MATHEMATICS OF COMPUTATION
Volume 89, Number 321, January 2020, Pages 387–394
https://doi.org/10.1090/mcom/3434
Article electronically published on April 1, 2019

SOME MODULAR ABELIAN SURFACES

FRANK CALEGARI, SHIVA CHIDAMBARAM, AND ALEXANDRU GHITZA

Abstract. In this note, we use the main theorem of Boxer, Calegari, Gee, and Pilloni in *Abelian surfaces over totally real fields are potentially modular* (arXiv:1812.09269, 2018) to give explicit examples of modular abelian surfaces A with $\mathrm{End}_{\mathbf{C}} A = \mathbf{Z}$ and A smooth outside 2, 3, 5, and 7.

1. Introduction

Let $C/\mathbf{Q}$ be a smooth projective curve of genus g. Let $\Gamma_{\mathbf{C}}(s) = (2\pi)^{-s}\Gamma(s)$.[1] Associated to C and its Jacobian $A = \mathrm{Jac}(C)$ is a completed L-function

$$\Lambda(C, s) = \Gamma_{\mathbf{C}}(s)^g \prod_p L_p(C, p^{-s})^{-1},$$

where, for any $\ell \neq p$, $L_p(C, T) = \det\left(I_{2g} - T \cdot \mathrm{Frob}_p \mid H^1_{\mathrm{et}}(C, \mathbf{Q}_\ell)^{I_p}\right)$. We say that C is automorphic if $\Lambda(C, s) = \Lambda(\pi, s)$, where π is an automorphic form for $\mathrm{GL}_{2g}(\mathbf{Q})$, and $\Lambda(\pi, s)$ is the completed L-function associated to the standard representation of GL_{2g}. If C is automorphic, then

$$\Lambda(C, s) = \pm N^{1-s}\Lambda(C, 2 - s),$$

where N is the conductor of A. One conjectures that all smooth projective curves C over $\mathbf{Q}$ are automorphic. When $g = 0$ and $g = 1$, one knows that C is automorphic by theorems of Riemann [Rie59] and Wiles et al. [Wil95, TW95, BCDT01], respectively. The conjecture seems completely hopeless with current technology for general curves when $g \geq 3$, but for $g = 2$ it was recently proved in [BCGP18] that all such curves over $\mathbf{Q}$ (and even over totally real fields) were potentially automorphic. For abelian surfaces over $\mathbf{Q}$, let us additionally say that $A = \mathrm{Jac}(C)$ is *modular* of level N if there exists a cuspidal Siegel modular form f of weight two such that $\Lambda(C, s) = \Lambda(f, s)$, where $\Lambda(f, s)$ is the completed L-function associated to the degree four spin representation of GSp_4. If A is modular in this sense, then it is also automorphic in the sense above by taking π to be the transfer of the automorphic representation associated to f from $\mathrm{GSp}(4)/\mathbf{Q}$ to $\mathrm{GL}(4)/\mathbf{Q}$. It was also shown in [BCGP18] that certain classes of abelian surfaces over $\mathbf{Q}$ were actually modular (see Theorem 1.1 below), and even that there were infinitely many modular abelian surfaces over $\mathbf{Q}$ up to twist with $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$. However, no explicit examples of such surfaces were given in that paper.

Received by the editor November 4, 2018, and, in revised form, February 5, 2019.
2010 *Mathematics Subject Classification.* Primary 11G10, 11F46; Secondary 11Y40, 11F80.
The first author was supported in part by NSF Grant DMS-1701703.

[1] There is some ambiguity in the literature as to whether one defines $\Gamma_{\mathbf{C}}(s)$ to be $(2\pi)^{-s}\Gamma(s)$ or $\Gamma_{\mathbf{R}}(s)\Gamma_{\mathbf{R}}(s+1) = 2 \cdot (2\pi)^{-s}\Gamma(s)$. It makes no difference as long as one uses the same choice for both $\Lambda(C, s)$ and $\Lambda(\pi, s)$. To be safe, we make the same choice as Serre [Ser70, §3(20)].

