{\text{arith}}(S, \overline{s}) \longrightarrow \mathrm{GL}_{V_l^*}(\mathbf{Q}_l). \tag{5}$$

The theory of l-adic cohomology of abelian varieties gives:

$$E_l \cong V_l^* \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l \,.$$

Under this isomorphism, $\rho_l \cong (r_l^*)_{\overline{\mathbf{Q}}_l}$, i.e. ρ_l is obtained from r_l^* by extension of scalars from $\mathbf{Q}_l$ to $\overline{\mathbf{Q}}_l$.

Finally, the polarisation φ induces the Weil pairing $\langle , \rangle : \mathcal{V}_l \times \mathcal{V}_l \to \mathbf{Q}_l(1)_S$, which is perfect alternating.

3. Family of abelian varieties with real multiplication

We keep the notations of the previous sections. Thus for $r \geq 3$ a fixed prime, let F be the totally real field $\mathbf{Q}(\cos \frac{2\pi}{r})$ of degree $g := \frac{r-1}{2}$ over $\mathbf{Q}$, $\mathcal{O}_F$ be its ring of integers. For a prime l, let $F_l := F \otimes_{\mathbf{Q}} \mathbf{Q}_l$.

In this section we consider, in addition, that the principally polarised abelian scheme p: $\mathcal{A} \longrightarrow S$ has real multiplication by $\mathcal{O}_F$. We'll be more precise about this later, *c.f.* section 6 below. For the moment, we give:

Definition 3.1. *The abelian scheme $p : \mathcal{A} \longrightarrow S$ with principal polarisation φ, has real multiplication by $\mathcal{O}_F$ in a weak sense, if there is an embedding*

$$i : \mathcal{O}_F \longrightarrow \mathrm{End}_S(\mathcal{A})$$

such that, if we let † be the Rosati involution defined by the principal polarisation φ, then † fixes the image of i. An equivalent way of saying this last condition is that the polarisation be linear over i, i.e. for any $b \in \mathcal{O}_F$, we have:

$$\varphi \circ i(b) = i(b)^t \circ \varphi,$$

here $i(b)^t$ is the endomorphism of $\mathcal{A}^t$ induced by $i(b)$.

Let i_l: $F_l \longrightarrow \mathrm{End}_S(\mathcal{A}) \otimes \mathbf{Q}_l$ be the map induced by i. By abuse of notation, we'll use the same notation i_l for its action on V_l. As in the above definition let † be the Rosati involution defined by the (principal) polarisation φ. Then for $x, y \in V_l$, $b \in F_l$,

$$\langle i_l(b)x, y\rangle = \langle x, i_l(b)^\dagger y\rangle. \tag{6}$$

By assumption, the action of the Rosati involution fixes the image of i, so we have

$$\langle i_l(b)x, y\rangle = \langle x, i_l(b)y\rangle. \tag{7}$$

Lemma 3.2 ([1], lemma 5.2). *$V_l = V_l\mathcal{A}_s$ is a free module of rank 2 over the ring $F_l = F \otimes_{\mathbf{Q}} \mathbf{Q}_l$.*

Proof. In order to apply lemma 5.2 of [1], we need to check the conditions (5.1) (a) – (d) on p.230 of [1] are satisfied. This follows from our setup; condition (5.1) (c) being our equation (3.2). □

Now an element in the image of r_l is an S-endomorphism of the abelian scheme $\mathcal{A}$, so the action of the arithmetic fundamental group is linear over the action of the image of i .Therefore, the representation r_l factors:

$$r_l : \pi_1^{\text{arith}}(S) \longrightarrow \operatorname{Res}_{F_l/\mathbf{Q}_l} \mathrm{GL}_{V_l/F_l}(\mathbf{Q}_l) \hookrightarrow \mathrm{GL}_{V_l}(\mathbf{Q}_l). \tag{8}$$

Here GL_{V_l/F_l} is the F_l-group scheme of F_l-linear transformations of the rank 2 F_l-module V_l, and $\operatorname{Res}_{F_l/\mathbf{Q}_l}$ is the Weil restriction of scalars. We'll generally regard $\operatorname{Res}_{F_l/\mathbf{Q}_l} \mathrm{GL}_{V_l/F_l}$ as an algebraic subgroup of GL_{V_l}.

Lemma 3.3 ([1], lemma 5.3). *Let $\chi_l : \mathrm{Gal}(\overline{k}/k) \longrightarrow \mathbf{Q}_l^* \subset F_l^*$ be the l-adic cyclotomic character, considered as a F_l-representation of $\mathrm{Gal}(\overline{k}/k)$ of rank 1. Let r_l be the representation as in (2.3) on the $\mathbf{Q}_l$ rational l-adic Tate module V_l, considered as representation over the ring F_l .Then*

$$\det_{F_l}(r_l) = \chi_l \circ \deg \tag{9}$$

as F_l-representation of $\pi_1^{\text{arith}}(S)$ of rank 1 (here the determinant is taken with respect to the ring F_l). □

A particular consequence of this lemma is that the image of the geometric fundamental group, being the kernel of the map deg, factors as

$$r_l : \pi_1^{\text{geom}}(S) \longrightarrow \operatorname{Res}_{F_l/\mathbf{Q}_l} \mathrm{SL}_{V_l/F_l}(\mathbf{Q}_l) \subset \mathrm{GL}_{V_l}(\mathbf{Q}_l). \tag{10}$$

Now since $\rho_l \cong (r_l^*)_{\overline{\mathbf{Q}}_l}$ we see that the monodromy representation for $\mathcal{E}$

$$\rho_l : \pi_1^{\text{arith}}(S, \overline{s}) \longrightarrow \mathrm{GL}_{E_l}(\overline{\mathbf{Q}}_l), \tag{11}$$

actually lands in

$$\rho_l : \pi_1^{\text{arith}}(S) \longrightarrow \operatorname{Res}_{F_l/\mathbf{Q}_l} \mathrm{GL}_{V_l^*/F_l}(\overline{\mathbf{Q}}_l), \tag{12}$$

and similarly

$$\rho_l : \pi_1^{\text{geom}}(S) \longrightarrow \operatorname{Res}_{F_l/\mathbf{Q}_l} \mathrm{SL}_{V_l^*/F_l}(\overline{\mathbf{Q}}_l). \tag{13}$$

Next we note that E_l, as a representation of $\pi_1^{\text{arith}}(S)$, has a decomposition :

$$(\rho_l, E_l) \cong \bigoplus_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} (\rho_{l,\tau}, E_{l,\tau}). \tag{14}$$

