

FINITENESS RESULTS FOR MODULAR CURVES OF GENUS AT LEAST 2

MATTHEW H. BAKER, ENRIQUE GONZÁLEZ-JIMÉNEZ, JOSEP GONZÁLEZ,
AND BJORN POONEN

ABSTRACT. A curve X over $\mathbb{Q}$ is modular if it is dominated by $X_1(N)$ for some N ; if in addition the image of its jacobian in $J_1(N)$ is contained in the new subvariety of $J_1(N)$, then X is called a new modular curve. We prove that for each $g \geq 2$, the set of new modular curves over $\mathbb{Q}$ of genus g is finite and computable. For the computability result, we prove an algorithmic version of the de Franchis-Severi Theorem. Similar finiteness results are proved for new modular curves of bounded gonality, for new modular curves whose jacobian is a quotient of $J_0(N)^{\text{new}}$ with N divisible by a prescribed prime, and for modular curves (new or not) with levels in a restricted set. We study new modular hyperelliptic curves in detail. In particular, we find all new modular curves of genus 2 explicitly, and construct what might be the complete list of all new modular hyperelliptic curves of all genera. Finally we prove that for each field k of characteristic zero and $g \geq 2$, the set of genus- g curves over k dominated by a Fermat curve is finite and computable.

1. INTRODUCTION

Let $X_1(N)$ be the usual modular curve over $\mathbb{Q}$; see Section 3.1 for a definition. (All curves and varieties in this paper are smooth, projective, and geometrically integral, unless otherwise specified. When we write an affine equation for a curve, its smooth projective model is implied.) A curve X over $\mathbb{Q}$ will be called *modular* if there exists a nonconstant morphism $\pi: X_1(N) \rightarrow X$ over $\mathbb{Q}$. If X is modular, then $X(\mathbb{Q})$ is nonempty, since it contains the image of the cusp $\infty \in X_1(N)(\mathbb{Q})$. The converse, namely that if $X(\mathbb{Q})$ is nonempty then X is modular, holds if the genus g of X satisfies $g \leq 1$ [10]. In particular, there are infinitely many modular curves over $\mathbb{Q}$ of genus 1. On the other hand, we propose the following:

Conjecture 1.1. *For each $g \geq 2$, the set of modular curves over $\mathbb{Q}$ of genus g is finite.*

Remark 1.2.

- (i) When we speak of the finiteness of the set of curves over $\mathbb{Q}$ satisfying some condition, we mean the finiteness of the set of $\mathbb{Q}$ -isomorphism classes of such curves.

Date: November 12, 2004.

2000 Mathematics Subject Classification. Primary 11G18, 14G35; Secondary 11F11, 11G10, 14H45.

Key words and phrases. Modular curves, modular forms, de Franchis-Severi Theorem, gonality, computability, hyperelliptic curves, automorphisms of curves.

The first author was supported in part by an NSF Postdoctoral Fellowship.

The second author was supported in part by DGICYT Grant BHA2000-0180 and a postdoctoral fellowship from the European Research Training Network “Galois Theory and Explicit Methods in Arithmetic”.

The third author was supported in part by DGICYT Grant BFM2003-06768-C02-02.

The fourth author was supported by NSF grants DMS-9801104 and DMS-0301280, and a Packard Fellowship.

This article has been published in *Amer. J. Math.* **127** (2005), 1325–1387.

- (ii) For any fixed N , the *de Franchis-Severi Theorem* (see Theorem 5.7) implies the finiteness of the set of curves over $\mathbb{Q}$ dominated by $X_1(N)$. Conjecture 1.1 can be thought of as a version that is uniform as one ascends the tower of modular curves $X_1(N)$, provided that one fixes the genus of the dominated curve.
- (iii) Conjecture 1.1 is true if one restricts the statement to quotients of $X_1(N)$ by subgroups of its group of modular automorphisms. See Remark 3.16 for details.
- (iv) If $X_1(N)$ dominates a curve X , then the jacobian $\text{Jac}X$ is a quotient of $J_1(N) := \text{Jac}X_1(N)$. The converse, namely that if X is a curve such that $X(\mathbb{Q})$ is nonempty and $\text{Jac}X$ is a quotient of $J_1(N)$ then X is dominated by $X_1(N)$, holds if the genus g of X is ≤ 1 , but can fail for $g \geq 2$. See Section 8.2 for other “pathologies.”

We remark that throughout this paper, quotients or subvarieties of varieties, and morphisms between varieties, are implicitly assumed to be defined over the same field as the original varieties. If X is a curve over $\mathbb{Q}$, and we wish to discuss automorphisms over $\mathbb{C}$, for example, we will write $\text{Aut}(X_{\mathbb{C}})$. When we refer to a “quotient of an abelian variety A ” we mean a quotient in the category of abelian varieties as opposed to, for instance, the quotient of A by the action of a finite subgroup of $\text{Aut}(A)$.

- (v) In contrast with Conjecture 1.1, there exist infinitely many genus-two curves over $\mathbb{Q}$ whose jacobians are quotients of $J_1(N)$ for some N . See Proposition 8.2(5).
- (vi) In Section 9, we use a result of Aoki [4] to prove an analogue of Conjecture 1.1 in which $X_1(N)$ is replaced by the Fermat curve $x^N + y^N = z^N$ in $\mathbb{P}^2$. In fact, such an analogue can be proved over arbitrary fields of characteristic zero, not just $\mathbb{Q}$.

We prove many results towards Conjecture 1.1 in this paper. Given a variety X over a field k , let $\Omega = \Omega_{X/k}^1$ denote the sheaf of regular 1-forms. Call a modular curve X over $\mathbb{Q}$ *new of level N* if there exists a nonconstant morphism $\pi: X_1(N) \rightarrow X$ (defined over $\mathbb{Q}$) such that $\pi^*H^0(X, \Omega)$ is contained in the new subspace $H^0(X_1(N), \Omega)_{\text{new}}$, or equivalently if the image of the homomorphism $\pi^*: \text{Jac}X \rightarrow J_1(N)$ induced by Picard functoriality is contained in the new subvariety $J_1(N)_{\text{new}}$ of $J_1(N)$. (See Section 3.1 for the definitions of $H^0(X_1(N), \Omega)_{\text{new}}$, $J_1(N)_{\text{new}}$, $J_1(N)^{\text{new}}$, and so on.) For example, it is known that every elliptic curve E over $\mathbb{Q}$ is a new modular curve of level N , where N is the conductor of E . Here the conductor $\text{cond}(A)$ of an abelian variety A over $\mathbb{Q}$ is a positive integer $\prod_p p^{f_p}$, where each exponent f_p is defined in terms of the action of an inertia subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at the prime p on a Tate module $T_{\ell}A$: for the full definition, see [51, §1], for instance. If A is a quotient of $J_1(N)^{\text{new}}$, then $\text{cond}(A) = N^{\dim A}$, by [12].

Theorem 1.3. *For each $g \geq 2$, the set of new modular curves over $\mathbb{Q}$ of genus g is finite and computable.*

The first results of this type were proved in [27], which showed that the set of new modular curves of genus 2 over $\mathbb{Q}$ is finite, and that there are exactly 149 such curves whose jacobian is $\mathbb{Q}$ -simple. Equations for these 149 curves are given in Tables 1 and 2 of [27].

Remark 1.4.

- (i) See Section 5 for the precise definition of “computable.”
- (ii) An analysis of the proof of Theorem 1.3 would show that as $g \rightarrow \infty$, there are at most $\exp((6 + o(1))g^2)$ new modular curves of genus g over $\mathbb{Q}$. Probably a much smaller bound holds, however. It is conceivable even that there is an upper bound not depending on g .

- (iii) If we consider all genera $g \geq 2$ together, then there are infinitely many new modular curves. For example, $X_1(p)$ is a new modular curve whenever p is prime, and its genus tends to infinity with p .

If we drop the assumption that our modular curves are new, we can still prove results, but (so far) only if we impose restrictions on the level. Given $m > 0$, let Sparse_m denote the set of positive integers N such that if $1 = d_1 < d_2 < \cdots < d_t = N$ are the positive divisors of N , then $d_{i+1}/d_i > m$ for $i = 1, \dots, t-1$. Define a function $B(g)$ on integers $g \geq 2$ by $B(2) = 13$, $B(3) = 17$, $B(4) = 21$, and $B(g) = 6g - 5$ for $g \geq 5$. (For the origin of this function, see the proofs of Propositions 2.1 and 2.8.) A positive integer N is called m -smooth if all primes p dividing N satisfy $p \leq m$. Let Smooth_m denote the set of m -smooth integers.

Theorem 1.5. *Fix $g \geq 2$, and let S be a subset of $\{1, 2, \dots\}$. The set of modular curves over $\mathbb{Q}$ of genus g and of level contained in S is finite if any of the following hold:*

- (i) $S = \text{Sparse}_{B(g)}$.
- (ii) $S = \text{Smooth}_m$ for some $m > 0$.
- (iii) S is the set of prime powers.

Remark 1.6. Since $\text{Sparse}_{B(g)} \cup \text{Smooth}_{B(g)}$ contains all prime powers, parts (i) and (ii) of Theorem 1.5 imply (iii).

Remark 1.7. In contrast with Theorem 1.3, we do not know, even in theory, how to compute the finite sets of curves in Theorem 1.5. The reason for this will be explained in Remark 5.12.

If X is a curve over a field k , and L is a field extension of k , let X_L denote $X \times_k L$. The *gonality* G of a curve X over $\mathbb{Q}$ is the smallest possible degree of a nonconstant morphism $X_{\mathbb{C}} \rightarrow \mathbb{P}_{\mathbb{C}}^1$. (There is also the notion of $\mathbb{Q}$ -gonality, where one only allows morphisms over $\mathbb{Q}$. By defining gonality using morphisms over $\mathbb{C}$ instead of $\mathbb{Q}$, we make the next theorem stronger.) In Section 4.3, we combine Theorem 1.3 with a known lower bound on the gonality of $X_1(N)$ to prove the following:

Theorem 1.8. *For each $G \geq 2$, the set of new modular curves over $\mathbb{Q}$ of genus at least 2 and gonality at most G is finite and computable.*

(We could similarly prove an analogue of Theorem 1.5 for curves of bounded gonality instead of fixed genus.)

Recall that a curve X of genus g over a field k is called *hyperelliptic* if $g \geq 2$ and the canonical map $X \rightarrow \mathbb{P}^{g-1}$ is not a closed immersion: equivalently, $g \geq 2$ and there exists a degree-2 morphism $X \rightarrow Y$ where Y has genus zero. If moreover $X(k) \neq \emptyset$ then $Y \simeq \mathbb{P}_k^1$, and if also k is not of characteristic 2, then X is birational to a curve of the form $y^2 = f(x)$ where f is a separable polynomial in $k[x]$ of degree $2g + 1$ or $2g + 2$. Recall that $X(k) \neq \emptyset$ is automatic if X is modular, because of the cusp ∞ .

Taking $G = 2$ in Theorem 1.8, we find that the set of new modular hyperelliptic curves over $\mathbb{Q}$ is finite and computable. We can say more:

Theorem 1.9. *Let X be a new modular hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 3$ and level N . Then*

- (i) $g \leq 16$.
- (ii) *If $\text{Jac} X$ is a quotient of $J_0(N)$, then $g \leq 10$. If moreover $3 \mid N$, then X is the genus-3 curve $X_0(39)$.*

(iii) If $\text{Jac} X$ is not a quotient of $J_0(N)$, then either g is even or $g \leq 9$.

Further information is given in Sections 6.3 and 6.5, and in the appendix. See Section 3.1 for the definitions of $X_0(N)$ and $J_0(N)$.

As we have already remarked, if we consider all genera $g \geq 2$ together, there are infinitely many new modular curves. To obtain finiteness results, so far we have needed to restrict either the genus or the gonality. The following theorem, proved in Section 7, gives a different type of restriction that again implies finiteness.

Theorem 1.10. *For each prime p , the set of new modular curves over $\mathbb{Q}$ of genus at least 2 whose jacobian is a quotient of $J_0(N)^{\text{new}}$ for some N divisible by p is finite and computable.*

Question 1.11. Does Theorem 1.10 remain true if $J_0(N)^{\text{new}}$ is replaced by $J_1(N)^{\text{new}}$?

Call a curve X over a field k of characteristic zero *k -modular* if there exists a nonconstant morphism $X_1(N)_k \rightarrow X$ (over k).

Question 1.12. Is it true that for every field k of characteristic zero, and every $g \geq 2$, the set of k -modular curves over k of genus g up to k -isomorphism is finite?

Remark 1.13. If X is a k -modular curve over k , and we define $k_0 = k \cap \overline{\mathbb{Q}} \subseteq \overline{k}$, then $X = X_0 \times_{k_0} k$ for some k_0 -modular curve X_0 . This follows from the de Franchis-Severi Theorem.

Remark 1.14. If k and k' are fields of characteristic zero with $[k' : k]$ finite, then a positive answer to Question 1.12 for k' implies a positive answer for k , since Galois cohomology and the finiteness of automorphism group of curves of genus at least 2 show that for each X' over k' , there are at most finitely many curves X over k with $X \times_k k' \simeq X'$. But it is *not* clear, for instance, that a positive answer for $\overline{\mathbb{Q}}$ implies or is implied by a positive answer for $\mathbb{Q}$.

2. RECOVERING CURVE INFORMATION FROM DIFFERENTIALS

2.1. Recovering a curve from partial expansions of its differentials. The goal of this section is to prove the following result, which will be used frequently in the rest of this paper.

Proposition 2.1. *Fix an integer $g \geq 2$. There exists an integer $B > 0$ depending on g such that if k is a field of characteristic zero, and $w_1, \dots, w_g$ are elements of $k[[q]]/(q^B)$, then up to k -isomorphism, there exists at most one curve X over k such that there exist $P \in X(k)$ and an analytic uniformizing parameter q in the completed local ring $\hat{\mathcal{O}}_{X,P}$ such that $w_1 dq, \dots, w_g dq$ are the expansions modulo q^B of some basis of $H^0(X, \Omega)$.*

Lemma 2.2. *Let k be a field, and let X/k be a curve of genus g . Let $P \in X(k)$ be a k -rational point, let $F \in k[t_1, \dots, t_g]$ be a homogeneous polynomial of degree d , and let q be an analytic uniformizing parameter in $\hat{\mathcal{O}}_{X,P}$. Suppose we are given elements $\omega_1, \dots, \omega_g \in H^0(X, \Omega)$, and for each $i = 1, \dots, g$, write $\omega_i = w_i dq$ with $w_i \in k[[q]]$. Then if $F(w_1, \dots, w_g) \equiv 0 \pmod{q^B}$ with $B > d(2g - 2)$, then $F(\omega_1, \dots, \omega_g) = 0$ in $H^0(X, \Omega^{\otimes d})$.*

Proof. A nonzero element of $H^0(X, \Omega^{\otimes d})$ has $d(2g - 2)$ zeros on X , so its expansion at any given point can vanish to order at most $d(2g - 2)$. $\square$

The following is a weak form of a theorem of Petri appearing as Theorem 2.3 on page 131 of [5], for example. A curve is *trigonal* if its gonality is 3.

Theorem 2.3 (Petri, 1923). *Let X be a nonhyperelliptic curve of genus $g \geq 4$ over a field k of characteristic zero. Then the image of the canonical map $X \rightarrow \mathbb{P}^{g-1}$ is the common zero locus of some set of homogeneous polynomials of degree 2 and 3. Moreover, if X is neither trigonal nor a smooth plane quintic, then degree 2 polynomials suffice.*

Corollary 2.4. *Let X be a curve of genus $g \geq 2$ over a field k of characteristic zero. Then the image X' of the canonical map $X \rightarrow \mathbb{P}^{g-1}$ is the common zero locus of the set of homogeneous polynomials of degree 4 that vanish on X' .*

Proof. We may assume that k is algebraically closed. If X is hyperelliptic of genus g , say birational to $y^2 = f(x)$ where f has distinct roots, then we may choose $\{x^i dx/y : 0 \leq i \leq g-1\}$ as basis of $H^0(X, \Omega)$, and then the image of the canonical map is the rational normal curve cut out by $\{t_i t_j - t_{i'} t_{j'} : i+j = i'+j'\}$ where $t_0, \dots, t_{g-1}$ are the homogeneous coordinates on $\mathbb{P}^{g-1}$. If X is nonhyperelliptic of genus 3, its canonical model is a plane quartic. In all other cases, we use Petri's Theorem. (The zero locus of a homogeneous polynomial h of degree $d < 4$ equals the zero locus of the set of homogeneous polynomials of degree 4 that are multiples of h .) $\square$

Lemma 2.5. *Let X be a hyperelliptic curve of genus g over a field k of characteristic zero, and suppose $P \in X(k)$. Let $\{\omega_1, \dots, \omega_g\}$ be a basis of $H^0(X, \Omega)$ such that $\text{ord}_P(\omega_1) < \dots < \text{ord}_P(\omega_g)$. Then $x := \omega_{g-1}/\omega_g$ and $y := dx/\omega_g$ generate the function field $k(X)$, and there is a unique polynomial $F(x)$ of degree at most $2g+2$ such that $y^2 = F(x)$. Moreover, F is squarefree. If P is a Weierstrass point, then $\deg F = 2g+1$ and $\text{ord}_P(\omega_i) = 2i-2$ for all i ; otherwise $\deg F = 2g+2$ and $\text{ord}_P(\omega_i) = i-1$ for all i . Finally, it is possible to replace each ω_i by a linear combination of $\omega_i, \omega_{i+1}, \dots, \omega_g$ to make $\omega_i = x^{g-i} dx/y$ for $1 \leq i \leq g$.*

Proof. This follows easily from Lemma 3.6.1, Corollary 3.6.3, and Theorem 3.6.4 of [25]. $\square$

Proof of Proposition 2.1. Suppose that X, P, q , and the w_i are as in the statement of the proposition. Let ω_i be the corresponding elements of $H^0(X, \Omega)$. We will show that X is determined by the w_i when $B = \max\{8g-7, 6g+1\}$.

Since $B > 8g-8$, Lemma 2.2 implies that the w_i determine the set of homogeneous polynomial relations of degree 4 satisfied by the ω_i , so by Corollary 2.4 the w_i determine the image X' of the canonical map. In particular, the w_i determine whether X is hyperelliptic, and they determine X if X is nonhyperelliptic.

Therefore it remains to consider the case where X is hyperelliptic. Applying Gaussian elimination to the w_i , we may assume $0 = \text{ord}_q(w_1) < \dots < \text{ord}_q(w_g) \leq 2g-2$ and that the first nonzero coefficient of each w_i is 1. We use Lemma 2.5 repeatedly in what follows. The value of $\text{ord}(w_2)$ determines whether P is a Weierstrass point.

Suppose that P is a Weierstrass point. Then $w_i = q^{2i-2}(1 + \dots + O(q^{B-2i+2}))$, where each “ $\dots$ ” here and in the rest of this proof represents some known linear combination of positive powers of q up to but not including the power in the big- O term. (“Known” means “determined by the original w_i .”)

Define $x = w_{g-1}/w_g = q^{-2}(1 + \dots + O(q^{B-2g+2}))$. Define $y = dx/(w_g dq) = -2q^{-(2g+1)}(1 + \dots + O(q^{B-2g+2}))$. Then $y^2 = 4q^{-(4g+2)}(1 + \dots + O(q^{B-2g+2}))$. Since $B \geq 6g+1$, we have $-(4g+2) + (B-2g+2) > 0$, so there is a unique polynomial F (of degree $2g+1$) such that $y^2 = F(x)$.

A similar calculation shows that in the case where P is not a Weierstrass point, then $B \geq 3g+2$ is enough. $\square$

Remark 2.6. Let us show that if the hypotheses of Proposition 2.1 are satisfied except that the w_i belong to $\bar{k}[[q]]/(q^B)$ instead of $k[[q]]/(q^B)$, and the ω_i are permitted to lie in $H^0(X_{\bar{k}}, \Omega)$, then the conclusion still holds. Let E be a finite Galois extension of k containing all the coefficients of the w_i . The E -span of the w_i must be stable under $\text{Gal}(E/k)$ if they come from a curve over $\mathbb{Q}$, and in this case, we can replace the w_i by a k -rational basis of this span. Then Proposition 2.1 applies.

Remark 2.7. We can generalize Proposition 2.1 to the case where q is not a uniformizing parameter on X :

Fix an integer $g \geq 2$, and let k be a field of characteristic zero. Let $B > 0$ be the integer appearing in the statement of Proposition 2.1, and let e be a positive integer. Then if $w_1, \dots, w_g$ are elements of $k[[q]]/(q^{eB})$, then up to k -isomorphism, there exists at most one curve X over k such that there exist $P \in X(k)$, an analytic uniformizing parameter $q' \in \hat{\mathcal{O}}_{X,P}$ and a relation $q' = c_e q^e + c_{e+1} q^{e+1} + \dots$ with $c_e \neq 0$, such that $w_1 dq, \dots, w_g dq$ are the expansions modulo q^{eB} of some basis of $H^0(X, \Omega)$.

The proof of this statement is similar to the proof of Proposition 2.1, and is left to the reader.

The rest of this section is concerned with quantitative improvements to Proposition 2.1, and is not needed for the general finiteness and computability results of Sections 4 and 5.

Proposition 2.8. *Proposition 2.1 holds with $B = B(g)$, where $B(2) = 13$, $B(3) = 17$, $B(4) = 21$, and $B(g) = 6g - 5$ for $g \geq 5$. Moreover, if we are given that the curve X to be recovered is hyperelliptic, then we can use $B(g) = 4g + 5$ or $B(g) = 2g + 4$, according as P is a Weierstrass point or not.*

Proof. For nonhyperelliptic curves of genus $g \geq 4$, we use Theorem 2.3 instead of Corollary 2.4 to see that $B > 6g - 6$ can be used in place of $B > 8g - 8$.

Now suppose that X is hyperelliptic. As before, assume $\text{ord}_q(w_1) < \dots < \text{ord}_q(w_g)$ and that the first nonzero coefficient of each w_i is 1. The value of $\text{ord}(w_2)$ determines whether P is a Weierstrass point.

Suppose that P is a Weierstrass point. Then $w_i = q^{2i-2}(1 + \dots + O(q^{B-2i+2}))$. (As in the proof of Proposition 2.1, $\dots$ means a linear combination of positive powers of q , whose coefficients are determined by the w_i .) Define $\tilde{x} = w_{g-1}/w_g = q^{-2}(1 + \dots + O(q^{B-2g+2}))$. For $1 \leq i \leq g-2$, the expression $\tilde{x}^{g-i}w_g = q^{2i-2}(1 + \dots + O(q^{B-2g+2}))$ is the initial expansion of $w_i + \sum_{j=i+1}^g c_{ij}w_j$ for some $c_{ij} \in k$, and all the c_{ij} are determined if $2 + (B - 2g + 2) > 2g - 2$, that is, if $B \geq 4g - 5$. Let $w'_i = w_i + \sum_{j=i+1}^g c_{ij}w_j = q^{2i-2}(1 + \dots + O(q^{B-2i+2}))$. Define $x = w'_1/w'_2 = q^{-2}(1 + \dots + O(q^{B-2}))$. Define $y = -2q^{-(2g+1)}(1 + \dots + O(q^{B-2}))$ as the solution to $w'_1 dq = x^{g-1} dx/y$. Then $y^2 = 4q^{-(4g+2)}(1 + \dots + O(q^{B-2}))$, and if $-(4g+2) + B - 2 > 0$, we can recover the polynomial F of degree $2g + 1$ such that $y^2 = F(x)$. Hence $B \geq 4g + 5$ suffices. A similar proof shows that $B \geq 2g + 4$ suffices in the case that P is not a Weierstrass point.

Hence $\max\{6g - 5, 4g + 5, 2g + 4\}$ suffices for all types of curves, except that the $6g - 5$ should be $8g - 7$ when $g = 3$. This is the function $B(g)$. $\square$

Remark 2.9. We show here that for each $g \geq 2$, the bound $B = 4g + 5$ for the precision needed to recover a hyperelliptic curve is sharp. Let $F(x) \in \mathbb{C}[x]$ be a monic polynomial of degree $2g + 1$ such that $X: y^2 = F(x)$ and $X': y^2 = F(x) + 1$ are curves of genus g that are

not birationally equivalent. Let q be the uniformizing parameter at the point at infinity on X such that $x = q^{-2}$ and $y = q^{-(2g+1)} + O(q^{-2g})$. Define q' similarly for X' . A calculation shows that the q -expansions of the differentials $x^i dx/y$ for $0 \leq i \leq g-1$ are even power series in q times dq , and modulo $q^{4g+4} dq$ they agree with the corresponding q' -expansions for X' except for the coefficient of $q^{4g+2} dq$ in $x^{g-1} dx/y$. By a change of analytic parameter $q = Q + \alpha Q^{4g+3}$ for some $\alpha \in \mathbb{C}$, on X only, we can make even that coefficient agree.

A similar proof shows that in the case that P is not a Weierstrass point, the bound $2g+4$ cannot be improved.

Remark 2.10. When studying new modular curves of genus g , we can also use the multiplicativity of Fourier coefficients of modular forms (see (3.7)) to determine some coefficients from earlier ones. Hence we can sometimes get away with less than $B(g)$ coefficients of each modular form.

2.2. Descending morphisms. The next result will be used a number of times throughout this paper. In particular, it will be an important ingredient in the proof of Theorem 1.9.

Proposition 2.11. *Let X, Y, Z be curves over a field k of characteristic zero, and assume that the genus of Y is > 1 . Then:*

- (i) *Given nonconstant morphisms $\pi: X \rightarrow Z$ and $\phi: X \rightarrow Y$ such that $\phi^* H^0(Y, \Omega) \subseteq \pi^* H^0(Z, \Omega)$, there exists a nonconstant morphism $u': Z \rightarrow Y$ making the diagram*

$$\begin{array}{ccc} X & & \\ \pi \downarrow & \searrow \phi & \\ Z & \xrightarrow{\quad u' \quad} & Y \end{array}$$

commute.

- (ii) *If $\pi: X \rightarrow Y$ is a nonconstant morphism and u is an automorphism of X such that u^* maps $\pi^* H^0(Y, \Omega)$ into itself, then there exists a unique automorphism u' of Y making the diagram*

$$\begin{array}{ccc} X & \xrightarrow{u} & X \\ \pi \downarrow & & \downarrow \pi \\ Y & \xrightarrow{\quad u' \quad} & Y \end{array}$$

commute.

Proof. The conclusion of (i) is equivalent to the inclusion $\phi^* k(Y) \subseteq \pi^* k(Z)$. It suffices to prove that every function in $\phi^* k(Y)$ is expressible as a ratio of pullbacks of meromorphic differentials on Z . If Y is nonhyperelliptic, then the field $k(Y)$ is generated by ratios of pairs of differentials in $H^0(Y, \Omega)$, so the inclusion follows from the hypothesis $\phi^* H^0(Y, \Omega) \subseteq \pi^* H^0(Z, \Omega)$. When Y is hyperelliptic, we must modify this argument slightly. We have $k(Y) = k(x, y)$, where $y^2 = F(x)$ for some polynomial $F(U)$ in $k[U]$ without double roots. The field generated by ratios of differentials in $H^0(Y, \Omega)$ is $k(x)$, so $\phi^* k(x) \subseteq \pi^* k(Z)$. To show that $\phi^* y \in \pi^* k(Z)$ too, write $y = x dx / (x dx / y)$ and observe that $x dx / y \in H^0(Y, \Omega)$.

Now we prove (ii). The hypothesis on u^* lets us apply (i) with $\phi = \pi \circ u$ to construct $u': Y \rightarrow Y$. Since Y has genus > 1 and k has characteristic zero, the Hurwitz formula implies that u' is an automorphism. Considering function fields proves uniqueness. $\square$

Remark 2.12. Both parts of Proposition 2.11 can fail if the genus of Y is 1. On the other hand, (ii) remains true under the additional assumption that $X \rightarrow Y$ is optimal in the sense that it does not factor nontrivially through any other genus 1 curve.

Remark 2.13. Proposition 2.11 remains true if k has finite characteristic, provided that one assumes that the morphisms are separable.

3. SOME FACTS ABOUT MODULAR CURVES

3.1. Basic facts about $X_1(N)$. We record facts about $X_1(N)$ that we will need for the proof of finiteness in Theorem 1.3. See [67] and [20] for a detailed introduction.

