Explicit Determination of the Images of the Galois Representations Attached to Abelian Surfaces with End(A)= $\mathbb{Z}$

Luis V. Dieulefait

CONTENTS

We give an effective version of a result reported by Serre asserting that the images of the Galois representations attached to an abelian surface with $\mathrm{End}(A) = \mathbb{Z}$ are as large as possible for almost every prime. Our algorithm depends on the truth of Serre's conjecture for two-dimensional odd irreducible Galois representations. Assuming this conjecture, we determine the finite set of primes with exceptional image. We also give infinite sets of primes for which we can prove (unconditionally) that the images of the corresponding Galois representations are large. We apply the results to a few examples of abelian surfaces.

1. INTRODUCTION

Let A be an abelian surface defined over $\mathbb{Q}$ with $\mathrm{End}(A) := \mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Let $\rho_\ell : G_\mathbb{Q} \to \mathrm{GSp}(4, \mathbb{Z}_\ell)$ be the compatible family of Galois representations given by the Galois action on $T_\ell(A) = A[\ell^\infty](\bar{\mathbb{Q}})$, the Tate modules of the abelian surface (we are assuming that A is principally polarized). Each ρ_ℓ is unramified outside ℓN, where N is the product of the primes of bad reduction of A. If we call G_{ℓ^∞} the image of ρ_ℓ, then we have the following result of Serre [Serre 86]:

Theorem 1.1. *If A is an abelian surface over $\mathbb{Q}$ with $\mathrm{End}(A) = \mathbb{Z}$ and principally polarized, then $G_{\ell^\infty} = \mathrm{GSp}(4, \mathbb{Z}_\ell)$ for almost every ℓ.*

Remark 1.2. If G_ℓ is the image of $\bar{\rho}_\ell$, the Galois representation on ℓ-division points of $A(\bar{\mathbb{Q}})$ (and the residual mod ℓ representation corresponding to ρ_ℓ), it is enough to show that $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for almost every ℓ [Serre 86]. Serre proposed the problem of giving an effective version of this result: "*...partir de courbes de genre* 2 *explicites, et tâcher de dire à partir de quand le groupe*

2000 AMS Subject Classification: Primary 11F80; Secondary 11G10

Keywords: Galois representations, abelian varieties

de Galois correspondant G_ℓ devient égal à $\mathrm{GSp}(4, \mathbb{F}_\ell)$.” But Serre’s proof depends on certain ineffective results of Faltings and therefore does not solve this problem.

In this article, we present an algorithm that computes a finite set $\mathcal{F}$ of primes containing all those primes (if any) with image of the corresponding Galois representation exceptional, i.e., different from $\mathrm{GSp}(4, \mathbb{F}_\ell)$. The validity of our method depends on the truth of Serre’s conjecture for 2-dimensional irreducible odd Galois representations, conjecture ($3.2.4_?$) in [Serre 87]. This means that if ℓ is a prime such that $G_\ell \neq \mathrm{GSp}(4, \mathbb{F}_\ell)$ and $\ell \notin \mathcal{F}$, then G_ℓ has a 2-dimensional irreducible (odd) component that violates Serre’s conjecture.

The method is inspired by the articles [Serre 72], [Ribet 75], [Ribet 85], and [Ribet 97] where the case of 2-dimensional Galois representations is treated.

In the examples, we also give infinite sets of primes for which we can prove the result on the images unconditionally, i.e., without assuming Serre’s conjecture. Results of this kind were previously obtained by Le Duff under the extra assumption of semiabelian reduction of the abelian surface at some prime. Our technique has two advantages: It does not have any restriction on the reduction type of the abelian surface, and in the case of semiabelian reduction, it allows us to prove the result on the images (unconditionally) for larger sets of primes.

2. MAIN TOOLS

2.1 Maximal Subgroups of $\mathrm{PGSp}(4, \mathbb{F}_\ell)$

In [Mitchell 14], Mitchell gives the following classification of maximal proper subgroups G of $\mathrm{PSp}(4, \mathbb{F}_\ell)$ (ℓ odd), as groups of transformations of the projective space having an invariant linear complex:

(1) a group having an invariant point and plane;

(2) a group having an invariant parabolic congruence;

(3) a group having an invariant hyperbolic congruence;

(4) a group having an invariant elliptic congruence;

(5) a group having an invariant quadric;

(6) a group having an invariant twisted cubic;

(7) a group G containing a normal elementary abelian subgroup E of order 16, with: $G/E \cong A_5$ or S_5;

(8) a group G isomorphic to A_6, S_6 or A_7.

For the relevant definitions, see [Hirschfeld 85], see also [Blichfeldt 19] and [Ostrom 77] for cases (7) and (8).

Remark 2.1. This classification is part of a general “philosophy”: The subgroups of $\mathrm{GL}(n, \mathbb{F}_\ell)$, ℓ large, are essentially subgroups of Lie type, with some exceptions independent of ℓ (see [Serre 86]).

From this, we obtain a classification of maximal proper subgroups H of $\mathrm{PGSp}(4, \mathbb{F}_\ell)$ with exhaustive determinant. It is similar to the above classification, except that cases (7) and (8) change according to the relation between H and G, given by the exact sequence:

$$1 \to G \to H \to \{\pm 1\} \to 1.$$

2.2 The Action of Inertia

From now on, we will assume that ℓ is a prime of good reduction for the abelian surface A. Then it follows from results of Raynaud that the restriction $\bar{\rho}_\ell|_{I_\ell}$ has the following property [Raynaud 74, Serre 72]:

Theorem 2.2. *If V is a Jordan-Hölder quotient of the I_ℓ-module $A[\ell](\bar{\mathbb{Q}})$ of dimension n over $\mathbb{F}_\ell$, then V admits an $\mathbb{F}_{\ell^n}$-vector space structure of dimension 1 such that the action of I_ℓ on V is given by a character $\phi : I_{\ell,t} \to \mathbb{F}_{\ell^n}^*$ (t stands for tame) with:*

$$\phi = \phi_1^{d_1} \ldots\phi_n^{d_n}, \tag{2–1}$$

where ϕ_i are the fundamental characters of level n and $d_i = 0$ or 1, for every $i = 1, 2, \ldots, n$.