Indeed, by virtue of the decomposition:

$$F_l \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l \cong F \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_l \cong \prod_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} \overline{\mathbf{Q}}_l, \tag{15}$$

we have

$$E_l \cong V_l^* \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l \cong V_l^* \otimes_{F_l} F_l \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l \cong \bigoplus_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} (V_l^* \otimes_{F_l} \overline{\mathbf{Q}}_l),$$

so define $E_{l,\tau}$ to be $V_l^* \otimes_{F_l} \overline{\mathbf{Q}}_l$ (with the map $F_l \to \overline{\mathbf{Q}}_l$ induced by $\tau : F \to \overline{\mathbf{Q}}$), which is a $\overline{\mathbf{Q}}_l$ vector space of dimension 2. The $(\rho_{l,\tau}, E_{l,\tau})$ are just the projections:

$$\rho_{l,\tau} : \pi_1^{\mathrm{arith}}(U) \longrightarrow \mathrm{Res}_{F_l/\mathbf{Q}_l} \mathrm{GL}_{V_l^*/F_l}(\overline{\mathbf{Q}}_l) \cong \prod_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} \mathrm{GL}_2(\overline{\mathbf{Q}}_l) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{Q}}_l) \tag{16}$$

whose restriction to $\pi_1^{\mathrm{geom}}(U)$ is:

$$\rho_{l,\tau} : \pi_1^{\mathrm{geom}}(U) \longrightarrow \mathrm{Res}_{F_l/\mathbf{Q}_l} \mathrm{SL}_{V_l^*/F_l}(\overline{\mathbf{Q}}_l) \cong \prod_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} \mathrm{SL}_2(\overline{\mathbf{Q}}_l) \longrightarrow \mathrm{SL}_2(\overline{\mathbf{Q}}_l). \tag{17}$$

(The last maps in (3.11) and (3.12) are the projection maps to the factor corresponding to τ). And we have the corresponding decomposition on the level of sheaves:

$$\mathcal{E} \cong \bigoplus_{\tau : F \to \overline{\mathbf{Q}}} \mathcal{E}_\tau$$

with $\mathcal{E}_\tau$ lisse of rank 2.

4. A specific one parameter family

As before, r is a fixed prime ≥ 3. We assume in addition that k is a finite field of characteristic $\neq 2,r$, with cardinality q. Fix an algebraic closure $\overline{k}$ of k.

By abuse of notation ζ_r will denote either a primitive r-th root of unity in $\overline{\mathbf{Q}}$ or in $\overline{k}$.

Let $g(x)$ be the minimal polynomial over $\mathbf{Q}$ of $-(\zeta_r + \zeta_r^{-1}) = -2\cos(\frac{2\pi}{r})$. Let $f(x)$ be the polynomial $xg(x^2-2)$, so $\deg(f) = r$ (recall that r is an odd prime).

We want to consider the one parameter family of hyperelliptic curves $y^2 = f(x) + t$. More precisely, in the affine 3-space $\mathbf{A}^3_{k(\zeta_r)}$ over $k(\zeta_r)$, with coordinates $[x, y, t]$, consider the affine hypersurface $\mathcal{C}^{\mathrm{aff}}$ defined by the equation:

$$y^2 = f(x) + t. \tag{18}$$

By taking projective closure in $\mathbf{P}^2_{k(\zeta_r)} \times \mathbf{P}^1_{k(\zeta_r)}$, $\mathcal{C}^{\mathrm{aff}}$ extends to a proper curve over $\mathbf{P}^1_{k(\zeta_r)}$, i.e. a proper morphism over $\mathbf{P}^1_{k(\zeta_r)}$ with geometrically connected fibres p: $\mathcal{C} \longrightarrow \mathbf{P}^1_{k(\zeta_r)}$ (t being affine coordinate on $\mathbf{P}^1_{k(\zeta_r)}$). By explicit calculation, we have

Theorem 4.1 ([2], Prop. 2.2)**.** *p: $\mathcal{C} \longrightarrow \mathbf{P}^1_{k(\zeta_r)}$ is smooth outside 2,-2,∞, whose non-singular fibers are hyperelliptic curves with genus $g = \frac{r-1}{2}$. It has semi-stable reduction at $t =$ 2,-2, each is irreducible with $g = \frac{r-1}{2}$ $k(\zeta_r)$-rational ordinary double point.*

Proof. This is implicit in [11] and [2], Prop 2.2. We give the details here. We have the relation in $k[x, x^{-1}]$:

$$x^{2r} + 1 = x^r(x + x^{-1})g(x^2 + x^{-2}). \tag{19}$$

which can be checked by noting that both sides define monic polynomials of the same degree with the same set of zeroes. Elementary manipulation of (4.2) gives the identities:

$$f(x) = xg(x^2 - 2) = g(-x)^2(x - 2) + 2 = g(x)^2(x + 2) - 2. \tag{20}$$

In particular, $f(\pm 2) = \pm 2$. From (4.3), we see that $g(x)|f'(x), g(-x)|f'(x)$. Simple root consideration shows that $g(x)$ and $g(-x)$ are relatively prime, and we get:

$$f'(x) = \pm rg(x)g(-x). \tag{21}$$

It follows immediately from (4.3) and (4.4) that p is smooth outside $t = 2, -2$. On the other hand, the polynomial $f(x)$ satisfies the following identity:

$$f(x) - f(z) = \pm(x - z) \prod_{i=1}^{\frac{r-1}{2}} (x^2 - \theta_i xz + z^2 - 4 + \theta_i^2),\ \theta_i = \zeta_r^i + \zeta_r^{-i} \tag{22}$$

(see [11], lemma 7, and the paragraph that follows). Hence by putting $z = \pm 2$ in (4.5), we have:

$$f(x) - 2 = \pm(x - 2) \prod_{i=1}^{\frac{r-1}{2}} (x - \theta_i)^2$$

(with a similar expression for $f(x) + 2$). The statement concerning the singular fibres of p follows immediately. $\square$

Henceforth, set $U := \mathbf{P}^1_{k(\zeta_r)} \setminus \{2, -2, \infty\}_{k(\zeta_r)}$ (as a scheme over $k(\zeta_r)$), $\mathcal{C}|_U := p^{-1}(U)$. The Jacobian of $p : \mathcal{C}|_U \longrightarrow U$ furnishes a abelian scheme over U with canonical principal polarisation (given by the theta divisor).