Let $\mathcal{H} = \{z \in \mathbb{C} : \text{Im } z > 0\}$. Let $q = e^{2\pi iz}$. The group $\text{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}$. The quotient of $\mathcal{H}$ by the subgroup

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{N} \right\}$$

is isomorphic as Riemann surface to the space of complex points on a smooth affine curve $Y_1(N)$ over $\mathbb{Q}$. The $\mathbb{Q}$ -structure on $Y_1(N)$ can be specified by the condition that its function field be the subset of the function field of $Y_1(N)$ whose Fourier expansions in q have coefficients in $\mathbb{Q}$. Alternatively, the $\mathbb{Q}$ -structure on $Y_1(N)$ can be specified by interpreting $Y_1(N)$ as a moduli space parametrizing elliptic curves E equipped with an immersion $\mu_N \rightarrow E$: one must use the group scheme μ_N of N^{th} roots of unity instead of $\mathbb{Z}/N\mathbb{Z}$ in order to get the same $\mathbb{Q}$ -structure as in the previous sentence. (See [43, Chapter II], where the moduli space (over $\mathbb{Z}$) is denoted $M(\Gamma_{00}(N))$, or see Variant 9.3.6 and Section 12.3 of [20], where the moduli space is denoted $\mathcal{Y}_\mu(N)$.)

Next, there is a uniquely determined smooth projective curve $X_1(N)$ over $\mathbb{Q}$ having $Y_1(N)$ as a dense open subset. The difference $X_1(N)(\mathbb{C}) \setminus Y_1(N)(\mathbb{C})$ is the (finite) set of *cusps* on $X_1(N)$. One such cusp is the point ∞ , which can be defined as the limit in $X_1(N)(\mathbb{C})$ as $t \rightarrow +\infty$ of the image of $it \in \mathcal{H}$ in $X_1(N)(\mathbb{C})$. In fact, $\infty \in X_1(N)(\mathbb{Q})$ [20, Variant 9.3.6]. Let $J_1(N)$ denote the jacobian of $X_1(N)$. We have the Albanese morphism $X_1(N) \rightarrow J_1(N)$ sending P to the class of the divisor $(P) - (\infty)$.

Pulling back 1-forms under $\mathcal{H} \rightarrow Y_1(N)(\mathbb{C}) \hookrightarrow X_1(N)(\mathbb{C}) \rightarrow J_1(N)(\mathbb{C})$ identifies $H^0(J_1(N)_{\mathbb{C}}, \Omega)$ and $H^0(X_1(N)_{\mathbb{C}}, \Omega)$ with $S_2(N) \frac{dq}{q}$ for some g -dimensional $\mathbb{C}$ -subspace $S_2(N)$ of $q\mathbb{C}[[q]]$. We will not define modular forms in general here, but $S_2(N)$ is known as the space of weight 2 cusp forms on $\Gamma_1(N)$.

If $M|N$ and $d|\frac{N}{M}$, then $z \mapsto d \cdot z$ on $\mathcal{H}$ induces a morphism $X_1(N) \rightarrow X_1(M)$, which in turn induces $S_2(M) \rightarrow S_2(N)$ and $J_1(M) \rightarrow J_1(N)$. The *old subspace* $S_2(N)_{\text{old}}$ of $S_2(N)$ is defined as the sum of the images of all such maps $S_2(M) \rightarrow S_2(N)$ for all d and M such that $M|N$, $M \neq N$, and $d|\frac{N}{M}$. Similarly define the *old subvariety* $J_1(N)_{\text{old}}$ of $J_1(N)$. The space $S_2(N)$ has a hermitian inner product called the *Petersson inner product*. Let $S_2(N)_{\text{new}}$ denote the orthogonal complement to $S_2(N)_{\text{old}}$ in $S_2(N)$. The identifications above also give us new and old subspaces of $H^0(X_1(N)_{\mathbb{C}}, \Omega)$ and $H^0(J_1(N)_{\mathbb{C}}, \Omega)$. Let $J_1(N)^{\text{new}} = J_1(N)/J_1(N)_{\text{old}}$. There is also an abelian subvariety $J_1(N)_{\text{new}}$ of $J_1(N)$ that can be characterized in two ways: either as the abelian subvariety such that

$$\ker(H^0(J_1(N)_{\mathbb{C}}, \Omega) \rightarrow H^0((J_1(N)_{\text{new}})_{\mathbb{C}}, \Omega)) = H^0(J_1(N)_{\mathbb{C}}, \Omega)_{\text{old}},$$

or as the abelian subvariety such that $J_1(N) = J_1(N)_{\text{old}} + J_1(N)_{\text{new}}$ with $J_1(N)_{\text{old}} \cap J_1(N)_{\text{new}}$ finite. (The latter description uniquely characterizes $J_1(N)_{\text{new}}$ because of a theorem that no $\mathbb{Q}$ -simple quotient of $J_1(N)_{\text{old}}$ is isogenous to a $\mathbb{Q}$ -simple quotient of $J_1(N)_{\text{new}}$; this theorem can be proved by comparing conductors, using [12].) The abelian varieties $J_1(N)_{\text{new}}$ and $J_1(N)_{\text{new}}$ are $\mathbb{Q}$ -isogenous. We define $X_0(N)$, $J_0(N)$, and $J_0(N)_{\text{new}}$ similarly, starting with

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

instead of $\Gamma_1(N)$.

For $n \geq 1$ with $\gcd(n, N) = 1$, there exist well-known correspondences T_n on $X_1(N)$, and they induce endomorphisms of $S_2(N)$ and of $J_1(N)$ known as *Hecke operators*, also denoted T_n . By [49, p. 294], there is a unique basis New_N of $S_2(N)_{\text{new}}$ consisting of $f = a_1q + a_2q^2 + a_3q^3 + \dots$ such that $a_1 = 1$ and $T_nf = a_nf$ whenever $\gcd(n, N) = 1$. The elements of New_N are called the *newforms of level N* . (For us, newforms are always normalized: this means that $a_1 = 1$.) Each a_n is an algebraic integer, bounded by $\sigma_0(n)\sqrt{n}$ in each archimedean absolute value, where $\sigma_0(n)$ is the number of positive integer divisors of n : [19, Théorème 8.2] proves this when n is a prime not dividing N , and then facts (3.7) through (3.11) below imply it for all $n \geq 1$. For each field k , let $G_k = \text{Gal}(\bar{k}/k)$. The Galois group $G_{\mathbb{Q}}$ acts on New_N . For any quotient A of $J_1(N)$, let $S_2(A)$ denote the image of $H^0(A_{\mathbb{C}}, \Omega) \rightarrow H^0(J_1(N)_{\mathbb{C}}, \Omega) \simeq S_2(N)$ (the last isomorphism drops the dq/q); similarly for any nonconstant morphism $\pi: X_1(N) \rightarrow X$ of curves, define $S_2(X) := \pi^*H^0(X_{\mathbb{C}}, \Omega) \frac{q}{dq} \subseteq S_2(N)$. G. Shimura [69, Theorem 1] associated to $f \in \text{New}_N$ an abelian variety quotient A_f of $J_1(N)$ such that $S_2(A_f)$ is spanned by the Galois conjugates of f ; this association induces a bijection

$$(3.1) \quad G_{\mathbb{Q}} \backslash \text{New}_N \xrightarrow{\sim} \frac{\{\mathbb{Q}\text{-simple quotients of } J_1(N)_{\text{new}}\}}{\mathbb{Q}\text{-isogeny}} \\ f \mapsto A_f.$$

(Earlier, in Theorem 7.14 of [67], Shimura had attached to f an abelian *subvariety* of $J_1(N)$.) Shimura proved that $J_1(N)$ is isogenous to a product of these A_f , and K. Ribet [65] proved that A_f is $\mathbb{Q}$ -simple. This explains the surjectivity of (3.1). The injectivity is well-known to experts, but we could not find a suitable reference, so we will prove it, as part of Proposition 3.2.

The subfield $E_f = \mathbb{Q}(a_2, a_3, \dots)$ of $\mathbb{C}$ is a number field, and $\dim A_f = [E_f : \mathbb{Q}]$. Moreover, $\text{End}(A_f) \otimes \mathbb{Q}$ can be canonically identified with E_f , and under this identification the element $\lambda \in \text{End}(A_f) \otimes \mathbb{Q}$ acts on f as multiplication by λ (considered as element of E_f), and on each Galois conjugate ${}^{\sigma}f$ by multiplication by ${}^{\sigma}\lambda$. (Shimura [69, Theorem 1] constructed an injection $\text{End}(A_f) \otimes \mathbb{Q} \hookrightarrow E_f$, and Ribet [65, Corollary 4.2] proved that it was an isomorphism.)

If A and B are abelian varieties over $\mathbb{Q}$, let $A \stackrel{\mathbb{Q}}{\sim} B$ denote the statement that A and B are isogenous over $\mathbb{Q}$.

Proposition 3.2. *Suppose $f \in \text{New}_N$ and $f' \in \text{New}_{N'}$. Then $A_f \stackrel{\mathbb{Q}}{\sim} A_{f'}$ if and only if $N = N'$ and $f = {}^{\tau}f'$ for some $\tau \in G_{\mathbb{Q}}$.*

Proof (K. Ribet). The “if” part is immediate from Shimura’s construction. Therefore it suffices to show that one can recover f , up to Galois conjugacy, from the isogeny class of A_f . Let ℓ be a prime. Let V be the $\mathbb{Q}_{\ell}$ -Tate module $V_{\ell}(A_f)$ attached to A_f . Let $\bar{V} = V \otimes_{\mathbb{Q}_{\ell}} \bar{\mathbb{Q}}_{\ell}$.

The proof of Proposition 4.1 of [65] shows that $\overline{V} = \bigoplus_{\sigma} V_{\sigma}$, where V_{σ} is an irreducible $\overline{\mathbb{Q}_{\ell}}[G_{\mathbb{Q}}]$ -module of dimension 2 over $\overline{\mathbb{Q}_{\ell}}$, indexed by embeddings $\sigma: E_f \hookrightarrow \overline{\mathbb{Q}_{\ell}}$. Moreover, for $p \nmid \ell N$, the trace of the p -Frobenius automorphism acting on V_{σ} equals $\sigma(a_p)$, where $a_p \in E_f$ is the coefficient of q^p in the Fourier expansion of f .

If $f' \in \text{New}'_N$ is another weight 2 newform, and $A_f \stackrel{\mathbb{Q}}{\sim} A_{f'}$, then (using $'$ in the obvious way to denote objects associated with f'), we have isomorphisms of $G_{\mathbb{Q}}$ -modules $V \simeq V'$ and $\overline{V} \simeq \overline{V}'$. Fix $\sigma: E_f \hookrightarrow \overline{\mathbb{Q}_{\ell}}$. Then V_{σ} is isomorphic to some irreducible component $V'_{\sigma'}$ of $\overline{V}'$, where σ' is some embedding $E_{f'} \hookrightarrow \overline{\mathbb{Q}_{\ell}}$. Taking traces of Frobenius elements, we find that $\sigma(a_p) = \sigma'(a'_p)$ for almost all p . Then Theorem 5 of [49] implies that f and f' have the same level and are Galois conjugate. $\square$

We have parallel decompositions

$$\begin{aligned} S_2(N)_{\text{new}} &= \bigoplus_{f \in G_{\mathbb{Q}} \backslash \text{New}_N} \bigoplus_{\tau: E_f \hookrightarrow \mathbb{C}} \mathbb{C}^{\tau f} \\ J_1(N)^{\text{new}} &\stackrel{\mathbb{Q}}{\sim} \bigoplus_{f \in G_{\mathbb{Q}} \backslash \text{New}_N} A_f \end{aligned}$$

and parallel decompositions

$$(3.3) \quad S_2(N) = \bigoplus_{M|N} \bigoplus_{f \in G_{\mathbb{Q}} \backslash \text{New}_M} \bigoplus_{d| \frac{N}{M}} \bigoplus_{\tau: E_f \hookrightarrow \mathbb{C}} \mathbb{C}^{\tau f(q^d)}$$

$$(3.4) \quad J_1(N) \stackrel{\mathbb{Q}}{\sim} \bigoplus_{M|N} \bigoplus_{f \in G_{\mathbb{Q}} \backslash \text{New}_M} A_f^{n_f}$$

where $n_f := \sigma_0(N/M)$. (When we write $f \in G_{\mathbb{Q}} \backslash \text{New}_N$, we mean that f runs through a set of representatives for the orbits of $G_{\mathbb{Q}}$ acting on New_M . See [41, Example 5.5] and [42, Remark 17] for more details concerning the relationship between the decompositions (3.3) and (3.4).) Because of Proposition 3.2, the given decompositions of $J_1(N)^{\text{new}}$ and $J_1(N)$ are exactly the decompositions up to isogeny into nonisogenous $\mathbb{Q}$ -simple abelian varieties occurring with multiplicity.

Lemma 3.5. *Let A be an abelian variety quotient of $J_1(N)$. Then $S_2(A)$ has a $G_{\mathbb{Q}}$ -stable basis consisting of cusp forms each of the form*

$$h(q) = \sum_{d| \frac{N}{M}} c_d f(q^d)$$

for some $M | N$ and $f \in \text{New}_M$ and elements $c_d \in E_f$ (all depending on h).

Proof. By multiplying the quotient map $J_1(N) \rightarrow A$ by a positive integer, we may assume that it factors through the isogeny

$$J_1(N) \rightarrow \bigoplus_{M|N} \bigoplus_{f \in G_{\mathbb{Q}} \backslash \text{New}_M} A_f^{n_f}$$

of (3.4). We may also assume that A is $\mathbb{Q}$ -simple, and even that A is isomorphic to A_f for some f , so that the quotient map $J_1(N) \rightarrow A$ is the composition of $J_1(N) \rightarrow A_f^{n_f}$ with

a homomorphism $A_f^{n_f} \rightarrow A$. The latter is given by an n_f -tuple $c = (c_d)$ of elements of $\text{End}(A_f)$, indexed by the divisors d of N/M . Under

$$X_1(N) \hookrightarrow J_1(N) \rightarrow A_f^{n_f} \xrightarrow{c} A,$$

the 1-form on $A_{\mathbb{C}} \simeq (A_f)_{\mathbb{C}}$ corresponding to f pulls back to $\sum_{d|N/M} c_d f(q^d) dq/q$. Finally, $H^0(A_{\mathbb{C}}, \Omega)$ has a basis consisting of this 1-form and its conjugates, and the pullbacks of these conjugates are sums of the same form. $\square$

Corollary 3.6. *Let $\pi: X_1(N) \rightarrow X$ be a nonconstant morphism of curves over $\mathbb{Q}$. Then $S_2(X)$ has a $G_{\mathbb{Q}}$ -stable basis T consisting of cusp forms each of the form*

$$h(q) = \sum_{d|N/M} c_d f(q^d)$$

for some $M \mid N$ and $f \in \text{New}_M$, where $c_d \in E_f$ depends on f and d .

Proof. Apply Lemma 3.5 to the Albanese homomorphism $J_1(N) \rightarrow \text{Jac}X$. $\square$

3.2. Automorphisms of $X_1(N)$.

3.2.1. Diamonds. The action on $\mathcal{H}$ of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ induces an automorphism of $X_1(N)$ over $\mathbb{Q}$ depending only on $(d \bmod N)$. This automorphism is called the *diamond operator* $\langle d \rangle$. It induces an automorphism of $S_2(N)$. Let ε be a Dirichlet character modulo N , that is, a homomorphism $(\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}^*$. Let $S_2(N, \varepsilon)$ be the $\mathbb{C}$ -vector space $\{h \in S_2(N) : h|\langle d \rangle = \varepsilon(d)h\}$. A form $h \in S_2(N, \varepsilon)$ is called a form of Nebentypus ε . Every newform $f \in \text{New}_N$ is a form of some Nebentypus, and is therefore an eigenvector for all the diamond operators. Character theory gives a decomposition

$$S_2(N) = \bigoplus_{\varepsilon} S_2(N, \varepsilon),$$

where ε runs over all Dirichlet characters modulo N . Define $S_2(N, \varepsilon)_{\text{new}} = S_2(N, \varepsilon) \cap S_2(N)_{\text{new}}$. When we write $\varepsilon = 1$, we mean that ε is the trivial Dirichlet character modulo N , that is,

$$\varepsilon(n) = \begin{cases} 1 & \text{if } (n, N) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

A form of Nebentypus $\varepsilon = 1$ is a form on $\Gamma_0(N)$.

We recall some properties of a newform $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(N, \varepsilon)$. Let $\text{cond } \varepsilon$ denote the smallest integer $M \mid N$ such that ε is a composition $(\mathbb{Z}/N\mathbb{Z})^* \rightarrow (\mathbb{Z}/M\mathbb{Z})^* \rightarrow \mathbb{C}^*$. Throughout this paragraph, p denotes a prime, and $\overline{}$ denotes complex conjugation. Let $v_p(n)$ denote the p -adic valuation on $\mathbb{Z}$. If $v_p(\text{cond } \varepsilon) < v_p(N)$, then ε is a composition

$(\mathbb{Z}/N\mathbb{Z})^* \rightarrow (\mathbb{Z}/(N/p)\mathbb{Z})^* \xrightarrow{\varepsilon'} \mathbb{C}^*$ for some ε' . Then

$$(3.7) \quad \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + p \varepsilon(p) p^{-2s})^{-1},$$

$$(3.8) \quad p \mid N \iff \varepsilon(p) = 0$$

$$(3.9) \quad v_p(\text{cond } \varepsilon) < v_p(N) \geq 2 \implies a_p = 0$$

$$(3.10) \quad v_p(\text{cond } \varepsilon) < v_p(N) = 1 \implies a_p^2 = \varepsilon'(p)$$

$$(3.11) \quad 1 \leq v_p(\text{cond } \varepsilon) = v_p(N) \implies |a_p| = \sqrt{p}$$

$$(3.12) \quad v_p(N) = 1, \varepsilon = 1 \implies f|W_p = -a_p f$$

$$(3.13) \quad p \nmid N \implies \bar{a}_p = \overline{\varepsilon(p)} a_p.$$

(The equivalence (3.8) is trivial. Facts (3.7), (3.9), (3.10), (3.11) follow from parts (i), (iii), (iii), (ii) of [49, Theorem 3], respectively. Fact (3.12) follows from (3.10), [6, Theorem 2.1], and lines 6–7 of [6, p. 224]. Fact (3.13) follows from the first case of [6, equation (1.1)] and the lines preceding it.)

3.2.2. Involutions. For every integer $M \mid N$ such that $(M, N/M) = 1$, there is an automorphism W_M of $X_1(N)_{\mathbb{C}}$ inducing an isomorphism between $S_2(N, \varepsilon)_{\text{new}}$ and $S_2(N, \bar{\varepsilon}_M \varepsilon_{N/M})_{\text{new}}$, where ε_M denotes the character mod M induced by ε . (For more on this action, see [6]). Given a newform $f \in S_2(N, \varepsilon)$, there is a newform $\bar{\varepsilon}_M \otimes f$ in $S_2(N, \bar{\varepsilon}_M \varepsilon_{N/M})$ whose p^{th} Fourier coefficient b_p is given by

$$b_p = \begin{cases} \bar{\varepsilon}_M(p) a_p & \text{if } p \nmid M, \\ \bar{\varepsilon}_{N/M}(p) \bar{a}_p & \text{if } p \mid M. \end{cases}$$

Then

$$(3.14) \quad f|W_M = \lambda_M(f)(\bar{\varepsilon}_M \otimes f)$$

for some $\lambda_M(f) \in \mathbb{C}$ with $|\lambda_M(f)| = 1$. Moreover, we have

$$f|W_M^2 = \bar{\varepsilon}_{N/M}(-M) f, \quad f|(W_{M'} W_M) = \bar{\varepsilon}_{M'}(M) f|W_{M' M}$$

whenever $(M, M') = 1$. In the particular case $M = N$, the automorphism W_N is an involution defined over the cyclotomic field $\mathbb{Q}(\zeta_N)$, called the *Weil involution*. For all $\tau \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, the automorphisms ${}^{\tau}W_N$ are involutions and are also called Weil involutions by some authors. The involution W_N maps each $S_2(A_f)$ into itself and satisfies

$$(3.15) \quad \langle d \rangle W_N = W_N \langle d \rangle^{-1}, \quad {}^{\tau_d} W_N = W_N \langle d \rangle \quad \text{for all } d \in (\mathbb{Z}/N\mathbb{Z})^*,$$

where τ_d is the element of $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ mapping ζ_N to ζ_N^d .

Let ε be a Dirichlet character modulo N . Define the congruence subgroup

$$\Gamma(N, \varepsilon) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid \varepsilon(d) = 1 \right\}.$$

Let $S_2(\Gamma(N, \varepsilon))$ denote the space of weight 2 cusp forms on $\Gamma(N, \varepsilon)$. Denote by $X(N, \varepsilon)$ the modular curve over $\mathbb{Q}$ such that $X(N, \varepsilon)(\mathbb{C})$ contains $\Gamma(N, \varepsilon) \backslash \mathcal{H}$ as a dense open subset. We

can identify $H^0(X(N, \varepsilon)_{\mathbb{C}}, \Omega)$ with $S_2(\Gamma(N, \varepsilon)) \frac{dq}{q}$. The Dirichlet characters modulo N whose kernel contains $\ker(\varepsilon)$ are exactly the powers of ε , so

$$S_2(\Gamma(N, \varepsilon)) = \bigoplus_{k=1}^n S_2(N, \varepsilon^k),$$

where n is the order of ε . The diamond operators and the Weil involution induce automorphisms of $X(N, \varepsilon)_{\mathbb{C}}$. If moreover $\varepsilon = 1$, the curve $X(N, 1)$ is $X_0(N)$ and the automorphisms W_M on $X_1(N)_{\mathbb{C}}$ induce involutions on $X_0(N)$ over $\mathbb{Q}$ that are usually called the Atkin-Lehner involutions.

Remark 3.16. Define the *modular automorphism group* of $X_1(N)$ to be the subgroup of $\text{Aut}(X_1(N)_{\overline{\mathbb{Q}}})$ generated by the W_M 's and the diamond automorphisms. The quotient of $X_1(N)$ by this subgroup equals the quotient of $X_0(N)$ by its group of Atkin-Lehner involutions, and is denoted $X^*(N)$. The genus of $X_0(N)$ is $N^{1+o(1)}$ as $N \rightarrow \infty$, so by Proposition 4.4, the gonality of $X_0(N)$ is at least $N^{1+o(1)}$. On the other hand, the degree of $X_0(N) \rightarrow X^*(N)$ is only $2^{\#\{\text{prime factors of } N\}} = N^{o(1)}$. Hence the gonality of $X^*(N)$ tends to infinity. Thus the genus of $X^*(N)$ tends to infinity. In particular, Conjecture 1.1 is true if one restricts the statement to modular curves X that are *quotients* of $X_1(N)$ by some subgroup of the modular automorphism group.

3.2.3. Automorphisms of new modular curves. By Proposition 2.11, if X is a new modular curve of level N and genus $g \geq 2$, then the diamond operators and the Weil involution W_N induce automorphisms of $X_{\overline{\mathbb{Q}}}$, which we continue to denote by $\langle d \rangle$ and W_N respectively. Throughout the paper, $\mathcal{D}$ will denote the abelian subgroup of $\text{Aut}(X_{\overline{\mathbb{Q}}})$ consisting of diamond automorphisms, and $\mathcal{D}_N := \langle \mathcal{D}, W_N \rangle$ will denote the subgroup of $\text{Aut}(X_{\overline{\mathbb{Q}}})$ generated by $\mathcal{D}$ and W_N . If moreover X is hyperelliptic, and w is its hyperelliptic involution, then the group generated by $\mathcal{D}$ and $W_N.w$ will be denoted by $\mathcal{D}'_N$.

Note that $\mathcal{D}$ is a subgroup of $\text{Aut}(X)$, and the groups $\mathcal{D}_N, \mathcal{D}'_N$ are $G_{\mathbb{Q}}$ -stable by (3.15). If $\text{Jac } X \stackrel{\mathbb{Q}}{\sim} A_f$ for some f with nontrivial Nebentypus, then $\mathcal{D}_N$ is isomorphic to the dihedral group with $2n$ elements, $D_{2,n}$, where n is the order of the Nebentypus of f .

For every nonconstant morphism $\pi: X_1(N) \rightarrow X$ of curves over $\mathbb{Q}$ such that $S_2(X) \subseteq \bigoplus_{i=1}^n S_2(N, \varepsilon^i)$ for some Nebentypus ε of order n , there exists a nonconstant morphism $\pi(\varepsilon): X(N, \varepsilon) \rightarrow X$ over $\mathbb{Q}$. This is clear when the genus of X is ≤ 1 , and follows from Proposition 2.11(i) if the genus of X is > 1 . In particular, for a new modular curve X of genus > 1 , there exists a surjective morphism $X_0(N) \rightarrow X$ if and only if $\mathcal{D}$ is the trivial group. More generally, we have the following result.

Lemma 3.17. *Let X be a new modular curve of level N , and let G be a $G_{\mathbb{Q}}$ -stable subgroup of $\text{Aut}(X_{\overline{\mathbb{Q}}})$. Let $X' = X/G$. If the genus of X' is at least 2, then the group $\mathcal{D}'$ of diamonds of X' is isomorphic to $\mathcal{D}/(G \cap \mathcal{D})$. In particular, if $G = \mathcal{D}$ or $\mathcal{D}_N$, then there is a nonconstant morphism $\pi': X_0(N) \rightarrow X'$ defined over $\mathbb{Q}$.*

Proof. By Proposition 2.11, each diamond automorphism of X induces an automorphism of X' . Hence we obtain a surjective homomorphism $\rho: \mathcal{D} \rightarrow \mathcal{D}'$. Let $K = \ker(\rho)$. Since $G \cap \mathcal{D} \subseteq K$, it suffices to show that $K \subseteq G$. Now $H^0(X', \Omega)$ pulls back to the space $H^0(X, \Omega)^G$ of G -invariant regular differentials of X , so K acts trivially on the latter. Therefore the result follows from Lemma 3.18 below. $\square$

Lemma 3.18. *Let X be a curve over a field of characteristic zero, and let G be a finite subgroup of $\text{Aut}(X)$. Assume that the genus g' of $X' := X/G$ is at least 2. Let*

$$\overline{G} := \{ \phi \in \text{Aut}(X) : \phi^* \omega = \omega \text{ for all } \omega \in H^0(X, \Omega)^G \}.$$

Then $\overline{G} = G$.

Proof. It is clear that $G \subseteq \overline{G}$. Now suppose $\phi \in \overline{G}$, and let $H := \langle G, \phi \rangle$. Also, set $X'' := X/H$, and let g'' be the genus of X'' . Then there is a natural dominant morphism $\pi: X' \rightarrow X''$. Moreover,

$$g'' = \dim H^0(X, \Omega)^H = \dim H^0(X, \Omega)^{\langle G, \phi \rangle} = \dim H^0(X, \Omega)^G = g'.$$

Since $g' \geq 2$ by hypothesis, the Hurwitz formula implies $\deg(\pi) = 1$. Therefore $\phi \in G$, so that $\overline{G} \subseteq G$ as required. $\square$

3.3. Supersingular points. We will use a lemma about curves with good reduction.

Lemma 3.19. *Let R be a discrete valuation ring with fraction field K . Suppose $f: X \rightarrow Y$ is a finite morphism of smooth, projective, geometrically integral curves over K , and X extends to a smooth projective model $\mathcal{X}$ over R (in this case we say that X has good reduction). If Y has genus ≥ 1 , then Y extends to a smooth projective model $\mathcal{Y}$ over R , and f extends to a finite morphism $\mathcal{X} \rightarrow \mathcal{Y}$ over R .*

Proof. This result is Corollary 4.10 in [50]. See the discussion there also for references to earlier weaker versions. $\square$

The next two lemmas are well-known, but we could not find explicit references, so we supply proofs.

