S. Anni et al. *Res. Number Theory* (2023) 9:21
https://doi.org/10.1007/s40993-022-00409-7

Research in Number Theory

RESEARCH

On smooth plane models for modular curves of Shimura type

Samuele Anni[1], Eran Assaf[2] and Elisa Lorenzo García[4,3*]

*Correspondence:
elisa.lorenzo@unine.ch
[3]Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, 2000 Neuchâtel, Switzerland
Full list of author information is available at the end of the article

Abstract

In this paper we prove that there are finitely many modular curves that admit a smooth plane model. Moreover, if the degree of the model is greater than or equal to 19, no such curve exists. For modular curves of Shimura type we show that none can admit a smooth plane model of degree 5, 6 or 7. Further, if a modular curve of Shimura type admits a smooth plane model of degree 8 we show that it must be a twist of one of four curves.

Keywords: Modular curves, Congruence subgroups, Cusp forms, Canonical model, Smooth plane model, Gonality

Mathematics Subject Classification: Primary 11G18, 14G35; Secondary 11F11, 14H45

1 Introduction

The compactification, by normalisation, of the quotient space of the complex upper half plane by the action of a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$, a modular group, is called a modular curve, X_Γ and it admits the structure of a compact Riemann surface. Serre's GAGA theorem tells us that $X_\Gamma(\mathbb{C})$ is a projective complex algebraic curve. Furthermore, Shimura, in [43, Proposition 6.9], proved that modular curves admit the structure of projective algebraic curves, see also [18, §7.7]. The problem of computing equations for such curves and their projective embeddings has been a central topic in numerous papers, motivated by a plethora of applications. We will describe some of those while making a summary of the state of the art.

Modular curves are moduli spaces for elliptic curves with a given level structure. Given a positive integer N and a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the modular curve X_G parametrises pairs (E, ϕ) up to isomorphism, where E is an elliptic curve and ϕ is a G-level structure on the N-torsion of E. Therefore, the explicit knowledge of models of modular curves becomes key for understanding properties of elliptic curves. This aspect leads to several different applications, for example towards coding theory or for solving Diophantine applications, starting with the proof of Fermat's last theorem where they appear in several steps. In this article we study whether it is possible to have "nice" models, that is smooth plane models, for modular curves defined over the rationals.

In general, finding equations for modular curves of large level is computationally difficult, as it involves computing group actions on large spaces and linear algebra over large cyclotomic fields. However, for some groups it is easier to compute such curves, e.g. in [23] Galbraith computes modular curves for the groups $\Gamma_0(N)$. One can look for a slightly larger class of groups: given a positive integer N, a *group of Shimura type* of level N, as introduced originally by Shimura in [43], is a subgroup $\Gamma(H,t) \subseteq \mathrm{PSL}_2(\mathbb{Z})$ which is the projection of the pullback from $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ of $G(H,t) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, where $G(H,t) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is a subgroup of the form

$$G(H,t) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}) : a \in H, t \mid b \right\},$$

where $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ is a subgroup and $t \mid N$. We will call a modular curve of Shimura type any modular curve corresponding to the choice of a group of Shimura type.

The main result of this article is the following:

Theorem 1.1 *There are finitely many modular curves which admit a smooth plane model over the rationals. There is no modular curve which admits a smooth plane model of degree greater or equal to* 19*. Moreover, there is no modular curve of Shimura type which admits a smooth plane model of degree* 5, 6 *or* 7*. A modular curve of Shimura type which admits a smooth plane model of degree* 8 *must be a twist of one of four curves.*

The four curves mentioned in Theorem 1.1 are listed in Sect. 5.6.

Surprisingly, during the computations we found the example of a Galois trigonal, i.e. superelliptic of degree 3, model of a modular curve of genus 6, see Sect. 5.3.