Theorem 4.2 ([2], Prop. 2.1, [11],Theorem 1)**.** *The abelian scheme* $\mathrm{Jac}(\mathcal{C}|_U) \longrightarrow U$*, with the canonical principal polarisation, has real multiplication by* $\mathcal{O}_F$ *in the weak sense.*

Proof. This is the main theorem of [11], except for the assertion that Rosati acts trivially on the image of $\mathcal{O}_F$, which is not explicitly mentioned in the references. This can be seen as follows. We need to check that the canonical principal polarisation of the Jacobian family is linear over the image of i. We notice that the family of curves (and their Jacobians) actually comes from a family over the integral scheme $\mathbf{P}^1_{\mathbf{Z}[\frac{1}{2r}, \zeta_r]} \setminus \{2, -2, \infty\}_{\mathbf{Z}[\frac{1}{2r}, \zeta_r]}$. So we'll be done if we prove the assertion over this scheme. By the rigidity lemma for abelian schemes ([10], Prop. 6.1), it suffices to prove this over the generic point of the scheme, i.e. $\mathrm{Spec}\, \mathbf{Q}(\zeta_r)(t)$. However, the endomorphism ring of the Jacobian over the generic point is exactly the image of $\mathcal{O}_F$ by i ([2], Prop. 2.1), in particular, the Rosati involution induces a field automorphism of F, and the assertion follows in a well-known way from the positivity of Rosati involution and the fact that F is totally real. Alternatively, in our case where $F = \mathbf{Q}(\cos(\frac{2\pi}{r}))$, it can be seen as follows: the Rosati $\dagger$ induce an element σ on $\mathrm{Gal}(F/\mathbf{Q}) \cong (\mathbf{Z}/r\mathbf{Z})^*/\pm 1$, say σ corresponds to $a \bmod r$ under the isomorphism. Since Rosati is an involution, we have $\sigma^2 = id$, i.e. $a^2 \equiv \pm 1 \bmod r$. Suppose that $a^2 \equiv -1 \bmod r$; in particular, $a \not\equiv \pm 1 \bmod r$. Now the positivity of the Rosati involution implies, for any $b \in F^*$:

$$\operatorname{tr}_{\mathbf{Q}(\zeta_r)/\mathbf{Q}}(bb^\sigma) = 2\operatorname{tr}_{F/\mathbf{Q}}(bb^\sigma) > 0.$$

However, taking $b = \zeta_r + \zeta_r^{-1}$, we calculate that:

$$\operatorname{tr}_{\mathbf{Q}(\zeta_r)/\mathbf{Q}}(bb^\sigma) = \operatorname{tr}_{\mathbf{Q}(\zeta_r)/\mathbf{Q}}(\zeta_r^{a+1} + \zeta_r^{a-1} + \zeta_r^{1-a} + \zeta_r^{-1-a}) = -4 < 0.$$

Thus we must have $a \equiv \pm 1 \bmod r$, i.e. $\sigma = \mathrm{Id}$. □

As before, consider the lisse l-adic sheaf on U, given by $\mathcal{E} = R^1 p_* \overline{\mathbf{Q}}_l|_{p^{-1}(U)}$. Let us take s to be the generic point η of U, with $\overline{\eta}$ a geometric point over η. Then $\mathcal{E}$ is given by a representation

$$\rho_l : \pi_1^{\mathrm{arith}}(U, \overline{\eta}) \longrightarrow \mathrm{GL}_{E_l}(\overline{\mathbf{Q}}_l). \tag{23}$$

Here $E_l = \mathcal{E}_{\overline{\eta}}$ is the geometric stalk of the lisse sheaf $\mathcal{E}$ over $\overline{\eta}$.

As we saw in section 3, the fact that the family has real multiplication (in a weak sense) implies that the monodromy representation for $\mathcal{E}$, actually lands in (we omit the reference to the base points):

$$\rho_l : \pi_1^{\mathrm{arith}}(U) \longrightarrow \mathrm{Res}_{F_l/\mathbf{Q}_l} \mathrm{GL}_{V_l^*/F_l}(\overline{\mathbf{Q}}_l) \tag{24}$$

and similarly

$$\rho_l : \pi_1^{\mathrm{geom}}(U) \longrightarrow \mathrm{Res}_{F_l/\mathbf{Q}_l} \mathrm{SL}_{V_l^*/F_l}(\overline{\mathbf{Q}}_l)$$

and that E_l, as a representation of $\pi_1^{\mathrm{arith}}(U)$, breaks up into :

$$(\rho_l, E_l) \cong \bigoplus_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} (\rho_{l,\tau}, E_{l,\tau}) \tag{25}$$

with the corresponding decomposition:

$$\mathcal{E} \cong \bigoplus_{\tau : F \to \overline{\mathbf{Q}}} \mathcal{E}_\tau. \tag{26}$$

Lemma 4.3. *in the above decomposition, the $E_{l,\tau}$ are geometrically irreducible, i.e. each is irreducible as $\overline{\mathbf{Q}}_l[\pi_1^{\mathrm{geom}}(U)]$ module. Furthermore, they are pairwise geometrically non-isomorphic.*

Proof. We'll prove this lemma in the next section. □

Now we need another:

Lemma 4.4. *The lisse sheaf $\mathcal{E}|_{U_{\overline{k}}}$ over $U_{\overline{k}}$ is tamely ramified at all the points of $\mathbf{P}^1_{\overline{k}} \setminus U_{\overline{k}}$.*

Proof. This can be proved in the same way as [8] lemma 10.1.12, by explicit computation, using the Euler-Poincaré formula and the explicit description of the singular fibers in theorem 4.1. □

Now we can prove:

Theorem 4.5. $G^{\mathrm{geom}} \cong (\mathrm{Res}_{F_l/\mathbf{Q}_l} \mathrm{SL}_{V_l^*/F_l}) \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l \cong \prod_{\tau : F \hookrightarrow \overline{\mathbf{Q}}} \mathrm{SL}_{2,\overline{\mathbf{Q}}_l}$ *(g copies).*

Proof. $\mathcal{E}|_{U_{\overline{k}}}$ is everywhere tame, so $\mathcal{E}|_{U_{\overline{k}}}$ is a representation of the tame quotient $\pi_1^{\mathrm{tame}}(U_{\overline{k}})$. As $\mathbf{P}^1_{\overline{k}}$ is simply connected, $\pi_1^{\mathrm{tame}}(U_{\overline{k}})$ is topologically generated by the local tame fundamental group $I(t)$, $t = 2, -2, \infty$, where each of them is pro-cyclic. Let T_2, T_{-2}, T_∞ be topological generators of the respective local tame fundamental groups.

Since our family (considered as curves or Jacobians) has semi-stable reduction at $t = 2, -2$, Grothendieck's semi-stable reduction theorem implies that the local monodromies T_2, T_{-2} are unipotent (SGA 7 [12] Expose. IX, Prop. 3.5).

Consider the projections $\rho_{l,\tau}$:

$$\rho_{l,\tau} : \pi_1^{\mathrm{geom}}(U) \longrightarrow \mathrm{Res}_{F_l/\mathbf{Q}_l}(\mathrm{SL}_{V_l^*/F_l})(\overline{\mathbf{Q}}_l) \cong \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SL}_2(\overline{\mathbf{Q}}_l) \longrightarrow \mathrm{SL}_2(\overline{\mathbf{Q}}_l).$$

Now if $\rho_{l,\tau}(T_2) = \rho_{l,\tau}(T_{-2}) = \mathrm{Id}$, then the image of $\rho_{l,\tau}$ is topologically generated by $\rho_{l,\tau}(T_\infty)$, in particular the image is abelian. This contradicts lemma 4.3, that $E_{l,\tau}$ is a 2 dimensional irreducible representation of $\pi_1^{\mathrm{geom}}(U)$.