Lemma 3.20. *Let p be a prime. Let $\Gamma \subseteq \text{SL}_2(\mathbb{Z})$ denote a congruence subgroup of level N not divisible by p . Let X_Γ be the corresponding integral smooth projective curve over $\overline{\mathbb{Q}}$, and let ψ be the degree of the natural map $X_\Gamma \rightarrow X(1)$. Then X_Γ has good reduction at any place above p , and the number of $\overline{\mathbb{F}}_p$ -points on the reduction mapping to supersingular points on $X(1)$ is at least $(p-1)\psi/12$.*

Proof. By [39], the curve $X(N)$ admits a smooth model over $\mathbb{Z}[1/N]$, and has a rational point (the cusp ∞). Since $p \nmid N$ and $X(N)$ dominates X_Γ , Lemma 3.19 implies that X_Γ has good reduction at p , at least if X_Γ has genus ≥ 1 . If X_Γ has genus 0, then the rational point on $X(N)$ gives a rational point on X_Γ , so $X_\Gamma \simeq \mathbb{P}^1$, so X_Γ has good reduction at p in any case. Replacing Γ by the group generated by Γ and $-\text{id}$ does not change X_Γ , so without loss of generality, we may assume that $-\text{id} \in \Gamma$. Then $\psi = (\text{SL}_2(\mathbb{Z}) : \Gamma)$.

If E is an elliptic curve, then Γ naturally acts on the finite set of ordered symplectic bases of $E[N]$. The curve $Y_\Gamma := X_\Gamma - \{\text{cusps}\}$ classifies isomorphism classes of pairs (E, L) , where E is an elliptic curve and L is a Γ -orbit of symplectic bases of $E[N]$.

Fix E . Since $\text{SL}_2(\mathbb{Z})$ acts transitively on the symplectic bases of $E[N]$, the number of Γ -orbits of symplectic bases is $(\text{SL}_2(\mathbb{Z}) : \Gamma) = \psi$. Two such orbits L and L' correspond to the same point of X_Γ if and only if $L' = \alpha L$ for some $\alpha \in \text{Aut}(E)$. Then ψ is the sum of the sizes of the orbits of $\text{Aut}(E)$ acting on the Γ -orbits, so

$$\psi = \sum_{(E, L) \in X_\Gamma} \frac{\#\text{Aut}(E)}{\#\text{Aut}(E, L)},$$

where the sum is over representatives (E, L) of the points on X_Γ above E , and $\text{Aut}(E, L)$ is the subgroup of $\text{Aut}(E)$ stabilizing L .

Dividing by $\#\text{Aut}(E)$ and summing over all supersingular E over $\overline{\mathbb{F}}_p$, we obtain

$$\sum_{\text{supersingular points } (E, L) \in X_\Gamma(\overline{\mathbb{F}}_p)} \frac{1}{\#\text{Aut}(E, L)} = \psi \sum_{\text{supersingular } E/\overline{\mathbb{F}}_p} \frac{1}{\#\text{Aut}(E)} = \frac{(p-1)\psi}{24},$$

where the last step is the mass formula of Deuring and Eichler (see Chapter 13, §4 of [38] for a proof). But $[-1] \in \text{Aut}(E, L)$, so $\#\text{Aut}(E, L) \geq 2$ at each $(E, L) \in X_\Gamma(\overline{\mathbb{F}}_p)$. Therefore the number of supersingular points on X_Γ must be at least $2(p-1)\psi/24 = (p-1)\psi/12$. $\square$

Lemma 3.21. *Let p be a prime. Given a supersingular elliptic curve E over $\overline{\mathbb{F}}_p$, there exists an elliptic curve E' over $\mathbb{F}_{p^2}$ such that $E \simeq E'_{\mathbb{F}_p}$ and the p^2 -power Frobenius endomorphism of E' equals $-p$.*

Proof. Honda-Tate theory supplies an elliptic curve $\mathcal{E}$ over $\mathbb{F}_p$ such that the characteristic polynomial of the p -power Frobenius endomorphism Frob_p satisfies $\text{Frob}_p^2 = -p$. All supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are isogenous, so there exists an isogeny $\phi: \mathcal{E}_{\overline{\mathbb{F}}_p} \rightarrow E$. The inseparable part of this isogeny is a power of Frob_p , so without loss of generality, we may assume that ϕ is separable. The kernel K of ϕ is preserved by $-p = \text{Frob}_p^2$, so K is defined over $\mathbb{F}_{p^2}$. Take $E' = \mathcal{E}_{\mathbb{F}_{p^2}}/K$. $\square$

The following is a generalization of inequalities used in [60].

Lemma 3.22. *Let X be a new modular hyperelliptic curve of level N and genus g over $\mathbb{Q}$. If p is a prime not dividing N , then $(p-1)(g-1) < 2(p^2+1)$.*

Proof. We may assume $g \geq 2$. Since $p \nmid N$, Lemma 3.19 implies that $X_1(N)$ and X have good reduction at p , and the morphism $\pi: X_1(N) \rightarrow X$ induces a corresponding morphism of curves over $\mathbb{F}_p$. By Proposition 2.11(ii), the diamond automorphism $\langle -p \rangle$ of $X_1(N)$ induces an automorphism of X , which we also call $\langle -p \rangle$. These automorphisms induces automorphisms of the corresponding curves over $\mathbb{F}_p$. For the rest of this proof, $X_1(N)$, X , π , $\langle -p \rangle$ represent these objects over $\mathbb{F}_p$. Also denote by $\langle -p \rangle$ the induced morphism $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ on the canonical image of the hyperelliptic curve X . On each curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, let F denote the p^2 -power Frobenius morphism.

Let s be the number of $x \in X_1(N)(\overline{\mathbb{F}}_p)$ satisfying $Fx = \langle -p \rangle x$. We will bound s in two different ways. On the one hand, Lemma 3.21 implies that all supersingular points on $X_1(N)(\overline{\mathbb{F}}_p)$ have this property. By Lemma 3.20, there are at least $(p-1)\psi/12$ such points, where ψ is the degree of $X_1(N) \rightarrow X(1)$. Thus $s \geq (p-1)\psi/12$.

On the other hand, any solution x to $Fx = \langle -p \rangle x$ in $X_1(N)(\overline{\mathbb{F}}_p)$ maps to a solution to the same equation on X or on $\mathbb{P}^1$. The number of solutions to $Fx = \langle -p \rangle x$ in $\mathbb{P}^1(\overline{\mathbb{F}}_p)$ is at most p^2+1 , because they can be counted by intersecting the graphs of F and $\langle -p \rangle$, which are curves of type $(1, p^2)$ and $(1, 1)$, respectively, on $\mathbb{P}^1 \times \mathbb{P}^1$. Therefore $s \leq (2 \deg \pi)(p^2+1)$.

Combining the inequalities from the previous two paragraphs gives $(p-1)\psi/12 \leq (2 \deg \pi)(p^2+1)$. By Proposition 1.40 of [67], the genus g_1 of $X_1(N)$ satisfies $g_1 - 1 < \psi/12$. By Hurwitz, $\deg \pi \leq (g_1 - 1)/(g - 1)$. Combining the last three inequalities yields $(p-1)(g-1) < 2(p^2+1)$. $\square$

Remark 3.23. One can extend the above arguments to prove the following more general result:

Let X be a new modular curve of genus g and level N , with $p \nmid N$. Suppose X admits a degree d map (defined over $\mathbb{Q}$) to a curve $X'/\mathbb{Q}$ of genus g' . Finally, suppose that the diamond automorphisms on $X_1(N)$ are compatible with automorphisms of X' . (This is automatic if $g' \geq 2$, or if $g \geq 2$, $g' = 0$, and $d = 2$.) Then $(g-1)(p-1) \leq d(p^2 + 1 + 2pg')$.

We omit the proof, since we will not use this result.

Corollary 3.24. *Let X be a new modular hyperelliptic curve of level N and genus g over $\mathbb{Q}$. If $g > 10$, then $6|N$. If $g > 13$, then $30|N$.*

Proof. Take $p = 2, 3$, and 5 in Lemma 3.22. □

In the case where X is a curve dominated by $X_0(N)$, $\langle -p \rangle$ is the identity, so in the proof of Lemma 3.22 we may replace the bound $(2 \deg \pi)(p^2 + 1)$ by $(\deg \pi) \#X(\mathbb{F}_{p^2})$ to obtain the following:

Lemma 3.25. *Suppose that X is a curve of genus $g \geq 2$ over $\mathbb{Q}$, and $\pi: X_0(N) \rightarrow X$ is a dominant morphism over $\mathbb{Q}$. Suppose that p is a prime not dividing N . Then X has good reduction at p , and $(p-1)(g-1) < \#X(\mathbb{F}_{p^2})$. In particular, if $G_{\mathbb{Q}}$ denotes the $\mathbb{Q}$ -gonality of X , then $g < G_{\mathbb{Q}} \frac{p^2+1}{p-1} + 1$.*

3.4. Previous work on curves dominated by modular curves. Except for the determination of all new modular genus-2 curves with $\mathbb{Q}$ -simple jacobian in [27], all work we know of on modular curves of genus ≥ 2 has focused on $X_0(N)$, $X_1(N)$, or quotients of these by a subgroup of the group of Atkin-Lehner involutions or diamonds, respectively. Here we summarize some of this work.

The 19 values of N for which $X_0(N)$ is hyperelliptic (of genus ≥ 2) were determined in [60], and all of their equations were given in [26]. The corresponding determination of the three values of N for which $X_1(N)$ is hyperelliptic was carried out in [55], and equations for these (and a few other $X_1(N)$) were given in [63]. In [40] it is proved that a curve strictly between $X_0(N)$ and $X_1(N)$ (that is, a quotient of $X_1(N)$ by a nontrivial proper subgroup of the diamond group) is never hyperelliptic. A series of works [46], [31], [30] led up to the determination of all 64 values of N for which the quotient of $X_0(N)$ by its Atkin-Lehner group, $X^*(N)$, is hyperelliptic, and this was generalized in [23] to quotients of $X_0(N)$ by an arbitrary subgroup of the Atkin-Lehner group. Similar results determining all *trigonal* curves of the form $X_0(N)$, $X_0(N)/W_d$ for a single Atkin-Lehner involution W_d , and $X^*(N)$, can be found in [32], [33], and [34], respectively. Some of these curves are not new, and hence do not appear in our tables.

The method of constructing equations for modular curves one at a time in terms of a basis of cusp forms has been used by many authors: in addition to the papers already mentioned, we have [58], [70], [24], for instance. In particular, [70] gives methods for both the hyperelliptic and nonhyperelliptic cases, using Petri's Theorem in the latter, as we do. F. Klein [45] gave an explicit model for $X(p)$ for every prime p in 1879. See [75] for a modern construction of $X(N)$ for every N . An analogous result for $X_1(p)$ can be found in [7].

4. FINITENESS THEOREMS

Our goal in this section is to prove the finiteness statements in Theorems 1.3, 1.5, and 1.8. Algorithmic and practical issues will be dealt with only in later sections, because we assume

that some readers will be interested only in the finiteness. In particular, the computability of the sets in question will be proved in Section 5, and practical algorithms in the hyperelliptic case will be given in Section 6.

4.1. New modular curves of fixed genus.

Proof of finiteness in Theorem 1.3. Fix $g \geq 2$. Let X be a new modular curve of level N and genus g , given by the nonconstant morphism $\pi: X_1(N) \rightarrow X$. Since the $\mathbb{Q}$ -simple factors A_f of $J_1(N)^{\text{new}}$ are pairwise nonisogenous, any abelian subquotient of $J_1(N)^{\text{new}}$ is isogenous to a product of some subset of these A_f . Applying this to $J = \text{Jac}X$ and then comparing 1-forms shows that there exists a $G_{\mathbb{Q}}$ -stable subset $T \subseteq \text{New}_N$ that is a basis for $S_2(X)$.

From now on, let $f = q + a_2q^2 + a_3q^3 + \dots$ denote an element of T . The map π is unramified at ∞ , since there exists $\omega \in H^0(X_{\mathbb{C}}, \Omega)$ such that $\pi^*\omega = f dq/q$, which is nonvanishing at ∞ . In other words, the analytic uniformizer q at ∞ on $X_1(N)$ serves also as analytic uniformizer at $\pi(\infty)$ on X .

The field E_f generated by the coefficients of f satisfies $[E_f : \mathbb{Q}] = \dim A_f \leq \dim J = g$. Let B be the integer of Proposition 2.1. Each a_n for $1 \leq n \leq B$ is an algebraic integer of degree at most g , bounded in every archimedean absolute value by $\sigma_0(n)\sqrt{n}$, so there are only finitely many possibilities for a_n . Thus there are only finitely many possibilities for $\{f \bmod q^B \mid f \in T\}$, given g . By Proposition 2.1 and Remark 2.6, each such possibility arises for at most one curve over $\mathbb{Q}$. $\square$

Remark 4.1. For this proof, any bound on the absolute values of $|a_n|$ in terms of n would have sufficed. But when we do computations, it will be useful to have the strong bound $\sigma_0(n)\sqrt{n}$.

4.2. Non-new modular curves of fixed genus. Our goal in this section is to prove the finiteness assertion of Theorem 1.5.

Proof of finiteness in Theorem 1.5(i). Let $X/\mathbb{Q}$ be a modular curve of genus $g \geq 2$ and level N , so that there exists a map $\pi: X_1(N) \rightarrow X$ over $\mathbb{Q}$. Let $B = B(g)$ be the integer of Proposition 2.1.

We will follow the basic strategy of the proof of Theorem 1.3, but two complications arise: the map π need not be unramified at ∞ , and the cusp forms whose Fourier coefficients we need to bound need not be newforms. The sparseness assumption will allow us to get around both of these difficulties.

Let T be as in Corollary 3.6. Choose $j \in T$ with $\text{ord}_q(j)$ minimal. Then $j dq/q$ corresponds to a regular differential on $X_{\mathbb{C}}$ not vanishing at $\pi(\infty)$. Since q is an analytic parameter at ∞ on $X_1(N)$, the ramification index e of π at ∞ equals $\text{ord}_q(j)$. In particular, $e \mid N$. By Remark 2.7, the curve X is determined by the set $\{h \bmod q^{eB} \mid h \in T\}$.

Fix $h = \sum_{n=1}^{\infty} a_n q^n \in T$. Since $\text{ord}_q(h) \geq e$, Corollary 3.6 implies that there exist an integer $M \mid N$, a newform $f \in \text{New}_M$, and $c_d \in \mathbb{C}$ such that

$$h = \sum_{d \mid \frac{N}{M}, d \geq e} c_d f(q^d).$$

Since $N \in \text{Sparse}_B$, we have $d > eB$ for all $d \mid N$ such that $d > e$. If $c_e = 0$, then $h \bmod q^{eB} = 0$; otherwise we may scale to assume that $c_e = 1$. In this case, the sparseness

of N implies that $a_n(h(q)) = a_n(f(q^e))$ for $1 \leq n < eB$. In other words, for $1 \leq n < eB$ we have

$$a_n(h) = \begin{cases} a_{n/e}(f) & \text{if } e \mid n, \\ 0 & \text{if } e \nmid n. \end{cases}$$

Since f is a *newform*, each $a_n(h)$ with $n \leq eB$ and $e \mid n$ is an algebraic integer satisfying $|a_n(h)| \leq \sigma_0(n/e) \sqrt{n/e}$ for all archimedean absolute values. As before, it then follows that there are only finitely many possibilities for $\{h \bmod q^{eB} \mid h \in T\}$, and therefore for X . $\square$

Proof of finiteness in Theorem 1.5(ii). Let $X/\mathbb{Q}$ be a modular curve of genus $g \geq 2$ and level $N \in \text{Smooth}_m$, with $m > 0$. Then $\text{Jac}X$ is isogenous to a subvariety of $J_1(N)$, so in particular $\text{Jac}X$ has good reduction outside the finite set Σ , where Σ is the set of primes p such that $p \leq m$. By combining the Shafarevich conjecture (proved by Faltings [22, Theorem 6]) with a well-known finiteness result for polarizations (see [56, Theorem 18.1]), it follows that for any number field K , any positive integer d , and any finite set S of places of K , there are only finitely many K -isomorphism classes of principally polarized abelian varieties of dimension d over K with good reduction outside S . In particular, there are only finitely many possible $\mathbb{Q}$ -isomorphism classes for $\text{Jac}X$ as a principally polarized abelian variety. By the Torelli theorem [57, Corollary 12.2], it follows that there are only finitely many possible $\mathbb{Q}$ -isomorphism classes for X . $\square$

As mentioned in the introduction, part (iii) of Theorem 1.5 (concerning prime power levels) follows from (i) and (ii).

To close this section, we remark that for modular curves of prime power level (as opposed to general non-new modular curves), one has good control over the ramification at the cusp infinity. More precisely:

Proposition 4.2. *Suppose that $N = p^r$ is a prime power. Suppose that X is modular of level N but not modular of level M for any $M < N$. Then the map $\pi: X_1(N) \rightarrow X$ is unramified at ∞ .*

Proof. Corollary 3.6 says that $S_2(X)$ has a basis in which each element h has the form $\sum_{d \mid \frac{N}{M}} c_d f(q^d)$ for some $M \mid N$ and $f \in \text{New}_M$. If π is ramified at ∞ , then $c_1 = 0$ in each such h . Then $\sum_{d \mid \frac{N}{M}, d > 1} c_d f(q^{d/p}) \in S_2(p^{r-1})$, according to the decomposition (3.3). Thus $\pi^* H^0(X_{\mathbb{C}}, \Omega) \subseteq B_p^* H^0(X_1(p^{r-1})_{\mathbb{C}}, \Omega)$, where $B_p: X_1(p^r) \rightarrow X_1(p^{r-1})$ denotes the degeneracy map induced by $q \mapsto q^p$. By Proposition 2.11(i), π factors through $X_1(p^{r-1})$, contradicting the minimality of N . $\square$

4.3. New modular curves of fixed gonality. In [2, p. 1006], one finds the following lower bound on the gonality of $X_1(N)$.

Theorem 4.3. *Let g' and G' be the genus and gonality, respectively, of $X_1(N)$. Then $G' \geq \frac{21}{200}(g' - 1)$.*

The linearity of the bound in the genus of $X_1(N)$ is what enables us to deduce the following.

Proposition 4.4. *If X is a $\mathbb{C}$ -modular curve of genus $g \geq 2$ and gonality G , then $g \leq \frac{200}{21}G + 1$.*

Proof. Let d be the degree of the given morphism $\pi: X_1(N)_\mathbb{C} \rightarrow X$. Let g' and G' be the genus and gonality of $X_1(N)$, so that $G' \geq \frac{21}{200}(g' - 1)$ by Theorem 4.3. Any morphism $X \rightarrow \mathbb{P}_\mathbb{C}^1$ can be composed with π to obtain a morphism $X_1(N)_\mathbb{C} \rightarrow \mathbb{P}_\mathbb{C}^1$, so $G' \leq dG$. The Hurwitz formula implies $g' - 1 \geq d(g - 1)$. Now combine these three inequalities. $\square$

Proposition 4.4 and Theorem 1.3 together imply the finiteness in Theorem 1.8.

Remark 4.5. Abramovich's result used the lower bound 0.21 for the positive eigenvalues of the Laplacian on $\Gamma \backslash \mathcal{H}$ for congruence subgroups Γ . In Appendix 2 to [44], Kim and Sarnak recently improved this to $975/4096 > 0.238$. This means that $200/21$ can be improved to $2/0.238 < 17/2$. In particular, taking $G = 2$, we find that a $\mathbb{C}$ -modular hyperelliptic curve has genus at most 17.

5. COMPUTABILITY

5.1. The meaning of computable. “Computable” will mean computable by a Turing machine. (See [37] for a definition of Turing machine.) To give a precise sense to each statement in our introduction, we must specify what the input and output of the Turing machine are to be. In particular, we will need to choose how to represent various objects, such as curves over number fields. In many cases, there exist algorithms for converting between various possible representations, so then the particular representation chosen is not important. A number field k can be represented by $f \in \mathbb{Z}[x]$ such that $k \simeq \mathbb{Q}[x]/(f(x))$. The representation is not unique, but we do not care, since a Turing machine can decide, given $f_1, f_2 \in \mathbb{Z}[x]$, whether f_1 and f_2 define isomorphic number fields (and if so, find an isomorphism) [48, §2.9]. An element $\alpha \in k$ can then be represented by $g \in \mathbb{Q}[x]$ (of degree at most $\deg f - 1$) whose image in $\mathbb{Q}[x]/(f(x))$ corresponds to α . Turing machines can also handle arithmetic over $\overline{\mathbb{Q}}$, thought of as a subfield of $\mathbb{C}$, by representing each $\alpha \in \overline{\mathbb{Q}}$ by its minimal polynomial over $\mathbb{Q}$, together with decimal approximations to its real and imaginary parts to distinguish α from its conjugates. If $k_0 = \mathbb{Q}$ or $k_0 = \overline{\mathbb{Q}}$, then a field finitely generated over k_0 can be represented as the fraction field of a domain $k_0[t_1, \dots, t_n]/(f_1, \dots, f_m)$, or alternatively as a finite extension of the rational function field $k_0(t_1, \dots, t_n)$ (in the same way that we handled finite extensions of $\mathbb{Q}$).

A curve X over a field k finitely generated over $\mathbb{Q}$ or $\overline{\mathbb{Q}}$ can be represented by $f \in k[x, y]$ such that the (possibly singular) affine curve $f(x, y) = 0$ is k -birational to X . Meromorphic differentials on X represented by $f \in k[x, y]$ can be expressed as $g(x, y)dx$ or $g(x, y)dy$, where $g = g_1/g_2$ with $g_1, g_2 \in k[x, y]$ and g_2 not divisible by f . A finite set of k -isomorphism classes of curves over k can be represented by a finite list of curves over k in which each class is represented exactly once.

A closed subvariety of $\mathbb{P}^n$ over a field k finitely generated over $\mathbb{Q}$ or $\overline{\mathbb{Q}}$ can be represented by a finite set of generators of its homogeneous ideal. A constructible subset of $\mathbb{P}^n$ (in the Zariski topology) can be represented as a Boolean combination of closed subvarieties. Morphisms or rational maps between quasiprojective varieties can be defined locally by rational functions on a finite number of affine open subsets. Elimination of quantifiers over algebraically closed fields is effective, and it follows that the image of a constructible subset of a quasiprojective variety under a morphism can be computed. (The elimination of quantifiers is usually attributed to Tarski; for a proof, see Section 3.2 of [53], especially Theorem 3.2.2 and Corollary 3.2.8(ii).) Irreducible components of a variety can also be computed: this follows from the primary decomposition algorithm in [35].

When in one of our theorems we claim that some set is computable, what we really mean is that there exists a Turing machine that takes as input the various parameters on which the set depends (such as a ground field, a curve, and/or an integer g), and, after a finite but unspecified amount of computation, terminates and outputs the set in question.

5.2. Computability lemmas for curves.

Lemma 5.1. *A Turing machine can solve the following problems: Given a field k finitely generated over $\mathbb{Q}$ or $\overline{\mathbb{Q}}$, and given curves X and Y over k ,*

- (1) *Compute the genus g of (the smooth projective model of) X .*
- (2) *If $g \geq 2$, decide whether or not X is hyperelliptic.*
- (3) *If either of the following holds:*
 - (i) $g(X) \geq 2$
 - (ii) $g(X) = 0$ and k is a number field or $\overline{\mathbb{Q}}$,*decide whether X and Y are k -birational.*

Proof.

- (1) See [1].
- (2) See [74].

(3) By (1) we may assume that X and Y have the same genus g , and that g is known. If $g \geq 2$, use [36]. From now on, suppose that $g = 0$. If $k = \overline{\mathbb{Q}}$, then X and Y are automatically birational. So from now on, suppose that k is a number field. By [73], we can find plane conics birational to X and Y , respectively. Diagonalize the corresponding quadratic forms to put each curve in the form $x^2 - ay^2 - bz^2 = 0$ for some $a, b \in k^*$. By the Hasse principle, the curves are isomorphic over k if and only if the order-2 Hilbert symbols $(a, b)_v$ match at every place v . In fact, one need only check the places above 2 and ∞ and the places occurring in the factorizations of the a and b for each curve. Each Hilbert symbol is computable: see [18] or II.7.1.5 and II.7.5 in [29]. (Alternatively, the question of whether the conic $x^2 - ay^2 - bz^2 = 0$ has a k_v -point can be answered by taking its restriction of scalars down to $\mathbb{Q}$ and using a general algorithm for deciding whether a variety over $\mathbb{Q}$ has a $\mathbb{Q}_p$ -point: see [72] or [59] for the archimedean and nonarchimedean cases, respectively.) $\square$

Remark 5.2. Most of these algorithms have been fully implemented. For instance, MAGMA [8] can compute the genus of a plane curve, and PARI-GP at <http://www.parigp-home.de/> has a function `nfhilbert` for computing Hilbert symbols.

Remark 5.3. Lemma 5.1(3) holds in the genus 1 case if and only if there exists an algorithm to decide, given a genus 1 curve Z over k , whether $Z(k) = \emptyset$. Such an algorithm exists trivially if $k = \overline{\mathbb{Q}}$. If k is a number field, the existence of such an algorithm is implied by the conjecture that the Shafarevich-Tate group $\text{III}(E)$ is finite for all elliptic curves E over k .

Lemma 5.4. *Let X be a curve over a number field k , and let $\ell \geq 1$ be an integer. Let $A = \text{Jac}X$, and let $M = A[\ell]$ be the Galois module of ℓ -torsion points. Then we can compute a description of M of the following type: a finite set equipped with an addition table and an action of $\text{Gal}(L/k)$ for some explicit finite Galois extension L of k over which all points of M are defined.*

Proof. Compute the genus g of X . We represent points of $A(\overline{\mathbb{Q}})$ (nonuniquely) by divisors on $X_{\overline{\mathbb{Q}}}$ whose support avoids any singularities of the given model. A solution of the “Riemann-Roch problem” decides whether a given divisor is principal: see the references cited in [61].

Hence we can decide when two given divisors represent the same element of $A(\overline{\mathbb{Q}})$. Now enumerate the countably many divisors on $X_{\overline{\mathbb{Q}}}$ avoiding the singularities, and continue until finding a set S of ℓ^{2g} such divisors D such that ℓD is principal, and such that they represent distinct elements of $A(\overline{\mathbb{Q}})$. For each pair in S , we can determine which divisor in S is linearly equivalent to their sum. Finally, we can compute a finite Galois extension L of k containing the coordinates of all points appearing in the divisors in S , and for each $\sigma \in \text{Gal}(L/k)$ and $D \in S$, we can determine which divisor in S is linearly equivalent to ${}^\sigma D$. $\square$

Lemma 5.5. *Given a Galois extension of number fields L/k , the set of ramified primes in k and the sequence of ramification groups for each ramified prime are computable.*

Proof. By Sections 2.2.4 and 2.3.5 respectively of [14], we can compute the relative discriminant ideal and factor it to obtain the ramified primes. For each ramified prime $\mathfrak{p}$ of k , we use [14, Algorithm 2.5.4] to extend it to an ideal of L , factor it to obtain a prime $\mathfrak{P}$ of L above $\mathfrak{p}$, and use [14, §2.2.3] find an element $\alpha \in \mathfrak{P}$ of $\mathfrak{P}$ -adic valuation 1. For each $\sigma \in \text{Gal}(L/k)$, we compute the valuation of $\sigma\alpha - \alpha$: this determines the ramification groups. $\square$

Proposition 5.6. *The conductor of the jacobian of a curve X over a number field k is computable.*

Proof. Let $\ell \in \mathbb{Z}$ be a prime, and let $A = \text{Jac}X$. Compute $A[\ell]$ and L as in Lemma 5.4. Use Lemma 5.5 to compute the ramification groups of $\text{Gal}(L/k)$ at each ramified prime of k . Their action on $A[\ell]$ gives us the exponent of $\mathfrak{p}$ in $\text{cond}(A)$ for each $\mathfrak{p}$ not dividing ℓ . Repeating the above with a different ℓ lets us compute the remaining exponents. $\square$

5.3. The de Franchis-Severi Theorem. The following result, which we have already mentioned, is known as the de Franchis-Severi Theorem; we show in addition that the finite set it promises is computable. We thank Matthias Aschenbrenner, Brian Conrad, Tom Graber, Tom Scanlon, and Jason Starr for discussions related to the proof.

Theorem 5.7 (de Franchis-Severi, computable version). *Let k be a number field or $\overline{\mathbb{Q}}$. Let X be a curve over k . Then the set of pairs (Y, π) where Y is a curve over k of genus at least 2 and $\pi: X \rightarrow Y$ is a morphism, up to k -isomorphism, is finite and computable.*

Remark 5.8. We consider (Y, π) and (Y', π') to be isomorphic if and only if there is an isomorphism $Y \rightarrow Y'$ whose composition with π gives π' .