The aim of this note is to give explicit examples of modular abelian surfaces $A/\mathbf{Q}$ with $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$ and such that A has good reduction outside a set S that is either $S = \{2, 5\}$, $S = \{2, 5, 7\}$, or $S = \{2, 3, 7\}$. Previous explicit examples of modular abelian surfaces with trivial endomorphisms were found by [BPP+18] (in 2015) and also by [BK17]; these results relied heavily on very delicate and explicit computations of spaces of low weight Siegel modular forms following [PY15, PSY17]. In particular, they rely on the conductor being relatively small and also take advantage of the fact that the conductor is odd and squarefree. (The examples in those papers are of conductors 277, 353, 587, and $731 = 17 \cdot 43$.) In contrast, the examples of this paper only require verifying some local properties of A at the prime p (with $p = 3$ or $p = 5$) and showing that the image of the action of $G_{\mathbf{Q}}$ on the p-torsion of $A = \mathrm{Jac}(C)$ is of a suitable form. Although the conductors of our examples have only small factors, the conductors themselves are quite large—the smallest of our examples has conductor $98000 = 2^4 \cdot 5^3 \cdot 7^2$. The modularity of the examples in this paper follows by applying the following result (with either $p = 3$ or $p = 5$) proved in [BCGP18, Propositions 10.1.1 and 10.1.3].

Theorem 1.1. *Let $A/\mathbf{Q}$ be an abelian surface with good ordinary reduction at $v|p$ and a polarization of degree prime to p, and suppose that the eigenvalues of Frobenius on $A[p](\overline{\mathbf{F}}_p)$ are distinct. Let*

$$\overline{\rho}_{A,p} : G_F \to \mathrm{GSp}_4(\mathbf{F}_p)$$

denote the mod-p Galois representation associated to $A[p]$, and assume that $\overline{\rho}_{A,p}$ has vast and tidy image in the notation of [BCGP18]. Suppose that either:

1. *$p = 3$, and $\overline{\rho}_{A,3}$ is induced from a 2-dimensional representation over a real quadratic extension $F/\mathbf{Q}$ in which 3 is unramified; or*
2. *$p = 5$, and $\overline{\rho}_{A,5}$ is induced from a 2-dimensional representation valued in $\mathrm{GL}_2(\mathbf{F}_5)$ over a real quadratic extension $F/\mathbf{Q}$ in which 5 is unramified.*

Then A is modular.

A precise definition of what representations are vast and tidy is included in §7.5 of [BCGP18], but we content ourselves with the following list which exhausts all of our examples.

Lemma 1.2 (Examples of vast and tidy representations from [BCGP18, Lemmas 7.5.13 and 7.5.21])**.** *The representation $\overline{\rho}_{A,p}$ is automatically vast and tidy when the image of $\overline{\rho}_{A,p}$ is one of the following conjugacy classes of subgroups of $\mathrm{GSp}_4(\mathbf{F}_p)$:*

1. *The groups G_{2304}, G_{768}, G'_{768}, or G_{480} in $\mathrm{GSp}_4(\mathbf{F}_3)$ of orders 2304, 768, 768, and 480, where:*
   (a) *The group G_{2304} is a semidirect product $\Delta \rtimes \mathbf{Z}/2\mathbf{Z}$, where*

$$\Delta = \left\{(A, B) \in \mathrm{GL}_2(\mathbf{F}_3)^2 \mid \det(A) = \det(B)\right\};$$

   it is (up to conjugacy) the unique subgroup of order 2304 of $\mathrm{GSp}_4(\mathbf{F}_3)$.