Thus for each τ, at least one of $\rho_{l,\tau}(T_2)$, $\rho_{l,\tau}(T_{-2})$ is a nontrivial unipotent element, and since $\rho_{\tau,l}$ is 2-dim representation, any non-trivial unipotent element must be a unipotent pseudo-reflection (i.e. the subspace of fixed vectors has codimension 1); also, E_τ is geometrically irreducible. Kazhdan-Magulis theorem ([7], Theorem 1.5) implies that the (geometric) monodromy group G_τ for the representation $\rho_{l,\tau}$, a piori an algebraic subgroup of $\mathrm{SL}_{2,\overline{\mathbf{Q}}_l}$, must be the whole of $\mathrm{SL}_{2,\overline{\mathbf{Q}}_l}$. In particular G_τ is a connected semisimple algebraic group over $\overline{\mathbf{Q}}_l$.

Clearly we have $G^{\mathrm{geom}} \subset \prod G_\tau$, and G^{geom} surjects onto G_τ under the projection on the factor corresponding to τ.

From lemma 4.3, we see that the Goursat-Kolchin-Ribet lemma ([7], Prop. 1.8.2) applies, so that we have the following relation between the derived groups:

$$\begin{aligned}(G^{\mathrm{geom},0})^{\mathrm{der}} &\supset \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} (G_\tau^0)^{\mathrm{der}} \\ &= \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} G_\tau \text{ (because } G_i \text{ is connected semisimple).}\end{aligned}$$

Thus we have:

$$G^{\mathrm{geom}} = \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} G_\tau \cong \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SL}_{2,\overline{\mathbf{Q}}_l}.$$

□

5. Proof of lemma 4.3

Most of the arguments below are due to Katz [6]. It is included here only for the convenience of the reader.

In general, for a pure lisse l-adic sheaf $\mathcal{F}$ on U, Deligne's semisimplicity theorem ([3], Théorème 3.4.1 (iii)) implies that $\mathcal{F}$, as a $\pi_1^{\mathrm{geom}}(U)$ representation, is completely reducibe. We may write:

$$\mathcal{F}|_{U_{\overline{k}}} = \oplus n_i \mathcal{F}_i \tag{27}$$

where $\mathcal{F}_i$ are pairwise non-isomorphic irreducible l-adic lisse sheaves on $U_{\overline{k}}$.

Define a positive number, called the "geometric irreducibility of $\mathcal{F}$", $\mathrm{Irr}(\mathcal{F})$, as $\sum {n_i}^2$. It's easy to check that if $\mathcal{F}, \mathcal{G}$ are lisse pure l-adic sheaves on U, then $\mathrm{Irr}(\mathcal{F} \oplus \mathcal{G}) \geq \mathrm{Irr}(\mathcal{F}) + \mathrm{Irr}(\mathcal{G})$, with equality if and only if $\mathcal{F}|_{U_{\overline{k}}}$ and $\mathcal{G}|_{U_{\overline{k}}}$ have no isomorphic irreducible components in common. Now the $\mathcal{E}$ of the previous section is lisse and pure of weight one, and from (4.9), we see that $\mathrm{Irr}(\mathcal{E}) \geq \sum_{\tau: F \to \overline{\mathbf{Q}}} \mathrm{Irr}(\mathcal{E}_\tau) \geq g$, so if we can show $\mathrm{Irr}(\mathcal{E}) \leq g$, then we must have equality everywhere, in particular $\mathrm{Irr}(\mathcal{E}_\tau) = 1$, *i.e.*, $\mathcal{E}_\tau$ is geometrically irreducible, and that the $\mathcal{E}_\tau$ are pairwise geometrically non-isomorphic.

Lemma 5.1. $\mathrm{Irr}\,\mathcal{E} = \dim_{\overline{\mathbf{Q}}_l} H^2_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E})$.

Proof. We have $\mathcal{E} \cong \mathcal{E}^*(-1)$ by Poincaré duality for the curve $p : \mathcal{C}|_U \to U$. Hence

$$\begin{aligned} \dim_{\overline{\mathbf{Q}}_l} H^2_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}) &= \dim_{\overline{\mathbf{Q}}_l} H^2_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}^*) \\ &= \dim_{\overline{\mathbf{Q}}_l} H^0_{\text{ét}}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}^*) \text{ (Poincaré duality on } U_{\overline{k}}) \\ &= \dim_{\overline{\mathbf{Q}}_l} H^0_{\text{ét}}(U_{\overline{k}}, \mathrm{End}(\mathcal{E})) \\ &= \dim_{\overline{\mathbf{Q}}_l} \mathrm{End}(E_l)^{\pi_1^{\mathrm{geom}}(U)} \\ &= \sum {n_i}^2 \text{ (Schur's lemma).} \end{aligned}$$

□

Now for d divisible by $r-1$, let k_d be the extension of k of degree d inside $\overline{k}$ that contains $k(\zeta_r)$, t be a k_d-valued point of U, $\mathcal{C}_t$ be the fibre of p: $\mathcal{C}|_U \longrightarrow U$ over t. Let $N(d,t)$ be the number $\#\mathcal{C}_t(k_d)$. Define $E(d,t)$ to be the "error term" $N(d,t) - (q^d + 1)$.

Lemma 5.2.

$$\limsup_{\substack{d \to \infty \\ r-1|d}} \frac{1}{q^{2d}} \sum_{t \in U(k_d)} E(d,t)^2 = \dim_{\overline{\mathbf{Q}}_l} H^2_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}).$$

Proof. Let F be the geometric Frobenius of the ground field k, and Frob_{t,k_d} be the geometric Frobenius associated to a k_d-valued point t, with geometric point $\overline{t}$ above t. By Lefschetz's trace formula for the fibres $\mathcal{C}_t$ and proper base change, we have

$$N(d,t) = q^d + 1 - \mathrm{trace}(F^d | H^1_{\text{ét},c}(C_{\overline{t}}, \overline{\mathbf{Q}}_l)) = q^d + 1 - \mathrm{trace}(\mathrm{Frob}_{t,k_d} | \mathcal{E}_t).$$

Hence $E(d,t) = -\mathrm{trace}(\mathrm{Frob}_{t,k_d} | \mathcal{E}_t)$, and $E(d,t)^2 = \mathrm{trace}(\mathrm{Frob}_{t,k_d} | (\mathcal{E} \otimes \mathcal{E})_t)$. Using Grothendieck's trace formula, we get

$$\sum_{t \in U(k_d)} \mathrm{trace}(\mathrm{Frob}_{t,k_d} | (\mathcal{E} \otimes \mathcal{E})_t) = \sum_{i=0}^{2} (-1)^i \,\mathrm{trace}(F^d | H^i_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}).$$