Proof. For the finiteness, see pp. 223–224 of [47]. We assume first that $k = \overline{\mathbb{Q}}$. The genus g of each Y is bounded by the genus g_X of X , so it suffices to show that for each fixed $g \geq 2$, we can compute the set $\mathcal{C}_g$ of isomorphism classes of pairs (Y, π) where Y has genus g .

View X as a subvariety of $\mathbb{P}^n$ using the tricanonical embedding. Compute equations defining X in $\mathbb{P}^n$. If $(Y, \pi) \in \mathcal{C}_g$ and $Y \subseteq \mathbb{P}^m$ is the tricanonical embedding of Y , then $3K_X - \pi^*(3K_Y)$ is linearly equivalent to an effective divisor, so the theory of linear systems implies that there is a linear subspace $L \subseteq \mathbb{P}^n$ of dimension $n - m - 1$ such that π and the linear projection $\pi_L: \mathbb{P}^n \dashrightarrow \mathbb{P}^m$ coincide on $X - L$. Riemann-Roch gives $n = 5g_X - 6$ and $m = 5g - 6$. Let G be the Grassmannian variety whose points correspond to linear subspaces $L \subseteq \mathbb{P}^n$ of dimension $n - m - 1$. Then $(Y, \pi) \mapsto L$ defines an injection $\iota: \mathcal{C}_g \rightarrow G(\overline{\mathbb{Q}})$.

Conversely, if we start with a linear subspace L , corresponding to a point $s \in G$, let Y_s be the Zariski closure of $\pi_L(X - L)$ in $\mathbb{P}^m$, and let $\pi_s: X \rightarrow Y_s$ denote the morphism induced by π_L . The map $s \mapsto (Y_s, \pi_s)$ restricted to $\iota(\mathcal{C}_g)$ is an inverse of ι , but in general (Y_s, π_s) need not be in $\mathcal{C}_g$. Moreover, the Y_s need not form the fibers of a smooth (or even flat) family.

Claim 1: Each closed subvariety $H \subseteq G$ can be (computably) partitioned into a finite number of irreducible locally closed subsets H_i such that for each i , either

- (1) For all $s \in H_i$, the curve Y_s is not smooth over the residue field of s , or
- (2) There is a smooth family $\mathcal{Y} \rightarrow H_i$ of curves, and an H_i -morphism $X \times_k H_i \rightarrow \mathcal{Y}$ whose fiber above $s \in H_i$ is $\pi_s: X \rightarrow Y_s$.

Proof: We use induction on $\dim H$. Because irreducible components can be computed, we may reduce to the case where H is irreducible.

We next use the principle that “whatever happens at the generic point also happens over some computable dense Zariski open subset.” Let η be the generic point of H , and let L be the corresponding linear subspace defined over the function field κ of H . Choose a dense open affine subset $\text{Spec} A$ of H , and write elements of κ as ratios of elements of A . Working over κ , we compute the intersection of L with X , the image of $X - L$ under the projection $\mathbb{P}^n \dashrightarrow \mathbb{P}^m$, its closure Y_η , and the morphism $\pi_\eta: X \rightarrow Y_\eta$. Using partial derivatives, we compute also whether or not Y_η is smooth over κ . Compute the localization A' of A obtained by adjoining to A the inverses of the numerators and denominators of the finitely many elements of κ that appear during these computations. Then the formulas computed over κ make sense over $\text{Spec} A'$, so that all the constructions can be performed over $\text{Spec} A'$. Moreover, for each $s \in \text{Spec} A'$, the curve Y_s is smooth over the residue field of s if and only if Y_η is smooth over κ .

Let $H_1 = \text{Spec} A' \subseteq H$. The complement $H - H_1$ is a closed subvariety of lower dimension than H , so using the inductive hypothesis, we can partition $H - H_1$ into $H_2, \dots, H_n$ with the desired properties. This completes the proof of Claim 1.

Apply Claim 1 to G , and discard the H_i in which the Y_s are not smooth. For each remaining H_i , the genus of Y_s is constant for $s \in H_i$, so we compute the genus of the generic fiber Y_η and discard H_i if this genus is not g .

Claim 2: For each remaining H_i , let J_i be the set of $s \in H_i$ for which the linear subspace $L \subseteq \mathbb{P}^n$ corresponding to s equals the linear subspace $L' \subseteq \mathbb{P}^n$ defined as the common zeros of the sections in the image of $H^0(Y_s, \omega^{\otimes 3}) \hookrightarrow H^0(X, \omega^{\otimes 3})$. Then J_i is constructible and computable.

Proof: The strategy of proof is the same as that of Claim 1. The equality of L and L' can be tested at the generic point η of H_i , and the outcome will be the same on some computable dense Zariski open subset of H_i . We finish the proof of Claim 2 by an induction on the dimension.

Let J be the (computable) union of the J_i . By definition, $J = \iota(\mathcal{C}_g)$. Since $\mathcal{C}_g$ is finite, J is finite. Therefore $\mathcal{C}_g$ can be computed by computing (Y_s, π_s) for $s \in J$. This completes the proof of Theorem 5.7 in the case where $k = \overline{\mathbb{Q}}$.

Finally, suppose that k is a number field. Compute the finite subset J for $\bar{k} = \overline{\mathbb{Q}}$ as above. Since ι is G_k -equivariant, it suffices to compute the G_k -invariant elements of J . For each $L \in J \subseteq G$, we compute the Plücker coordinates for L relative to a k -basis of $H^0(X, \omega^{\otimes 3})$, and discard those for which the Plücker embedding does not map L to a k -point of projective space. The (Y_s, π_s) corresponding to the remaining elements of J are the ones over k , each appearing once. $\square$

Remark 5.9. Suppose that k is a number field. Then the finiteness of the set of Y (without the morphism) in Theorem 5.7 holds even if we include curves Y of genus ≤ 1 ! It is also

possible to compute a finite set of curves over k representing all the k -isomorphism classes of such Y , but with some classes represented more than once. Eliminating the redundancy in genus 1 would require an algorithm as in Remark 5.3.

5.4. Computability of modular curves. Here we use the results of the previous section to prove that the finite sets in Theorems 1.3, 1.8, and 1.10 are computable.

Proposition 5.10. *Fix $N \geq 1$ and a number field k . The set of k -modular curves of level dividing N up to k -isomorphism is finite and computable.*

Proof. By Theorem 5.7, it suffices to compute $X_1(N)$. First compute the genus g of $X_1(N)$ (a formula can be found in Example 9.1.6 on page 77 of [20], for example). Using modular symbols we can compute a basis of $S_2(N)$, with each q -expansion computed up to an error of $O(q^{B(g)+1})$. (This follows from [52], and an explicit method was described first in [54, §4.3]: see also the earlier paper [16] and the later thesis [71] for some related work.) Multiplying each basis element by dq/q results in expansions for a basis of differentials, and then Section 2.1 explains how to recover either an equation $y^2 = f(x)$ if $X_1(N)$ is hyperelliptic, or equations defining the image of the canonical embedding if $X_1(N)$ is not hyperelliptic. In the latter case, we can try various linear projections and use elimination theory until we find one that yields a plane curve birational to $X_1(N)$: we can detect whether a linear projection mapped the canonical model birationally by checking the genus of the image. Since we can enumerate all linear projections, we will eventually find one that will work. (In practice, almost any projection will work.) $\square$

Question 5.11. The de Franchis-Severi Theorem lets us prove the finiteness of modular curves of *fixed level* whether or not they are new. Can the proof of the de Franchis-Severi Theorem somehow be combined with our proof of Theorem 1.3 to prove Conjecture 1.1 in general?

Proof of computability in Theorems 1.3, 1.8, and 1.10. The proof of finiteness in Theorem 1.3 produces a finite list of candidate curves X . For each X , we compute $N := \text{cond}(\text{Jac}X)^{1/g}$, which will be the level of X if X is a new modular curve of genus g and level N . (If N is not an integer, discard X immediately.) By Proposition 5.10, we can list all modular curves of level N . Lemma 5.1(3) determines if X is birational to a curve in this list; discard X if not. If X is in this list, then it is modular of genus g and level N , and it must be new, since otherwise $\text{cond}(\text{Jac}X)$ would be less than N^g . Thus we can obtain a list of all new modular curves of genus g . Finally, we can use Lemma 5.1(3) to eliminate redundancy.

Computability in Theorem 1.8 now follows from computability in Theorem 1.3 and Proposition 4.4. Computability in Theorem 1.10 follows from computability in Theorem 1.8 and Proposition 7.4. $\square$

Remark 5.12. We now explain the difficulty in proving computability of the sets in Theorem 1.5. In the proof of finiteness in part (i) (with $S = \text{Sparse}_{B(g)}$), we obtained a finite list of candidates X . The problem is that we do not know how to bound the level of a given non-new modular curve; in fact, we do not even know how to test if a curve is modular. The levels of the modular forms corresponding to the regular differentials on X can be bounded by the conductor of the jacobian of X , but this is not enough, since the level of X can be higher than the levels of these forms: see Section 8.2.

Our proof of Theorem 1.5(ii) is ineffective, because there is no known effective proof of the Shafarevich conjecture.

6. NEW MODULAR HYPERELLIPTIC CURVES

By Theorem 1.8, the set of the new modular hyperelliptic curves over $\mathbb{Q}$ is finite. By Remark 4.5, the genus of such a curve is ≤ 17 . The goal of this section is to improve this by proving Theorem 1.9 and other restrictions on these curves. The main results are summarized in Table 1 and proved in Section 6.3. The computational results are given in tables in the appendix, and summarized in Section 6.5.

6.1. Criterion to determine new modular hyperelliptic curves. In this subsection we will characterize effectively the class of new modular hyperelliptic curves. From now on, for a hyperelliptic curve X we denote by $\text{WP}(X)$ the set of Weierstrass points of X .

Lemma 6.1. *Assume that there exists a nonconstant morphism $\pi: X_1(N)_{\mathbb{C}} \rightarrow X$ of curves over $\mathbb{C}$ such that X is hyperelliptic of genus g and $\pi^*H^0(X, \Omega) = H^0(A_{\mathbb{C}}, \Omega)$, for some abelian variety A over $\mathbb{Q}$ which is a quotient of $J_1(N)^{\text{new}}$. We denote by $f^{(j)} = \sum_{n \geq 1} a_n^{(j)} q^n$, $1 \leq j \leq g$, a basis for $S_2(A)$ consisting of elements of New_N , and we set $P = \pi(\infty)$. Then:*

(1) *There exists a unique basis $\{h_1, \dots, h_g\}$ of $S_2(A)$ such that for all $1 \leq j \leq g$:*

$$\begin{cases} h_j \equiv q^j & (\text{mod } q^{g+1}) & \text{if } P \notin \text{WP}(X), \\ h_j \equiv q^{2j-1} + \sum_{i=j}^{g-1} C_{j,2i} q^{2i} & (\text{mod } q^{2g}) & \text{if } P \in \text{WP}(X). \end{cases}$$

(2) *Moreover,*

(i) *If $P \notin \text{WP}(X)$, then $\det(a_i^{(j)})_{1 \leq i, j \leq g} \neq 0$.*

(ii) *If $P \in \text{WP}(X)$, then $\det(a_{2i-1}^{(j)})_{1 \leq i, j \leq g} \neq 0$.*

Proof. Applying Lemma 2.5 and the fact that π is unramified at the cusp ∞ , we obtain the existence of a basis $\{h'_1, \dots, h'_g\}$ of $S_2(A)$ which satisfies:

$$\begin{cases} h'_j \equiv q^{2j-1} & (\text{mod } q^{2j}) & \text{if } P \in \text{WP}(X) \\ h'_j \equiv q^j & (\text{mod } q^{j+1}) & \text{if } P \notin \text{WP}(X) \end{cases}$$

for all $1 \leq j \leq g$. Therefore, (1) is obtained by Gaussian elimination. To obtain (2), it suffices to observe that the matrices in (i) and (ii) are the change of basis matrices from $\{f^{(j)}\}$ to the basis $\{h_j\}$. $\square$

Remark 6.2. Later, in Proposition 6.7, we prove that if $P \in \text{WP}(X)$ then $a_{2n}^{(j)} = 0$ for all $n \geq 1$ and $j \leq g$. In particular, $4 \mid N$ and the basis h_j satisfies

$$h_j \equiv q^{2j-1} \pmod{q^{2g}}.$$

Remark 6.3. If moreover X comes from a curve over $\mathbb{Q}$ having jacobian isogenous to A_f with $f = q + \sum_{n \geq 2} a_n q^n \in \text{New}_N$, then part (2) of the lemma implies that $\{1, a_2, \dots, a_g\}$ (resp. $\{1, a_3, \dots, a_{2g-1}\}$) is a $\mathbb{Q}$ -basis of E_f if $P \notin \text{WP}(X)$ (resp. $P \in \text{WP}(X)$).

Remark 6.4. If A is a quotient of $J_1(N)$ (over $\mathbb{Q}$), and the $\mathbb{C}$ -vector space $S_2(A)$ has a basis $\{h_1, \dots, h_g\}$ as in part (1) of the previous lemma, then each h_i has Fourier coefficients in $\mathbb{Q}$, since $S_2(A)$ has a basis contained in $\mathbb{Q}[[q]]$.

The following proposition provides us with an effective criterion to determine when a $\mathbb{Q}$ -factor of $J_1(N)^{\text{new}}$ is $\mathbb{Q}$ -isogenous to the jacobian of a modular hyperelliptic curve of level N . Let $\langle v_1, \dots, v_n \rangle$ denote the span of elements $v_1, \dots, v_n$ of a vector space.

Proposition 6.5. *Let A be a quotient of $J_1(N)^{\text{new}}$ of dimension $g > 1$. The following conditions are equivalent:*

- (1) *There exists a modular hyperelliptic curve X of level N over $\mathbb{Q}$ such that $\text{Jac} X \simeq A$.*
- (2) *There exists a hyperelliptic curve X' over $\mathbb{C}$ and a nonconstant morphism $\pi' : X_1(N)_{\mathbb{C}} \rightarrow X'$ such that $\pi'^* H^0(X', \Omega) = H^0(A_{\mathbb{C}}, \Omega)$.*
- (3) *There exists a basis $\{h_1, \dots, h_g\}$ of $S_2(A)$ as in part (1) of Lemma 6.1 such that for every pair $g_1, g_2 \in S_2(A)$ satisfying $\langle g_1, g_2 \rangle = \langle h_{g-1}, h_g \rangle$ and $g_2 \in \langle h_g \rangle$, there exists $F(U) \in \mathbb{C}[U]$ of degree $2g+1$ or $2g+2$ without double roots such that the functions on $X_1(N)$ given by*

$$x = \frac{g_1}{g_2}, \quad y = \frac{q dx/dq}{g_2}$$

satisfy the equation $y^2 = F(x)$.

Proof. It is clear that (1) implies (2). Also, (3) implies (1), because when we apply (3) with $g_1 = h_{g-1}$ and $g_2 = h_g$, the modular functions x and y have rational q -expansion, so the corresponding polynomial F has coefficients in $\mathbb{Q}$.

We now assume (2) and prove (3). By Lemma 6.1, there exists such a basis $\{h_1, \dots, h_g\}$. As before, we put $P = \pi'(\infty)$. Let u and v be nonconstant functions on X' such that:

- $\text{div } u = (Q) + (w(Q)) - (P) - (w(P))$ for some $Q \in X'$ and where w denotes the hyperelliptic involution of X' .
- $v^2 = G(u)$, where $G(U)$ is a polynomial in $\mathbb{C}[U]$ of degree $2g+1$ or $2g+2$, without double roots.

By looking at $\text{ord}_P du/v$ and $\text{ord}_P udu/v$, and using the fact that π' is unramified at ∞ , we have:

$$\langle \pi'^*(du/v), \pi'^*(udu/v) \rangle = \langle h_{g-1}dq/q, h_g dq/q \rangle, \quad \langle \pi'^*(du/v) \rangle = \langle h_g dq/q \rangle.$$

Thus, for every pair g_1, g_2 as in part (3), there exists a matrix $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{GL}_2(\mathbb{C})$ such that

$$\begin{cases} g_1 dq/q = a \pi'^*(udu/v) + b \pi'^*(du/v) \\ g_2 dq/q = d \pi'^*(du/v). \end{cases}$$

Now, one can check easily that the modular functions

$$x := \frac{g_1}{g_2}, \quad y := \frac{q dx/dq}{g_2}$$

satisfy the equation $y^2 = F(x)$, where

$$F(U) = \frac{a^2}{d^4} G\left(\frac{dU - b}{a}\right).$$

□

In practice, the previous proposition will be used together with the next result.

Lemma 6.6. *Let Y be a curve of genus $g_Y > 0$ over $\mathbb{C}$. Let q be an analytic uniformizing parameter in $\hat{\mathcal{O}}_{Y,P}$ for a point $P \in Y(\mathbb{C})$ and let $F \in \mathbb{C}[t]$ be a polynomial of degree $d > 0$. Suppose we are given $\omega_1, \omega_2 \in H^0(Y, \Omega)$ such that the functions $x = \omega_1/\omega_2$ and $y = dx/\omega_2$ satisfy*

$$y^2 - F(x) \equiv 0 \pmod{q^c} \quad \text{for some } c \geq (2g_Y - 2) \text{Max}\{6, d\} + 1.$$

Then we have $y^2 = F(x)$.

Proof. Put $d' = \text{Max}\{6, d\}$. Now, it suffices to observe that $y\omega_2^3 \in H^0(Y, \Omega^{\otimes 3})$ and, thus, $(y^2 - F(x))\omega_2^{d'} \in H^0(Y, \Omega^{\otimes d'})$ and has at P a zero of order $d'(2g_Y - 2) + 1$ at least. $\square$

The following proposition improves part (1) of Lemma 6.1 and is useful for computations.

Proposition 6.7. *Let X be a new modular hyperelliptic curve of genus g and level N over $\mathbb{Q}$ and let $\pi: X_1(N) \rightarrow X$ be the corresponding morphism. If $\pi(\infty) \in \text{WP}(X)$ and $f = q + \sum_{n \geq 2} a_n q^n \in \text{New}_N \cap S_2(X)$, then $a_{2n} = 0$ for all $n \geq 1$ and $4 \mid N$.*

Proof. Write $S_2(X) = \oplus_{i=1}^m S_2(A_{f^{(j)}})$, where $f^{(j)} = q + \sum_{n \geq 2} a_n^{(j)} q^n$ is a newform in $S_2(N, \varepsilon_j)$. The condition that $a_{2n}^{(j)} = 0$ for all n and j is equivalent to the condition that $a_2^{(j)} = 0$ for all j and $2 \mid N$. We consider three cases.

Case 1: $g = 2$ and $\text{Jac}X$ is $\mathbb{Q}$ -simple.

Put $f := f^{(1)} = \sum_{n \geq 0} a_n q^n$. The coefficients of f generate some quadratic field $\mathbb{Q}(\sqrt{d})$. Let σ denote the nontrivial element of $\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, so that $f^{(2)} = \sigma f$. By parts (1) and (2)(ii) of Lemma 6.1, respectively, we have $a_2 \in \mathbb{Q}$ and $a_3 \notin \mathbb{Q}$. Write $a_n := A_n + B_n \sqrt{d}$, where $A_n, B_n \in \mathbb{Q}$. Define $\varepsilon := \varepsilon_1$. By (3.7) the q -expansion of f is:

$$q + A_2 q^2 + (A_3 + B_3 \sqrt{d}) q^3 + (A_2^2 - 2\varepsilon(2)) q^4 + (A_5 + B_5 \sqrt{d}) q^5 + A_2(A_3 + B_3 \sqrt{d}) q^6 + O(q^7),$$

where $B_3 \neq 0$. Put $\varepsilon(2) = C + D\sqrt{d}$. Following Lemma 6.1 and Proposition 6.5, we compute

$$h_1 = \frac{f + \sigma f}{2}, \quad h_2 = \frac{f - \sigma f}{2B_3 \sqrt{d}}, \quad x = \frac{h_1}{h_2} = \frac{1}{q^2} + \dots, \quad y = -\frac{q dx/dq}{2h_2} = \frac{1}{q^5} + \dots$$

For $F \in \mathbb{C}((q))$, let $\text{Coeff}[q^n, F]$ denote the coefficient of q^n in F . Since $y^2 - x^5$ is at most a quartic polynomial in x , and x is $O(q^{-2})$, we have $\text{Coeff}[q^{-9}, y^2 - x^5] = 0$. On the other hand, we compute $\text{Coeff}[q^{-9}, y^2 - x^5] = -4(A_2 B_3 + D)/B_3$, so $D = -A_2 B_3$. Thus $D = 0$ if and only if $A_2 = 0$. We claim that $A_2 = D = 0$. If $2 \mid N$ then $\varepsilon(2) = 0$, so $D = 0$. If $2 \nmid N$, then $\bar{a}_2 = \varepsilon(2)a_2$ by (3.13), so $A_2 = (C \pm D\sqrt{d})A_2$ and equating coefficients of $\sqrt{d}$ yields $DA_2 = 0$. Thus $A_2 = D = 0$ in both cases.

Now $y^2 - x^5 - \text{Coeff}[q^{-8}, y^2 - x^5]x^4$ is at most a cubic polynomial in x , so

$$0 = \text{Coeff}[q^{-7}, y^2 - x^5 - \text{Coeff}[q^{-8}, y^2 - x^5]x^4] = 12C.$$

Thus $C = 0$, so $\varepsilon(2) = 0$. By (3.7), $a_2 = \varepsilon(2) = 0$ implies $a_{2n} = 0$ for all n . By (3.10) and (3.11), we have $4 \mid N$.

Case 2: $g = 2$ and $\text{Jac}X$ is not $\mathbb{Q}$ -simple.

Then $\text{Jac}X \cong A_{f^{(1)}} \times A_{f^{(2)}}$ with $\dim A_{f^{(1)}} = \dim A_{f^{(2)}} = 1$. Since $\dim A_{f^{(1)}}$ is odd, the Nebentypus ε of $f^{(1)}$ is the trivial character modulo N (cf. the proof of Lemma 6.17). The same holds for $f^{(2)}$. By part (1) of Lemma 6.1, $f^{(1)}$ and $f^{(2)}$ share the same coefficient of q^2 , say a . By (3.7),

$$\begin{aligned} f^{(1)} &= q + a q^2 + a_3 q^3 + (a^2 - 2\varepsilon(2)) q^4 + a_5 q^5 + a a_3 q^6 + O(q^7), \\ f^{(2)} &= q + a q^2 + b_3 q^3 + (a^2 - 2\varepsilon(2)) q^4 + b_5 q^5 + a b_3 q^6 + O(q^7), \end{aligned}$$

with $a, a_n, b_n \in \mathbb{Z}$. By part (2) of Lemma 6.1, $a_3 \neq b_3$. As in Case 1, we compute

$$h_1 = \frac{f^{(1)} + f^{(2)}}{2}, \quad h_2 = \frac{f^{(1)} - f^{(2)}}{a_3 - b_3}, \quad x = \frac{h_1}{h_2} = \frac{1}{q^2} + \dots, \quad y = -\frac{q dx/dq}{2h_2} = \frac{1}{q^5} + \dots$$

From $0 = \text{Coeff}[q^{-9}, y^2 - x^5] = -4a$ we obtain $a = 0$. From

$$0 = \text{Coeff}[q^{-7}, y^2 - x^5 - \text{Coeff}[q^{-8}, y^2 - x^5]x^4] = 12\varepsilon(2)$$

we obtain $\varepsilon(2) = 0$. The result follows from $a = \varepsilon(2) = 0$, as in Case 1.

Case 3: $g > 2$.

Put

$$f^{(j)} = \sum_{n \geq 0} a_n^{(j)} q^n, \quad E_j = \mathbb{Q}(\{a_n^{(j)}\}).$$

Let $\mathbb{E}$ denote the $\mathbb{Q}$ -algebra $E_1 \times \dots \times E_m$. Let $\mathbb{E}^\vee$ denote the dual vector space $\text{Hom}_{\mathbb{Q}}(\mathbb{E}, \mathbb{Q})$, and let $\phi \cdot \widehat{a}$ denote the evaluation of a functional $\phi \in \mathbb{E}^\vee$ at an element $\widehat{a} = (a^{(j)})$ of $\mathbb{E}$. For $n \geq 1$, set $\widehat{a}_n = (a_n^{(j)}) \in \mathbb{E}$. Let $\widehat{\varepsilon(2)} = (\varepsilon_i(2)) \in \mathbb{E}$. By (3.7), we have

$$(6.8) \quad \widehat{a}_{nm} = \widehat{a}_n \widehat{a}_m \quad \text{when } (n, m) = 1,$$

$$(6.9) \quad \widehat{a}_{2^n} = \widehat{a}_{2^{n-1}} \widehat{a}_2 - 2 \widehat{\varepsilon(2)} \widehat{a}_{2^{n-2}} \quad \text{when } n \geq 2.$$

By part (2)(ii) of Lemma 6.1, $\{\widehat{a}_1, \widehat{a}_3, \widehat{a}_5, \dots, \widehat{a}_{2g-1}\}$ is a $\mathbb{Q}$ -basis of $\mathbb{E}$. Let $\{\phi_1, \phi_2, \dots, \phi_g\}$ denote the dual basis of $\mathbb{E}^\vee$. Let $h_i = \sum_{n=1}^{\infty} (\phi_i \cdot \widehat{a}_n) q^n$ for $1 \leq i \leq g$. Then h_i is a $\mathbb{Q}$ -combination of conjugates of the $f^{(j)}$, and hence $\{h_1, \dots, h_g\}$ is the basis of $S_2(X)$ promised by part (1) of Lemma 6.1. Thus the q -expansion of h_i has the form

$$h_i = q^{2i-1} + \sum_{j=i}^{g-1} C_{i,2j} q^{2j} + \sum_{j=2g}^{\infty} C_{i,j} q^j.$$

In particular, $\phi_i \cdot \widehat{a}_2 = 0$ for $i > 1$, so $\widehat{a}_2 \in \mathbb{Q} \widehat{a}_1 = \mathbb{Q}$. That is, $a_2^{(j)}$ has a value $a_2 \in \mathbb{Q}$ independent of j . Let γ equal g or $g-1$, depending on whether g is odd or even. Then by (6.8),

$$C_{\gamma, 2\gamma} = \phi_\gamma \cdot \widehat{a}_{2\gamma} = a_2 \phi_\gamma \cdot \widehat{a}_\gamma = 0,$$

since $1 < \gamma < 2\gamma - 1$. The same computation shows $C_{1,2} = a_2$. Define $x = h_{g-1}/h_g$ and $y = \frac{q dx/dq}{-2h_g}$ so that X has the equation $y^2 = F(x)$ for some monic F of degree $2g+1$. Then

$$x = q^{-2} + bq^{-1} + O(q^0) \quad \text{and} \quad y = q^{-(2g+1)} + cq^{-2g} + O(q^{-(2g-1)}),$$

for some $b, c \in \mathbb{Q}$. Also, $y^2 = F(x)$ implies $2c = (2g+1)b$. Moreover $h_i dq/q = P_{g-i}(x) dx/(-2y)$ for some monic $P_{g-i}(x) \in \mathbb{Q}[x]$ of degree $g-i$, and equating coefficients of $q^{2i-1} dq$ (just after the monic leading term) yields

$$C_{i,2i} = (g-i)b + (b/2) - c = -ib.$$

Setting $i = \gamma$ and $i = 1$ yields $0 = -\gamma b$ and $a_2 = -b$, so $a_2 = b = 0$.