(b) *The groups* G_{768} *and* G'_{768} *are subgroups of* G_{2304} *of index* 3, *and are (up to conjugacy) the only two subgroups of order* 768 *of* $\mathrm{GSp}_4(\mathbf{F}_3)$. *They are isomorphic as abstract groups, but they are distinguished up to conjugacy inside* $\mathrm{GSp}_4(\mathbf{F}_3)$ *by their intersections* H_{384} *and* H'_{384} *with* $\mathrm{Sp}_4(\mathbf{F}_3)$. *In particular,* $(H_{384})^{\mathrm{ab}} \simeq \mathbf{Z}/6\mathbf{Z}$ *and* $(H'_{384})^{\mathrm{ab}} \simeq \mathbf{Z}/2\mathbf{Z}$. *According to the small groups database of* `magma` *(cf.* [BEO02]*),*

$$G_{768} \simeq G'_{768} \simeq \texttt{SmallGroup(768,1086054)},$$

whereas

$$H_{384} \simeq \texttt{SmallGroup(384, 18130)}, \quad H'_{384} \simeq \texttt{SmallGroup(384, 618)}.$$

These groups can also be distinguished by their images P_{192} *and* P'_{192} *in* $\mathrm{PSp}_4(\mathbf{F}_3) \subset \mathrm{PGSp}_4(\mathbf{F}_3)$, *namely*

$$P_{192} \simeq \texttt{SmallGroup(192, 1493)}, \quad P'_{192} \simeq \texttt{SmallGroup(192, 201)}.$$

(c) *The group* G_{480} *is a semidirect product* $\widetilde{A}_5 \rtimes \langle\sigma\rangle$, *where* $\widetilde{A}_5 \subset \mathrm{GL}_2(\mathbf{F}_9)$ *is a central extension of* A_5 *by* $\mathbf{Z}/4\mathbf{Z}$. *There are precisely two subgroups of this order up to conjugacy in* $\mathrm{GSp}_4(\mathbf{F}_3)$. *The second subgroup* G'_{480} *also contains* $\widetilde{A}_5$ *with index two, but it is not a semidirect product. According to the small groups database of* `magma`,

$$G_{480} \simeq \texttt{SmallGroup(480, 948)}, \quad G'_{480} \simeq \texttt{SmallGroup(480, 947)}.$$

(2) *The group* G_{115200} *in* $\mathrm{GSp}_4(\mathbf{F}_5)$ *is a semidirect product* $\Delta \rtimes \mathbf{Z}/2\mathbf{Z}$, *where*

$$\Delta = \left\{(A, B) \in \mathrm{GL}_2(\mathbf{F}_5)^2 \mid \det(A) = \det(B)\right\};$$

it is (up to conjugacy) the unique subgroup of order 115200 *of* $\mathrm{GSp}_4(\mathbf{F}_5)$.

The conditions of the theorem are all very easy to verify in any given example (once found) with the possible exception of computing the image of the mod-p representation for $p = 3$ or 5. We describe how we computed this in the section below. The second problem is then to find a list of candidate curves. Our original approach involved searching for curves in a large box, which did indeed result in a number of examples. However, we then switched to using a collection of curves provided to us by Andrew Sutherland, all of which had the property that they had good reduction outside the set $\{2, 3, 5, 7\}$ (these were found during the construction of [BSS+16] but discarded because their minimal discriminants were too large). This list consisted of some 20 million curves, so the next task was to identify examples to which we could apply Theorem 1.1. For a genus two curve C on Sutherland's list, we applied the following algorithm:

(1) Fix a real quadratic field F of fundamental discriminant D dividing Δ_C in which $p \in \{3, 5\}$ is unramified. Since Δ_C is only divisible by primes in $\{2, 3, 5, 7\}$, there are at most seven such F. Let χ_D denote the quadratic character associated to F.
(2) Check whether $a_q \equiv 0 \mod p$ for all primes $q \leq 100$ of good reduction for C with $\chi_D(q) = -1$.
(3) Check that $a_q \neq 0$ for at least one prime $q \leq 100$ of good reduction for C with $\chi_D(q) = -1$.