This statement is proved by Serre in [Serre 72] except for the bound for the exponents, which is the result of Raynaud mentioned above, later generalized by Fontaine-Messing.

We will use the following lemmas repeatedly (see [Dickson 01]):

Lemma 2.3. *Let $M \in \mathrm{Sp}(4, F)$ be a symplectic transformation over a field F. The roots of the characteristic polynomial of M can be written as $\alpha, \beta, \alpha^{-1}, \beta^{-1}$, for some α, β.*

Remark 2.4. A similar result holds in general for the groups $\mathrm{Sp}(2n, F)$.

In the case of the Galois representations attached to A, we know that $\det(\bar{\rho}_\ell) = \chi^2$, where χ is the mod ℓ cyclotomic character. Therefore, we obtain:

Lemma 2.5. *The roots of the characteristic polynomial of* $\bar{\rho}_\ell(\text{Frob } p) \in G_\ell$ *can be written as* $\alpha, \beta, p/\alpha, p/\beta$ $(p \nmid \ell N)$.

Remark 2.6. Here Frob p denotes the (arithmetic) Frobenius element, defined up to conjugation. The value of the representation in it is well-defined precisely because of the fact that the representation is unramified at p.

Proof: Use Lemma 2.3, $G_\ell \subseteq \text{GSp}(4, \mathbb{F}_\ell)$, and the exact sequence:

$$1 \to \text{Sp}(4, \mathbb{F}_\ell) \to \text{GSp}(4, \mathbb{F}_\ell) \to \mathbb{F}_\ell^* \to 1.$$

□

Remark 2.7. The same is true for $\rho_\ell(\text{Frob } p) \in G_{\ell^\infty}$. Thus, the characteristic polynomial of $\rho_\ell(\text{Frob } p)$ has the form

$$x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2$$

with $a_p, b_p \in \mathbb{Z}$, $a_p = \text{trace}(\rho_\ell(\text{Frob } p))$.

From Equation (2-1), we obtain the following possibilities for $\bar{\rho}_\ell|_{I_\ell}$ $(\ell \nmid N)$:

$$\begin{pmatrix} 1 & * & * & * \\ 0 & \chi & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & \chi \end{pmatrix}; \quad \begin{pmatrix} \psi_2 & 0 & * & * \\ 0 & \psi_2^\ell & * & * \\ 0 & 0 & \psi_2 & 0 \\ 0 & 0 & 0 & \psi_2^\ell \end{pmatrix};$$

$$\begin{pmatrix} \psi_2 & 0 & * & * \\ 0 & \psi_2^\ell & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & \chi \end{pmatrix}; \quad \begin{pmatrix} \psi_4^{\ell+\ell^2} & 0 & 0 & 0 \\ 0 & \psi_4^{\ell^2+\ell^3} & 0 & 0 \\ 0 & 0 & \psi_4^{\ell^3+1} & 0 \\ 0 & 0 & 0 & \psi_4^{1+\ell} \end{pmatrix},$$

where ψ_i is a fundamental character of level i.

3. STUDY OF THE IMAGES

3.1 Reducible Case: 1-Dimensional Constituent

Let c be the conductor of the compatible family $\{\rho_\ell\}$. For the case of the Jacobian of a genus 2 curve, it can be computed using an algorithm of Liu, except for the exponent of 2 in c, which can easily be bounded using the discriminant of an integral model of the curve [Liu 94].

Suppose that the representation $\bar{\rho}_\ell$ is reducible with a 1-dimensional sub(or quotient) representation given by a character μ. This character is unramified outside ℓN and takes values in $\bar{\mathbb{F}}_\ell$; therefore from the description of $\bar{\rho}_\ell|_{I_\ell}$ given in Section 2.2 we have $\mu = \varepsilon \chi^i$, with ε unramified outside N and $i = 0$ or 1. Clearly $\text{cond}(\varepsilon) \mid c$. After semisimplification, we have:

$$\bar{\rho}_\ell \cong \varepsilon \chi^i \oplus \pi,$$

for a 3-dimensional representation π with $\det(\pi) = \varepsilon^{-1} \chi^{2-i}$. Therefore, $\text{cond}(\varepsilon)^2 \mid c$. Let d be the maximal integer such that $d^2 \mid c$. If we take a prime $p \equiv 1 \pmod{d}$, we have $\varepsilon(p) = 1$ so χ^i is a root of the characteristic polynomial of $\bar{\rho}_\ell(\text{Frob } p)$. This gives:

$$b_p - a_p(p+1) + p^2 + 1 \equiv 0 \pmod{\ell}, \tag{3–1}$$

both for $i = 0$ and $i = 1$ (in agreement with Lemma 2.5).

By the Riemann hypothesis, the roots of the characteristic polynomial of $\rho_\ell(\text{Frob } p)$ have absolute value $\sqrt{p}$. This gives automatic bounds for the absolute values of the coefficients a_p and b_p, and from these bounds, we see that for large enough p congruence, Equation (3-1) is not an equality. Therefore, only finitely many primes ℓ may verify (3-1)

Variant. Instead of taking a prime $p \equiv 1 \pmod{d}$, we can work in general with p of order f in $(\mathbb{Z}/d\mathbb{Z})^*$. Let $Pol_p(x)$ be the characteristic polynomial of $\bar{\rho}_\ell(\text{Frob } p)$. Then $\varepsilon(p)p^i$ is a root of $Pol_p(x)$, with $i = 0$ or 1, and $\varepsilon(p)^f = 1 \in \mathbb{F}_\ell$. Then

$$\text{Res}(Pol_p(x), x^f - 1) \equiv 0 \pmod{\ell} \tag{3–2}$$

where Res stands for resultant (again, cases $i = 0$ and 1 agree). This variant is used in the examples to avoid computing $Pol_p(x)$ for large p.