Setting $i = 2$ yields $\phi_2 \cdot \widehat{a}_4 = C_{2,4} = 0$. But $\phi_i \cdot \widehat{a}_4 = 0$ also for $i > 2$, so $\widehat{a}_4 \in \mathbb{Q}$. By (6.9), $\widehat{\varepsilon(2)} \in \mathbb{Q}$. Induction using (6.9) shows that $\widehat{a}_{2^n} \in \mathbb{Q}$ for all $n \geq 0$. By (6.8), $\widehat{a}_n \in \mathbb{Q} \widehat{a}_{\text{odd}(n)}$,

where $\text{odd}(n)$ is the largest odd divisor of n . Using this, $g \geq 3$, and the definition of ϕ_i , we now prove that $C_{g,2g} = C_{g,2g+2} = C_{g-1,2g-2} = C_{g-1,2g} = 0$. Indeed,

$$(6.10) \quad \begin{aligned} C_{g,2g} &= \phi_g \cdot \widehat{a}_{2g} = 0, & \text{since } \text{odd}(2g) < 2g - 1; \\ C_{g,2g+2} &= \phi_g \cdot \widehat{a}_{2g+2} = 0, & \text{since } \text{odd}(2g+2) < 2g - 1; \\ C_{g-1,2g-2} &= \phi_{g-1} \cdot \widehat{a}_{2g-2} = 0, & \text{since } \text{odd}(2g-2) < 2g - 3; \\ C_{g-1,2g} &= \phi_{g-1} \cdot \widehat{a}_{2g} = 0, & \text{since } \text{odd}(2g) < 2g - 3; \end{aligned}$$

except that in the last equation, when $g = 3$, $\text{odd}(2g) < 2g - 3$ fails so we use $\widehat{a}_{2g} = a_2 \widehat{a}_3 = 0$ instead to deduce the same result. Therefore

$$\begin{aligned} h_{g-1} &= q^{2g-3}(1 + O(q^4)), \\ h_g &= q^{2g-1}(1 + C_{g,2g+1}q^2 + O(q^4)), \\ x &= h_{g-1}/h_g = q^{-2}(1 - C_{g,2g+1}q^2 + O(q^4)), \end{aligned}$$

and the new basis defined by $h'_i := x^{g-i}h_g$ for $1 \leq i \leq g$ satisfies

$$h'_i = q^{2i-1}(1 + c_i q^2 + O(q^4))$$

for some $c_i \in \mathbb{Q}$. The coefficient of q^4 in h'_i is zero for all i , so $\widehat{a}_4 = 0$. By (6.9), $\widehat{\varepsilon(2)} = 0$. The result follows from $\widehat{a}_2 = \widehat{\varepsilon(2)} = 0$, as in Case 1. $\square$

6.2. Automorphisms of hyperelliptic curves. Throughout this subsection we make the following assumptions:

- k is a field of characteristic zero,
- X is the smooth projective model of a curve $y^2 = F(x)$ for some squarefree $F \in k[x]$ of degree $2g + 1$ or $2g + 2$ for some $g \geq 2$ (so in particular X is a hyperelliptic curve of genus g), and
- w is the hyperelliptic involution of X .

Proposition 6.11. *Let X' be a curve of the same type as X , that is, a genus- g curve $y'^2 = F'(x')$, where $F' \in k[U]$ is squarefree. Every isomorphism $u: X_{\bar{k}} \rightarrow X'_{\bar{k}}$ is given by an expression of the following form:*

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}} \right),$$

for some $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\bar{k})$ and $e \in \bar{k}^*$. The pair (M, e) is unique up to replacement by $(\lambda M, e\lambda^{g+1})$ for $\lambda \in \bar{k}^*$. If u is defined over k , then one can take $M \in \text{GL}_2(k)$ and $e \in k^*$. Moreover, if $u': X'_{\bar{k}} \rightarrow X''_{\bar{k}}$ is another isomorphism, given by (M', e') , then the composition $u'u$ is given by $(M'M, e'e)$.

Proof. An isomorphism $X \rightarrow X'$ induces an isomorphism on the canonical images $\mathbb{P}^1 \rightarrow \mathbb{P}^1$. An automorphism of $\mathbb{P}^1$ over $\bar{k}$ is given by some $M \in \text{GL}_2(\bar{k})$. The functions $f \in \bar{k}(X)$ such that $w^*f = -f$ are those in $\bar{k}(x)y$, so y' corresponds to $ey/(cx + d)^{g+1}$ for some $e \in \bar{k}(x)$. The image of $(x, y) \in X$ must be on X' , so

$$\left(\frac{ey}{(cx + d)^{g+1}} \right)^2 = F' \left(\frac{ax + b}{cx + d} \right),$$

or equivalently,

$$e^2 F(x) = (cx + d)^{2g+2} F' \left(\frac{ax + b}{cx + d} \right).$$

The right hand side is a squarefree polynomial, since it can be obtained from F' by homogenizing to a polynomial $z^{2g+2} F'(x/z)$ of degree $2g+2$, performing a linear change of variable on x and z , and dehomogenizing. But $F(x)$ on the left is a squarefree polynomial too. Thus $e \in \bar{k}^*$. The rest of the statements follow easily. $\square$

Recall that $\text{Aut}(X)$ denotes the group of automorphisms of X defined over k .

Lemma 6.12. *Let $u \in \text{Aut}(X)$. We use the (M, e) notation as in Proposition 6.11. Then:*

- (1) *If g is even, u is represented by a unique pair $(M, e) \in \text{GL}_2(k) \times k^*$ satisfying $e = (\det M)^{g/2}$. Then $u \mapsto M$ defines an injective homomorphism $\text{Aut}(X) \rightarrow \text{GL}_2(k)$ mapping w to $-\text{id}$.*
- (2) *If g is odd, u is represented by exactly two pairs $(\pm M, e) \in \text{GL}_2(\bar{k}) \times \bar{k}^*$ satisfying $e^2 = (\det M)^g$. Then $u \mapsto e$ defines a homomorphism $\text{Aut}(X) \rightarrow \mu(k)$ mapping w to -1 , where $\mu(k)$ denote the group of roots of unity in k .*

Proof. Suppose g is even. For a fixed pair $(M_0, e_0) \in \text{GL}_2(k) \times k^*$, the condition $e_0 \lambda^{g+1} = (\det(\lambda M_0))^{g/2}$ on $\lambda \in \bar{k}^*$ is equivalent to $\lambda = (\det M_0)^{g/2} / e_0$. Thus λ is unique and, in particular, $\lambda \in k^*$. Uniqueness also implies that $u \mapsto M$ is a homomorphism. Since $e = (\det M)^{g/2}$, M determines (M, e) , so the homomorphism is injective.

Now suppose g is odd. If g is odd, the condition $(e_0 \lambda^{g+1})^2 = (\det(\lambda M_0))^g$ determines λ up to sign. It follows that $\lambda^2 \in k^*$ and that $e := e_0 \lambda^{g+1}$ is in k . Then $u \mapsto e$ defines a homomorphism $\text{Aut}(X) \rightarrow k^*$. Its image is contained in $\mu(k)$, since $\text{Aut}(X)$ is finite. $\square$

Lemma 6.13. *Suppose $k = \mathbb{Q}$. If g is even, then $\text{Aut}(X)$ is isomorphic to a subgroup of $D_{2.4}$ or $D_{2.6}$. If g is odd, then $\text{Aut}(X)$ is the direct product of $\langle w \rangle$ and a subgroup isomorphic to a subgroup of $D_{2.4}$ or $D_{2.6}$. In either case, every element of $\text{Aut}(X)$ has order 1, 2, 3, 4, or 6.*

Proof. Suppose g is even. By Lemma 6.12, $\text{Aut}(X)$ is isomorphic to a finite subgroup G of $\text{GL}_2(\mathbb{Q})$. By averaging an inner product on $\mathbb{Q}^2$, we obtain a G -invariant inner product, so G can be embedded in the orthogonal group $O_2(\mathbb{R})$. All finite subgroups of $O_2(\mathbb{R})$ are cyclic or dihedral, so it remains to show that elements of G have order dividing 4 or 6. This follows since the eigenvalues of G are roots of unity in a number field of degree at most 2.

Now suppose g is odd. Let $\overline{\text{Aut}(X)}$ denote the image of the homomorphism $\text{Aut}(X) \rightarrow \text{Aut}(\mathbb{P}^1) \simeq \text{PGL}_2(\mathbb{Q})$ mapping $u \in \text{Aut}(X)$ to its action on the canonical image of X . The first map in the exact sequence

$$0 \rightarrow \langle w \rangle \rightarrow \text{Aut}(X) \rightarrow \overline{\text{Aut}(X)} \rightarrow 0$$

has a section $\text{Aut}(X) \rightarrow \mu(\mathbb{Q}) = \{\pm 1\} \simeq \langle w \rangle$ mapping u to e as in Lemma 6.12. Thus $\text{Aut}(X) \simeq \langle w \rangle \times \overline{\text{Aut}(X)}$. Every finite subgroup of $\text{PGL}_2(\mathbb{Q})$ is isomorphic to a subgroup of $D_{2.4}$ or $D_{2.6}$, by Proposition A in [28]. $\square$

Proposition 6.14. *Suppose $k = \bar{k}$. Then*

- (1) *$\text{Aut}(X)$ does not contain $(\mathbb{Z}/2\mathbb{Z})^4$.*
- (2) *If $\text{Aut}(X)$ contains $(\mathbb{Z}/2\mathbb{Z})^3$, then g is odd.*
- (3) *If $\text{Aut}(X)$ contains $\mathbb{Z}/2\mathbb{Z} \times D_{2.4}$, then $4|(g+1)$.*

- (4) If $\text{Aut}(X)$ contains $\mathbb{Z}/2\mathbb{Z} \times D_{2 \cdot 6}$, then $6|(g+1)$.
- (5) If $\text{Aut}(X)$ contains $D_{2 \cdot 6}$, then $g \not\equiv 1 \pmod{3}$.

Proof. This follows from Proposition 2.1 and Satz 5.1 of [9]. See [11] for more, including a complete classification of the groups that can be the automorphism group of a hyperelliptic curve of given genus. $\square$

Lemma 6.15. *Let $\pi: X \rightarrow X'$ be a degree- d morphism between curves of genus g and g' , respectively, over a field of characteristic zero. Assume that $g \geq 2$ and X is hyperelliptic. Then*

- (1) *If $g' \geq 2$, then X' is hyperelliptic.*
- (2) *If $g' \geq 2$, then $\pi(\text{WP}(X)) \subseteq \text{WP}(X')$.*
- (3) *Suppose that $X' = X/\langle \alpha \rangle$ for some $\alpha \in \text{Aut}(X)$ of order d . Assume that the hyperelliptic involution w of X is not in $\langle \alpha \rangle$. Let g'' be the genus of $X'' = X/\langle \alpha w \rangle$.*
 - (a) *If d is odd, then $g' = \lfloor g/d \rfloor$.*
 - (b) *If d is even and $g \not\equiv -1 \pmod{d}$, then $g' = \lfloor g/d \rfloor$.*
 - (c) *If d is even and $g \equiv -1 \pmod{d}$, then g' and g'' equal $\lfloor g/d \rfloor$ and $\lceil g/d \rceil$ in some order.*

Proof. (1) The image Y of the canonical map $X \rightarrow \mathbb{P}^{g-1}$ has genus zero and dominates the corresponding image for X' , which implies that its genus is zero too. Therefore, X' is hyperelliptic.

(2) Let w and w' denote the hyperelliptic involutions on X and X' , respectively. Since the function field $k(X)$ is of degree 2 over $k(Y)$, it must equal the compositum of $k(X')$ and $k(Y)$ over $k(Y')$, and the unique nontrivial element w^* of $\text{Gal}(k(X)/k(Y))$ must restrict to the unique nontrivial element $(w')^*$ of $\text{Gal}(k(X')/k(Y'))$. Thus $\pi w = w' \pi$. Hence fixed points of w map to fixed points of w' . (Alternatively, (1) and (2) could have been deduced from Proposition 2.11(ii).)

(3) We may assume $k = \bar{k}$. Since $w \notin \langle \alpha \rangle$, the automorphisms α and w induce an automorphism of Y of degree d and an involution on X' respectively. Let us denote $Y' = X'/\langle w \rangle$, where w stands for the involution induced on X' . Up to conjugacy, $\text{Aut}(Y) = \text{PGL}_2(k)$ contains only one cyclic subgroup of order d . Thus we may choose coordinates so that the morphism $\mathbb{P}^1 \simeq Y \rightarrow Y' \simeq \mathbb{P}^1$ induced by $X \rightarrow X'$ is $x \mapsto x' = x^d$. In particular, $Y \rightarrow Y'$ is ramified above two points $0, \infty \in Y'$, each with ramification index d .

Let $r' \in \{0, 1, 2\}$ be the number of points of Y' among 0 and ∞ that ramify in $X' \rightarrow Y'$. Concerning the behavior of the points in X above 0 and ∞ in $X \rightarrow X'$: if d is odd, we have $2(2 - r') + r'$ points with ramification index d ; if d is even, we have $2(2 - r')$ points with ramification index d , and $2r'$ points with ramification index $d/2$. The Hurwitz formula gives

$$2g - 2 = d(2g' - 2) + \begin{cases} (4 - r')(d - 1) & \text{if } d \text{ is odd} \\ (4 - 2r')(d - 1) + (2r')(d/2 - 1) & \text{if } d \text{ is even.} \end{cases}$$

This implies $g = dg' + (d - 1) - r'\lfloor d/2 \rfloor$. If d is odd, then we deduce $g' = \lfloor g/d \rfloor$. If d is even and $g \not\equiv -1 \pmod{d}$, then $r' = 1$, and $g' = \lfloor g/d \rfloor$.

Finally suppose that d is even and $g \equiv -1 \pmod{d}$. Then $r' \in \{0, 2\}$. Since X is birational to $y^2 = f(x^d)$ for some polynomial f , and d is even, the points 0 and ∞ have a total of 4 preimages in X . Each of these four preimages is fixed by α or αw , but not both. There are $2(2 - r')$ fixed points of α , so there are $2r'$ fixed points of αw . Applying the same arguments to the analogous number r'' defined for X'' , we find $2(2 - r'')$ fixed points

of αw , so $r' + r'' = 2$. Thus either $(r', r'') = (0, 2)$, in which case $(g', g'') = (\lfloor g/d \rfloor, \lceil g/d \rceil)$, or $(r', r'') = (2, 0)$, in which case $(g', g'') = (\lceil g/d \rceil, \lfloor g/d \rfloor)$. $\square$

Remark 6.16. It is not necessarily true that $\pi(\text{WP}(X)) = \text{WP}(X')$.

6.3. Restrictions on new modular hyperelliptic curves.

Proof of part (ii) of Theorem 1.9. If $3 \nmid N$, then Lemma 3.22 implies $g < 11$. Therefore assume $3 \mid N$ from now on. We are given that $\text{Jac } X$ is a quotient of $J_0(N)$. By Proposition 2.11(i), the morphism $\pi: X_1(N) \rightarrow X$ factors through a morphism $\pi_0: X_0(N) \rightarrow X$. Let $\{f^{(1)}, \dots, f^{(g)}\}$ be the basis of newforms of $S_2(X)$. Write $f^{(j)} = \sum_{n \geq 1} a_n^{(j)} q^n$. Then $a_1^{(j)} = 1$ for all j , and $g \geq 3$, so Lemma 6.1(2) implies that $a_3^{(j)}$ cannot also be independent of j . In particular there exists j such that $a_3^{(j)} \neq 0$. By (3.9), it follows that $9 \nmid N$. Hence we have the Atkin-Lehner involution W_3 on $X_0(N)$, which is defined over $\mathbb{Q}$. By (3.10), $a_3^{(j)} \in \{1, -1\}$. By (3.12), $f^{(j)}|W_3 = -a_3^{(j)} f^{(j)}$ for all j . Set $X' := X/\langle W_3 \rangle$, where W_3 denotes the automorphism of X induced from W_3 on $X_0(N)$ by Proposition 2.11(ii). Then X' also is new of level N and $S_2(X')$ is spanned by the $f^{(j)}$ with $a_3^{(j)} = -1$. There is at least one such j , since otherwise $a_3^{(j)} = 1$ for all j , contradicting Lemma 6.1(2). Applying Lemma 6.1(2) to X' shows that the genus g' of X' is ≤ 2 . Similarly, if $X'' = X/\langle wW_3 \rangle$ then $S_2(X'')$ is spanned by the $f^{(j)}$ with $a_3^{(j)} = 1$, and the genus g'' of X'' is ≤ 2 . But $g' + g'' = g \geq 3$, so either $g' = 2$ or $g'' = 2$ (maybe both). Hence X is a new modular hyperelliptic curve of genus 3 or 4 having the same level as some new modular curve of genus 2. We know the latter levels, so we can compute all such curves using the methods to be discussed in Section 6.4, one level at a time. We find only the curve $C_{39}^{A,B}$ in Table 8. This must be $X_0(39)$, because $X_0(39)$ is a new modular genus-3 curve of level divisible by 3. $\square$

Lemma 6.17. *Let X be a new modular curve of genus g and let $\mathcal{D}'$ be a subgroup of $\mathcal{D}$. If the quotient $X' := X/\mathcal{D}'$ has genus g' , then $g - g'$ is even. In particular, if X is hyperelliptic and the hyperelliptic involution w belongs to $\mathcal{D}$, then g is even.*

Proof. Assume $\mathcal{D}' \neq \{1\}$. If a newform $f \in S_2(X)$ lies outside the image of $S_2(X')$ then f has nontrivial Nebentypus, so the number field E_f is a CM field and then $\dim A_f$ is even. Indeed, it was proved in [64] (see Proposition 3.3 and the subsequent remark) that given a newform f of weight k and with nontrivial Nebentypus ε , the number field E_f (which must be either a totally real field or a CM field) is totally real if and only if f has complex multiplication by an imaginary quadratic field K and ε is the quadratic character χ attached to K . By Theorem 3.4 of [64], if f has complex multiplication by K then the character $\eta = \varepsilon \cdot \chi$ satisfies $\eta(-1) = (-1)^{k-1}$. In particular, if k is even then the character ε is different from χ and E_f must be a CM field.

The quotient of $\text{Jac } X$ by the image of $\text{Jac } X'$ is isogenous to a product of such A_f , so it has even dimension. $\square$

Proposition 6.18. *Let X be a new modular hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$. Then $\mathcal{D}$ is cyclic of order 1, 2, 3, 4 or 6. If $\#\mathcal{D} = 4$ or 6, then the hyperelliptic involution w is in $\mathcal{D}$. If $\#\mathcal{D} = 6$, then g is 2, 12 or 14.*

Proof. We may assume $\mathcal{D} \neq \{1\}$. If $\mathcal{D}$ is cyclic, let u denote a generator.

Since $\langle \mathcal{D}, w \rangle$ is an abelian subgroup of $\text{Aut}(X)$ of even order, Lemma 6.13 implies that it is isomorphic to one of the following:

$$(6.19) \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^2, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^3.$$

We label these Cases 1 through 7, respectively.

By (3.15), $W_N \notin \text{Aut}(X)$, and the group $\mathcal{D}_N'' = \langle \mathcal{D}, w, W_N \rangle$ is a semidirect product $\langle \mathcal{D}, w \rangle \rtimes \langle W_N \rangle$ with W_N acting on the normal subgroup $\langle \mathcal{D}, w \rangle$ as -1 . Hence in Cases 4, 5, 6, 7, the group $\mathcal{D}_N''$ is isomorphic to

$$(\mathbb{Z}/2\mathbb{Z})^3, \quad \mathbb{Z}/2\mathbb{Z} \times D_{2,4}, \quad \mathbb{Z}/2\mathbb{Z} \times D_{2,6}, \quad (\mathbb{Z}/2\mathbb{Z})^4,$$

respectively. Case 7 is impossible by Proposition 6.14(1).

In Cases 4, 5, 6, Proposition 6.14 implies $2|(g+1)$, $4|(g+1)$, $6|(g+1)$, respectively. In particular, g is odd, so Lemma 6.17 implies that $w \notin \mathcal{D}$, so $\mathcal{D}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, respectively. This proves the first statement of Proposition 6.18. To prove the second statement, it suffices to rule out Cases 5 and 6.

Case 5: $\mathcal{D} \simeq \mathbb{Z}/4\mathbb{Z}$, $w \notin \mathcal{D}$.

Combining $4|(g+1)$ with the inequality $g \leq 17$ of Remark 4.5 shows that g is 3, 7, 11, or 15. Lemma 6.17 implies that the genus g' of $X' := X/\mathcal{D}$ is odd. Hence Lemma 6.15(3) implies that (g, g') is $(3, 1)$, $(7, 1)$, $(11, 3)$, or $(15, 3)$. In the last two cases (with $g' = 3$), parts (1) and (3) of Lemma 6.15 imply that either $X'' = X'/W_N = X/\mathcal{D}_N$ or $X''' = X'/\langle W_N w \rangle = X/\mathcal{D}_N'$ has genus 2 and is dominated by $X_0(N)$. In the first two cases, Lemma 6.15(3) implies that the curve $X/\langle u^2 w \rangle$ (resp. $X/\langle uw \rangle$) has genus 2 and has a nontrivial diamond of order 4 (resp. 2) by Lemma 3.17 (the nontrivial diamond prevents the genus from being 1). Using the methods of Section 6.4 to check all levels where there are such new genus-2 curves, we find that no X in Case 5 exists.

Case 6: $\mathcal{D} \simeq \mathbb{Z}/6\mathbb{Z}$, $w \notin \mathcal{D}$

Combining $6|(g+1)$ with $g \leq 17$ shows that g is 5, 11, or 17. In the first (resp. second or third) case, Lemma 6.15(3) and Lemma 6.17 together imply that the curve $X/\langle u^3 w \rangle$ (resp. $X/\langle uw \rangle$) has genus 2, and by Lemma 3.17 it has a nontrivial diamond of order 6 (resp. 2). We check as before that such curves do not exist.

To finish the proof of Proposition 6.18, we must show that if $\mathcal{D} \simeq \mathbb{Z}/6\mathbb{Z}$ and $w \in \mathcal{D}$, then g is 2, 12 or 14. By Lemmas 3.17 and 6.17, $X'' := X/\langle u^2 \rangle$ has diamond group $\langle w \rangle$ and its genus g'' is even. On the other hand, g is even, $g \leq 17$, and $g'' = \lfloor g/3 \rfloor$ by Lemma 6.15(3), so (g, g'') is one of $(2, 0)$, $(6, 2)$, $(8, 2)$, $(12, 4)$, or $(14, 4)$. We rule out $(6, 2)$ and $(8, 2)$ by checking all levels of genus 2 curves with diamond group of order 2. $\square$

Remark 6.20. Assume $g \geq 3$ and $\mathcal{D} = \langle u \rangle$. If $\#\mathcal{D} = 2$ and $w \notin \mathcal{D}$ (resp. if $\#\mathcal{D} = 6$), then $X/\langle u.w \rangle$ (resp. $X/\langle u^2 \rangle$) is a new modular hyperelliptic curve of genus ≥ 2 of the same level, and by Lemma 3.17 its group of diamonds has 2 elements and contains w . Therefore, in order to find all levels of new modular hyperelliptic curves with $\#\mathcal{D} > 1$, it suffices to determine the cases such that $\#\mathcal{D} = 2, 3$ or 4 with the additional requirement that $w \in \mathcal{D}$ when $\#\mathcal{D}$ is even.

Proposition 6.21. *Let X be a new modular hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$ such that $2 \mid \#\mathcal{D}$ and $w \notin \mathcal{D}$. Then $\#\mathcal{D} = 2$, and g is 3, 7, 8, or 9. If $g = 3$, then X is one of the seven curves in Table 12. If $g > 3$, then $3 \nmid N$.*

Proof. Proposition 6.18 implies $\#\mathcal{D} = 2$. Let u be the generator of $\mathcal{D}$. Let $X' = X/\mathcal{D}$ and $X'' = X/\langle uw \rangle$, and let g' and g'' be their genera, respectively. By Lemma 6.15(3), g' and g'' equal $\lfloor g/2 \rfloor$ or $\lceil g/2 \rceil$ in some order. Moreover $g'' = g - g'$ is even (by Lemma 6.17) and positive (since $X \not\cong X/\mathcal{D}$). In particular $g \not\equiv 2 \pmod{4}$, so $g \notin \{2, 6, 10, 14\}$.

Suppose $g'' = 2$. For each new modular curve of genus 2 with diamond group of order 2, we compute all new modular curves at that level; we find only the seven curves in Table 12, all of genus 3. Therefore we may assume $g'' \neq 2$ from now on, so $g'' \geq 4$. Since $|g' - g''| \leq 1$, we have $g' \geq 3$, and $g \geq 7$.

Case 1: $3 \mid N$.

Since $X/\mathcal{D}$ is of genus $g' \geq 3$ with trivial diamond group, Theorem 1.9(ii) implies $X/\mathcal{D} \simeq X_0(39)$, so $N = 39$. Computations show that $X_0(39)$ is the only new modular hyperelliptic curve of level 39 and genus ≥ 3 .

Case 2: $3 \nmid N$.

Then $g \leq 10$ by Corollary 3.24. The possibility $g = 10$ was already ruled out. $\square$

Proposition 6.22. *Let X be a new modular hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 3$ such that $\#\mathcal{D} = 3$. Then $g = 3$ or $g = 5$. If $g = 3$, then X is one of the five curves in Table 11. If $g = 5$ there are at least two such curves, which are given in Table 13.*

Proof. Since $\text{Aut}(X_{\overline{\mathbb{Q}}})$ contains $\mathcal{D}_N'' := \langle \mathcal{D}, w, W_N \rangle \simeq D_{2 \cdot 6}$, Proposition 6.14 implies $g \not\equiv 1 \pmod{3}$. Also $g \leq 17$, so g must be 17, 15, 14, 12, 11, 9, 8, 6, 5 or 3.

Suppose $g > 5$. Then we claim that there is a quotient X' of X , such that X' is a new modular curve of genus 2, of the same level N , and dominated by $X_0(N)$. Indeed, by repeated application of Lemma 6.15(3), at least one of the curves $X/\mathcal{D}_N$, $X/\mathcal{D}'_N$ or $X/\mathcal{D}$ has genus 2 in each possible case. We now consult the list of new modular curves of genus-2 to check that X does not exist.

Finally we consider the case $g = 3$. By Lemma 6.17, we have $\text{Jac} X \stackrel{\mathbb{Q}}{\sim} A_f \times A_h$, where $\dim A_f = 2$ and $\dim A_h = 1$. If ${}^\sigma f$ denotes the nontrivial Galois conjugate of f , then $\{f, {}^\sigma f, h\}$ is a basis of eigenvectors of a generator u of $\mathcal{D}$ acting on $S_2(X)$. Since the $\mathcal{D}$ -invariant subspace of $S_2(X)$ is 1-dimensional, corresponding to A_h , and since u is defined over $\mathbb{Q}$, the eigenvalues must be $\{\zeta, \zeta^2, 1\}$, respectively, where ζ is a primitive cube root of 1. In particular, the basis of eigenvectors is unique up to scalar multiples. Moreover, the field E_f contains the eigenvalue of u acting on f , so $E_f = \mathbb{Q}(\zeta)$.

On the other hand, all elements of order 3 in $\text{PGL}_2(\mathbb{C})$ are conjugate, so we can choose a coordinate function x on $\mathbb{P}_{\mathbb{C}}^1 = X_{\mathbb{C}}/\langle w \rangle$ so that u induces $x \mapsto \zeta x$. Then $X_{\mathbb{C}}$ is the smooth projective model of $y^2 = F(x)$ for some squarefree polynomial F , and $\{dx/y, x dx/y, x^2 dx/y\}$ is a basis of eigenvectors of u acting on $H^0(X, \Omega) = S_2(X) \frac{dq}{q}$. In particular, there exists a unique eigenvector whose square equals the product of the other two, at least up to a constant factor c .

The same must be true of $\{f, {}^\sigma f, h\}$ and the corresponding constant factor c is in $\mathbb{Q}(\zeta)$. For such a relation to be consistent with the action of σ , it must be that $h^2 = c f {}^\sigma f$. Comparing leading coefficients of q -expansions shows that $c = 1$. Thus $h^2 = f {}^\sigma f$.

Using the methods of Section 6.4 we run through all possibilities with $M = 18$, $f = \sum_{i=1}^M a_i q^i + O(q^{M+1})$ with $a_i \in \mathbb{Z}[\zeta]$, and $h = \sum_{i=1}^M b_i q^i + O(q^{M+1})$ with $b_i \in \mathbb{Z}$ satisfying $h^2 = f {}^\sigma f$. We obtained only the five curves of Table 11. $\square$

Proof of parts (i) and (iii) of Theorem 1.9. Part (i) follows from parts (ii) and (iii) together with Remark 4.5. Part (ii) was already proved, so we need only prove (iii). Suppose $\#\mathcal{D} > 1$, and g is odd. Lemma 6.17 implies $w \notin \mathcal{D}$, and Proposition 6.18 then implies that $\#\mathcal{D}$ is 2 or 3. Propositions 6.21 and 6.22 complete the proof in these two cases, respectively. $\square$

Remark 6.23. In order to make the process of discarding levels easier in the previous propositions, we used some additional information, such as Corollary 3.24. In cases where we know that there are quotient curves of some smaller genus ≥ 2 , and we have already determined all the hyperelliptic curves of that level and genus, we have used this information.