Any C that passes this test is likely to have the following two properties: $\overline{\rho}_{A,p}$ is induced from F, but the p-adic representation $\rho_{A,p}$ itself is not induced. The third condition in particular guarantees that A itself is not isogenous to a base

change of an elliptic curve defined over F. Note that this test is very fast—one can discard a C as soon as one finds a prime q with $\chi_D(q) = -1$ and $a_q \not\equiv 0 \mod p$, so for almost all curves C, one only has to compute a_q for very small primes q. In addition, the following postage stamp calculation with the Chebotarev density theorem suggests that false positives will be few in number: for each of the allowable discriminants D (there are seven such D for either $p = 3$ or $p = 5$), there are at least $M \geq 10$ primes in the interval $[10, 100]$ with $\chi_D(q) = -1$. A "random" abelian surface A will have $a_q \equiv 0 \mod p$ for any such prime q approximately $1/p$ of the time (the exact expectation depends on $A[p]$—if the mod-p representation is surjective, the exact expectation that $a_q \equiv 0 \mod p$ for a random prime q is 231/640 for $p = 3$ and 3095/14976 for $p = 5$), and so one might expect a false positive to occur with probability approximately $1/p^M$. On the other hand, false positives are certainly not impossible. In our original box search, we did find the one curve $C : y^2 = x^5 - 2x^4 + 6x^3 + 5x^2 + 10x + 5$ that "passed" the test for $\overline{\rho}_{A,3}$ to be induced from $\mathbf{Q}(\sqrt{7})$, whereas it turns out instead to be induced from $\mathbf{Q}(\sqrt{85})$—requiring only an accidental vanishing of a_q for $q = 23$, 73, 89, and 97. The smallest prime guaranteeing that $\overline{\rho}_{A,3}$ is not induced from $\mathbf{Q}(\sqrt{7})$ in this case is $a_{151} = 5 \not\equiv 0 \mod 3$.

2. Determining the mod-p representation

Consider a genus two curve

$$C : Y^2 = f(X),$$

with $\deg(f) = 6$. The desingularization of the corresponding projective curve has two points $\mathfrak{b}_1$ and $\mathfrak{b}_2$ at infinity. The canonical class $\mathfrak{O}$ in $\mathrm{Pic}^2(C)$ is represented by the divisor $\mathfrak{b}_1 + \mathfrak{b}_2$, and the Jacobian $A = \mathrm{Jac}(C)$ can be identified with $\mathrm{Pic}^2(C)$ under addition of the canonical class. By Riemann–Roch, every class in $\mathrm{Pic}^2(C)$ except $\mathfrak{O}$ has precisely one effective divisor. Thus, we may represent any point of A as an unordered pair $\{P, Q\}$ of points on C.

If we assume $f(X)$ has a rational root, then, by suitably transforming the variables X and Y, we can make $\deg(f) = 5$; then, there will be exactly one point $\mathfrak{b}$ at infinity, and the canonical class will be represented by $2\mathfrak{b}$. We will not need this assumption, however, and several of our examples do not have any Weierstrass points over $\mathbf{Q}$.

2.1. $p = 3$**.** Let $K/\mathbf{Q}$ denote the Galois closure of the corresponding projective representation. It will contain the field $\mathbf{Q}(x + u, xu, yv)$ for any 3-torsion point $\{P, Q\}$ of A, where $P = (x, y)$ and $Q = (u, v)$. There exist polynomials B_{ij}, given in [CF96, Theorem 3.4.1 and Appendix II], using which the multiplication-by-n map can be described explicitly at the level of the Kummer surface of A. Writing the equation $[2]\{P, Q\} = -\{P, Q\}$ in terms of the Kummer coordinates explicitly, taking resultants, and eliminating spurious solutions, one can compute the minimal polynomials of $x + u$, xu, and yv in any particular case, as well as determine the Galois group of the corresponding extension.

Note that the first coordinates determine the $\mathrm{GSp}_4(\mathbf{F}_3)/\langle \pm 1 \rangle = \mathrm{PGSp}_4(\mathbf{F}_3)$-representation, so this determines the image of $\overline{\rho}_{A,3}$ modulo the central subgroup of order 2 as an abstract group. One can similarly compute the field $\mathbf{Q}(y + v, yv)$ if one wants to know the full $\mathrm{GSp}_4(\mathbf{F}_3)$-representation. In any case of interest, this is enough (purely by considering possible orders) to determine the order of the image

of $\overline{\rho}_{A,3}$ itself. It then remains to determine the precise subgroup of $\mathrm{GSp}_4(\mathbf{F}_3)$ in the cases where this is ambiguous. The group $\mathrm{PGSp}_4(\mathbf{F}_3)$ has a natural permutation representation on 40 points, corresponding to the non-zero points of $A[3]$ up to sign (warning: the group $\mathrm{PGSp}_4(\mathbf{F}_3)$ has a second non-conjugate representation on 40 points). From this data, one can distinguish between G_{480} and G'_{480} purely based on the degrees of the polynomials arising from the computation above. The following table gives the corresponding decomposition in the cases of interest:

G	Orbits
G_{2304}	8, 32
G_{768}	8, 32
G'_{768}	8, 32
G_{480}	20, 20
G'_{480}	40

The groups G_{768} and G'_{768} cannot be distinguished by this method. This is not important for establishing modularity since both groups give representations with vast and tidy image. However, in order to complete the tables, we distinguish between these cases as follows: we *explicitly* compute (using `magma`) the Galois group of the corresponding degree 32 polynomial over the field $\mathbf{Q}(\sqrt{-3})$, and see whether the resulting group is P_{192} or P'_{192} (in which case the group is G_{768} or G'_{768}, respectively).

2.2. $p = 5$**.** Similar to the $p = 3$ case, for an arbitrary point $\{P = (x, y), Q = (u, v)\}$ of A, we write the equation $3\{P, Q\} = -2\{P, Q\}$ in terms of the Kummer coordinates of the point, and take resultants to find the minimal polynomials of $x + u, xu$, and yv of 5-torsion points on A. The splitting field of these polynomials is the Galois closure $K/\mathbf{Q}$ of the representation to $\mathrm{PGSp}_4(\mathbf{F}_5) = \mathrm{GSp}_4(\mathbf{F}_5)/\langle\pm 1\rangle$.

We describe an algorithm for showing that the image $\overline{\rho}_{A,5}$ of a mod-5 representation in $\mathrm{GSp}_4(\mathbf{F}_5)$ with cyclotomic determinant has image G_{115200}. The group $\mathrm{GSp}_4(\mathbf{F}_5)$ has a representation on $312 = (5^4-1)/2$ points, given by the action on the non-trivial 5-torsion points up to sign (which factors through $\mathrm{PGSp}_4(\mathbf{F}_5)$).

Lemma 2.3. *Let $G \subset \mathrm{GSp}_4(\mathbf{F}_5)$ be a subgroup, and suppose that the similitude character is surjective on G, or equivalently that $[G : G \cap \mathrm{Sp}_4(\mathbf{F}_5)] = 4$. Suppose, in addition, that G acts on the degree 312 permutation representation above with two orbits of size 288 and 24, respectively. Then:*

(1) *G is one of four groups, distinguished by their orders: 2304, 4608, 57600, and 115200.*
(2) *The degree 24 permutation representation of G factors through a group of order 576, 1152, 14400, and 28800, respectively.*

In particular, we can distinguish these representations by computing the Galois group of the factor of size 24. Hence by computing the corresponding polynomials of order 24 and 288 we can verify that the image is indeed G_{115200}.

2.4. **Checking the Sato–Tate group.** For all the residual representations we consider, it turns out that the image of $\overline{\rho}$ is big enough to guarantee that the Sato–Tate group is either $\mathrm{USp}(4)$ or the normalizer of $\mathrm{SU}(2) \times \mathrm{SU}(2)$. More precisely:

Lemma 2.5. *Suppose that $p = 3$ and that $\overline{\rho}_{A,p}$ has image either G_{480}, G_{768}, G'_{768}, G_{2304}, or that $p = 5$ and $\overline{\rho}_{A,p}$ has image G_{115200}. Then the Sato–Tate group*

of A is either $\mathrm{USp}(4)$ *or* $N(\mathrm{SU}(2)\times\mathrm{SU}(2))$. *Moreover, if the Sato–Tate group is* $N(\mathrm{SU}(2)\times\mathrm{SU}(2))$, *the quadratic extension* $F/\mathbf{Q}$ *over which* A *has Sato–Tate group* $\mathrm{SU}(2)\times\mathrm{SU}(2)$ *is the quadratic field* F *from which* $\overline{\rho}$ *is induced.*