1.1 State of the art

Galbraith in [23] presented several techniques to obtain explicit models of modular curves by computing projective embeddings, relying on the computation of spaces of modular forms. Let us recall Galbraith's approach for the modular curves $X_0(N)$ for a positive integer N. There is a well-known canonical affine equation for $X_0(N)$ using N-modular polynomials that are symmetric polynomials $\phi(x,y) \in \mathbb{Z}[x,y]$, of degree $N+1$ in each variable, such that $\phi(j(\tau), j(N\tau)) = 0$, where $j(\tau)$ is the classical modular j-function. These equations have very large degree, the model is highly singular, and the coefficients involved are enormous. Galbraith's approach consists in obtaining equations via the canonical embedding, which is suitable for practical computation since the differentials on the curve correspond to the weight 2 cusp forms for $\Gamma_0(N)$. Choosing a basis $\{f_1, \ldots, f_g\}$ for the weight 2 cusp forms, the canonical map is translated into $\tau \mapsto [f_1(\tau) : \cdots : f_g(\tau)]$ and gives a map from $X_0(N)$ to $\mathbb{P}^{g-1}(\mathbb{C})$ from the modularity of the forms $f_i(\tau)$. Galbraith's strategy is a key element in our approach towards the main theorem of this article.

Kohel in [33] presented a different method which involves quaternions and a different approach towards the computation of the differentials. These approaches have been used, together with others, to collect the database of small modular curve models available in `Magma` [12].

Despite the lack of a general algorithm, models for several modular curves have been found in the literature with a wide range of applications in mind. We mention some of these, as well as their relevance towards various research directions.

Baran found models for the isomorphic curves $X_{\mathrm{ns}^+}(13)$ and $X_{s^+}(13)$ in [7]. The study of integral points on these curves relates to the Serre's uniformity question over $\mathbb{Q}$, as in [42]. More recently, Dose, Mercuri and Stirpe [19] proposed a new approach for computing (singular) models in order to study Serre's question.

Derickx et al. [17] proved that elliptic curves over totally real cubic fields are "modular" meaning that their L-functions match the L-function of the associated Hilbert modular forms. A key step to obtain this result is the study of points on a plane (singular) model of $X(\mathrm{b5, ns7})$.

Banwait and Cremona [6] examined the failure of the local-to-global principle for the existence of ℓ-isogenies between elliptic curves over number fields by, among other elements, determining a model for the exceptional modular curve $X_{S_4}(13)$. Zywina, in [48], generalised the work of Banwait and Cremona, by relying on numerical approximation of pseudo–eigenvalues of Atkin–Lehner operators. Through his approach it is possible to determine q-expansions and models for modular curves.

Box in [13] described an algorithm [13, Algorithm 4.13], that has been implemented by the second named author, see [2], for computing the canonical model for $X_G/\mathbb{Q}$ in the case where G has surjective determinant, $-I \in G$ and G is normalised by $J := \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. In this algorithm, one first determines the q-expansions of a basis for the corresponding space of cusp forms and then a model, using the techniques developed by Galbraith [23] when the genus is at least 2. Box's algorithm presents the advantage that, for a finite group $\mathcal{A}$ of the automorphism group of X_G, it is possible to determine a model for the quotient curve $X_G/\mathcal{A}$ directly, without computing X_G first. Box's algorithm is another key ingredient to reach the conclusion of the main result of this article.

Notice that for degree larger than 3 all smooth plane curves are non-hyperelliptic, see for example [27, Ex. IV.5.1]. In [8] the authors prove that for $N \geq 8$ all geometrically connected modular curves $X(N)$ defined over $\mathbb{Q}$ are neither hyperelliptic nor bielliptic.

Enge and Schertz [21] presented (singular) models for the modular curves $X_0(N)$ for N the product of two arbitrary primes using Dedekind's η functions. Kodrnja in [32], relying on the embeddings in projective space through modular forms and modular functions presented by Muić in [36] for computing models of modular curves, was able to find an explicit recipe to obtain plane (singular) models for all modular curves $X_0(N)$ for $N \geq 2$. The equation of the model is the minimal polynomial of the modular function $\Delta(Nz)/\Delta$ over $\mathbb{C}(j)$, where Δ is the Ramanujan Δ function and j is the modular j function. Some plane (singular) models for modular curves $X_0(N)$ were already found by Hasegawa and Shimura in [30] using different ideas, in particular studying the gonality of modular curves.