3.2 Reducible Case: "Related" 2-Dimensional Constituents

Suppose that, after semisimplification, $\bar{\rho}_\ell$ decomposes as the sum of two 2-dimensional irreducible Galois representations: $\bar{\rho}_\ell \cong \pi_1 \oplus \pi_2$. Assume also that these two constituents are related by Lemma 2.5, i.e., if α, β are the roots of the characteristic polynomial of $\pi_1(\text{Frob } p)$, then $p/\alpha, p/\beta$ are the roots of that of $\pi_2(\text{Frob } p)$. If not, then it follows from Lemma 2.5 that $\alpha = p/\beta$, so $\det(\pi_1) = \det(\pi_2) = \chi$; this case will be studied in the next subsection.

Using the description of $\bar{\rho}_\ell|_{I_\ell}$ given in Section 2.2, we see that one of the following must happen (where ε is a character unramified outside N):

- Case 1: $\det(\pi_1) = \varepsilon \chi^2$, $\quad \det(\pi_2) = \varepsilon^{-1}$.
- Case 2: $\det(\pi_1) = \varepsilon \chi$, $\quad \det(\pi_2) = \varepsilon^{-1} \chi$.

Case 1. In this case, we have the factorization

$$Pol_p(x) \equiv (x^2-rx+p^2\varepsilon(p))\,(x^2-\frac{rx}{p\varepsilon(p)}+\varepsilon^{-1}(p)) \pmod{\ell}.$$

As in the previous subsection, $\mathrm{cond}(\varepsilon) \mid d$. Eliminating r from the equation, we obtain

$$Q_p(b_p, a_p, \varepsilon(p)) := (\varepsilon(p)b_p - 1 - p^2\varepsilon(p)^2)(p\varepsilon(p)+1)^2 \\ - a_p^2 p\varepsilon(p)^2 \equiv 0 \pmod{\ell}.$$

If we take $p \equiv 1 \pmod{d}$, we obtain

$$(b_p - 1 - p^2)\,(p+1)^2 \equiv a_p^2\, p \pmod{\ell}. \qquad (3\text{–}3)$$

Again, from the bounds for the coefficients, we see that for large enough p, this is not an equality. Thus only finitely many ℓ can satisfy (3-3). Alternatively, for computational purposes, we may take p with $p^f \equiv 1 \pmod{d}$. Then we have

$$\mathrm{Res}(Q_p(b_p, a_p, x), x^f - 1) \equiv 0 \pmod{\ell}. \qquad (3\text{–}4)$$

Case 2. This case is quite similar to the previous one. We start with

$$Pol_p(x) \equiv (x^2-rx+p\varepsilon(p))\,(x^2-\frac{rx}{\varepsilon(p)}+p\varepsilon^{-1}(p)) \pmod{\ell}$$

with $\mathrm{cond}(\varepsilon) \mid d$. From this,

$$Q'_p(b_p, a_p, \varepsilon(p)) := (\varepsilon(p)b_p - p - p\varepsilon(p)^2)(\varepsilon(p)+1)^2 \\ - a_p^2\varepsilon(p)^2 \equiv 0 \pmod{\ell}.$$

Thus, if $p \equiv 1 \pmod{d}$,

$$4(b_p - 2p) \equiv a_p^2 \pmod{\ell}. \qquad (3\text{–}5)$$

In general, if $p^f \equiv 1 \pmod{d}$,

$$\mathrm{Res}(Q'_p(b_p, a_p, x), x^f - 1) \equiv 0 \pmod{\ell}. \qquad (3\text{–}6)$$

In this case, the fact that this holds only for finitely many primes ℓ is nontrivial. It may be thought of as a consequence of Theorem 1.1.

3.3 The Remaining Reducible Case

As explained above, in the remaining reducible case, we have $\bar\rho_\ell^{ss} \cong \pi_1 \oplus \pi_2$ with $\det(\pi_1) = \det(\pi_2) = \chi$. In Section 2.2, we described the possibilities for $\bar\rho_\ell|_{I_\ell}$. This gives for $\pi_1|_{I_\ell}$ and $\pi_2|_{I_\ell}$:

$$\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^\ell \end{pmatrix}.$$

In addition, $\mathrm{cond}(\pi_1)\mathrm{cond}(\pi_2) \mid c$.

At this point, we invoke Serre's conjecture (3.2.4?) (see [Se 87]) that gives us a control on π_1 and π_2. Both representations should be modular of weight 2, i.e., there exist two cusp forms f_1, f_2 with

$$\bar\rho_{f_1,\ell} \cong \pi_1,\ \bar\rho_{f_2,\ell} \cong \pi_2, \quad f_1 \in S_2(N_1),\ f_2 \in S_2(N_2),$$

$N_1N_2 \mid c$ (we are assuming π_1, π_2 to be irreducible; otherwise, they are covered by Section 3.1). Both cusp forms have trivial nebentypus.

There are finitely many cusp forms in these finitely many spaces. We have an algorithm to detect the primes ℓ falling in this case by comparing characteristic polynomials mod ℓ, since

$$\bar\rho_\ell^{ss} \cong \bar\rho_{f_1,\ell} \oplus \bar\rho_{f_2,\ell}.$$

We take all pairs of integers N_1, N_2 with $N_1N_2 = c$ and all pairs of cusp forms $f_1 \in S_2(N_1)$, $f_2 \in S_2(N_2)$ (either newforms or oldforms). If we denote by $Pol_{f_i,p}(x)$ the characteristic polynomial of $\rho_{f_i,\ell}(\mathrm{Frob}\ p)$ $(i = 1, 2)$, we should have for some such pair f_1, f_2:

$$Pol_{f_1,p}(x)Pol_{f_2,p}(x) \equiv Pol_p(x) \pmod{\ell} \qquad (3\text{–}7)$$

for every $p \nmid \ell N$. Theorem 1.1 guarantees that this can only happen for finitely many primes.