We summarize most of the results of this section in Table 1. For each possibility for $\mathcal{D}$ and for each possible answer to the question “Is $w \in \mathcal{D}$?”, we give all integers ≥ 2 which *might* be the genus of a new modular hyperelliptic curve over $\mathbb{Q}$ having that $\mathcal{D}$ and such a w . A **bold** number indicates that our computations have found a curve of that genus. The other numbers might not actually occur; in fact, most of them probably do not.

$\mathcal{D}$	$w \in \mathcal{D}$?	Potential values of g
$\{1\}$	no	2, 3, 4, 5, 6 , 7, 8, 9, 10
$\mathbb{Z}/2\mathbb{Z}$	yes	2, 4, 6, 8, 10, 12, 14, 16
	no	3, 7, 8, 9
$\mathbb{Z}/3\mathbb{Z}$	no	3, 5
$\mathbb{Z}/4\mathbb{Z}$	yes	2, 4, 6, 8, 10, 12, 14, 16
$\mathbb{Z}/6\mathbb{Z}$	yes	2, 12, 14

TABLE 1. Possibilities for the diamond group and genus of a new modular hyperelliptic curve. See Theorem 1.9 and Propositions 6.18, 6.21, and 6.22.

6.4. Computational methods. Recall that [27] computed all new modular genus-two curves with $\mathbb{Q}$ -simple jacobian. Using similar reasoning, and using some of the sieves described there, we compute all new modular genus-two curves with jacobian *not* $\mathbb{Q}$ -simple: there are exactly 64 of such curves (see Table 4). In principle, we can also compute all the equations, levels and newforms for new modular hyperelliptic curves of genus g for each $g > 2$. But the enormous number of possibilities for the coefficients a_p prevents us from completing these computations in practice.

We demonstrate the method in the case of new modular hyperelliptic genus-3 curves with $\mathbb{Q}$ -simple jacobian. Let f be a corresponding newform. Then $\dim A_f$ is odd, so f has trivial Nebentypus ε . The only subfields of E_f are $\mathbb{Q}$ and E_f itself, so part (2) of Lemma 6.1 implies:

$$E_f = \begin{cases} \mathbb{Q}(a_2) = \mathbb{Q}(a_3), & \text{if } \pi(\infty) \notin \text{WP}(X), \\ \mathbb{Q}(a_3) = \mathbb{Q}(a_5) \quad (a_{2n} = 0), & \text{otherwise.} \end{cases}$$

For simplicity, we outline the computation in the case where $a_2 \neq 0$ (or equivalently, $\pi(\infty) \notin \text{WP}(X)$). In this case, $E_f = \mathbb{Q}(a_2)$, so $a_2 \notin \{-1, 0, 1\}$, and (3.9) and (3.10) imply that $2 \nmid N$.

- (1) We determine all possible polynomials $H_2(x) = \prod_{i=1}^3 (x - \sigma_i a_2)$, that is, all the monic irreducible cubic polynomials in $\mathbb{Z}[x]$ such that all zeros are real and of absolute value $\leq 2\sqrt{2}$. In total, there are 80 such polynomials.

- (2) For each $H_2(x)$, we fix a zero a_2 . Let $M = 2g + 5 = 11$, which is the bound in Proposition 2.8 plus 1 (since we multiply newforms by dq/q instead of dq). For every prime p satisfying $3 \leq p \leq M$, the possible values of $\varepsilon(p)$ and a_p are those such that $\varepsilon(p) \in \{0, 1\}$ and a_p is an algebraic integer in $\mathbb{Q}(a_2)$ with $|a_p| \leq 2\sqrt{p}$ with respect to every archimedean absolute value. We may restrict the possibilities by imposing $\mathbb{Q}(a_3) = \mathbb{Q}(a_2)$ and $\varepsilon(2) = \varepsilon(3) = 1$.
- (3) For each possible $f = q + \sum_{n=2}^M a_n q^n + O(q^{M+1})$, we write $f = g_0 + a_2 g_1 + a_2^2 g_2$ with $g_i \in \mathbb{Q}[[q]]$. The g_i have the same span as the conjugates of f . Applying linear algebra to the g_i , we compute the basis $\{h_1, h_2, h_3\}$ of part (1) of Lemma 6.1. Next we compute $\tilde{x} = h_2/h_3$ and $h'_1 = \tilde{x}^2 h_3$.
- (4) We impose the condition $h'_1 \in \langle h_1, h_2, h_3 \rangle$ to sieve out some possibilities. Also we use this condition to extend the precision of h'_1 , to determine the first M coefficients of h'_1 . Next compute $x = h_2/h'_1$ and $y = (q dx/dq)/h'_1$.
- (5) We impose the condition that $y^2 = F(x)$ for a polynomial F of degree 8 without double roots. In the cases that survive, we compute $F(x)$.
- (6) Now we have a list of candidate curves. In principle, we should compute the conductor $\mathcal{N}$ of each jacobian and keep only those such that $N := \mathcal{N}^{1/3} \in \mathbb{Z}$ and there exists a newform in $S_2(X_0(N))$ giving rise to $y^2 = F(x)$. In practice, since computing the conductor can be difficult, it is easier to try to recognize the candidates in a list of new modular curves calculated from newforms of small level (as discussed later in this subsection) and hope that all candidates show up.

Remark 6.24. If X is a new modular curve of level N , and p is a prime not dividing N , then Eichler-Shimura theory shows that the product $P(x)$ of $x^2 - a_p x + p\varepsilon(p)$ over all $f \in S_2(X) \cap \text{New}_N$ must equal the characteristic polynomial of Frobenius acting on the Tate module of the jacobian of the mod p reduction of X .

In the calculation above, we know $2 \nmid N$, so we can compute the characteristic polynomials for all genus-3 hyperelliptic curves over $\mathbb{F}_2$, in order to restrict the possibilities for $H_2(x)$ in step (1). Moreover, we can restrict attention to the curves such that $\#X(\mathbb{F}_2) \geq 1$ (because of $\pi(\infty)$) and such that $\#X(\mathbb{F}_4) > 2$ (by Lemma 3.25).

Similar ideas restrict the possibilities for a_3 , even when $\pi(\infty) \in \text{WP}(X)$, i.e., when N is even. For larger g , if it becomes too time-consuming to list all genus- g hyperelliptic curves over $\mathbb{F}_3$, one can at least rule out certain a_3 by translating the following into conditions on a_3 :

- $\#X(\mathbb{F}_3) \geq 1$, because of the image of the cusp ∞ ,
- $\#X(\mathbb{F}_3) \leq 8$ and $\#X(\mathbb{F}_9) \leq 20$, since X is hyperelliptic,
- $\#X(\mathbb{F}_3) \leq \#X(\mathbb{F}_9)$,
- $\#X(\mathbb{F}_9) > 2g - 2$, by Lemma 3.25, if $\text{Jac } X$ is a quotient of $J_0(N)^{\text{new}}$.

The computation in steps (1) through (6) (of new modular hyperelliptic genus-3 curves with $a_2 \neq 0$ and with $\mathbb{Q}$ -simple jacobian) shows that only two such curves exist. These are given in Table 5 as C_{41}^A and C_{95}^A .

In the $a_2 = 0$ case, the number of possibilities to analyze is considerably higher, because there are more possible values for a_3 , hence more possibilities for E_f . Furthermore, in this case, Proposition 2.8 requires knowledge of a_p for primes $p \leq 4g + 6$ (which is 18 for $g = 3$) in order to determine the relation $y^2 = F(x)$.

Performing all these computations would be extremely time-consuming. Therefore instead we conducted a search of all new modular hyperelliptic curves X of some bounded level. We used W. A. Stein's Modular Symbols package to implement a program in MAGMA [8] that detects whether a set of newforms corresponds to a new modular hyperelliptic curve X and that computes an equation for this curve if so. This program, based on Proposition 6.5, was used to determine the $\geq$ entries in Table 2.

Remark 6.25. If there is a nonconstant morphism $\pi(\varepsilon): X(N, \varepsilon) \rightarrow X$, then we compute the bound c as in Lemma 6.6 replacing g_Y by the genus of $X(N, \varepsilon)$. If moreover $\varepsilon = 1$ and $\text{Jac } X$ is $\mathbb{Q}$ -simple, then for each Atkin-Lehner involution W_M we have ${}^\sigma f|W_M = \lambda(M)^\sigma f$ for all σ , where $\lambda(M) \in \{-1, 1\}$. Let $B'(N) = \{W_M \in B(N) \mid \lambda(M) = 1\}$, where $B(N)$ is the group of Atkin-Lehner involutions. Then X is dominated by $X_0(N)/B'(N)$ and the bound c is computed taking g_Y as the genus of $X_0(N)/B'(N)$. Note that $B'(N) = B(N)$ or $B(N)/B'(N) \simeq \mathbb{Z}/2\mathbb{Z}$, so $B'(N) = \{\text{id}\}$ if and only if N is a power of a prime with $\lambda(N) = -1$.

6.5. Computational results. Table 2 summarizes the results of the computations. Each entry indicates the number of new modular hyperelliptic curves over $\mathbb{Q}$ with the genus prescribed by the column, and with jacobian satisfying the conditions prescribed by the row heading. In the first (resp. second, third, fourth) row, a number following $\geq$ is the number of curves of that type of level ≤ 3000 (resp. 569, 2000, 569). We do not know if there are others of higher level. The zeros in the second row for odd g are from Lemma 6.17.

	$g = 2$	$g = 3$	$g = 4$	$g = 5$	$g = 6$	$g \geq 7$
$\mathbb{Q}$ -simple, $\#\mathcal{D} = 1$	120	≥ 14	≥ 13	≥ 3	≥ 0	≥ 0
$\mathbb{Q}$ -simple, $\#\mathcal{D} > 1$	29	0	≥ 1	0	≥ 0	≥ 0
not $\mathbb{Q}$ -simple, $\#\mathcal{D} = 1$	64	≥ 32	≥ 7	≥ 0	≥ 1	≥ 0
not $\mathbb{Q}$ -simple, $\#\mathcal{D} > 1$	0	≥ 12	≥ 3	≥ 2	≥ 0	≥ 0
Total	213	≥ 58	≥ 23	≥ 5	≥ 1	≥ 0

TABLE 2. The number of new modular hyperelliptic curves of genus g .

Equations for the $120 + 29$ genus-two curves with $\mathbb{Q}$ -simple jacobian have appeared in [27]. Equations for all the rest of the curves are in the tables of the appendix of this paper.

Of the 120 genus-two curves counted in row 1, only six have level > 3000 : their levels are 3159, 4160, 7280, 7424 (twice), and 7664. Of the 64 genus-two curves counted in row 3, only two have level > 2000 : both are of level 2208. Similarly, of the 29 genus-two curves counted in rows 2 and 4, only four have level > 569 : their levels are 768 (twice), and 928 (twice). Moreover, for $g \geq 3$, the largest level we found in the curves of row 1 (resp. row 3, resp. rows 2 and 4) was 1664 (resp. 944, resp. 512 even though we computed up to level 3000 (resp. 2000, resp. 569). This leads us to believe that the lower bounds in Table 2 are close to the exact numbers.

Finally, we note that all levels obtained when $g > 2$ have at most two different odd prime divisors and only the levels $N = 36, 72, 144, 784$ are divisible by the square of an odd prime.

7. NEW MODULAR CURVES WITH TRIVIAL CHARACTER

7.1. A finiteness result for curves with p in the level. The goal of this section is to prove the finiteness statement in Theorem 1.10. We first give some equivalent characterizations of what it means for a curve to have “trivial character”.

Lemma 7.1. *Let X be a new modular curve of genus $g \geq 2$, and let N be a positive integer. The following are equivalent:*

- (i) *There exists a morphism $\pi_0: X_0(N) \rightarrow X$ with $S_2(X) \subseteq S_2(X_0(N))^{\text{new}}$.*
- (ii) *There exists a morphism $\pi_1: X_1(N) \rightarrow X$ with $S_2(X) \subseteq S_2(X_0(N))^{\text{new}}$.*
- (iii) *The jacobian J of X is a quotient of $J_0(N)^{\text{new}}$.*

We say that a new modular curve X has trivial character (and level N) if any of the above conditions are satisfied.

Proof. It is clear that (i) implies (iii). Furthermore, it follows from Lemma 2.11(i) that (ii) implies (i). It remains to show that (iii) implies (ii). Since X is a new modular curve, there exists an integer M and a morphism $\pi: X_1(M) \rightarrow X$ with $S_2(X) \subseteq S_2(X_1(M))^{\text{new}}$. Then J is $\mathbb{Q}$ -isogenous to a product of abelian varieties of the form A_f with each f a newform of level M . By assumption J is a quotient of $J_0(N)^{\text{new}}$, so J is $\mathbb{Q}$ -isogenous also to a product of abelian varieties of the form $A_{f'}$ with each f' a newform of level N and trivial Nebentypus character. Applying Proposition 3.2, we deduce that $N = M$ and $S_2(X) \subseteq S_2(X_0(N))^{\text{new}}$. $\square$

The following lemma will be used in the proof of Proposition 7.4 below, and will be used repeatedly in Section 7.2.

Lemma 7.2. *Suppose X is a curve of genus $g > 0$ over a field k and that q is an analytic local uniformizing parameter at the point $P \in X(k)$. Let $\omega_1, \dots, \omega_g$ be a basis for $H^0(X, \Omega)$ with $\omega_i = (\sum_{j=1}^{\infty} a_j^{(i)} q^j) \frac{dq}{q}$ and $a_1^{(i)} = 1$ for all i . Let $m \geq 2$ be an integer, and suppose that $a_m^{(i)} = a_m^{(i')}$ for all $1 \leq i, i' \leq g$. Then there exists a rational function f of degree m , defined over k , with poles only at P .*

Proof. As usual, if D is a divisor on X , let $l(D)$ denote the dimension of the vector space $L(D)$ consisting of 0 and the rational functions on X whose divisor is $\geq -D$. Let K denote a canonical divisor on X .

By hypothesis, if $\omega = (\sum_{j=1}^{\infty} a_j q^j) \frac{dq}{q}$ is any linear combination of $\omega_1, \dots, \omega_g$ with $a_1 = 0$, then $a_m = 0$. Therefore no regular differential on X vanishes to order exactly $m-1$ at P . In other words, we have $l(K - (m-1)P) = l(K - mP)$, which by Riemann-Roch is equivalent to $l(mP) - l((m-1)P) = 1$. Any $f \in L(mP) - L((m-1)P)$ works. $\square$

Corollary 7.3. *With the same notation as in Lemma 7.2, we have:*

- (i) *If $a_2^{(i)} = a_2^{(i')}$ for all $1 \leq i, i' \leq g$, then either $g = 1$, or X is hyperelliptic and P is a Weierstrass point.*
- (ii) *If $a_2^{(i)} = a_2^{(i')}$ and $a_3^{(i)} = a_3^{(i')}$ for all $1 \leq i, i' \leq g$, then $g = 1$.*
- (iii) *If $g \geq 2$ and every differential in $H^0(X, \Omega)$ vanishing at P vanishes to order at least r at P , then $r \leq 2$, and $r = 2$ if and only if X is hyperelliptic and P is a Weierstrass point.*

Proof. Part (i) follows from Lemma 7.2, and (iii) follows from (i) and (ii). Therefore we need only prove (ii).

The argument of Lemma 7.2 yields rational functions in $L(2P) - L(P)$ and in $L(3P) - L(2P)$. Taking products, we find rational functions in $L(mP) - L((m-1)P)$ for all $m \geq 2$.

By induction, we prove $l(mP) \geq m$ for $m \geq 1$. If we take m large, Riemann-Roch implies $g \leq 1$. $\square$

Proposition 7.4. *Let X be a new modular curve of level N and trivial character. If p is a prime divisor of N , then the $\mathbb{Q}$ -gonality of X is at most p^2 .*

Proof. The value of a_{p^2} is the same for each newform $f = \sum_{n \geq 1} a_n q^n$ in New_N : it is 0 or 1, depending on whether $p^2 \mid N$ or not. (This follows from the more general statements (3.7), (3.8), (3.9), and (3.10) by taking ε to be the trivial Dirichlet character modulo N .) Also, recall from the proof of Theorem 1.3 that q serves as an analytic uniformizing parameter at the image P of the cusp ∞ under $\pi: X_1(N) \rightarrow X$. The result therefore follows from Lemma 7.2. $\square$

Proof of Theorem 1.10. Combine Proposition 7.4 with Theorem 1.8. $\square$

7.2. Curves with level divisible by small primes. Theorem 1.10 shows that there are only finitely many new modular curves X with trivial character and level divisible by a given prime number p . In this section, we prove some further results about the levels of new modular curves with trivial character.

In addition to relying heavily on Lemma 7.2 and Corollary 7.3, we make use of a classical lemma of Castelnuovo and Severi. Before stating it, we make the following definition. If $f_1: C \rightarrow C_1$ and $f_2: C \rightarrow C_2$ are nonconstant morphisms (of degree d_1, d_2 , respectively) between curves, we say that f_1 and f_2 are *independent* if the product morphism $(f_1, f_2): C \rightarrow C_1 \times C_2$ maps C birationally to its image C' . A consideration of degrees shows that if $\gcd(d_1, d_2) = 1$, then f_1 and f_2 are automatically independent.

Lemma 7.5. *Let C_1, C_2, C be curves of genera g_1, g_2 , and g , respectively, over the field k of characteristic zero. Let $f_i: C \rightarrow C_i$ be morphisms of degree d_i , $i = 1, 2$. Assume that f_1 and f_2 are independent. Then*

$$g \leq (d_1 - 1)(d_2 - 1) + d_1 g_1 + d_2 g_2.$$

Proof. See Theorem 3.5 of [3]. $\square$

Remark 7.6. Lemma 7.5 is true over any field k , but the proof in [3] assumes that k has characteristic zero. See Exercise VIII.C-1 in [5] for an approach that can be generalized to any characteristic.

We now investigate some restrictions on the powers of 2 and 3 dividing the level of new modular curves with trivial character.

Proposition 7.7. *Let X be a new modular curve over $\mathbb{Q}$ of genus $g \geq 2$, level N , and trivial character. Then:*

- (i) *If $2 \mid N$, then X admits a map of degree 2, defined over $\mathbb{Q}$, to a curve of genus at most 1, and $g \leq 16$.*
- (ii) *$4 \mid N$ if and only if X is hyperelliptic and $\pi(\infty)$ is a Weierstrass point.*
- (iii) *If $6 \mid N$, then $g \leq 5$.*
- (iv) *If $12 \mid N$, then $g = 2$.*
- (v) *If $18 \mid N$, then $g \leq 4$.*
- (vi) *$36 \nmid N$.*

Proof. Let $f_1, \dots, f_g$ be a basis of newforms for $\Gamma_0(N)$ spanning $S_2(X)$.

To prove (ii), first note that, as in the proof of Theorem 1.3, the map π is unramified at ∞ , so that q serves as an analytic uniformizing parameter at $P := \pi(\infty)$. If $4 \mid N$, then $a_2(f_i) = 0$ for all i by (3.9), so it follows from Corollary 7.3 that X is hyperelliptic and P is a Weierstrass point. The other direction of (ii) is a special case of Proposition 6.7.

Before proving (i), note that if $2 \mid N$, then Proposition 7.4 implies that the $\mathbb{Q}$ -gonality $G_{\mathbb{Q}}$ of X satisfies $G_{\mathbb{Q}} \leq 4$. Remark 4.5 then implies that $g \leq 34$. We seek to sharpen both of these statements.

If X is hyperelliptic, then Theorem 1.9(ii) implies $g \leq 10$. Therefore we may suppose that X is not hyperelliptic. We may then assume by (ii) that $4 \nmid N$, so that it makes sense to consider the Atkin-Lehner involution W_2 on X .

Let $X' = X/W_2$, let P' be the image in X' of P under the natural map, and let $f'_1, \dots, f'_{g'}$ be a basis of newforms spanning $S_2(X')$. Then since $f_i|W_2 = -a_2(f_i)f_i$ by (3.12), we have $a_2(f'_i) = -1$ for all i . Therefore every regular differential on X' vanishing at P' vanishes to order at least 2 at P' . We claim that X' has genus 1. Indeed, if the genus of X' were at least 2, then Corollary 7.3 would then imply that X' is hyperelliptic and that P' is a Weierstrass point, but then we find by applying (ii) to X' that $4 \mid N$, contrary to what we just assumed. Also, X' cannot have genus 0 or else X would be hyperelliptic, contrary to assumption. Thus X' has genus 1 as claimed, and X is a degree 2 cover (over $\mathbb{Q}$) of the elliptic curve X' .

If $3 \nmid N$, then we have $\#X(\mathbb{F}_9) \leq 2\#X'(\mathbb{F}_9) \leq 2(9+1+2\sqrt{9}) = 32$. But also $(3-1)(g-1) < \#X(\mathbb{F}_9)$ by Lemma 3.25. Thus $g \leq 16$.

Finally, if $3 \mid N$, then the conclusion $g \leq 16$ follows from the stronger conclusion of (iii) proved below.

To prove (v), we suppose that $18 \mid N$. It follows by Theorem 1.9(ii) that if X is hyperelliptic then $g < 3$. Thus by (i), we may assume that X is a double cover of an elliptic curve X' .

Since $9 \mid N$, we have $a_3(f_i) = 0$ for all i , so Lemma 7.2 implies that X is trigonal (i.e., X admits a degree 3 map to $\mathbb{P}^1$). It therefore follows from Lemma 7.5 that $g \leq 4$.

To prove (iii), we may assume by (v) that $3 \mid N$ but $9 \nmid N$. As before, we may also assume that $2 \mid N$ but $4 \nmid N$, that X is not hyperelliptic, and that X is a double cover of the elliptic curve $X' = X/W_2$.

Let $w_j(f_i)$ denote the eigenvalue of W_j on the newform f_i for $j = 2, 3, 6$ and $i = 1, \dots, g$. We have $w_2(f_i) = -a_2(f_i)$, $w_3(f_i) = -a_3(f_i)$, and $w_6(f_i) = a_6(f_i)$ for all i . Let g_j be the genus of X/W_j ($j = 2, 3, 6$), so $g_j = \#\{i \mid w_j(f_i) = +1\}$. Since X/W_2 has genus 1, all the $w_2(f_i)$'s are equal to -1 except for one, which is equal to $+1$. Suppose that f is the newform on which W_2 acts with eigenvalue $+1$. The identity $w_2w_3 = w_6$ and the fact that the w_2 's are $+1, -1, -1, -1, \dots, -1$ implies that $g_3 + g_6$ is equal to either $g - 1$ or $g + 1$, depending on whether $f|W_3$ equals $-f$ or $+f$. We consider these two cases separately.

Case 1: $f|W_3 = -f$.

If $g_3 \geq 2$, then X/W_3 is a curve of genus at least 2 with all w_2 's equal to -1 , so as before we would have $4 \mid N$, contrary to assumption. Thus $g_3 \leq 1$. Similarly, $g_6 \leq 1$. But $g_3 + g_6 = g - 1$, so $g \leq 3$.

Case 2: $f|W_3 = f$.

In this case, we have $g_3 \geq 1$. Also $f|W_6 = f$, so $g_6 \geq 1$. Assume first that $g_3 = 1$. Then $w_2(f_j) = w_3(f_j)$ for all j , so a simple argument using Riemann-Roch (as in the proof of

Lemma 7.2) shows that there is a rational function on X in $L(3P) - L(2P)$. Since (as in the proof of Proposition 7.4) all a_4 's are equal to $+1$, there is also a function in $L(4P) - L(3P)$. Taking products, we also find functions in $L(mP) - L((m-1)P)$ for all $m \geq 6$, so that the Weierstrass gap sequence at P is contained in $\{1, 2, 5\}$. By Riemann-Roch, the gap sequence at any point contains exactly g integers, so $g \leq 3$.

Assume now that $g_6 = 1$. Then $w_2(f_j) = w_6(f_j)$ for all j , so $w_3(f_j) = 1$ for all j . Corollary 7.3 gives a function in $L(3P) - L(2P)$, and as before we deduce that $g \leq 3$.

In the general case, we may apply the previous reasoning to X/W_3 , since $(X/W_3)/W_6$ is of genus 1 (its only newform is f). The conclusion is that $g_3 \leq 3$. Similarly, since $(X/W_6)/W_3$ has genus 1, we conclude that $g_6 \leq 3$. Since $g_3 + g_6 = g + 1$ in Case II, we have $g \leq 5$ as desired.

To prove (vi), suppose that $36 \mid N$. Then $a_2(f_i) = a_3(f_i) = 0$ for all i . By the same argument as in the proof of (ii), it follows that every differential on X vanishing at P vanishes to order at least 3 at P , contradicting Corollary 7.3.

For (iv), assume $12 \mid N$. Then X is hyperelliptic by part (ii). By Theorem 1.9(ii), it follows that $g = 2$ as desired. $\square$

We can deduce stronger results if we assume furthermore that the jacobian of X is $\mathbb{Q}$ -simple.

Proposition 7.8. *Let X be a new modular curve of genus $g \geq 2$, level N , and trivial character. Assume furthermore that the jacobian J of X is $\mathbb{Q}$ -simple. Then:*

- (i) *If $2 \mid N$, then $4 \mid N$.*
- (ii) *$6 \nmid N$.*

Proof. Let $f_1, \dots, f_g$ as before be a basis of newforms for $\Gamma_0(N)$ spanning $S_2(X)$. Since J is $\mathbb{Q}$ -simple, the f_i 's are all Galois conjugates of one another. To prove (i), suppose $2 \mid N$ but $4 \nmid N$. Then $a_2(f_i) = \pm 1$ for all i . Since in particular $a_2(f_i) \in \mathbb{Q}$, all the $a_2(f_i)$'s must be equal to one another. It follows by Corollary 7.3 that X is hyperelliptic and P is a Weierstrass point. But then $4 \mid N$ by Proposition 7.7(ii), contradicting our assumption.

To prove (ii), suppose that $6 \mid N$. By (i) we have in fact that $12 \mid N$. Also, we know by Proposition 7.7(vi) that $36 \nmid N$. Therefore we have $a_2(f_i) = 0$ and $a_3(f_i) = \pm 1$ for all i . As above, it follows that all the $a_3(f_i)$'s are in fact equal, contradicting Corollary 7.3. $\square$

8. EXAMPLES AND PATHOLOGIES

8.1. Examples of non-new hyperelliptic curves. We can construct non-new modular hyperelliptic curves from certain pairs of new modular hyperelliptic curves. For some levels, there exist at least two new modular hyperelliptic curves of level N such that it is possible to take the same modular function x in both their equations. In other words, $\mathbb{Q}(x, \sqrt{P_1(x)}, \sqrt{P_2(x)})$ is a subfield of the function field of $X_1(N)$, where the two new modular curves are

$$C_{N,1}: y_1^2 = P_1(x), \quad C_{N,2}: y_2^2 = P_2(x).$$

Then $\mathbb{Q}(x, \sqrt{P_1(x)P_2(x)})$ also is a subfield of the function field of $X_1(N)$, so $y^2 = P_1(x)P_2(x)$ is a modular hyperelliptic curve C'_N dominated by $X_1(N)$. (If desired, one may discard square

factors of $P_1(x)P_2(x)$ to make the right hand side squarefree.) In each example we give, C'_N is not new of level N , although sometimes it is new of a smaller level.

We found 33 non-new modular curves C'_N of this type. Five of these 33 are not *primitive* (cf. definition 2.2 in [27]): this means that the minimum N' such that $\text{Jac}C'_N$ is a quotient of $J_1(N')$ is different from the minimum M such that C'_N is dominated by $X_1(M)$. The following table shows these five curves.

C'_N	Decomposition of $\text{Jac}C$	M	g'
$C_{184}^{3,3}$	$A_{23A} = J_0(23)$	46	2
$C_{248}^{2,3}$	$A_{31A} = J_0(31)$	62	2
$C_{376}^{2,2}$	$A_{47A} = J_0(47)$	94	4
$C_{544}^{2,3}$	$E_{34A} \times A_{68A}$	136	3
$C_{704}^{3,4}$	$E_{44A} \times E_{88A} \times A_{88B}$	176	4

In the first column appears the label for each curves. For each curve the subscript denotes the level N and the superscript denotes the genus of the curves $C_{N,1}$ and $C_{N,2}$. In the second column appears the decomposition over $\mathbb{Q}$ of the jacobians of the curves in the first column (throughout this section we use the labelling of modular forms and abelian varieties described in the appendix). In the third column appears the minimum level M such that $X_1(M)$ dominates C'_N , and in the last column appears the genus of C'_N .