Borisov, Gunnells and Popescu [11] showed that it is possible to determine explicitly an embedding of the modular curve $X_1(p)$ into $\mathbb{P}^{\frac{(p-3)}{2}}$, where $p \geq 5$ is a prime, using weight one Eisenstein series. The equations obtained are (singular) quadratic equations. More recently, Baziz [3] proposed different (singular) models for $X_1(N)$ using N-division polynomials, and so with the advantage of keeping track explicitly of the corresponding pairs (E, P) parametrised by the curve.

In this article we are interested only in modular curves as classically presented: projective complex algebraic curves corresponding to the compactification of the quotient space of the complex upper half plane by the action of a modular subgroup. Nevertheless, it is possible to define curves that are modular: a curve C over $\mathbb{Q}$ is modular if it is dominated

by $X_1(N)$ for some N. Moreover, if in addition the image of the jacobian of the curve in $J_1(N)$ is contained in the new subvariety of $J_1(N)$, then C is new-modular. Under this definition, the modular curves associated to the classical modular groups $\Gamma_0(N)$ and $\Gamma_1(N)$, for some positive integer N, are curves that are modular. In particular there are infinitely many curves over $\mathbb{Q}$ that are modular and of genus 1: elliptic curves over $\mathbb{Q}$ are modular. Baker, González-Jiménez, González and Poonen in [5] showed that for each genus $g \geq 2$, the set of curves over $\mathbb{Q}$ of genus g that are new-modular curves is finite and computable. In particular, by analysing the automorphism group of the curve and the dominant map, they describe explicitly all curves that are new-modular of genus 2, and construct a list of new-modular hyperelliptic curves of all genera (this list might be complete, but there are pathologies presented in the last sections of the aforementioned paper). In [24] González-Jiménez and Oyono gave an algorithm to compute explicit equations for non-hyperelliptic curves that are modular of genus 3 over $\mathbb{Q}$. Moreover they conjectured that the list of non-hyperelliptic curves that are new-modular and of genus 3 consists of 44 curves, and provided equations for all of them. The issue, as in [5], is giving a bound for the coefficients of the modular forms involved.

1.2 Structure of the paper

In §2 we prove that there are a finite number of modular curves admitting a smooth plane model. To achieve this result, we bound the genus of such curves and notice that there is a finite number of congruence subgroups of any given genus. Moreover, we explicitly bound the level and the index of such groups. These results give us a finite list of groups corresponding to modular curves that may admit a smooth plane model. In §3 we discuss how to perform the computation of the canonical model of the relevant modular curves. In particular, we present the analysis regarding the runtime of the algorithm for computing q-expansions, with the precision required to prove the correctness of the resulting equations. Later, in §4 we present an algorithm that, given a canonical model of a non-hyperelliptic curve, checks whether the curve admits a smooth plane model and, if it is the case, computes it. Finally, in §5 we present our computations regarding Shimura type modular forms and modular curves.

2 A bound for the genus

In this section we prove the first two parts of the main theorem, Theorem 1.1.

Theorem 2.1 *There are a finite number of modular curves admitting a smooth plane model. Moreover, the degree of such a model is less than or equal to* 18*.*

Proof The genus–degree formula tells us that a smooth plane curve of degree d has genus $g = \frac{(d-1)(d-2)}{2}$. The gonality (over the algebraic closure) of a smooth plane curve of degree d is $d-1$, see [14, Theorem A]. The gonality of a modular curve of genus g is greater or equal to $\frac{1}{2} \cdot 975(g-1)/4096$, see [38, Remark 1.2] and [5, Remark 4.5]. Therefore, for a modular curve admitting a smooth plane model we have that $975d^2 - 19309d + 16384 \leq 0$ and so

$$1 \leq d \leq 18 \quad \text{and} \quad g \in \{0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136\}.$$

There are a finite number of modular curves of a given genus, see [15], so there are a finite number of modular curves admitting a smooth plane model. □

For degree 1 and 2, i.e. genus 0, the list of levels is given in [15, Table 4.24].