Now $\mathcal{E}$ is pure of weight 1, hence $\mathcal{E} \otimes \mathcal{E}$ is pure of weight 2. By Deligne's main theorem of Weil II ([3], Théorème 3.3.1),

$$H^0_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}) \text{ is mixed (actually pure) of weight} \leq 2,$$

$$H^1_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E}) \text{ is mixed of weight} \leq 3.$$

Hence

$$\mathrm{trace}(F^d | H^0_{\text{ét},c}(U_{\overline{k}}, \mathcal{E} \otimes \mathcal{E})) = O(q^d),$$

$$\mathrm{trace}(F^d|H^1_{\text{ét},c}(U_{\overline{k}},\mathcal{E}\otimes\mathcal{E}))=O(q^{\frac{3d}{2}}),$$

so we get:

$$\begin{aligned}\limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\sum_{t\in U(k_d)}E(d,t)^2 &= \limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\sum_{t\in U(k_d)}\mathrm{trace}(\mathrm{Frob}_{t,k_d}|(\mathcal{E}\otimes\mathcal{E})_t)\\ &= \limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\mathrm{trace}(F^d|H^2_{\text{ét},c}(U_{\overline{k}},\mathcal{E}\otimes\mathcal{E})).\end{aligned}$$

Now $H^2_{\text{ét},c}(U_{\overline{k}},\mathcal{E}\otimes\mathcal{E})\cong(\mathcal{E}\otimes\mathcal{E})_{\pi_1^{\mathrm{geom}(U)}}(-1)$ is pure of weight 4, so if $\alpha_1\cdots\alpha_m$ are the eigenvalues (with multiplicity) of F on $H^2_{\text{ét},c}(U_{\overline{k}},\mathcal{E}\otimes\mathcal{E})$ (which are algebraic numbers), then $|\alpha_i|=q^2$, and

$$\limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\mathrm{trace}(F^d|H^2_{\text{ét},c}(U_{\overline{k}},\mathcal{E}\otimes\mathcal{E}))=\limsup_{\substack{d\to\infty\\ r-1|d}}|(\frac{\alpha_1}{q^2})^d+\cdots+(\frac{\alpha_m}{q^2})^d|.$$

So it remains to show, that if $\beta_1\cdots\beta_m$ are unitary complex numbers, then

$$\limsup_{\substack{d\to\infty\\ r-1|d}}|\beta_1^d+\cdots+\beta_m^d|=m.$$

This is a standard argument using the pigeon-hole principle, *c.f.* Lang's Abelian Varieties [9], p.138. □

Hence we get

Lemma 5.3.

$$\mathrm{Irr}(\mathcal{E})=\limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\sum_{t\in U(k_d)}E(d,t)^2.$$

□

For our purpose, we'll use the following variant instead, which enables us to calculate with only affine varieties.

For our family p: $\mathcal{C}|_U\to U$, there is a closed subscheme $Y\subset\mathcal{C}|_U$, namely the ∞ section of the family of hyperelliptic curves, which is finite étale over U. In our previous notation $\mathcal{C}|_U\setminus Y$ is just $\mathcal{C}^{\mathrm{aff}}|_U$, where we recall $\mathcal{C}^{\mathrm{aff}}$ is defined by (notations as in section 4):

$$\{y^2=f(x)+t\}\subset\mathbf{A}^3_{k(\zeta_r)}.$$

Let $pr_3:\mathcal{C}^{\mathrm{aff}}\to\mathbf{A}^1_{k(\zeta_r)}$ be the projection to the t-coordinate. There are 2 singular fibres above $t=2,-2$.

For each k_d-valued point t of $\mathbf{A}^1_{k(\zeta_r)}$, let

$$E^{\mathrm{aff}}(d,t)=\#\{(x,y)\in k_d^2|y^2=f(x)+t\}-q^d$$

be the "affine error term" for the number of k_d-valued points of the fibre of pr_3 over t. (i.e. we are comparing the number of k_d points with $\mathbf{A}^1_{k(\zeta_r)}$ instead). Then taking the effect of the ∞ section and the singular fibres into account, one can show that ([6], section V)

$$\limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\sum_{t\in U(k_d)}E(d,t)^2\le\limsup_{\substack{d\to\infty\\ r-1|d}}\frac{1}{q^{2d}}\sum_{t\in\mathbf{A}^1_k(k_d)}E^{\mathrm{aff}}(d,t)^2.$$

Hence we get:

Lemma 5.4.

$$\operatorname{Irr}\mathcal{E} \leq \limsup_{\substack{d\to\infty \\ r-1|d}} \frac{1}{q^{2d}} \sum_{t\in\mathbf{A}^1_k(k_d)} E^{\mathrm{aff}}(d,t)^2. \tag{28}$$

□

We'll finish the proof by using the following asymptotic expression for the sum $\sum_{t\in\mathbf{A}^1_k(k_d)} E^{\mathrm{aff}}(d,t)^2$ (as $d\to\infty$). In the following it suffices to consider any finite field $\tilde{k}$ of cardinality $\tilde{q}$, with characteristic $\neq 2, r$, and we just write $E^{\mathrm{aff}}(t)$ for the affine error term.

Lemma 5.5. *For a finite field $\tilde{k}$ of cardinality $\tilde{q}$, we have the asymptotic formula*

$$\sum_{t\in k} E^{\mathrm{aff}}(t)^2 = g\,\tilde{q}^2 + O(\tilde{q}^{3/2}) \ \textit{(recall } g = \frac{r-1}{2}\textit{)}.$$

Proof. Let $\chi\colon \tilde{k}^* \longrightarrow \mu_2$ be the non-trivial quadratic character, extended as usual by setting $\chi(0)=0$.