In the rest of this subsection, we discuss the surprising case $N = 376$. We have that $J_0(376)^{\text{new}}$ splits over $\mathbb{Q}$ as the product of the $\mathbb{Q}$ -simple modular abelian varieties A_{376A} , A_{376B} , A_{376C} and A_{376D} . Furthermore, each of these abelian varieties is $\mathbb{Q}$ -isogenous to the jacobian of a new modular hyperelliptic curve. Namely, we have

$$A_{376A} \stackrel{\mathbb{Q}}{\sim} \text{Jac } C_{376}^A, \quad A_{376B} \stackrel{\mathbb{Q}}{\sim} \text{Jac } C_{376}^B, \quad A_{376C} \stackrel{\mathbb{Q}}{\sim} \text{Jac } C_{376}^C, \quad A_{376D} \stackrel{\mathbb{Q}}{\sim} \text{Jac } C_{376}^D,$$

where the four curves have the following affine models:

$$\begin{aligned} C_{376}^A: y_A^2 &= P_A(x), & C_{376}^C: y_C^2 &= P_B(x)Q(x), \\ C_{376}^B: y_B^2 &= P_B(x), & C_{376}^D: y_D^2 &= P_A(x)Q(x), \end{aligned}$$

where

$$\begin{aligned} x &= q^{-2} + q^2 + q^6 + q^8 + q^{10} + \dots, \\ P_A(x) &= x^5 - x^3 + 2x^2 - 2x + 1, \\ P_B(x) &= x^5 + 4x^4 + 3x^3 - 2x^2 + 2x + 5, \\ Q(x) &= x^4 - 2x^3 - 3x^2 + 4x - 4. \end{aligned}$$

Since the modular function x is the same for all four curves, $X_0(376)$ also dominates the hyperelliptic curves $C_{376}^{2,2}: (y_A y_B)^2 = P_A(x)P_B(x)$ and $C_{376}^{2,4}: (y_B y_D)^2 = P_A(x)P_B(x)Q(x)$ (and the genus-one curve $(y_B y_C / P_B(x))^2 = Q(x)$ isomorphic to the curve labelled 94A1 in [17]). In addition, $X_0(376)$ dominates $X_0(47)$, which also is hyperelliptic. We will identify the smallest levels of $C_{376}^{2,2}$ and $C_{376}^{2,4}$.

First consider $C_{376}^{2,2}$. Let f be the newform labeled by 47A. It is easy to check that there is a modular hyperelliptic curve X over $\mathbb{Q}$ of level 94 attached to the $\mathbb{C}$ -vector space spanned by the Galois conjugates of the eigenform $h(q) = f(q) - 2f(q^2) \in S_2(94)$ and that X is the curve $C_{376}^{2,2}$. Therefore, $\text{Jac}C_{376}^{2,2}$ and $J_0(47)$ are $\mathbb{Q}$ -isogenous. But one can check that $C_{376}^{2,2}$

and $X_0(47)$ are not $\mathbb{Q}$ -isomorphic. Hence 94 is the minimum level for $C_{376}^{2,2}$ while 47 is the minimum level for its jacobian.

Now consider $C_{376}^{2,4}$. We compute that $\text{Jac}C_{376}^{2,4} \stackrel{\mathbb{Q}}{\sim} J_0(47) \times J_0(94)^{\text{new}}$. More precisely, $C_{376}^{2,2}$ is a non-new modular curve of minimum level 94: it is attached to the $\mathbb{C}$ -vector space generated by the Galois conjugates of $f(q) + 2f(q^2)$ and g , where f is as above and g is the newform labeled by 94B with $\dim A_{94B} = 2$. The curve $C_{376}^{2,4}$ has genus 6, and its jacobian has one factor in the new part and another in the old part.

Finally, we note that the highest genus yet found for a modular hyperelliptic curve is 7: the curve is given by the equation

$$C_{1664}^{2,5}: y^2 = (x^2 - 2x + 2)(x^2 + 2x + 2)(x^3 - x + 2)(x^3 - x - 2)(x^6 + 2x^4 + x^2 + 4),$$

and has level $N = 1664$. Its jacobian splits as $\text{Jac}C_{1664}^{2,5} \stackrel{\mathbb{Q}}{\sim} E_{26A} \times A_{104B} \times A_{416F}$.

8.2. “Pathologies”. There are many statements about elliptic curve quotients of $J_1(N)$ that fail for modular curves of higher genus or for higher-dimensional abelian quotients of $J_1(N)$. We begin with a statement about abelian quotients.

Proposition 8.1. *There exists an abelian variety A over $\mathbb{Q}$ such that the following statement is false: “If A is a quotient of $J_1(N)$ and N is the smallest integer with this property, and M is any other integer such that A is a quotient of $J_1(M)$, then N divides M .”*

Proof. Take $A = J_0(22)$. One computes that there are no weight 2 newforms on $\Gamma_0(22)$, so $A \stackrel{\mathbb{Q}}{\sim} J_0(11)^2$. Now A is not a quotient of $J_1(M)$ for any M prime to 11 because A has bad reduction at 11, but A is also not a quotient of $J_1(11)$, since $\dim J_1(11) = 1$. Hence $N = 22$ is the smallest integer for which A is a quotient of $J_1(N)$. On the other hand, (3.4) shows that A is also a quotient of $J_1(11m)$ for any $m \geq 2$. $\square$

Next we list a few false statements about modular curves.

Proposition 8.2. *For each of the statements below, there is a curve X over $\mathbb{Q}$ of genus $g \geq 2$ for which the statement is false. Let $J = \text{Jac}X$.*

- (1) “If X is modular, then X is a new modular curve of some level.”
- (2) “If X is non-new modular of level N , then J is a quotient of $J_1(N)_{\text{old}}$.”
- (3) “If X is modular and N is the smallest level such that J is a quotient of $J_1(N)$ defined over $\mathbb{Q}$, then N is the smallest level of X .”
- (4) “If X is modular, then the smallest level of X and $\text{cond}(J)$ are divisible by the same rational primes.”
- (5) “If J is a $\mathbb{Q}$ -simple quotient of $J_1(N)^{\text{new}}$ and $X(\mathbb{Q})$ is nonempty, then X is a new modular curve of level N .”

In fact, there exist infinitely many X over $\mathbb{Q}$ of genus 2 for which (5) fails.

Proof.

(1) Let $X = X_1(p^2)$ where $p \geq 11$ is prime. It follows from an explicit formula for the genus of $X_1(N)$ (see Example 9.1.6 of [20]) that $0 < 2g(X_1(p)) < g(X_1(p^2))$. Therefore, $\dim J_1(p^2)_{\text{old}} = 2g(X_1(p)) > 0$ and $\dim J_1(p^2)^{\text{new}} = g(X_1(p^2)) - \dim J_1(p^2)_{\text{old}} > 0$. Now, by Proposition 3.2 we obtain that if $J_1(p^2)^{\text{new}}$ is a quotient of $J_1(N)^{\text{new}}$ over $\mathbb{Q}$ then N must be p^2 . Hence, X is not new for any level because $J_1(p^2)_{\text{old}}$ is not a quotient of $J_1(p^2)^{\text{new}}$.

(2) Let $X = X_1(p^2)$ for prime $p \geq 11$ again. Then X is modular of level p^2 and not new of any level, but $\text{Jac}X$ is not a quotient of $J_1(p^2)_{\text{old}}$.

(3) Let X be the genus 4 curve $C_{376}^{2,2}$ constructed above. Then $\text{Jac}X$ is a quotient of $J_0(47)$ (they are isogenous), but the smallest N for which X is modular of level N is 94.

(4) Again let $X = C_{376}^{2,2}$. Then $\text{cond}(\text{Jac}X) = 47^4$ but the smallest N for which X is modular of level N is 94. A simpler example is the genus 2 curve $X = X_0(22)$: then $\text{cond}(\text{Jac}X) = 11^2$, but the smallest N for which X is modular of level N is 22.

(5) Let $a \in \mathbb{Z} - \{0\}$, and let X_a be the smooth projective model of the affine curve

$$y^2 = x^5 + ax^3 - 4x$$

over $\mathbb{Q}$ of genus two. Then $X_a(\mathbb{Q}) \neq \emptyset$, since $(0, 0) \in X_a(\mathbb{Q})$. We will show that for infinitely many values of a , the jacobian $J_a := \text{Jac}X_a$ is a $\mathbb{Q}$ -simple quotient of some $J_1(N)$. It can be checked that the group $\text{Aut}(X_a)$ is isomorphic to $D_{2,4}$ and is generated by the hyperelliptic involution and the automorphisms u, v over $\mathbb{Q}(i)$, represented as in Lemma 6.12(1) by $M_u = \begin{pmatrix} 0 & 1+i \\ (1-i)/2 & 0 \end{pmatrix}$, $M_v = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ (and $e = \det M$). It can be checked that the Galois action on $\text{Aut}(X_a)$ corresponds to the case C_2^C of section 3 of [13]. By Proposition 5.3 of [13], we obtain $(\text{End } J_a) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{2})$. In particular, J_a is $\mathbb{Q}$ -simple. On the other hand, the quotient $E_a = X_a/u$ is the elliptic curve

$$y^2 = x^3 + 27(3a - 20i)x - 108(28 + 9ai)(1 - i),$$

whose j -invariant j_a equals $64(3a - 20i)^3(a - 4i)/(a^2 + 16)^2$. Thus J_a is isogenous to the Weil restriction of E_a over $\mathbb{Q}$. Solving $j_a = \bar{j}_a$ for a shows that j_a is never real, so E_a does not have CM. Thus $(\text{End } J_a) \otimes \mathbb{Q}$ is a real quadratic field, and the sign of the 2-cocycle attached to E_a by Ribet in [66] is trivial (see Theorem 5.4 of [62]). In particular, its local component at 3 is trivial. For every nonzero $a \in \mathbb{Z}$, E_a has good ordinary reduction at 3, so Theorem 5.1 of [21] implies that E_a is modular (over $\mathbb{Q}(i)$), so J_a is modular. Since J_a is $\mathbb{Q}$ -simple, it must be a quotient of $J_1(N)^{\text{new}}$ for some N depending on a . Since j_a is nonconstant, the family X_a is not isotrivial. (In fact, it can be proved that X_a and X_b are isomorphic over $\overline{\mathbb{Q}}$ if and only if $a = \pm b$.) Hence by Theorem 1.3, at most finitely many of the X_a can be new modular curves. (In fact, X_a is a new modular curve exactly for $a = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 7, \pm 8, \pm 10, \pm 22$.) $\square$

Question 8.3. Is there a curve analogue of Proposition 8.1? More precisely, does there exist a curve X dominated by some $X_1(N)$, but such that the set of such N for X are not all multiples of the smallest N ?

9. CURVES DOMINATED BY FERMAT CURVES

Here we prove an analogue of Conjecture 1.1 for Fermat curves. Let k be a field of characteristic zero and let $N \geq 1$. The N^{th} Fermat curve $X_{N,k}$ is the smooth plane curve over k given by the homogeneous equation $x^N + y^N = z^N$ in $\mathbb{P}_k^2$. Our goal in this section is to prove the following.

Theorem 9.1. *For each field k of characteristic zero, and integer $g \geq 2$, the set of genus- g curves over k dominated by $X_{N,k}$ for some $N \geq 1$ is finite. If k is a number field or $\overline{\mathbb{Q}}$, then the set is also computable.*

Let J_N denote the jacobian of $X_{N,k}$. For each $M|N$, there is a morphism $\psi_{N,M}: X_{N,k} \rightarrow X_{M,k}$ mapping $(x : y : z)$ to $(x^{N/M} : y^{N/M} : z^{N/M})$. Define $J_{N,\text{old}} = \sum_{M|N} \psi_{N,M}^* J_M$, and $J_N^{\text{new}} = J_N/J_{N,\text{old}}$. We may consider $X_{M,k}$ as the quotient of $X_{N,k}$ by a G_k -stable subgroup

$\Gamma_{N,M} \subseteq \text{Aut}(X_{N,\bar{k}})$. If we decompose the space $H^0(X_{N,\bar{k}}, \Omega)$ into characters of $\Gamma_{N,1}$, and group those for which a particular divisor M is the smallest M for which $\Gamma_{N,M}$ acts trivially, then we see that J_N is k -isogenous to $\prod_{M|N} J_M^{\text{new}}$.

Lemma 9.2. *If $N > 180$, then each k -simple quotient of J_N^{new} has dimension at least $\phi(N)/8$, where $\phi(N) := \#(\mathbb{Z}/N\mathbb{Z})^*$.*

Proof. We may assume $k = \mathbb{C}$. According to Theorem 1.3 of [4], $J_N^{\text{new}} \sim \prod A_S$, where each A_S is an abelian variety of dimension $\phi(N)/2$, and S ranges over the elements of a certain finite set Σ . Moreover, if N is not in an explicit finite set of natural numbers (whose largest element is 180), then Theorem 0.2 of [4] shows that for each $S \in \Sigma$, $A_S = B_S^{W_S}$, where B_S is a simple abelian variety and $W_S \leq 4$. The result follows. $\square$

Lemma 9.3. *There exists a function $M = M(g)$ such that the following holds: If k is a field of characteristic zero, and X is a curve of genus $g \geq 2$ over k dominated by $X_{N,k}$ for some $N \geq 1$, then X is dominated also by $X_{M',k}$ for some $M' \leq M$.*

Proof. Choose $m > 180$ such that $\phi(n)/8 > g$ for all $n > m$. Let $M = m!$. Suppose X is a curve of genus $g \geq 2$ over k dominated by $X_{N,k}$ for some $N \geq 1$. Let $M' = \gcd(M, N)$. By Lemma 9.2, the composition $\text{Jac}X \rightarrow J_N \rightarrow J_{m'}^{\text{new}}$ is trivial for each $m'|N$ greater than m , so the image of $\text{Jac}X \rightarrow J_N$ is contained in an abelian subvariety of J_N isogenous to $\prod_{m'|N, m' \leq m} J_{m'}^{\text{new}}$, which in turn is contained in the image of $J_{M'} \rightarrow J_N$. Considering differentials and applying Proposition 2.11(i), we find that the morphism $X_{N,k} \rightarrow X$ factors through $X_{M',k}$. $\square$

Proof of Theorem 9.1. Use Lemma 9.3, and then apply Theorem 5.7 (our de Franchis-Severi Theorem) to $X_{M',k}$ for each $M' \leq M(g)$ to obtain a finite list of curves dominated by Fermat curves over k , guaranteed to contain all those of genus g . If we now assume that k is a number field or $\overline{\mathbb{Q}}$, then this list is also computable. To eliminate curves of genus not g , and to eliminate possible redundancy, apply parts (1) and (3) of Lemma 5.1. $\square$

Remark 9.4.

- (i) If k is a number field, we can obtain finiteness and computability also for dominated curves of genus ≤ 1 in Theorem 9.1. This follows from Remark 5.9: the genus-1 isomorphism problem is not a problem here, because each dominated curve has a rational point, thanks to the point $(1 : 0 : 1)$ on each $X_{N,k}$.
- (ii) The natural analogue of Theorem 9.1 for bounded *gonality* is false. In affine coordinates, $(x, y) \mapsto (xy, y^N)$ defines a dominant morphism from $x^N + y^N = 1$ to the hyperelliptic curve $u^N = v(1 - v)$. This gives infinitely many Fermat-dominated curves of gonality 2. These curves are even new, if N is prime. Perhaps the failure of the gonality result is not surprising, since in contrast with Theorem 4.3, the gonality of high-degree smooth plane curves is small compared to the genus.

Question 9.5. Are there finiteness results for curves over $\mathbb{Q}$ of fixed genus $g \geq 2$ that are dominated by curves in some other families, such as the family of Shimura curves associated to orders in a fixed or varying indefinite quaternion algebra over $\mathbb{Q}$?

APPENDIX

Labeling. We use a deterministic procedure to label newforms, and in particular to fix an ordering of (Galois conjugacy classes of) newforms having a given level and Nebentypus. An

ordering was introduced by J. Cremona in [17] in the case of trivial Nebentypus and weight 2 and generalized by W. A. Stein in [71] to the case of weight greater than 2. We are going to use this last labeling for the case of weight 2 and arbitrary Nebentypus.

We will define a function mapping each newform $f \in \bigcup_{N=1}^{\infty} \text{New}_N$ to a label of the form NX_ε (for example, $13A_{\{2\}}$), where N is the level of f , where X is a letter or string in $\{A, B, \dots, Z, AA, BB, \dots\}$ and ε is (some encoding) of the Nebentypus of f . If $\varepsilon = 1$, we omit the subscript ε and use a label of the form NX (for example, $11A$), and if the Fourier coefficients of f are integers we will use the labeling in [17]. The labeling function will not be injective: our definition will be such that if f has label NX_ε and $\sigma \in G_{\mathbb{Q}}$, then ${}^\sigma f$ will have label $NX_{\sigma(\varepsilon)}$, which could be the same as NX_ε , even if ${}^\sigma f \neq f$.

Two things must be explained: how is X constructed from f , and how is ε encoded? First we construct X . Fix N and ε . To $f = \sum a_n q^n \in \text{New}_N \cap S_2(N, \varepsilon)$ associate the infinite sequence of integers $\mathbf{t}_f = (\text{Tr}_{E_f/\mathbb{Q}} a_1, \text{Tr}_{E_f/\mathbb{Q}} a_2, \dots)$, where E_f is the number field $\mathbb{Q}(a_1, a_2, \dots)$. Choose $X \in \{A, B, \dots, Z, AA, BB, \dots\}$ according to the position of $\mathbf{t}_f$ in the set $\{\mathbf{t}_g : g \in \text{New}_N \cap S_2(N, \varepsilon)\}$ sorted in increasing dictionary order. Notice that $\mathbf{t}_f$ determines the Galois conjugacy class of f .

The encoding of Dirichlet characters we now describe was suggested by J. Quer. Suppose $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}^*$ is a Dirichlet character. Let $N = \prod p_n^{\alpha_n}$ be the prime-ordered factorization. Then there exist unique $\varepsilon_{p_n} : (\mathbb{Z}/p_n^{\alpha_n}\mathbb{Z})^* \rightarrow \mathbb{C}^*$ such that $\varepsilon = \prod \varepsilon_{p_n}$. If p is an odd prime, let g_p be the smallest positive integer that generates $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$, and if $p = 2$ and $\alpha \leq 2$, let $g_p = -1$; in these cases ε_p is determined by the integer $e_p \in [0, \varphi(p^\alpha))$ such that $\varepsilon_p(g_p) = e^{2\pi i e_p / \varphi(p^\alpha)}$. If $p = 2$ and $\alpha > 2$, then ε_2 is determined by the integers $e'_2, e''_2 \in [0, \varphi(2^\alpha))$ such that $\varepsilon_2(-1) = e^{2\pi i e'_2 / \varphi(2^\alpha)}$ and $\varepsilon_2(5) = e^{2\pi i e''_2 / \varphi(2^\alpha)}$, and we write $e_2 = \{e'_2, e''_2\}$. (Note: here and in the next sentence, we use set notation although we mean sequences.) Assuming that N is implicit, we denote ε by $\{e_p : p|N\}$.

If $f \in S_2(N, \varepsilon)$ is a newform with label NX_ε , then A_{NX_ε} will denote the corresponding modular abelian variety A_f , except that when $\dim A_f = 1$, we instead follow the labeling in [15] and use the letter E instead of A to denote the modular elliptic curve A_f .

We give an example illustrating the above notation: the 2-dimensional space $S_2(13)$ splits as $S_2(13, \varepsilon) \oplus S_2(13, \varepsilon^{-1})$, where $\varepsilon = \{2\}$ is a Dirichlet character modulo 13 (of order 6), and there is only one Galois conjugacy class of newforms of level 13. Thus $J_1(13) \stackrel{\mathbb{Q}}{\sim} A_{13A_{\{2\}}}$.

Each new modular hyperelliptic curve in our tables will be denoted $C_{NL_1, \dots, L_{n_\varepsilon}}^{M_1, \dots, M_m}$ where N is the level, the L_i and M_j are letters (or in one case, the string AA) indicating the simple factors of the jacobian J of the curve, and ε is (the label of) a Dirichlet character $(\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}^*$. More precisely, the notation indicates that J is isogenous to the product of the $\mathbb{Q}$ -simple modular abelian varieties with the following labels: A_{NM_j} for each superscript M_j and $A_{NL_{i_\varepsilon}}$ for each subscript L_i . (It turns out that in all known cases, there is at most one Galois conjugacy class of nontrivial characters ε involved.)

Tables. Table 4 shows the 64 new modular curves of genus two with jacobian not $\mathbb{Q}$ -simple. (The 149 new modular curves of genus two with $\mathbb{Q}$ -simple jacobian were already listed in [27].) Tables 5, 6 and 7 show the 30 new modular hyperelliptic curves of genus > 2 with $\mathbb{Q}$ -simple jacobian, trivial character, and level ≤ 3000 , grouped by their genus. Recall that by Proposition 1.3 of [68], a new modular curve with $\mathbb{Q}$ -simple jacobian and nontrivial

character must have even genus; this explains why we may omit the hypothesis $\#\mathcal{D} = 1$ in Tables 5 and 7.

Tables 8, 9 and 10 show the 40 new modular hyperelliptic curves that have genus > 2 and level ≤ 2000 such that the jacobian is a quotient of $J_0(N)^{\text{new}}$ that is not $\mathbb{Q}$ -simple. Table 11 shows the five curves with genus 3 and $\#\mathcal{D} = 3$. Table 12 contains all new modular hyperelliptic curves with $2 \mid \#\mathcal{D}$, $w \notin \mathcal{D}$ and genus $3 \leq g \leq 4$. All of them have genus 3 and their jacobians are neither $\mathbb{Q}$ -simple nor a $\mathbb{Q}$ -factor of $J_0(N)^{\text{new}}$. Table 13 contains the remaining curves with $\#\mathcal{D} > 1$ and level ≤ 569 . These curves have $\#\mathcal{D} = 2, 3$ or 4.

Remark 9.6. By inspection, the first curve in Table 13, namely $C_{52A,B_{\{0,4\}}}^A$, has a degree-2 unramified cover that dominates $y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1$, which is a equation for $X_1(13)$. The fourth curve, $C_{208A,D_{\{0,0,4\}}}^C$, similarly has a degree-2 unramified cover that dominates $X_1(13)$. The second and third curves in Table 13, namely $C_{160A,E_{\{\{1,0\},1\}}}$ and $C_{160B,F_{\{\{1,0\},1\}}}$, have degree-2 unramified covers dominating $y^2 = p(x)$ and $y^2 = -p(-x)$, respectively, where $p(x) = (x-1)(x^2-2x+2)(x^2-x-1)$; the latter two curves are the new modular curves $C_{160,C}$ and $C_{160,D}$ of genus 2 from [27]. We do not have a good explanation for this phenomenon.

Table 4: Not $\mathbb{Q}$ -simple, $g = 2$

C	: $y^2 = F(x)$
$C_{26}^{A,B}$	: $y^2 = x^6 + 4x^5 - 12x^4 - 114x^3 - 308x^2 - 384x - 191$
$C_{37}^{A,B}$	: $y^2 = x^6 - 4x^5 - 40x^4 + 348x^3 - 1072x^2 + 1532x - 860$
$C_{50}^{A,B}$	: $y^2 = x^6 + 2x^5 - 5x^4 - 30x^3 - 55x^2 - 48x - 16$
$C_{54}^{A,B}$	: $y^2 = x^6 - 34x^3 + 1$
$C_{56}^{A,B}$	: $y^2 = x^5 + 6x^4 - 45x^3 - 490x^2 - 1503x - 1564$
$C_{58}^{A,B}$	: $y^2 = x^6 - 2x^5 + 11x^4 - 22x^3 + 21x^2 - 12x + 4$
$C_{66}^{A,B}$	: $y^2 = x^6 + 2x^5 - 5x^4 - 22x^3 - 31x^2 - 24x - 8$
$C_{80}^{A,B}$	: $y^2 = x^5 + 2x^4 - 26x^3 - 132x^2 - 231x - 142$
$C_{84}^{A,B}$	: $y^2 = x^5 + 4x^4 - 25x^3 - 172x^2 - 339x - 222$
$C_{90}^{A,B}$	: $y^2 = x^6 - 18x^3 + 1$
$C_{91}^{A,B}$	: $y^2 = x^6 + 2x^5 - x^4 - 8x^3 - x^2 + 2x + 1$
$C_{96}^{A,B}$	: $y^2 = x^5 - 34x^3 + x$
$C_{112}^{A,C}$	: $y^2 = x^5 - 2x^4 + 10x^3 - 16x^2 + 21x - 14$
$C_{112}^{A,B}$	: $y^2 = x^5 - 6x^4 - 45x^3 + 490x^2 - 1503x + 1564$
$C_{128}^{B,D}$	: $y^2 = x^5 - 24x^3 + 16x$
$C_{128}^{A,C}$	: $y^2 = x^5 + 24x^3 + 16x$
$C_{138}^{A,C}$	: $y^2 = x^6 + 8x^4 + 6x^3 + 8x^2 + 1$
$C_{142}^{B,D}$	: $y^2 = x^6 - 2x^5 - 5x^4 + 18x^3 - 19x^2 + 12x - 4$
$C_{160}^{A,B}$	: $y^2 = x^5 + 12x^3 + 16x$

C	$: y^2 = F(x)$
$C_{162}^{A,D}$	$: y^2 = x^6 + 14x^3 + 1$
$C_{162}^{B,C}$	$: y^2 = x^6 - 10x^3 + 1$
$C_{184}^{C,D}$	$: y^2 = x^5 - 10x^3 - 15x^2 - 9x - 7$
$C_{189}^{A,C}$	$: y^2 = x^6 - 12x^4 + 36x^3 - 48x^2 + 36x - 12$
$C_{189}^{A,B}$	$: y^2 = x^6 - 12x^4 + 12x^3 + 24x^2 - 36x + 12$
$C_{192}^{C,D}$	$: y^2 = x^5 - 14x^3 + x$
$C_{192}^{B,D}$	$: y^2 = x^5 + 4x^4 - 6x^3 - 58x^2 - 111x - 70$
$C_{192}^{A,C}$	$: y^2 = x^5 - 4x^4 - 6x^3 + 58x^2 - 111x + 70$
$C_{192}^{A,B}$	$: y^2 = x^5 + 34x^3 + x$
$C_{200}^{C,E}$	$: y^2 = x^5 - 10x^3 - 15x^2 + 8$
$C_{240}^{C,D}$	$: y^2 = x^5 - 2x^4 + 6x^3 - 13x^2 + 12x - 4$
$C_{256}^{A,D}$	$: y^2 = x^5 + 16x$
$C_{264}^{A,B}$	$: y^2 = x^5 + 2x^4 - 6x^3 - 23x^2 - 24x - 8$
$C_{312}^{B,C}$	$: y^2 = x^5 - 2x^4 - x^3 + 8x^2 - 9x + 3$
$C_{320}^{A,C}$	$: y^2 = x^5 - 2x^4 - 2x^3 - 2x^2 + x$
$C_{320}^{D,E}$	$: y^2 = x^5 - 12x^3 + 16x$
$C_{320}^{B,F}$	$: y^2 = x^5 + 2x^4 - 2x^3 + 2x^2 + x$
$C_{336}^{A,F}$	$: y^2 = x^5 - 4x^4 - 25x^3 + 172x^2 - 339x + 222$
$C_{368}^{A,G}$	$: y^2 = x^5 - 10x^3 + 15x^2 - 9x + 7$
$C_{384}^{A,D}$	$: y^2 = x^5 + 10x^3 + x$
$C_{384}^{B,C}$	$: y^2 = x^5 - 10x^3 + x$
$C_{400}^{B,E}$	$: y^2 = x^5 - 25x^2 + 20x - 4$
$C_{400}^{A,H}$	$: y^2 = x^5 - 10x^3 + 15x^2 - 8$
$C_{405}^{A,F}$	$: y^2 = x^6 - 12x^4 + 28x^3 - 24x^2 + 12x - 4$
$C_{405}^{B,F}$	$: y^2 = x^6 - 12x^4 + 20x^3 - 12x + 4$
$C_{448}^{A,D}$	$: y^2 = x^5 - 2x^4 + 10x^3 - 2x^2 + x$
$C_{448}^{B,G}$	$: y^2 = x^5 + 2x^4 + 10x^3 + 2x^2 + x$
$C_{480}^{B,C}$	$: y^2 = x^5 + 2x^4 - 4x^3 - 17x^2 - 18x - 6$
$C_{480}^{B,G}$	$: y^2 = x^5 - 7x^3 + x$
$C_{480}^{A,G}$	$: y^2 = x^5 - 2x^4 - 4x^3 + 17x^2 - 18x + 6$
$C_{528}^{A,D}$	$: y^2 = x^5 - 2x^4 - 6x^3 + 23x^2 - 24x + 8$
$C_{544}^{B,C}$	$: y^2 = x^5 - 9x^3 + 16x$
$C_{624}^{C,D}$	$: y^2 = x^5 + 2x^4 - x^3 - 8x^2 - 9x - 3$
$C_{672}^{A,G}$	$: y^2 = x^5 + 5x^3 + x$