For degree 3, i.e. genus 1, the complete list of the relevant congruence subgroups is given in [16].

For degree 4 we need to consider curves of genus 3. The non-hyperelliptic ones are given by smooth plane quartics. Indeed, we find modular curves of genus 3 admitting a smooth plane model of degree 4, see Table 6 for the complete list we have computed.

Nevertheless, the following question arises naturally:

Question 2.2 *Is there any modular curve of genus greater than* 3 *admitting a smooth plane model?*

For degrees 5 and 6 we did not find any example of a modular curve admitting a smooth plane model, restricting to Shimura type modular curves, see §5.

For each genus up to 24 the complete explicit list of congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ is known: see [16, Theorem 2.8] and the associated website[1].

One way to count how many modular curves may admit a smooth plane model is to count congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ whose index is bounded in terms of the degree of the model, as follows.

Proposition 2.3 *The index ι of a congruence subgroup in* $\mathrm{PSL}_2(\mathbb{Z})$ *whose associated modular curve admits a smooth plane model of degree $d \geq 3$ satisfies*

$$6(d-1)(d-2) - 12 \leq \iota \leq 101(d-1) \tag{2.1}$$

Proof On the one hand, combining [46, Theorem 3] (see also [30, Theorem 4.3]) and an improvement presented in [16] due to Kim and Sarnak [31, Appendix 2], the index of a congruence subgroup in $\mathrm{PSL}_2(\mathbb{Z})$ is bounded by 101 times the gonality of the corresponding modular curve. By assumption, the modular curve admits a smooth plane model, so its gonality is $d-1$. The index is therefore bounded by $101(d-1)$.

On the other hand, the genus g of a modular curve admitting a smooth plane model of degree $d \geq 3$ satisfies $g = \frac{(d-1)(d-2)}{2} > 0$ and $g \leq 1 + \frac{\iota}{12}$, where ι is the index of the corresponding congruence subgroup, see [18, Theorem 3.1.1].

Therefore the index ι is bounded above and below as in Equation 2.1. □

Remark 2.4 The coefficient 101 used in Proposition 2.3 is obtained by taking the ceiling of a rational number $\alpha = 2^{15}/325$. A sharper upper bound can be obtained by rounding only after multiplication.

Remark 2.5 The result of Proposition 2.3 together with the bound for the degree presented in Theorem 2.1, and the previous remark, implies in each case the lower and upper bounds for the index ι described in Table 1.

The logarithm of the number of congruence subgroups in $\mathrm{PSL}_2(\mathbb{Z})$ of index bounded by 1714 is approximately 1897, see [9, Proposition 8.1]. Therefore naively listing all subgroups would be not feasible, and the list of [16] contains only groups of genus less than or equal to 24.

[1] https://mathstats.uncg.edu/sites/pauli/congruence/

Table 1 Index bounds

Degree	Genus	Index bound	Degree	Genus	Index bound
3	1	$0 \le \iota \le 201$	11	45	$528 \le \iota \le 1008$
4	3	$24 \le \iota \le 302$	12	55	$648 \le \iota \le 1109$
5	6	$60 \le \iota \le 403$	13	66	$780 \le \iota \le 1209$
6	10	$108 \le \iota \le 504$	14	78	$924 \le \iota \le 1310$
7	15	$168 \le \iota \le 604$	15	91	$1080 \le \iota \le 1411$
8	21	$240 \le \iota \le 705$	16	105	$1248 \le \iota \le 1512$
9	28	$324 \le \iota \le 806$	17	120	$1428 \le \iota \le 1613$
10	36	$420 \le \iota \le 907$	18	136	$1620 \le \iota \le 1714$

Table 2 Level bounds

Genus	Level bound	Genus	Level bound
1	169	45	922
3	214	55	1074
6	275	66	1237
10	351	78	1412
15	441	91	1600
21	542	105	1799
28	657	120	2010
36	784	136	2234

Let us also remark that for any given genus we can bound the level N of the congruence subgroups occurring using the following formula, due to Cox and Parry [15, Equation (4.22)],

$$N \le \begin{cases} 168 & \text{if } g = 0 \\ 12g + \frac{1}{2}(13\sqrt{48g+121} + 145) & \text{if } g \ge 1 \end{cases} \tag{2.2}$$

Analysing the genera in Theorem 2.1 we produce the level bounds appearing in Table 2.