Then for $t\in\tilde{k}$,

$$E^{\mathrm{aff}}(t) = \sum_{x\in\tilde{k}} \chi(f(x)+t),$$

$$\sum_{t\in\tilde{k}} E^{\mathrm{aff}}(t)^2 = \sum_{t,x,z\in\tilde{k}} \chi((f(x)+t)(f(z)+t)).$$

For fixed x,z, the sum $\sum_{t\in k}\chi((f(x)+t)(f(z)+t))$ is the affine error term for the number of $\tilde{k}$-rational points of the conic in (A,B) space defined by

$$B^2 = (A+f(x))(A+f(z)).$$

If $f(x)\neq f(z)$, this is an affine smooth conic with 2 rational points at ∞ (the characteristic of $\tilde{k}$ is not 2), so

$$\sum_{t\in\tilde{k}} \chi((f(x)+t)(f(z)+t)) = \#\mathbf{P}^1_{\tilde{k}}(\tilde{k}) - 2 - \tilde{q} = (\tilde{q}+1) - 2 - \tilde{q} = -1.$$

If $f(x)=f(z)$, then clearly the character sum is:

$$\sum_{t\in\tilde{k}} \chi((f(x)+t)(f(z)+t)) = \sum_{t\neq 0} \chi(t^2) = \tilde{q}-1.$$

Hence

$$\begin{aligned}
\sum_{t\in\tilde{k}} E^{\mathrm{aff}}(t)^2 &= (\tilde{q}-1)\#\{(x,z)|f(x)=f(z)\} - \{(x,z)|f(x)\neq f(z)\} \\
&= (\tilde{q}-1)\#\{(x,z)|f(x)=f(z)\} - (\tilde{q}^2 - \{(x,z)|f(x)=f(z)\}) \\
&= -\,\tilde{q}^2 + \tilde{q}\,\#\{(x,z)|f(x)=f(z)\}.
\end{aligned}$$

Now recall we have the factorisation used in the proof of theorem 4.1: (see [11], lemma 7)

$$f(X) - f(Z) = \pm(X - Z) \prod_{i=1}^{\frac{r-1}{2}} (X^2 - \theta_i XY + Y^2 - 4 + \theta_i^2) \; (\theta_i = \zeta_r^i + \zeta_r^{-i}).$$

Thus the affine curve $f(X) - f(Z) = 0$ in X, Z plane has $1 + \frac{r-1}{2}$ components.
By the Lang-Weil estimate,

$$\#\{(x,z) | f(x) = f(z)\} = (1 + \frac{r-1}{2}) \, \tilde{q} + O(\tilde{q}^{1/2}).$$

The proof follows.

□

6. A universal family of principally polarised abelian varieties with real multiplication

We follow [8], § 11.0.1 and [4], § 4. As before let F be the field $\mathbf{Q}(\cos \frac{2\pi}{r})$, $\mathcal{O}_F$ be its ring of integers. We recall the data of linear rigidification: for an abelian scheme $p : \mathcal{A} \longrightarrow S$ of relative dimension $g = \frac{r-1}{2}$, with a principal polarisation $\varphi : \mathcal{A} \longrightarrow \mathcal{A}^t$, let $\mathcal{L}_\varphi$ be the line bundle $(\mathrm{Id}_{\mathcal{A}} \times \varphi)^* \mathcal{P}$, where $\mathcal{P}$ is the Poincaré invertible sheaf on $\mathcal{A} \times \mathcal{A}^t$. One knows that $\mathcal{L}_\varphi^{\otimes 3}$ is relatively very ample over S, and by the Riemann-Roch theorem $p_* \mathcal{L}_\varphi^{\otimes 3}$ is locally free $\mathcal{O}_S$ module of rank 6^g. A choice of $\mathcal{O}_S$-basis, called a level $3\mathcal{L}$ structure and denoted as α, gives an embedding of $\mathcal{A}/S$ into $\mathbf{P}_S^{6^g - 1}$ and provides rigidification. A level $3\mathcal{L}$ structure always exist Zariski locally (as opposed to level n structure, which exists only étale locally) for a principally polarised abelian scheme.

We consider triples $(\mathcal{A}, \varphi, i)_{/S}$, where (*c.f.* [5], chapter 4):

- **rm1:** $\mathcal{A}/S$ is an abelian scheme over S.
- **rm2:** $i : \mathcal{O}_F \hookrightarrow \mathrm{End}_S(\mathcal{A})$ an embedding.
- **rm3:** φ is a principal polarisation $\varphi : \mathcal{A} \longrightarrow \mathcal{A}^t$, which is linear over the image of $\mathcal{O}_F$ by i (this is the equivalent to saying that the image of i is fixed by the Rosati involution defined by φ).
- **rm4:** $\mathrm{Lie}(\mathcal{A}/S)$ is a locally free $\mathcal{O}_F \otimes_{\mathbf{Z}} \mathcal{O}_S$ module of rank one.

Such a triple is called an "HBAV" (Hilbert-Blumenthal Abelian Variety) over S. If we put in the rigidification data α, the the quadruple $(\mathcal{A}, \varphi, i, \alpha)_{/S}$ called a "rigidified HBAV" over S. For an HBAV, one can construct, for n invertible on S, the $\mathcal{O}_F$-linear Weil pairing (*c.f.* [4], equation (4.4)):

$$\bigwedge_{\mathcal{O}_F}^{2} \mathcal{A}[n] \xrightarrow{\sim} \mathcal{D}_{F/\mathbf{Q}}^{-1} \otimes_{\mathbf{Z}} \mu_n. \tag{29}$$

(The exterior product being taken with respect to $\mathcal{O}_F$; here $\mathcal{D}_{F/\mathbf{Q}}^{-1}$ is the inverse different of $F/\mathbf{Q}$, μ_n is the group scheme of n-th roots on unity on S. Composing equation (6.1) with the trace map $\mathrm{tr}_{F/\mathbf{Q}}$ gives the usual Weil pairing.)

Now let $M_{g,3\mathcal{L}}$ be the functor

$$S \longrightarrow \{\text{isomorphism classes of quadruples } (\mathcal{A}, \varphi, i, \alpha)_{/S}\}$$

Theorem 6.1. *The functor $M_{g,3\mathcal{L}}$ is representable by a scheme $\mathcal{M}_{g,3\mathcal{L}}$ which is smooth over $\mathbf{Z}$ with geometrically connected fibres of dimension $g+6^{2g}$*

Proof. To prove representability, it suffices to do so over $\mathbf{Z}[1/n]$ for two relatively prime value of $n \geq 3$. For $n \geq 3$, consider the raw level n moduli problem $M_{g,\mathrm{raw}\ n}$ on HBAV $\mathcal{A}/S/\mathbf{Z}[1/n]$, where one imposes two sections of $\mathcal{A}[n](S)$ which, on each geometric fibre, form a $\mathcal{O}_F/n\mathcal{O}_F$ basis. It is representable by a quasiprojective scheme $\mathcal{M}_{g,\mathrm{raw}\ n}$ smooth over $\mathbf{Z}[1/n]$, whose geometric fibres are of dimension g (*c.f.* [4], p.254-255). Over this, we consider the moduli problem $M_{g,\mathrm{raw}\ n,3\mathcal{L}}$, where one imposes in addition a level $3\mathcal{L}$ structure, i.e. an $\mathcal{O}_S$ basis of $p_*\mathcal{L}_\varphi^{\otimes 3}$. It is seen that this problem is representable by the total space of a $\mathrm{GL}(6^g)$ torsor, which we call $\mathcal{M}_{g,\mathrm{raw}\ n,3\mathcal{L}}$, over $\mathcal{M}_{g,\mathrm{raw}\ n}$. The solution to the problem $M_{g,3\mathcal{L}}$ is then obtained by taking the quotient of $\mathcal{M}_{g,\mathrm{raw}\ n,3\mathcal{L}}$ by the free action of $GL_2(\mathcal{O}_F/n\mathcal{O}_F)$ (since level $3\mathcal{L}$ structure rigidifies), hence is smooth of relative dimension dimension $g+6^{2g}$ over $\mathbf{Z}[1/n]$.