C	: $y^2 = F(x)$
$C_{760}^{A,E}$	: $y^2 = x^5 + 3x^3 + 14x^2 + 15x + 5$
$C_{768}^{D,F}$	: $y^2 = x^5 - 4x^3 + x$
$C_{768}^{B,H}$	: $y^2 = x^5 + 4x^3 + x$
$C_{960}^{A,F}$	: $y^2 = x^5 + 7x^3 + x$
$C_{1088}^{L,N}$	: $y^2 = x^5 + 9x^3 + 16x$
$C_{1344}^{C,F}$	: $y^2 = x^5 - 5x^3 + x$
$C_{1520}^{B,D}$	: $y^2 = x^5 + 3x^3 - 14x^2 + 15x - 5$
$C_{1664}^{F,G}$	: $y^2 = x^5 - 2x^4 + x^3 + 2x - 4$
$C_{1664}^{O,S}$	: $y^2 = x^5 + 2x^4 + x^3 + 2x + 4$
$C_{2208}^{A,E}$	: $y^2 = x^5 + 2x^4 + 8x^3 + 19x^2 + 18x + 6$
$C_{2208}^{G,I}$	: $y^2 = x^5 - 2x^4 + 8x^3 - 19x^2 + 18x - 6$

Table 5: $\mathbb{Q}$ -simple, $g = 3$, $N \leq 3000$

C	: $y^2 = F(x)$
C_{41}^A	: $y^2 = x^8 + 4x^7 - 8x^6 - 66x^5 - 120x^4 - 56x^3 + 53x^2 + 36x - 16$
C_{95}^A	: $y^2 = (x^4 + x^3 - 6x^2 - 10x - 5)(x^4 + x^3 - 2x^2 + 2x - 1)$
C_{152}^C	: $y^2 = x(x^3 - 2x^2 - 7x - 8)(x^3 + 4x^2 + 4x + 4)$
C_{248}^E	: $y^2 = (x^3 + x - 1)(x^4 - 2x^3 - 3x^2 - 4x + 4)$
C_{284}^A	: $y^2 = x^7 + 4x^6 + 5x^5 + x^4 - 3x^3 - 2x^2 + 1$
C_{284}^B	: $y^2 = x^7 - 7x^5 - 11x^4 + 5x^3 + 18x^2 + 4x - 11$
C_{304}^G	: $y^2 = x(x^3 - 4x^2 + 4x - 4)(x^3 + 2x^2 - 7x + 8)$
C_{496}^J	: $y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4)$
C_{544}^I	: $y^2 = (x + 1)(x^2 + x - 4)(x^4 - x^2 - 4)$
C_{544}^J	: $y^2 = (x - 1)(x^2 - x - 4)(x^4 - x^2 - 4)$
C_{896}^I	: $y^2 = (x - 2)(x^2 + 2x - 1)(x^4 - 2x^2 - 7)$
C_{896}^K	: $y^2 = (x + 2)(x^2 - 2x - 1)(x^4 - 2x^2 - 7)$
C_{1136}^G	: $y^2 = x^7 - 7x^5 + 11x^4 + 5x^3 - 18x^2 + 4x + 11$
C_{1136}^J	: $y^2 = x^7 - 4x^6 + 5x^5 - x^4 - 3x^3 + 2x^2 - 1$

Table 6: $\mathbb{Q}$ -simple, $g = 4$, $\#\mathcal{D} = 1$, $N \leq 3000$

C	: $y^2 = F(x)$
C_{47}^A	: $y^2 = (x^5 - 5x^3 - 20x^2 - 24x - 19)(x^5 + 4x^4 + 7x^3 + 8x^2 + 4x + 1)$
C_{119}^A	: $y^2 = (x^5 - 2x^4 + 3x^3 - 6x^2 - 7)(x^5 + 2x^4 + 3x^3 + 6x^2 + 4x + 1)$

C	: $y^2 = F(x)$
C_{164}^A	: $y^2 = x(x^8 + 4x^7 - 8x^6 - 66x^5 - 120x^4 - 56x^3 + 53x^2 + 36x - 16)$
C_{376}^C	: $y^2 = (x^4 - 2x^3 - 3x^2 + 4x - 4)(x^5 + 4x^4 + 3x^3 - 2x^2 + 2x + 5)$
C_{376}^D	: $y^2 = (x^4 - 2x^3 - 3x^2 + 4x - 4)(x^5 - x^3 + 2x^2 - 2x + 1)$
C_{416}^F	: $y^2 = x(x^2 + 4)(x^3 - 2x^2 + x - 4)(x^3 + 2x^2 + x + 4)$
C_{512}^G	: $y^2 = x(x^4 - 4x^2 - 4)(x^4 + 4x^2 - 4)$
C_{656}^I	: $y^2 = x(x^8 - 4x^7 - 8x^6 + 66x^5 - 120x^4 + 56x^3 + 53x^2 - 36x - 16)$
C_{752}^G	: $y^2 = (x^4 + 2x^3 - 3x^2 - 4x - 4)(x^5 - x^3 - 2x^2 - 2x - 1)$
C_{752}^I	: $y^2 = (x^4 + 2x^3 - 3x^2 - 4x - 4)(x^5 - 4x^4 + 3x^3 + 2x^2 + 2x - 5)$
C_{832}^P	: $y^2 = x(x + 2)(x - 2)(x^6 + 2x^4 - 15x^2 + 16)$
C_{1216}^W	: $y^2 = (x^3 - 2x + 2)(x^6 + 2x^4 - 7x^2 + 8)$
C_{1216}^X	: $y^2 = (x^3 - 2x - 2)(x^6 + 2x^4 - 7x^2 + 8)$

Table 7: $\mathbb{Q}$ -simple, $g = 5$, $N \leq 3000$

C	: $y^2 = F(x)$
C_{59}^A	: $y^2 = (x^9 + 2x^8 - 4x^7 - 21x^6 - 44x^5 - 60x^4 - 61x^3 - 46x^2 - 24x - 11)(x^3 + 2x^2 + 1)$
C_{1664}^Y	: $y^2 = (x^2 + 2x + 2)(x^3 - x + 2)(x^6 + 2x^4 + x^2 + 4)$
C_{1664}^{AA}	: $y^2 = (x^2 - 2x + 2)(x^3 - x - 2)(x^6 + 2x^4 + x^2 + 4)$

Table 8: Not $\mathbb{Q}$ -simple, $g = 3$, $\#\mathcal{D} = 1$, $N \leq 2000$

C	: $y^2 = F(x)$
$C_{35}^{A,B}$	: $y^2 = (x^2 + 3x + 1)(x^6 + x^5 - 10x^4 - 39x^3 - 62x^2 - 51x - 19)$
$C_{39}^{A,B}$	: $y^2 = (x^4 - 3x^3 - 4x^2 - 2x - 1)(x^4 + 5x^3 + 8x^2 + 6x + 3)$
$C_{88}^{A,B}$	: $y^2 = (x - 2)(x^3 - 2x^2 + 4x - 4)(x^3 + 2x^2 - 4x + 8)$
$C_{104}^{A,B}$	: $y^2 = (x + 2)(x^6 + 4x^5 - 12x^4 - 114x^3 - 308x^2 - 384x - 191)$
$C_{116}^{A,B,C}$	: $y^2 = (x + 2)(x^6 + 2x^5 - 17x^4 - 66x^3 - 83x^2 - 32x - 4)$
$C_{128}^{A,B,D}$	: $y^2 = (x - 2)(x^2 - 2x + 2)(x^4 - 12x^2 + 32x - 28)$
$C_{128}^{B,C,D}$	: $y^2 = (x + 2)(x^2 + 2x + 2)(x^4 - 12x^2 - 32x - 28)$
$C_{160}^{A,C}$	: $y^2 = (x - 2)(x^2 + 2x - 7)(x^4 - 4x^3 + 10x^2 - 20x + 17)$
$C_{160}^{B,C}$	: $y^2 = (x + 2)(x^2 - 2x - 7)(x^4 + 4x^3 + 10x^2 + 20x + 17)$
$C_{176}^{A,D}$	: $y^2 = (x + 2)(x^3 - 2x^2 - 4x - 8)(x^3 + 2x^2 + 4x + 4)$
$C_{184}^{B,E}$	: $y^2 = (x - 1)(x^3 - 2x^2 + 3x - 1)(x^3 + x^2 - x + 7)$
$C_{184}^{A,C,D}$	: $y^2 = (x - 1)(x^6 - x^5 + 4x^4 - x^3 + 2x^2 + 2x + 1)$

C	$: y^2 = F(x)$
$C_{196}^{B,C}$	$: y^2 = (x^3 + 2x^2 - x - 1)(x^4 - 2x^3 - 9x^2 + 10x - 3)$
$C_{208}^{B,E}$	$: y^2 = (x - 2)(x^6 - 4x^5 - 12x^4 + 114x^3 - 308x^2 + 384x - 191)$
$C_{224}^{A,D}$	$: y^2 = x(x - 1)(x + 1)(x^4 - 6x^2 + 16x - 7)$
$C_{224}^{B,C}$	$: y^2 = x(x - 1)(x + 1)(x^4 - 6x^2 - 16x - 7)$
$C_{248}^{B,D}$	$: y^2 = (x^3 + 4x^2 + 5x + 3)(x^4 - 2x^3 - 3x^2 - 4x + 4)$
$C_{256}^{B,E}$	$: y^2 = x(x^2 + 2)(x^4 + 12x^2 + 4)$
$C_{256}^{C,E}$	$: y^2 = x(x^2 - 4x + 2)(x^2 - 2)(x^2 + 4x + 2)$
$C_{280}^{A,D}$	$: y^2 = (x - 1)(x^6 - x^5 + 7x^3 - 16x^2 + 15x - 5)$
$C_{368}^{C,I}$	$: y^2 = (x + 1)(x^3 - x^2 - x - 7)(x^3 + 2x^2 + 3x + 1)$
$C_{368}^{A,D,G}$	$: y^2 = (x + 1)(x^6 + x^5 + 4x^4 + x^3 + 2x^2 - 2x + 1)$
$C_{416}^{A,E}$	$: y^2 = x(x^6 - 2x^5 - 2x^4 + 2x^2 - 2x - 1)$
$C_{416}^{B,C}$	$: y^2 = x(x^6 + 2x^5 - 2x^4 + 2x^2 + 2x - 1)$
$C_{464}^{D,E,F}$	$: y^2 = (x - 2)(x^6 - 2x^5 - 17x^4 + 66x^3 - 83x^2 + 32x - 4)$
$C_{496}^{C,G}$	$: y^2 = (x^3 - 4x^2 + 5x - 3)(x^4 + 2x^3 - 3x^2 + 4x + 4)$
$C_{560}^{A,G}$	$: y^2 = (x + 1)(x^6 + x^5 - 7x^3 - 16x^2 - 15x - 5)$
$C_{640}^{C,K}$	$: y^2 = x(x^2 - 2x - 1)(x^4 + 2x^3 - 2x + 1)$
$C_{640}^{G,I}$	$: y^2 = x(x^2 + 2x - 1)(x^4 - 2x^3 + 2x + 1)$
$C_{704}^{B,N}$	$: y^2 = x(x^3 - 4x + 4)(x^3 + 2x^2 - 2)$
$C_{704}^{C,O}$	$: y^2 = x(x^3 - 2x^2 + 2)(x^3 - 4x - 4)$
$C_{784}^{G,M}$	$: y^2 = (x^3 - 2x^2 - x + 1)(x^4 + 2x^3 - 9x^2 - 10x - 3)$

Table 9: Not $\mathbb{Q}$ -simple, $g = 4$, $\#\mathcal{D} = 1$, $N \leq 2000$

C	$: y^2 = F(x)$
$C_{224}^{C,D}$	$: y^2 = x(x^4 - 2x^3 - 5x^2 - 2x + 1)(x^4 + 2x^3 - 5x^2 + 2x + 1)$
$C_{236}^{B,C}$	$: y^2 = x^9 + 2x^8 - 4x^7 - 21x^6 - 44x^5 - 60x^4 - 61x^3 - 46x^2 - 24x - 11$
$C_{368}^{B,F,H}$	$: y^2 = (x^3 - x^2 - x - 7)(x^6 + x^5 + 4x^4 + x^3 + 2x^2 - 2x + 1)$
$C_{448}^{I,J}$	$: y^2 = x(x^8 + 14x^6 + 19x^4 + 14x^2 + 1)$
$C_{704}^{D,E,M}$	$: y^2 = (x^3 - 4x - 4)(x^3 - 4x + 4)(x^3 + 2x^2 - 2)$
$C_{704}^{F,I,P}$	$: y^2 = (x^3 - 2x^2 + 2)(x^3 - 4x - 4)(x^3 - 4x + 4)$
$C_{944}^{J,L}$	$: y^2 = x^9 - 2x^8 - 4x^7 + 21x^6 - 44x^5 + 60x^4 - 61x^3 + 46x^2 - 24x + 11$

Table 10: Not $\mathbb{Q}$ -simple, $g = 6$, $\#\mathcal{D} = 1$, $N \leq 2000$

C	: $y^2 = F(x)$
$C_{71}^{A,B}$	: $y^2 = (x^7 - 7x^5 - 11x^4 + 5x^3 + 18x^2 + 4x - 11)$ $(x^7 + 4x^6 + 5x^5 + x^4 - 3x^3 - 2x^2 + 1)$

Table 11: $g = 3$, $\#\mathcal{D} = 3$

C	: $y^2 = F(x)$
$C_{21A_{\{0,2\}}}^A$	: $y^2 = (x^2 - x + 1)(x^6 + x^5 - 6x^4 - 3x^3 + 14x^2 - 7x + 1)$
$C_{36A_{\{0,2\}}}^A$	: $y^2 = (x + 1)(x + 2)(x^2 + 3x + 3)(x^3 - 9x - 9)$
$C_{72A_{\{0,0,2\}}}^A$	: $y^2 = x(x + 1)(x^2 + x + 1)(x^3 - 3x - 1)$
$C_{144A_{\{0,0,2\}}}^A$	: $y^2 = (x - 2)(x - 1)(x^2 - 3x + 3)(x^3 - 9x + 9)$
$C_{144B_{\{0,0,2\}}}^B$	: $y^2 = (x - 1)x(x^2 - x + 1)(x^3 - 3x + 1)$

Table 12: $g = 3$, $2 \mid \#\mathcal{D}$, $w \notin \mathcal{D}$

C	: $y^2 = F(x)$
$C_{40A_{\{0,0,2\}}}^A$	: $y^2 = x(x + 1)(x + 2)(x^2 - 2x - 4)(x^2 + 3x + 1)$
$C_{48A_{\{1,0,1\}}}^A$	: $y^2 = (x + 1)(x^2 - 2x - 2)(x^2 + x + 1)(x^2 + 2x + 2)$
$C_{64A_{\{0,8\}}}^A$	: $y^2 = x(x - 1)(x + 1)(x^2 - 2x - 1)(x^2 + 2x - 1)$
$C_{80A_{\{0,0,2\}}}^A$	: $y^2 = x(x - 1)(x - 2)(x^2 - 3x + 1)(x^2 + 2x - 4)$
$C_{80A_{\{0,0,2\}}}^B$	: $y^2 = (x + 1)(x^2 - x - 1)(x^4 + 4x^2 + 8x + 4)$
$C_{128A_{\{0,16\}}}^B$	: $y^2 = (x - 2)(x^2 - 2x - 1)(x^4 - 6x^2 - 16x + 41)$
$C_{128A_{\{0,16\}}}^D$	: $y^2 = (x + 2)(x^2 + 2x - 1)(x^4 - 6x^2 + 16x + 41)$

Table 13: $g \geq 4$, $\#\mathcal{D} > 1$, $N \leq 569$

C	: $y^2 = F(x)$
$C_{52A,B_{\{0,4\}}}^A$	: $y^2 = x(x + 1)(x^3 - x^2 - 4x - 1)(x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1)$
$C_{160A,E_{\{1,0,1\}}}^A$	: $y^2 = (x - 1)(x^2 - 2x + 2)(x^2 - x - 1)(x^4 - 8x + 8)$
$C_{160B,F_{\{1,0,1\}}}^A$	: $y^2 = (x + 1)(x^2 + 2x + 2)(x^2 + x - 1)(x^4 + 8x + 8)$
$C_{208A,D_{\{0,0,4\}}}^C$	: $y^2 = x(x - 1)(x^3 + x^2 - 4x + 1)(x^6 - 4x^5 + 6x^4 - 2x^3 + x^2 - 2x + 1)$
$C_{512D_{\{0,64\}}}^C$	: $y^2 = x(x^8 + 24x^4 + 16)$

ACKNOWLEDGEMENTS

We thank Dinakar Ramakrishnan and Ken Ribet for discussing Proposition 3.2 with us. The proof of Theorem 5.7 grew out of discussions with Matthias Aschenbrenner, Brian Conrad, Tom Graber, Tom Scanlon, and Jason Starr. We thank also Paul Gunnells, Sorin Popescu, Xavier-François Roblot, William Stein and Tonghai Yang for suggesting references. Finally we thank a referee for an especially helpful report.

REFERENCES

- [1] Shreeram S. Abhyankar and Chanderjit L. Bajaj. Automatic parameterization of rational curves and surfaces. III. Algebraic plane curves. *Comput. Aided Geom. Design*, 5(4):309–321, 1988.
- [2] Dan Abramovich. A linear lower bound on the gonality of modular curves. *Internat. Math. Res. Notices*, (20):1005–1011, 1996.
- [3] Robert D. M. Accola. *Topics in the theory of Riemann surfaces*. Springer-Verlag, Berlin, 1994.
- [4] Noboru Aoki. Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves. *Amer. J. Math.*, 113(5):779–833, 1991.
- [5] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*. Springer-Verlag, New York, 1985.
- [6] A. O. L. Atkin and Wen Ch’ing Winnie Li. Twists of newforms and pseudo-eigenvalues of W -operators. *Invent. Math.*, 48(3):221–243, 1978.
- [7] Lev A. Borisov, Paul E. Gunnells, and Sorin Popescu. Elliptic functions and equations of modular curves. *Math. Ann.*, 321(3):553–568, 2001.
- [8] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993), homepage at <http://magma.maths.usyd.edu.au/magma/>.
- [9] Rolf Brandt and Henning Stichtenoth. Die Automorphismengruppen hyperelliptischer Kurven. *Manuscripta Math.*, 55(1):83–92, 1986.
- [10] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.
- [11] E. Bujalance, J. M. Gamboa, and G. Gromadzki. The full automorphism groups of hyperelliptic Riemann surfaces. *Manuscripta Math.*, 79(3-4):267–282, 1993.
- [12] Henri Carayol. Sur les représentations l -adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.
- [13] G. Cardona and J. Quer. Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12} . Preprint, 2002.
- [14] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [15] J. E. Cremona. Elliptic curve data. 21 June 2004, <http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html>.
- [16] J. E. Cremona. Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction. *Math. Proc. Cambridge Philos. Soc.*, 111(2):199–218, 1992.
- [17] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.
- [18] Mario Daberkow. On computations in Kummer extensions. Computational algebra and number theory (Milwaukee, WI, 1996). *J. Symbolic Comput.*, 31 (1–2):113–131, 2001.
- [19] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.
- [20] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat’s Last Theorem (Toronto, ON, 1993–1994)*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.
- [21] Jordan S. Ellenberg and Chris Skinner. On the modularity of $\mathbf{Q}$ -curves. *Duke Math. J.*, 109(1):97–122, 2001.
- [22] Gerd Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986. Translated from the German original [*Invent. Math.*, 73(3): 349–366, 1983; *ibid.* 75(2): 381, 1984] by Edward Shipz.

- [23] Masahiro Furumoto and Yuji Hasegawa. Hyperelliptic quotients of modular curves $X_0(N)$. *Tokyo J. Math.*, 22(1):105–125, 1999.
- [24] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999.
- [25] David Goldschmidt. *Algebraic Functions and Projective Curves*. Springer-Verlag, New York, 2002.
- [26] J. González. Equations of hyperelliptic modular curves. *Ann. Inst. Fourier (Grenoble)*, 41(4):779–795, 1991.
- [27] E. González-Jiménez and J. González. Modular curves of genus 2. *Math. Comp.*, 72(241):397–418, 2003.
- [28] Andrew Granville. ABC allows us to count squarefrees. *Internat. Math. Res. Notices*, (19):991–1009, 1998.
- [29] Georges Gras. *Class field theory. From theory to practice*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French manuscript by Henri Cohen.
- [30] Yuji Hasegawa. Hyperelliptic modular curves $X_0^*(N)$. *Acta Arith.*, 81(4):369–385, 1997.
- [31] Yuji Hasegawa and Ki-ichiro Hashimoto. Hyperelliptic modular curves $X_0^*(N)$ with square-free levels. *Acta Arith.*, 77(2):179–193, 1996.
- [32] Yuji Hasegawa and Mahoro Shimura. Trigonal modular curves. *Acta Arith.*, 88(2):129–140, 1999.
- [33] Yuji Hasegawa and Mahoro Shimura. Trigonal modular curves $X_0^{+d}(N)$. *Proc. Japan Acad. Ser. A Math. Sci.*, 75(9):172–175, 1999.
- [34] Yuji Hasegawa and Mahoro Shimura. Trigonal modular curves $X_0^*(N)$. *Proc. Japan Acad. Ser. A Math. Sci.*, 76(6):83–86, 2000.
- [35] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95:736–788, 1926.
- [36] Florian Hess. An algorithm for computing isomorphisms of algebraic function fields. In *Algorithmic Number Theory: 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004. Proceedings*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 263–271. Springer, Berlin, 2004.
- [37] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to automata theory, languages, and computation*. Addison-Wesley Publishing Co., Reading, Mass., 1979. Addison-Wesley Series in Computer Science.
- [38] Dale Husemöller. *Elliptic curves*. Springer-Verlag, New York, 1987. With an appendix by Ruth Lawrence.
- [39] Jun-ichi Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81:561–577, 1959.
- [40] N. Ishii and F. Momose. Hyperelliptic modular curves. *Tsukuba J. Math.*, 15(2):413–423, 1991.
- [41] E. Kani. Abelian subvarieties and the Shimura construction. Preprint, September 2004. <http://www.mast.queensu.ca/~kani/papers/abs4.pdf>.
- [42] E. Kani. Endomorphisms of Jacobians of modular curves. Preprint, August 2004. <http://www.mast.queensu.ca/~kani/papers/endos2.pdf>.
- [43] Nicholas M. Katz. p -adic interpolation of real analytic Eisenstein series. *Ann. of Math. (2)*, 104(3):459–571, 1976.
- [44] Henry H. Kim. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2 . *J. Amer. Math. Soc.*, 16(1):139–183 (electronic), 2003. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.
- [45] Felix Klein. Über die Transformation elfter Ordnung der elliptischen Funktionen. *Math. Ann.*, 15, 1879. reprinted in *Ges. Math. Abh.*, Bd. III, art. LXXXVI, pp. 140–168.
- [46] Peter George Kluit. *Hecke operators on $\Gamma^*(N)$ and their traces*. Vrije Universiteit te Amsterdam, Amsterdam, 1979. With a computer-aided study of low genus $X^*(N)$, Dissertation, Vrije Universiteit, Amsterdam, 1979, With a Dutch summary.
- [47] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.
- [48] H. W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992.
- [49] Wen Ch'ing Winnie Li. Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.
- [50] Qing Liu and Dino Lorenzini. Models of curves and finite covers. *Compositio Math.*, 118(1):61–102, 1999.
- [51] Paul Lockhart, Michael Rosen, and Joseph H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993.
- [52] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

- [53] David Marker. *Model theory. An introduction*. Volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [54] Loïc Merel. Universal Fourier expansions of modular forms. In *On Artin's conjecture for odd 2-dimensional representations*, volume 1585 of *Lecture Notes in Math.*, pages 59–94. Springer, Berlin, 1994.
- [55] J.-F. Mestre. Corps euclidiens, unités exceptionnelles et courbes elliptiques. *J. Number Theory*, 13(2):123–137, 1981.
- [56] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.
- [57] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.
- [58] Naoki Murabayashi. On normal forms of modular curves of genus 2. *Osaka J. Math.*, 29(2):405–418, 1992.
- [59] A. Nerode. A decision method for p -adic integral zeros of diophantine equations. *Bull. Amer. Math. Soc.*, 69:513–517, 1963.
- [60] A. P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.
- [61] Bjorn Poonen. Computational aspects of curves of genus at least 2. In *Algorithmic number theory (Talence, 1996)*, pages 283–306. Springer, Berlin, 1996.
- [62] Jordi Quer. $\mathbf{Q}$ -curves and abelian varieties of GL_2 -type. *Proc. London Math. Soc. (3)*, 81(2):285–317, 2000.
- [63] Markus A. Reichert. Détermination explicite des courbes elliptiques ayant un groupe de torsion non trivial sur des corps de nombres quadratiques sur $\mathbb{Q}$. In *Seminar on number theory, 1983–1984 (Talence, 1983/1984)*, pages Exp. No. 11, 33. Univ. Bordeaux I, Talence, 1984.
- [64] Kenneth A. Ribet. Galois representations attached to eigenforms with Nebentypus. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 17–51. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.
- [65] Kenneth A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.
- [66] Kenneth A. Ribet. Fields of definition of abelian varieties with real multiplication. In *Arithmetic geometry (Tempe, AZ, 1993)*, pages 107–118. Amer. Math. Soc., Providence, RI, 1994.
- [67] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.
- [68] Goro Shimura. Class fields over real quadratic fields and Hecke operators. *Ann. of Math. (2)*, 95:130–190, 1972.
- [69] Goro Shimura. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan*, 25:523–544, 1973.
- [70] Mahoro Shimura. Defining equations of modular curves $X_0(N)$. *Tokyo J. Math.*, 18(2):443–456, 1995.
- [71] William Arthur Stein. Explicit approaches to modular abelian varieties. Ph. D. thesis, University of California, Berkeley, 2000.
- [72] Alfred Tarski. *A decision method for elementary algebra and geometry*. University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.
- [73] Mark van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *J. Symbolic Comput.*, 23(2-3):209–227, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).
- [74] Mark van Hoeij. An algorithm for computing the Weierstrass normal form of hyperelliptic curves, 2002. [arXiv:math.AG/0203130](https://arxiv.org/abs/math/0203130).
- [75] Jacques Vélú. Courbes elliptiques munies d'un sous-groupe $\mathbf{Z}/n\mathbf{Z} \times \mu_n$. *Bull. Soc. Math. France Mém.*, (57):5–152, 1978.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602-7403, USA

Current address: School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332-0160, USA

E-mail address: mbaker@math.gatech.edu

SCHOOL OF MATHEMATICAL SCIENCES. UNIVERSITY OF NOTTINGHAM. UNIVERSITY PARK. NOTTINGHAM, NG7 2RD, UK

Current address: Departamento de Análisis Económico: Economía Cuantitativa, Facultad de Ciencias Económicas y Empresariales, Universidad Autónoma de Madrid, 28049 Madrid, Spain

E-mail address: enrique.gonzalez.jimenez@uam.es

ESCOLA UNIVERSITÀRIA POLITÈCNICA DE VILANOVA I LA GELTRÚ, AV. VÍCTOR BALAGUER S/N, E-08800 VILANOVA I LA GELTRÚ, SPAIN

E-mail address: josepg@mat.upc.es

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CA 94720-3840, USA

E-mail address: poonen@math.berkeley.edu