Remark 3.1. The Galois representations $\rho_{f_i,\ell}$ attached to f_i were constructed by Deligne (cf. [De 71]). The polynomials $Pol_{f_i,p}(x)$ are of the form

$$Pol_{f_i,p}(x) = x^2 - c_p x + p,$$

where c_p is the eigenvalue of f_i corresponding to the Hecke operator T_p. These eigenvalues, and *a fortiori* the characteristic polynomials $Pol_{f,p}(x)$ for any cusp form f, can be computed with an algorithm of W. Stein (cf. [St]). The compatible family of Galois representations constructed by Deligne, in the case of a cusp form $f \in S_2(N)$, shows up in the Jacobian $J_0(N)$ of the modular curve $X_0(N)$: It agrees with a two-dimensional constituent of the one attached to the abelian variety A_f corresponding to f.

For computational purposes, we introduce the following variant: Observe that either N_1 or N_2 (say N_1) satisfy

$$N_1 \mid c,\ N_1 \le \sqrt{c}.$$

Consider all divisors of c verifying this, maximal (among divisors of c) with this property. Call S the set of such divisors. Then we are supposing that there exists $f \in S_2(t)$ with $t \in S$ and

$$\mathrm{Res}(Pol_{f,p}(x), Pol_p(x)) \equiv 0 \pmod{\ell},$$

for every $p \nmid \ell N$. Therefore, for some $t \in S$

$$\mathrm{Res}(\prod_{f \in S_2(t)} Pol_{f,p}(x), Pol_p(x)) \equiv 0 \pmod{\ell}, \quad (3\text{–}8)$$

for every $p \nmid \ell N$.

With this formula, we compute in any given example all primes ℓ falling in this case.

Remark 3.2. In all reducible cases (Sections 3.1, 3.2, and 3.3), we have considered reducibility over $\bar{\mathbb{F}}_\ell$.

3.4 Stabilizer of a Hyperbolic or Elliptic Congruence

If G_ℓ corresponds to an irreducible subgroup inside (its projective image) some of the maximal subgroups in cases (3) and (4) of Mitchell's classification, there is a normal subgroup of index 2 of G_ℓ such that

$$1 \to M_\ell \to G_\ell \to \{\pm 1\} \to 1,$$

and the subgroup M_ℓ is reducible (not necessarily over $\mathbb{F}_\ell$).

In fact, a hyperbolic (elliptic) congruence is composed of all lines meeting two given skew lines in the projective three-dimensional space over $\mathbb{F}_\ell$ defined over $\mathbb{F}_\ell$ ($\mathbb{F}_{\ell^2}$, respectively), called the axes of the congruence (see [Hi 85]). The stabilizer of such congruences consists of those transformations that fix or interchange the two axes, and it contains the normal reducible index two subgroup of those transformations that fix both axes.

From the description of $\bar{\rho}_\ell|_{I_\ell}$ given in Section 2.2, we see that if $\ell > 3$, it is contained in M_ℓ. Therefore, if we take the quotient G_ℓ / M_ℓ, we obtain a representation $G_{\mathbb{Q}} \to C_2$ whose kernel is a quadratic field unramified outside N. Then there is a quadratic character $\phi : (\mathbb{Z}/c\mathbb{Z})^* \to C_2$ with $\phi(p) = -1 \;\Rightarrow\; \bar{\rho}_\ell(\mathrm{Frob}\ p)$ is of the form

$$\begin{pmatrix} 0 & 0 & * & * \\ 0 & 0 & * & * \\ * & * & 0 & 0 \\ * & * & 0 & 0 \end{pmatrix}.$$

Therefore, $\mathrm{trace}(\bar{\rho}_\ell(\mathrm{Frob}\, p)) = 0$, i.e.,

$$a_p \equiv 0 \pmod{\ell}, \quad (3\text{–}9)$$

for every $p \nmid \ell N$ with $\phi(p) = -1$.

Considering all quadratic characters ramifying only at the primes in N, we detect the primes ℓ falling in this case. Once again, from Theorem 1.1, it follows that this set is finite (of course, this fact strongly depends on the assumption $\mathrm{End}(A) = \mathbb{Z}$).

3.5 Stabilizer of a Quadric

This case can be treated exactly as the one above: Assuming again absolute irreducibility of the image G_ℓ, it contains a normal subgroup of index 2, and we obtain a quadratic character unramified outside N verifying Equation (3-9). In this case, $\bar{\rho}_\ell$ is the tensor product of two irreducible 2-dimensional Galois representations (see [Hi 85], page 28), one of them dihedral (this is the necessary and sufficient condition for the tensor product to be symplectic; see [B-R 89], page 51), so the matrices in G_ℓ are of the form:

$$\begin{pmatrix} av & 0 & cv & 0 \\ 0 & az & 0 & cz \\ bv & 0 & dv & 0 \\ 0 & bz & 0 & dz \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & az & 0 & cz \\ av & 0 & cv & 0 \\ 0 & bz & 0 & dz \\ bv & 0 & dv & 0 \end{pmatrix},$$

depending on the value of the quadratic character ϕ.

3.6 Stabilizer of a Twisted Cubic

This case is incompatible with the description of $\bar{\rho}_\ell|_{I_\ell}$ given in Section 2.2. In this case, all upper-triangular matrices are of the form (see [Hi 85], page 233):

$$\begin{pmatrix} a^3 & * & * & * \\ 0 & a^2 d & * & * \\ 0 & 0 & ad^2 & * \\ 0 & 0 & 0 & d^3 \end{pmatrix}.$$

In no case is the subgroup of G_ℓ given by $\bar{\rho}_\ell|_{I_\ell}$ of this form.