Proof. The image of $\overline{\rho}_{A,p}$ is constrained by the Sato–Tate group, and thus the fact that the Sato–Tate group can only be $\mathrm{USp}(4)$ or $N(\mathrm{SU}(2)\times\mathrm{SU}(2))$ follows directly from a classification of all such groups in [FKRS12]. (In fact, when the image is G_{480}, only the first case can occur.) In the latter case, the representation becomes reducible over the quadratic extension F, where A has Sato–Tate group $\mathrm{SU}(2)\times\mathrm{SU}(2)$, and (for the given $\overline{\rho}$) this forces F to be the field from which $\overline{\rho}$ is induced. □

In particular, in all our examples, our initial selection process requires the existence of a prime q of good reduction with $\chi(q)=-1$ and $a_q\neq 0$, which implies that $\rho_{A,p}$ cannot be induced from F, and thus the Sato–Tate group in each example below is $\mathrm{USp}(4)$.

3. Examples

Of the curves we consider, a number satisfy the conditions of the main theorem, and are thus provably modular. For any curve C that is modular, so too are any quadratic twists. Hence we only list a single representative curve for each equivalence class of abelian surfaces under both $\mathbf{Q}$-isogenies and twisting by quadratic characters.

3.1. **Inductions from $\mathrm{GL}_2(\mathbf{F}_3)$ and $\mathrm{GL}_2(\mathbf{F}_9)$.** We first give the examples of modular curves whose mod-3 representation is induced from either $\mathrm{GL}_2(\mathbf{F}_3)$ or $\mathrm{GL}_2(\mathbf{F}_9)$-representations of G_F for real quadratic fields F. It turns out that, in the range of our computation, the representation $\overline{\rho}$ up to twist determined the representation ρ up to twist—after applying our other desiderata, including that $A/\mathbf{Q}$ had good reduction at p and had Sato–Tate group $\mathrm{USp}(4)$. In particular, all the examples below give rise to mod-3 representations that are not twist equivalent. The examples C we choose to list are of minimal conductor amongst all those with Jacobian isogenous to a twist of $\mathrm{Jac}(C)$. The conductors were computed rigorously away from 2 using `magma`. The conductors at 2 were computed for us by Andrew Sutherland using an analytic algorithm discussed in §5.2 of [BSS+16]. This computation *assumes* the analytic continuation and functional equation for $L(A,s)$, which we know to be true in this case. (More precisely, as explained to us by Andrew Booker, one version of this program gives a non-rigorous computation of these conductors and a second slower but more rigorous version then confirms these values.) In the case of ties, we chose the curve with smaller minimal discriminant. In the case of subsequent ties, we eyeballed the different forms and chose the one that looked the prettiest.

Theorem 3.2. *The Jacobians* $A=\mathrm{Jac}(C)$ *of the following smooth genus two curves* C *over* $\mathbf{Z}[1/70]$ *are modular. In particular, the* L*-function* $L(A,s)$ *is holomorphic in* $\mathbf{C}$ *and satisfies the corresponding functional equation. Each* A *has good ordinary reduction at* 3 *and is* 3*-distinguished and* $\mathrm{End}_{\mathbf{C}}(A)=\mathbf{Z}$. *Moreover, the representation* $\overline{\rho}_{A,3}$ *is induced from a* $\mathrm{GL}_2(\overline{\mathbf{F}}_3)$*-valued representation of* G_F *that is vast and tidy.*