It remains to check this finite number of possibilities, a task which we proceed to describe in the rest of the paper.

3 Computing modular curves

Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be a congruence subgroup of level N. Then the modular curve X_Γ can be given the structure of an algebraic curve over $\mathbb{Q}(\zeta_N)$. This structure depends on the choice of a group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that the projection of its pullback to $\mathrm{SL}_2(\mathbb{Z})$, denoted by PG, coincides with Γ. We denote such a model by X_G. The Galois action on the connected components of the curve X_G is given by the homomorphism $\sigma_d \mapsto \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where $\sigma_d(\zeta_N) = \zeta_N^d$. Therefore, the field of definition of X_G is the fixed field of $\det(G) \subseteq (\mathbb{Z}/N\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$, where det denotes the usual determinant map from $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $(\mathbb{Z}/N\mathbb{Z})^\times$. The connected components of the curve X_G are indexed by $(\mathbb{Z}/N\mathbb{Z})^\times / \det(G)$, and each component is defined over the field $\mathbb{Q}(\zeta_N)^{\det(G)}$. In particular, X_G is geometrically connected and defined over $\mathbb{Q}$ if and only if $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Therefore, X_Γ, which is one of the components of X_G, admits a model over $\mathbb{Q}$ only if there exists $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $PG = \Gamma$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$.

The methods of Galbraith and Box, described briefly in the introduction, for computing modular curves use duality with modular symbols, and therefore require G also to be of real type, i.e. such that $JGJ = G$, where $J = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Since J acts via complex conjugation

Table 3 Congruence subgroups of low genus

Degree	Genus	Congruence subgroups	Real type & Surjective det	Shimura type
3	1	163	108	38
4	3	241	160	26
5	6	175	74	8
6	10	235	120	17
7	15	485	244	23
8	21	729	431	55

on the Fourier coefficients of modular forms, it is equivalent to requiring the Fourier coefficients to be fixed by complex conjugation.

We therefore restrict our attention to congruence subgroups Γ such that there exists G of real type with surjective determinant and $PG = \Gamma$. Note further that for these groups, when the degree is prime to 3, it suffices to check one such model X_G by [4, Corollary 2.7]. In the range of degrees we are interested in, the only relevant case is that of degree 6, i.e. genus 10. In this case, for groups of Shimura type, the curve always admits a rational point, and so it is again enough to consider a single model by [4, Corollary 2.2]. For the other congruence subgroups of genus 10 for which we compute the curve, we verify that the resulting curves indeed have rational points, hence in these cases it also suffices to check a single model.

Our method of enumerating these subgroups of specific genus is to run over the finite list of conjugacy classes of congruence subgroups of this genus in $\mathrm{PSL}_2(\mathbb{Z})$, and for a representative $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$, we look at the projection of its pullback $H \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. As for any compatible $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, H will be a normal subgroup, we start by looking for a conjugate H' of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which satisfies $JH'J = H'$, or equivalently $J \in N(H)$, where the normalization takes place in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $N(gHg^{-1}) = gN(H)g^{-1}$, it suffices to consider conjugates of $N(H)$, and look for one which contains J. We then note that if G is such that $G \cap SL_2(\mathbb{Z}/N\mathbb{Z}) = H$, then $H \trianglelefteq G$, so that $G \subseteq N(H)$. Thus, looking for G with surjective determinant amounts to enumerating the subgroups of $N(H)/H$ of order $\phi(N)$.

In Table 3 we list how many congruence subgroups Γ exist, up to conjugacy, for each degree $3 \leq d \leq 8$, and how many of these admit a model $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of real type with surjective determinant. In Table 3 we also record the number of groups of Shimura type of each degree $3 \leq d \leq 8$.