3.7 Exceptional Cases

The cases already studied cover all possibilities in the classification except the exceptional groups, i.e., cases (7) and (8). In these cases, comparing the exceptional group $H \subseteq \mathrm{PGSp}(4, \mathbb{F}_\ell)$ (its order and structure) with the fact that $\mathbb{P}(G_\ell)$ contains the image of $\mathbb{P}(\bar{\rho}_\ell|_{I_\ell})$ described in Section 2.2, we end up with the only possibilities ($\ell > 3$):

$$\ell = 5, 7.$$

For these two primes, as for any prime we suspect of satisfying $G_\ell \neq \mathrm{GSp}(4, \mathbb{F}_\ell)$, we compute several characteristic polynomials $Pol_p(x)$ mod ℓ. At the end, either we prove that it must be $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ (because the orders of the roots of the computed polynomials do not give any other option) or we reinforce our suspicion that ℓ is exceptional.

3.8 Conclusion

Having gone through all cases in the classification (the stabilizer of a parabolic congruence is reducible, it has an invariant line of the complex, cf. [Mi 14]) we conclude that for all primes ℓ except those whose image, according to our algorithm, may fall in a proper subgroup (according to Theorem 1.1, only finitely many) the image of $\mathbb{P}(\bar{\rho}_\ell)$ is $\mathrm{PGSp}(4, \mathbb{F}_\ell)$.

From this, it easily follows that if ℓ is not one of the finitely many exceptional primes, we have $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ and applying a lemma of [Se 86] (see also [Se 68]) we obtain $G_{\ell^\infty} = \mathrm{GSp}(4, \mathbb{Z}_\ell)$. Recall that at one step, we have assumed the veracity of Serre's conjecture ($3.2.4_?$).

4. AN EXAMPLE

We have applied the algorithm to the example given by the Jacobian of the genus 2 curve given by the equation

$$y^2 = x^6 - x^3 - x + 1.$$

The algorithm of Q. Liu computes the prime-to-2 part of the conductor. From this computation and the bound of the conductor in terms of the discriminant of an integral equation ([Liu 94]), we obtain $c \mid 2^{12} \cdot 23 \cdot 5$.

We exclude a priori the primes dividing the conductor: $2, 5$ and 23. We sketch some of the computations performed:

Reducible cases with 1-dimensional constituent or two related 2-dimensional constituents. The maximal possible value of the conductor of ε is $d = 64$. We compute the characteristic polynomials of $\rho_\ell(\mathrm{Frob}\, p)$ for the primes $p = 229, 257, 641, 769$ and applying the algorithm (Equations (3-2), (3-4), and (3-6)), we easily check that no prime $\ell > 3$ falls in these cases.

Remark 4.1. The characteristic polynomials used at this and the remaining steps can be found in Section 6.

Remaining reducible case. First we describe the set of special divisors of c:

$$S = \{368, 460, 512, 640\}.$$

Then we compute, for each $t \in S$ and each Hecke eigenform $f \in S_2(t)$, the characteristic polynomial $Pol_{f,p}(x)$ for $p = 3, 7, 11, 13, 17, 19$ with the algorithm implemented by W.Stein ([St]). Then, comparing these polynomials with the characteristic polynomials of $\rho_\ell(\mathrm{Frob}\ p)$ as in Equation (3-8), we see that no prime $\ell > 3$ falls in this case.

Cases "governed" by a quadratic character. We have to consider all possible quadratic characters ϕ unramified outside c (there are 15) and for each of them take a couple of primes p with $\phi(p) = -1$ and $a_p \neq 0$. Applying the algorithm (Equation (3-9)), we see that no prime $\ell > 3$ falls in these cases. At this step, we have used the values a_p for the primes $p = 3, 7, 13, 97, 113, 569, 769$.

Exceptional cases. We compute the reduction of a few characteristic polynomials modulo 7 and we find elements whose order (in $\mathrm{PGSp}(4, \mathbb{F}_7)$) does not correspond to the structure of any of the exceptional groups.
From all the above computations, we conclude:

Theorem 4.2. *Let A be the jacobian of the genus 2 curve:*

$$y^2 = x^6 - x^3 - x + 1.$$

Let G_{ℓ^∞} be the image of $\rho_{A,\ell}$, the Galois representation on $A[\ell^\infty](\bar{\mathbb{Q}})$, whose conductor divides $2^{12} \cdot 5 \cdot 23$. Then, assuming Serre's conjecture ($3.2.4_?$),

$$G_{\ell^\infty} = \mathrm{GSp}(4, \mathbb{Z}_\ell)$$

for every $\ell > 5$, $\ell \neq 23$.

Remark 4.3. We are not claiming that the image is not maximal for any of the four excluded primes.

5. UNCONDITIONAL RESULTS AND MORE EXAMPLES

5.1 The Case of Semiabelian Reduction

For certain genus 2 curves one can prove that the image is large for an infinite set of primes by using the following results of Le Duff [LeD 98]:

Proposition 5.1. *Let A be an abelian surface defined over $\mathbb{Q}$. Suppose that for a prime p of bad reduction of A, $\tilde{A}_p^0$ (the connected component of 0 in the special fiber of the Nron Model of A at p) is an extension of an elliptic curve by a torus. Then, for every prime $\ell \neq p$ with $\ell \nmid \Phi(p)$ (number of connected components of $\tilde{A}_p$), G_ℓ contains a transvection.*

Recall that a transvection is an element u such that $\mathrm{Image}(u - 1)$ has dimension 1.

Proposition 5.2. *([LeD 98]) If $G \subset \mathrm{Sp}(4, \mathbb{F}_\ell)$ is a proper maximal subgroup containing a transvection, all its elements have reducible (over $\mathbb{F}_\ell$) characteristic polynomial. Therefore, a transvection together with a matrix with irreducible characteristic polynomial generate* $\mathrm{Sp}(4, \mathbb{F}_\ell)$.