To show that the fibres $\mathcal{M}_{g,3\mathcal{L}}$ are geometrically connected, it suffices to do so after extension of scalars to $\mathbf{Z}[1/n,\zeta_n]$. Over this, we have the more usual level n problem $M_{g,n,3\mathcal{L}}$, where we impose also the condition that the $\mathcal{O}_F$-linear Weil pairing of the two basis elements of $\mathcal{A}[n](S)$ is $1\otimes\zeta_n$. This moduli problem is representable by $\mathcal{M}_{g,n,3\mathcal{L}}$ over $\mathbf{Z}[1/n,\zeta_n]$, which is smooth, geometrically connected of relative dimension g (*loc.cit*). Then $\mathcal{M}_{g,3\mathcal{L}}$ is obtained by taking the quotient of the free action of $\mathrm{SL}_2(\mathcal{O}_k/n\mathcal{O}_F)$, hence is also geometrically connected. □

Denote by

$$p_{\mathrm{univ}} : \mathcal{A}_{\mathrm{univ}} \longrightarrow \mathcal{M}_{g,3\mathcal{L}}$$

the universal family over $\mathcal{M}_{g,3\mathcal{L}}$.

As before, k is a finite field of characteristic $\neq 2,r$. We then obtain from the above results the universal family:

$$p_{\mathrm{univ}}\otimes k : \mathcal{A}_{\mathrm{univ}}\otimes k \longrightarrow \mathcal{M}_{g,3\mathcal{L}}\otimes k$$

of principally polarised abelian varieties over k with $\mathcal{O}_F$ multiplication and level $3\mathcal{L}$ structure.

We have the l-adic lisse sheaf:

$$\mathcal{E}_{\mathrm{univ}} = R^1(p_{\mathrm{univ}}\otimes k)_*\,\overline{\mathbf{Q}}_l\,.$$

The vector spaces $E_{\mathrm{univ},l}, V_{\mathrm{univ},l}, E_{\mathrm{univ},l,\tau}$ and the representations $\rho_{\mathrm{univ},l}, \rho_{\mathrm{univ},l,\tau}$ are then the $E_l, V_l, E_{l,\tau}, \rho_l, \rho_{l,\tau}$ for this family $p_{\mathrm{univ}}\otimes k$. In particular, we have the monodromy representation:

$$\pi_1^{\mathrm{arith}}(\mathcal{M}_{g,3\mathcal{L}}\otimes k) \longrightarrow \mathrm{GL}_{E_{\mathrm{univ},l}}(\overline{\mathbf{Q}}_l).$$

As before, we know that the geometric monodromy group $G_{\mathrm{univ}}^{\mathrm{geom}}$ for this universal family has to be contained in $(\mathrm{Res}_{F_l/\mathbf{Q}_l}\mathrm{SL}_{V^*_{\mathrm{univ},l}/F_l})\otimes_{\mathbf{Q}_l}\overline{\mathbf{Q}}_l$.

Theorem 6.2. *The geometric monodromy group $G_{\mathrm{univ}}^{\mathrm{geom}}$ of $\mathcal{E}_{\mathrm{univ}}$ is*

$$(\mathrm{Res}_{F_l/\mathbf{Q}_l}\mathrm{SL}_{V^*_{\mathrm{univ},l}/F_l})\otimes_{\mathbf{Q}_l}\overline{\mathbf{Q}}_l \cong \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SL}_{2,\overline{\mathbf{Q}}_l}\,.$$

Proof. For the proof of this theorem, we may, after extension of scalars, assume $\zeta_r \in k$. In the notations of theorem 4.3, the family $\mathrm{Jac}(\mathcal{C}|_U) \longrightarrow U$ is an HBAV over U. Indeed, the only condition not yet checked is **rm4**. However, it's known that this condition is automatically satisfied since our family lifts to characteristic 0. Now since level $3\mathcal{L}$ structure exists Zariski locally, we can, by restricting to a non-empty open $\tilde{U} \subset U$, assume that a level $3\mathcal{L}$ structure exists on $\tilde{U}$. Note that theorem 4.5 concerning the (geometric) monodromy group holds verbatim, since $\pi_1^{\mathrm{geom}}(\tilde{U})$ surjects to $\pi_1^{\mathrm{geom}}(U)$. We thus obtain a map:

$$\tilde{U} \longrightarrow \mathcal{M}_{g,3\mathcal{L}} \otimes k,$$

and the monodromy representation for the family $\mathrm{Jac}(\mathcal{C}|_{\tilde{U}}) \longrightarrow \tilde{U}$ is obtained (up to conjugation) as:

$$\pi_1^{\mathrm{arith}}(\tilde{U}) \longrightarrow \pi_1^{\mathrm{arith}}(\mathcal{M}_{g,3\mathcal{L}} \otimes k) \longrightarrow \mathrm{GL}_{E_{\mathrm{univ},l}}(\overline{\mathbf{Q}}_l),$$

which, by theorem 4.5, has geometric group $(\mathrm{Res}_{F_l/\mathbf{Q}_l} \mathrm{SL}_{V^*_{\mathrm{univ},l}/F_l}) \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l$, the biggest possible. This forces the geometric monodromy of the universal family to be the biggest possible.

□

7. Equidistribution

Let k_n/k be a sequence of finite extensions of k inside $\overline{k}$, with $\#k_n \to \infty$ as $n \to \infty$. For $t \in (\mathcal{M}_{g,3\mathcal{L}} \otimes k)(k_n)$, Let Frob_{t,k_n} be the conjugacy class of a geometric Frobenius element associted to t in $\pi_1^{\mathrm{arith}}(\mathcal{M}_{g,3\mathcal{L}} \otimes k)$.

With the notations of [8], let $\rho_{\mathrm{univ},l}(\frac{1}{2})$ be the generalised Tate-twisted representation of $\rho_{\mathrm{univ},l}$. Since $\rho_{\mathrm{univ},l}$ is pure of weight 1, $\rho_{\mathrm{univ},l}(\frac{1}{2})$ is pure of weight 0. From the decomposition:

$$(\rho_{\mathrm{univ},l}, E_{\mathrm{univ},l}) \cong \bigoplus_{\tau: F \hookrightarrow \overline{\mathbf{Q}}} (\rho_{\mathrm{univ},l,\tau}, E_{\mathrm{univ},l,\tau}) \tag{30}$$

we see that each of $\rho_{\mathrm{univ},l,\tau}(\frac{1}{2})$ is pure of weight 0.