The methods we use for computing equations of modular curves make use of explicit computation of the q-expansions and the canonical map. We briefly recall the map and its properties.

3.1 The canonical map

Let k be a perfect field. Let C/k be a smooth projective curve of genus $g \geq 2$ with canonical divisor K. Let $\{z_0, ..., z_{g-1}\}$ be a basis defined over k of the Riemann-Roch space $\mathcal{L}(K)$. The canonical map of C is given by

$$\phi_K : C \to \mathbb{P}^{g-1}, \quad P \mapsto (z_0(P) : ... : z_{g-1}(P)).$$

The curve C is non-hyperelliptic if and only if ϕ_K is an embedding. In this case $\phi_K(C)$ is defined over k and it is unique up to a linear transformation of $\mathbb{P}^{g-1}$. Otherwise, when ϕ_K

is not an embedding, the curve C is hyperelliptic and ϕ_K is the quotient by the hyperelliptic involution: $\phi_K(C) \simeq \mathbb{P}^1$.

Theorem 3.1 (Noether-Enriques-Petri, [37]) *Let C be a smooth projective non-hyperelliptic curve of genus g. The homogeneous ideal defining the canonical curve $\phi_K(C) \subseteq \mathbb{P}^{g-1}$ is generated by its elements of degree 2, except in the following cases:*

- *$g = 3$, so C is a smooth plane quartic.*
- *$g \geq 4$ and C is a trigonal curve. In this case an element of degree 3 is also needed to generate the ideal.*
- *$g = 6$ and C is a smooth plane quintic. Again in this case an element of degree 3 is also needed.*

Therefore, to compute an equation for the modular curve, using the identification $S_2(\Gamma, \mathbb{Q}(\zeta_N))^G \simeq \Omega^1(X_G)$, it suffices to compute q-expansions up to sufficient precision and look for relations in low degrees. We proceed by describing first the required precision.

3.2 Bounds

In order to distinguish modular forms we will use a finite number of coefficients of the associated q-expansions thanks to the following result due to Sturm [45, Theorem 1], see also [44, Sect. 9.4]. Let us recall that for a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ the width of the cusp ∞ is the positive integer h defined by $\left(\begin{smallmatrix} 1 & h\mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right) = \Gamma \cap \left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)$.

Theorem 3.2 ([45, Theorem 1]) *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let h be the width of the cusp ∞ for Γ. Let f be a modular form on Γ of weight κ, with coefficients in a discrete valuation ring R contained in $\mathbb{C}$. Let $\mathbb{F}$ be the residue field of R. Suppose that the image $\sum a_n q^{n/h}$ in $\mathbb{F}[[q^{1/h}]]$ of the q-expansion of the form f has $a_n = 0$ for all $n \leq \kappa[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12$. Then $a_n = 0$ for all n, i.e. f is congruent to 0 modulo the maximal ideal of R.*

Moreover, we can state the following corollary, derived from an observation at the end of [45] and stated in this form in [39]:

Corollary 3.3 ([39, Theorem 2.1]) *Under the same hypotheses of the theorem above, let us assume furthermore that f is a cusp form. If the image $\sum a_n q^{n/h}$ in $\mathbb{F}[[q^{1/h}]]$ of the q-expansion of the form f has $a_n = 0$ for all $n \leq \kappa[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12 - \#(\text{cusps})$. Then $a_n = 0$ for all n, i.e. f is congruent to 0 modulo the maximal ideal of R.*

The integer $\kappa[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12$ (resp. $\kappa[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12 - \#(\text{cusps})$) is known as the Sturm bound (resp. Sturm bound for cusp forms) and we will use the notation $B(\Gamma, \kappa)$ (resp. $B(\Gamma, \kappa)_c$) to refer to such a bound.