Remark 5.3. We can also find in [Mi 14] the list of maximal subgroups of $\mathrm{PSp}(4, \mathbb{F}_\ell)$ containing central elations, and a central elation is the image in $\mathrm{PSp}(4, \mathbb{F}_\ell)$ of a transvection in $\mathrm{Sp}(4, \mathbb{F}_\ell)$. These groups correspond to cases (1) and (3) in Section 2.1 or to a group having an invariant line of the complex, defined over $\mathbb{F}_\ell$.

Recall that $Pol_q(x)$ denotes the characteristic polynomial of $\rho_\ell(\mathrm{Frob}\ q)$ for any prime q of good reduction for the abelian surface A and $\ell \neq p$. From the two previous results, we have the following theorem:

Theorem 5.4. (Le Duff.) *Let p be a bad reduction prime verifying the condition of Proposition 5.1 and q a prime with $Pol_q(x)$ irreducible, then for every $\ell \nmid 2pq\Phi(p)$ such that $Pol_q(x)$ is irreducible modulo ℓ, $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$. If Δ_q is the discriminant of $Pol_q(x)$ and Δ_{Q_q} the discriminant of $Q_q(x) := x^2 - a_q x + b_q - 2q$, the irreducibility condition is:*

$$(\frac{\Delta_q}{\ell}) = -1 \text{ and } (\frac{\Delta_{Q_q}}{\ell}) = -1.$$

Example 5.5. (Le Duff.) Take the genus 2 curve:

$$C_2 : \quad y^2 = x^5 - x + 1.$$

$A_2 = J(C_2)$ has good reduction outside $2, 19, 151$. For $p = 19, 151$, the condition in Proposition 5.1 is satisfied with $\Phi(p) = 1$. Take $q = 3$, $Pol_3(x)$ is irreducible and Theorem 5.4 gives: $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for every $\ell > 3$ with $(\frac{61}{\ell}) = -1$ and $(\frac{5}{\ell}) = -1$.

Remark 5.6. Of course, considering more irreducible characteristic polynomials, one can obtain the same result for other primes. In particular, $G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell)$ for $\ell = 19, 151$ (cf. [LeD 98]).

Remark 5.7. The example in the previous section also verifies Le Duff's condition.

Let us apply our method to this example. The invariants are $c = \mathrm{cond}(A_2) \mid 2^8 \cdot 19 \cdot 151$ (computed with Liu's algorithm); then $\mathrm{cond}(\varepsilon) \mid d = 16$; and the set $S = \{256, 604, 608\}$.

In this example, we only have to worry about those maximal subgroups in Mitchell's classification containing central elations. Therefore, we only have to discard the maximal subgroups considered in Sections 3.1, 3.3, and 3.4.

- The reducible case with 1-dimensional constituent is easily handled using the characteristic polynomials (see Section 6) $Pol_p(x)$ for $p = 17, 97$ and we conclude that no prime $\ell > 2$ falls in this case.

- Due to the fact that the spaces of modular forms $S_2(t)$ for $t \in S$ are rather large, we decided to save computations and to apply the procedure described in Section 3.3, Equation (3-8), only to the prime $p = 3$. After computing all resultants of $Pol_3(x)$ with all the characteristic polynomials $Pol_{f,3}(x)$ for $f \in S_2(t)$, $t \in S$, we find the possibly exceptional primes $\ell > 2$:

  $$\ell = 3, 5, 11, 19, 29, 31, 41, 61, 109, 151.$$

  Having computed the characteristic polynomials

  $$Pol_p(x) \quad \text{for} \quad p = 11, 41, 79, 101, 199, 211$$

  (see Section 6), we checked that for each of the ten possibly exceptional primes ℓ listed above, one of these six polynomials is irreducible modulo ℓ. Then, applying Theorem 5.4, we conclude that none of these primes is exceptional. Thus, no $\ell > 2$ has reducible image.

- For cases governed by a quadratic character, we have to consider all possible quadratic characters ϕ unramified outside c and for each of them take a couple of primes p with $\phi(p) = -1$ and $a_p \neq 0$. We use the values a_p for $p = 3, 5, 97, 257$ (see Section 6) and an application of the algorithm (Equation (3-9)) proves that the only possibly exceptional primes $\ell > 2$ are

  $$\ell = 3, 5, 11, 97, 257.$$

We already mentioned that $3, 5$, and 11 are not exceptional. Applying Theorem 5.4 again, we see that 97 and 257 are also nonexceptional because $Pol_{11}(x)$ is irreducible modulo 97 and $Pol_{281}(x)$ is irreducible modulo 257. We have the following theorem:

Theorem 5.8. *Let A_2 be the Jacobian of the genus 2 curve given by the equation $y^2 = x^5 - x + 1$. Assume Serre's* *conjecture* (3.2.4?) ([Serre 87]). *Then the images of the Galois representations on the ℓ-division points of A_2 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every } \ell > 2.$$

Remark 5.9. $\bar{\rho}_2$ is also irreducible over $\mathbb{F}_2$. This irreducibility for all ℓ is equivalent to the fact that A_2 is isolated in its isogeny class in the sense that any abelian variety isogenous to A_2 over $\mathbb{Q}$ is isomorphic to A_2 over $\mathbb{Q}$. Unfortunately, this condition of being isolated is not effectively verifiable.