Also, we see from equation (3.4), that $\det_{F_l} \rho_{\mathrm{univ},l}(\frac{1}{2})(\mathrm{Frob}_{t,k_n}) = 1$. Thus the image of $\mathrm{Frob}_{t,k_n} \in \pi_1^{\mathrm{arith}}(U)$ under $\rho_{\mathrm{univ},l}(\frac{1}{2})$ lies in $G^{\mathrm{geom}}_{\mathrm{univ}} \cong \prod_{\tau: F \hookrightarrow \overline{\mathbf{Q}}} \mathrm{SL}_{2,\overline{\mathbf{Q}}_l}$.

Thus we can write

$$\det(1 - T\,\mathrm{Frob}_{t,k_n} | \rho_{\mathrm{univ},l,\tau}(\frac{1}{2})) = (1 - T\alpha_\tau(t))(1 - T\alpha_\tau(t)^{-1})$$

with $\alpha_\tau(t)$ pure of weight 0. Now fix an isomorphism: $\iota : \overline{\mathbf{Q}}_l \to \mathbf{C}$. Then $\iota(\alpha_i(t))$ is unitary, and we can specify $\alpha_\tau(t)$ by requiring that its image under ι to be of the form $e^{i\theta_\tau(t)}$, with $\theta_\tau(t) \in [0, \pi]$. So corresponding to the decomposition (7.1), we have factorisation of characteristic polynomial:

$$\begin{aligned} \iota(\det(I - T\,\mathrm{Frob}_{t,k_n} | \rho_{\mathrm{univ},l}(\frac{1}{2}))) \quad &= \quad \prod_{\tau: F \hookrightarrow \overline{\mathbf{Q}}} \iota(\det(1 - T\,\mathrm{Frob}_{t,k_n} | \rho_{\mathrm{univ},l,\tau}(\frac{1}{2}))) \\ = \prod_{\tau: F \hookrightarrow \overline{\mathbf{Q}}} \iota((1 - T\alpha_\tau(t))(1 - T\alpha_\tau(t)^{-1})) \quad &= \quad \prod_{\tau: F \hookrightarrow \overline{\mathbf{Q}}} (1 - Te^{i\theta_\tau(t)})(1 - Te^{-i\theta_\tau(t)}). \end{aligned}$$

We can then define a map:

$$\theta : \mathcal{M}_{g,3\mathcal{L}}(k_n) \longrightarrow \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} [0,\pi]$$

by associating to t the g-tuple of angles $\theta(t) = (\theta_\tau(t))_{\tau\hookrightarrow\overline{\mathbf{Q}}}$.

We can also define this map more invariantly as follows: the semisimple part of the image $\rho_{\mathrm{univ},l}(\frac{1}{2})(\mathrm{Frob}_{t,k_n})^{ss}$ lies in $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SL}_{2,\overline{\mathbf{Q}}_l}$, which when viewed as element in $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SL}_{2,\mathbf{C}}$ via $\iota : \overline{\mathbf{Q}}_l \to \mathbf{C}$, is conjugate in $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SL}_{2,\mathbf{C}}$ to an element in the maximal compact subgroup $\mathrm{K} = \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SU}(2)$, whose conjugacy class in K is well-defined. Recall that each element of SU(2) is SU(2)-equivalent to an element of the form $\begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix}$, for a unique $\theta \in [0,\pi]$. Thus we may identify the set of conjugacy classes of $\mathrm{K} = \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \mathrm{SU}(2)$ with g-tuple of angles $\{\theta_\tau\}_{\tau:F\to\overline{\mathbf{Q}}} \in \prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} [0,\pi]$. Our contended map is the g-tuple of angles in $[0,\pi]$ associated to this conjugacy class in K.

On the product $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} [0,\pi]$, we have the Sato-Tate measure:

$$\mu_{ST} = \bigwedge_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} \frac{2}{\pi} \sin^2(\theta_\tau) d\theta_\tau$$

which is the push-forward to the space of K-conjugacy classes of the normalised Haar measure on K.

The hypotheses for Deligne's equidistribution theorem ([3], Théorème 3.5.3, [8], Theorem 9.2.6) are now satisfied, and we obtain theorem 1.1, which we recall:

Theorem 7.1. *Let $\delta_{\theta(t)}$ be the delta measure on $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} [0,\pi]$ associated to $\theta(t)$, then the sequence of measures on $\prod_{\tau:F\hookrightarrow\overline{\mathbf{Q}}} [0,\pi]$ given by*

$$\frac{1}{\#\mathcal{M}_{g,3\mathcal{L}}(k_n)} \sum_{t\in\mathcal{M}_{g,3\mathcal{L}}(k_n)} \delta_{\theta(t)} \tag{31}$$

converges weakly (as $\#k_n \to \infty$) to the product Sato-Tate measure μ_{ST}.

Acknowledgements

The author would like to thank Professor Mazur for his suggestion of this problem, the referee for his helpful comments, and Harvard University for the financial support.

References

1. W.Casselman, *On abelian varieties with many endomorphisms and a conjecture of Shimura's*, Invent. Math. **12** (1971) 225-236.
2. H,Darmon and J-F. Mestre, *Courbes hyperelliptiques à multiplications réelles et une construction de Shih*, Canad. Math. Bull. **43** (2000) no. 3, 304-311.
3. P.Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. No. 52 (1980) 137-252.
4. P.Deligne, K.Ribet, *Values of abelian L functions at negative integers over totally real fields* Invent. Math. **59** (1980) no. 3, 227-286.
5. H.Hida, *p-adic Automorphic Forms on Shimura Varieties*, Springer-Verlag, New York (2004)
6. N.Katz, *Monodromy of families of curves: applications of some results of Davenport-Lewis*, Progr. Math. **12** Birkhäuser, Boston. Mass. (1981) 171-195.

7. ______, *Exponential Sums and Differential Equations*, Annals of Mathematics Studies **124** Princeton University Press (1990)
8. ______, *Random matrices, Frobenius eigenvalues, and monodromy,* American Mathematical Society Colloquium Publications **45** American Mathematical Society, Providence, RI (1999)
9. S.Lang, *Abelian Varieties,* Interscience Publishers, Inc., New York; Intescience Publishers Ltd., London (1959)
10. D.Mumford, *Geometric Invariant Theory,* Springer-Verlag, Berlin-New York (1965)
11. W.Tautz, J.Top, A.Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, Canad. J. Math. **43** (1991), no. 5, 1055-1064.
12. SGA 7 I, *Groupes de monodromie en géométrie algébrique. I,* Lecture Notes in Mathematics **288** Springer-Verlag, Berlin-New York (1972)

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138

E-mail address: mok@math.harvard.edu