Curve	*Cond*	*Disc*	$\mathrm{im}(\overline{\rho})$	Δ_F
$y^2 = x^6 - 10x^4 + 2x^3 + 31x^2 - 13x - 18$	$2^4 5^3 7^2$	$2^8 5^3 7^3$	G_{480}	5
$y^2 = -5x^6 - 20x^5 - 10x^4 + 36x^3 + 22x^2 - 20x$	$2^{10} 5^3 7$	$2^{20} 5^4 7^3$	G'_{768}	5
$y^2 + y = -4x^5 - 23x^4 - 22x^3 + 74x^2 - 40x + 6$	$2^8 5^3 7^2$	$2^{19} 5^7 7^2$	G_{2304}	5
$y^2 = 16x^6 - 46x^4 + 10x^3 + 46x^2 - 9x - 17$	$2^{12} 5^2 7^4$	$2^{19} 5^9 7^4$	G_{480}	5
$y^2 = 2x^5 - 8x^4 + 26x^2 - 7x - 26$	$2^{15} 5$	$2^{16} 5^3$	G_{2304}	8
$y^2 = x^5 - x^4 - 4x^3 - 44x^2 - 60x - 100$	$2^{14} 5 \cdot 7$	$2^{33} 5^3 7$	G_{2304}	8
$y^2 = x^5 - 17x^4 + 70x^3 + 26x^2 - 35x - 29$	$2^{16} 5 \cdot 7$	$2^{37} 5^3 7$	G_{2304}	8
$y^2 + x^2 y = 13x^6 - 29x^5 - 10x^4 + 41x^3 + 6x^2 + 20x + 20$	$2^7 5^2 7^4$	$2^{16} 5^2 7^{16}$	G_{2304}	8
$y^2 = x^5 - 11x^4 - 2x^3 - 34x^2 - 5x - 25$	$2^{20} 5 \cdot 7$	$2^{21} 5^3 7^3$	G_{768}	8
$y^2 = -2x^6 - 41x^5 - 48x^4 + 54x^3 + 42x^2 - 49x$	$2^{14} 5^2 7^4$	$2^{32} 5^2 7^{11}$	G_{2304}	8
$y^2 = 2x^5 + 34x^4 - 16x^3 - 52x^2 - 13x - 1$	$2^{19} 5^3 7^2$	$2^{20} 5^5 7^6$	G'_{768}	8
$y^2 = 8x^6 - 24x^5 - 4x^4 + 20x^3 + 49x^2 - 21x - 28$	$2^{15} 5^2 7^4$	$2^{23} 5^6 7^9$	G_{2304}	8
$y^2 + (x+1)y = 64x^5 - 8x^4 + 39x^3 + x^2 + 2x + 1$	$2^7 5^3 7^3$	$2^{27} 5^6 7^6$	G_{480}	40
$y^2 = 15x^5 + 23x^4 + 20x^3 + 28x^2 + 12x - 4$	$2^{14} 3 \cdot 5^3$	$2^{33} 3^2 5^4$	G_{2304}	40
$y^2 = 3x^5 + 7x^4 + 28x^3 + 20x^2 + 28x - 36$	$2^{14} 3 \cdot 5^3$	$2^{36} 3^2 5^4$	G_{2304}	40

Example 3.3. Precisely one curve in this table is actually smooth over a smaller ring, namely the curve of conductor $163840 = 2^{15} \cdot 5$ which is smooth over $\mathbf{Z}[1/10]$. This curve has a quadratic twist with particularly small naïve height, namely the curve

$$y^2 = 4x^5 + 6x^4 + 4x^3 + 6x^2 + 2x + 3$$

which also has conductor $163840 = 2^{15} \cdot 5$ but larger minimal discriminant

$$131072000000 = 2^{23} \cdot 5^6$$

rather than $8192000 = 2^{16} \cdot 5^3$ as the curve in the table. The mod-3 representation of both of these curves is actually unramified at 5, and is congruent up to twist to the mod-3 representation attached to the curve $y^2 = 4x^5 - 4x^4 + 4x^3 - 2x^2 + x$ of conductor 2^{15}. The Jacobian of this latter curve is isogenous to $\mathrm{Res}_{\mathbf{Q}(\sqrt{2})/\mathbf{Q}}(E)$, where E is the elliptic curve

$$y^2 + \sqrt{2}xy = x^3 + (-1 - \sqrt{2})x^2 + 2(\sqrt{2} + 1)x - 3\sqrt{2} - 5.$$

3.4. **Inductions from $\mathrm{GL}_2(\mathbf{F}_5)$.** We now consider the case $p = 5$.