Among the subgroups containing central elations, we have used Serre's conjecture only to eliminate the following one:

$$G_\ell \subseteq \{A \times B \in \mathrm{GL}(2, \mathbb{F}_\ell) \times \mathrm{GL}(2, \mathbb{F}_\ell) : \det(A) = \det(B) = \chi\}. \tag{5–1}$$

Take q with $Pol_q(x)$ irreducible. If $(\frac{\Delta_{Q_q}}{\ell}) = -1$ case (5-1) cannot hold, because the matrices A and B would have their traces in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$. This follows from the factorization

$$Pol_q(x) =$$
$$\Big(x^2 - (\frac{a_q + \sqrt{\Delta_{Q_q}}}{2})x + q\Big)\Big(x^2 - (\frac{a_q - \sqrt{\Delta_{Q_q}}}{2})x + q\Big).$$

Then, again using $Pol_3(x)$, we prove the following theorem without using Serre's conjecture:

Theorem 5.10. *The images of the Galois representations on the ℓ-division points of A_2 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every} \quad \ell > 3 \quad \textit{with} \quad \left(\frac{5}{\ell}\right) = -1.$$

Observe that we have obtained an unconditional result that is stronger than the one in [LeD 98], because it only uses the condition on one of the discriminants (thus, it applies to more primes). We warn the reader that there is a mistake in [Le Duff 98], page 521; the polynomial Pol_{11} corresponding to this example is wrongly computed. It should read:

$$x^4 + 7x^3 + 31x^2 + 77x + 121.$$

5.2 Unconditional Results in the General Case

We will show now that even in the case that the condition of Proposition 5.1 is not verified at any prime, we can obtain similar unconditional results. In an arbitrary example, if we do not use Serre's conjecture, there is another case to consider (in addition to case (5-1)):

$$G_\ell \subseteq \{M \in \mathrm{GL}(2, \mathbb{F}_{\ell^2}) : \det(M) = \chi\}. \tag{5–2}$$

The inclusion of this group in $\mathrm{GSp}(4, \mathbb{F}_\ell)$ is given by the map: $M \to \mathrm{diag}(M, M^{\mathrm{Frob}})$, where Frob is the nontrivial element in $\mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$.

Two tricks allow us to discard this case:

(i) Suppose that for a prime q, $Pol_q(x)$ decomposes over $\mathbb{Q}$ as follows:

$$Pol_q(x) = (x^2 + Ax + q)(x^2 + Bx + q), \quad A \neq B.$$

Then case (5-2) cannot hold if $\ell \nmid B - A$ and $\ell \neq q$.

(ii) Suppose that $p^{2k+1} \parallel \mathrm{cond}(A)$, then for every $\ell \nmid p\Phi(p)$, case (5-2) cannot hold. The condition on ℓ is imposed to ensure that for these ℓ $p^{2k+1} \parallel \mathrm{cond}(\bar{\rho}_\ell)$ also holds.

Example 5.11. (Smart.) The following curve is taken from the list given in [Smart 97] of all genus 2 curves defined over $\mathbb{Q}$ with good reduction away from 2:

$$C_3: \quad y^2 = x(x^4 + 32x^3 + 336x^2 + 1152x - 64),$$

$A_3 = J(C_3)$, $c \mid 2^{20}$ (this is the uniform bound for the 2-part of the conductor of abelian surfaces over $\mathbb{Q}$, [Brumer and Kramer 94]). Le Duff's method cannot be applied to this example; the condition of Proposition 5.1 is not verified at 2.

We eliminate ALL maximal proper subgroups in Mitchell's classification using the characteristic polynomials $Pol_p(x)$ for several primes p and $\mathrm{cond}(\varepsilon) \mid 1024$, $S = \{1024\}$, with the algorithm described in Section 3.

To be more precise, the reducible cases treated in Section 3.1 and 3.2 are excluded using the polynomials $Pol_p(x)$ for $p = 3, 17, 19, 31$. Assuming Serre's conjecture, the remaining reducible case is excluded using the polynomials $Pol_p(x)$ for $p = 7, 11, 13$. The cases considered in Sections 3.4 and 3.5 are excluded using the polynomials $Pol_p(x)$ for $p = 3, 5$. Finally, with the technique described in Section 3.7, we check that $\ell = 5, 7$ are nonexceptional. All characteristic polynomials used are listed in Section 6.
After these computations we find no exceptional primes.

Theorem 5.12. *Assume Serre's conjecture* (3.2.4?) ([Serre 87]). *Then the images of the Galois representations on the ℓ-division points of A_3 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every } \ell > 3.$$

Without Serre's conjecture, trick (i) is used to discard case (5-2). In fact, $Pol_5(x)$ decomposes as in (i) with $A = -2$ and $B = 0$. The same happens to $Pol_{17}(x)$. To deal with case (5-1), we check that $Pol_3(x)$ is irreducible and $\Delta_{Q_3} = 12$ (see Section 6). We obtain the unconditional result:

Theorem 5.13. *The images of the Galois representations on the ℓ-division points of A_3 are*

$$G_\ell = \mathrm{GSp}(4, \mathbb{F}_\ell), \quad \textit{for every} \quad \ell > 3 \quad \textit{with} \quad \left(\frac{3}{\ell}\right) = -1.$$

5.3 Further Examples

In [Leprévost 91], Leprévost gives a genus 2 curve over $\mathbb{Q}(t)$ with 13-rational torsion. For $t = 13$ we obtain:

$$C: \ y^2 = -4x^5 + 300x^4 - 1404x^3 + 5408x^2 - 8788x + 28561,$$

$A = J(C)$ has $\mathrm{cond}(A) = 2^a \cdot 13^3 \cdot 5^2 \cdot 17^2$. Le Duff's condition is not verified at any prime. We can determine the image as in the previous example, with or without assuming Serre's conjecture (in the "reducible case with 1-dimensional constituent," we find $\ell = 13$ an exceptional prime).

Remark 5.14. Here trick (ii) eliminates case (5-2) for every $\ell \neq 13$ because

$$13^3 \parallel \mathrm{cond}(A) \quad \text{and} \quad \Phi(13) = 13.$$

Brumer and Kramer (unpublished) have given examples of Jacobians of genus 2 curves with prime conductor. For them, our algorithm determines the image with just a few computations. For instance, when applying Serre's conjecture, no computation is necessary because we have $S = \{1\}$ and $S_2(1) = 0$.

One of these examples is given by the Jacobian of the genus two curve:

$$C: \quad y^2 = x(x^2+1)(1729x^3 + 45568x^2 + 25088x - 76832).$$

The conductor of $J(C)$ is 709.

Remark 5.15. All the examples of abelian surfaces considered in this article verify the condition $\mathrm{End}(A) = \mathbb{Z}$. This follows in particular from our result on the images of the attached Galois representations (the condition on the endomorphism algebra is also necessary for this result to hold).

p	a_p	b_p
3	-3	6
7	-2	6
11	-4	18
13	-5	16
17	0	22
19	-6	42
97	6	154
113	18	250
229	24	534
257	15	148
569	6	-118
641	12	-266
769	-6	402

TABLE 1. Abelian surface A (Section 4).

6. COMPUTED CHARACTERISTIC POLYNOMIALS

We list all the characteristic polynomials $Pol_p(x)$ that have been used in the examples of the abelian surface A in Section 4 and the abelian surfaces A_2 and A_3 in Section 5.

Recall that in any case the polynomial $Pol_p(x)$ is of the form

$$x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2,$$

so it is enough to give the values a_p, b_p.

p	a_p	b_p
3	-3	7
5	-5	15
17	-3	16
97	-8	86
257	-11	-113
11	-7	31
41	-7	72
79	7	75
101	-8	-16
199	25	338
211	-17	103
281	1	148

(a)

p	a_p	b_p
3	2	4
5	2	10
7	-2	2
11	-2	12
13	-6	18
17	4	22
19	-2	-4
31	4	46

(b)

TABLE 2. (a) Abelian surface $A_2 = J(C_2)$ (Section 5.1); (b) Abelian surface $A_3 = J(C_3)$ (Section 5.2).

ACKNOWLEDGMENTS

I want to thank N. Vila, A. Brumer, and J-P. Serre for useful remarks and comments. This work was supported by TMR – Marie Curie Fellowship ERBFMBICT983234.

REFERENCES

[Blasius and Ramakrishnan] D. Blasius and D. Ramakrishnan. “Maass Forms and Galois Representations,” in *Galois Groups over* $\mathbb{Q}$, edited by Y. Ihara, K. Ribet, and J-P. Serre, pp. 33–78, MSRI Publications. New York: Springer-Verlag, 1989.

[Brumer and Kramer 94] A. Brumer and K. Kramer. “The Conductor of an Abelian Variety.” *Compositio Math.* 92 (1994), 227–248.

[Brumer and Kramer 01] A. Brumer and K. Kramer. “Non-Existence of Certain Semistable Abelian Varieties.” Preprint, 2001.

[Blichfeldt 19] H. Blichfeldt. *Finite Collineation Groups.* Chicago: University of Chicago Press, 1917.

[Deligne 71] P. Deligne. *Formes modulaires et représentations* ℓ*-adiques,* pp. 139–172, Lect. Notes in Mathematics 179. Berlin-Heidelberg: Springer-Verlag, 1971.

[Dickson 01] L. Dickson. “Canonical Forms of Quaternary Abelian Substitutions in an Arbitrary Galois Field.” *Trans. Amer. Math. Soc.* 2 (1901), 103–138.

[Hirschfeld 85] J. Hirschfeld. *Finite Projective Spaces of Three Dimensions.* Oxford: Clarendon Press, 1985.

[Leprévost 91] F. Leprévost. “Famille de courbes de genre 2 munies d’une classe de diviseurs rationnels d’ordre 13.” *C. R. Acad. Sci. Paris* 313 Série I (1991), 451–454.

[Le Duff 98] P. Le Duff. “Représentations Galoisiennes associées aux points d’ordre ℓ des jacobiennes de certaines courbes de genre 2.” *Bull. Soc. Math. France* 126 (1998), 507–524.

[Liu 94] Q. Liu. “Conducteur et discriminant minimal de courbes de genre 2.” *Compositio Math.* 94 (1994), 51–79.

[Mitchell 14] H. Mitchell. “The Subgroups of the Quaternary Abelian Linear Group.” *Trans. Amer. Math. Soc.* 15 (1914), 379–396.

[Ostrom 77] T. Ostrom. “Collineation Groups whose Order is Prime to the Characteristic.” *Math. Z.* 156 (1977), 59–71.

[Raynaud 74] M. Raynaud. “Schémas en groupes de type $(p, ..., p)$.” *Bull. Soc. Math. France* 102 (1974), 241–280.

[Ribet 75] K. A. Ribet. “On ℓ-adic Representations Attached to Modular Forms.” *Invent. Math.* 28 (1975), 245–275.

[Ribet 85] K. A. Ribet. “On ℓ-adic Representations Attached to Modular Forms II.” *Glasgow Math. J.* 27 (1985), 185–194.

[Ribet 97] K. A. Ribet. “Images of Semistable Galois Representations.” *Pacific J. of Math.* 181 (1997), 277–297.

[Serre 68] J-P. Serre. *Abelian* ℓ*-adic Representations and Elliptic Curves*, San Francisco: Benjamin, 1968.

[Serre 72] J-P. Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques.” *Invent. Math.* 15 (1972), 259–331.

[Serre 86] J-P. Serre. *Oeuvres*, Vol. 4, pp. 1–55. Berlin: Springer-Verlag, 2000.

[Serre 87] J-P. Serre. “Sur les reprsentations modulaires de degr 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$).” *Duke Math. J.* 54 (1987), 179–230.

[Smart 97] N. P. Smart. “S-unit Equations, Binary Forms and Curves of Genus 2.” *Proc. Lond. Math. Soc., III.* Ser. 75, 2 (1997), 271–307.

[Stein 00] W. Stein. “Hecke: The Modular Forms Calculator.” Available from World Wide Web: (http://modular.fas.harvard.edu/Tables/index.html), 2000.

Luis V. Dieulefait, Centre de Recerca Matemàtica, Apartat 50, E-08193 Bellaterra, Barcelona, Spain (luisd@mat.ub.es)

Received May 29, 2001; accepted in revised form June 21, 2002.