Theorem 3.5. *The Jacobians $A = \mathrm{Jac}(C)$ of the following smooth genus two curves C over $\mathbf{Z}[1/42]$ are modular. In particular, the L-function $L(A, s)$ is holomorphic in $\mathbf{C}$ and satisfies the corresponding functional equation. Each A has good ordinary reduction at 5 and is 5-distinguished and $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$. Moreover, the representation $\overline{\rho}_{A,5}$ is induced from a $\mathrm{GL}_2(\mathbf{F}_5)$-valued representation of G_F that is vast and tidy.*

Curve	*Cond*	*Disc*	$\mathrm{im}(\overline{\rho})$	Δ_F
$y^2 + xy = 7x^6 - 22x^5 - 7x^4 + 61x^3 - 3x^2 - 54x - 12$	$2^7 3^2 7^3$	$2^{11} 3^9 7^4$	G_{115200}	8
$y^2 = 8x^6 - 24x^5 - 30x^4 + 8x^3 - 24x^2 - 48x - 8$	$2^6 3^8 7$	$2^{51} 3^8 7$	G_{115200}	8

The second curve also admits a quadratic twist of smaller naïve height, namely

$$y^3 + x^2 y = x^6 - 3x^5 - 4x^4 + x^3 - 3x^2 - 6x - 1$$

of conductor $5878656 = 2^7 \cdot 3^8 \cdot 7$ and minimal discriminant $96315899904 = 2^{21} \cdot 3^8 \cdot 7$.

Acknowledgments

We would like to thank Andrew Booker, Andrew Sutherland, and John Voight for useful discussions about this project. We would also like to thank Andrew Sutherland for providing us with a large list of genus two curves over $\mathbf{Q}$ with good

reduction outside $\{2, 3, 5, 7\}$. Finally, we would like to thank Andrew Sutherland and Andrew Booker for help computing the 2-part of the conductors of our curves.

References

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939, DOI 10.1090/S0894-0347-01-00370-8. MR1839918

[BCGP18] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, *Abelian surfaces over totally real fields are potentially modular*, arXiv:1812.09269 [math.NT], 2018.

[BEO02] H. U. Besche, B. Eick, and E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644, DOI 10.1142/S0218196702001115. MR1935567

[BK17] T. Berger and K. Klosin, *Deformations of Saito-Kurokawa type and the Paramodular Conjecture (with an appendix by Cris Poor, Jerry Shurman, and David S. Yuen)*, arXiv:1710.10228 [math.NT], 2017.

[BPP+18] A. Brumer, A. Pacetti, C. Poor, G. Tornaría, J. Voight, and D. S. Yuen, *On the paramodularity of typical abelian surfaces*, arXiv:1805.10873 [math.NT], 2018.

[BSS+16] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, and D. Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 235–254, DOI 10.1112/S146115701600019X. MR3540958

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090

[FKRS12] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442, DOI 10.1112/S0010437X12000279. MR2982436

[PSY17] C. Poor, J. Shurman, and D. S. Yuen, *Siegel paramodular forms of weight 2 and squarefree level*, Int. J. Number Theory **13** (2017), no. 10, 2627–2652, DOI 10.1142/S1793042117501469. MR3713095

[PY15] C. Poor and D. S. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), no. 293, 1401–1438, DOI 10.1090/S0025-5718-2014-02870-6. MR3315514

[Rie59] B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsberichte der Berliner Akademie, 1859, pp. 671–680.

[Ser70] J.-P. Serre, *Facteurs locaux des fonctions zêta des varietés algébriques (définitions et conjectures)* (French), Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des Nombres. Fasc. 1: Exposés 1 à 15; Fasc. 2: Exposés 16 à 24, Secrétariat Math., Paris, 1970, pp. 15. MR3618526

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572, DOI 10.2307/2118560. MR1333036

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035

Department of Mathematics, The University of Chicago, 5734 S University Avenue, Chicago, Illinois 60637; and School of Mathematics and Statistics, University of Melbourne, Parkville, VIC, 3010, Australia

Email address: fcale@math.uchicago.edu

Department of Mathematics, The University of Chicago, 5734 S University Avenue, Chicago, Illinois 60637

Email address: shivac@uchicago.edu

School of Mathematics and Statistics, University of Melbourne, Parkville, VIC, 3010, Australia

Email address: aghitza@alum.mit.edu