3.3 Groups of Shimura type

For groups of Shimura type, the methods described in [1] can be used to compute the q-expansions. Alternatively, conjugating by $\alpha_t = \left(\begin{smallmatrix} 1 & 0 \\ 0 & t \end{smallmatrix}\right)$, we see that

$$\Gamma_1(Nt) \subseteq \alpha_t \Gamma(H, t) \alpha_t^{-1} \subseteq \Gamma_0(Nt).$$

Moreover, if we decompose the space by Dirichlet characters as

$$S_2(\Gamma_1(Nt)) = \bigoplus_{\chi : (\mathbb{Z}/Nt\mathbb{Z})^\times \to \mathbb{C}^\times} S_2(\Gamma_0(Nt), \chi),$$

Table 4 Level bounds for Shimura type modular curve admitting a smooth plane model

Genus	Level bound	Genus	Level bound
1	199	45	997
3	293	55	1103
6	401	66	1201
10	503	78	1307
15	601	91	1409
21	701	105	1511
28	797	120	1609
36	887	136	1709

then we obtain

$$S_2(\alpha_t\Gamma(H,t)\alpha_t^{-1}) = \bigoplus_{\chi:\chi(H)=1} S_2(\Gamma_0(Nt),\chi).$$

The q-expansions for modular forms in the spaces in this decomposition are then straightforward to compute.

In order to compute equations for all modular curves of Shimura type of genus 1, 3, 6, 10, 15, we will need to compute weight 2 cusp forms and then check quadratic and cubic relations, according to Theorem 3.1. The number of coefficients of the q-expansions of the weight 2 cusp forms needed to certify the computation performed, is equal to $B(\Gamma,\kappa)_c$, where κ is either 4 or 6.

Proposition 3.4 *The level of a congruence subgroup in* $\mathrm{PSL}_2(\mathbb{Z})$ *associated to a Shimura type modular curve admitting a smooth plane model is bounded by* 1709. *More precisely, we can bound the level for each genus as shown in Table* 4.

Proof A congruence subgroup Γ in $\mathrm{PSL}_2(\mathbb{Z})$ corresponding to a Shimura type modular curve is contained in $\Gamma_0(M)$ and contains $\Gamma_1(M)$ for an appropriate level M, after conjugation in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Its index is bounded by 1714 as in Table 1 and so by direct computation the level is bounded by 1709 (Table 4). □

3.4 Other congruence subgroups

For groups that are not of Shimura type, we apply the (generalization of the) method of twists described by Box in [13]. We note that Box uses an auxiliary divisor M of the level N such that $G_M = B_0(M)$, where $B_0(M)$ is the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$, but this constraint can be relaxed to allow for $B_1(M) \subseteq G_M \subseteq B_0(M)$, where $B_1(M)$ is the unipotent subgroup of $B_0(M)$, by decomposing according to the action of Dirichlet characters. More precisely, if $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is such that $G \trianglelefteq G'$ and G'/G is abelian, we can decompose according to the characters of G'/G, namely

$$S_2(G) = \bigoplus_{\varepsilon:G'/G\to\mathbb{C}^\times} S_2(G',\varepsilon).$$

In the cases where $G' = B_0(M)$ and $\Gamma_1(M)\cap\Gamma(K) \subseteq G$ for some relatively prime K, M, such that $KM = N$, we may further identify

$$S_2(G',\varepsilon) = \bigoplus_{\substack{\chi:(\mathbb{Z}/MK^2\mathbb{Z})^\times\to\mathbb{C}^\times \\ \chi|_{(K\mathbb{Z}+1)/MK^2\mathbb{Z}}=\varepsilon}} S_2(\Gamma_0(MK^2),\chi)^{G'=\varepsilon}$$

by conjugating with $\alpha_K = \left(\begin{smallmatrix} 1 & 0 \\ 0 & K \end{smallmatrix}\right)$. We can then create the space of modular symbols corresponding to $S_2(\Gamma_0(MK^2), \chi)$, and cut out the subspace on which G' acts via ε by a method similar to the algorithm described in [13, Algorithm 4.11]. Putting together all these elements, we obtain an algorithm that, given a group G such that $B_1(M) \subseteq G_M \subseteq B_0(M)$, returns the q-expansions of a basis for the space of cusp forms $S_2(G)$. Denote by $\pi_M : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ the natural projection map (Tables 4, tab:hyperellipticgenus3).

Proposition 3.5 *The running time complexity of the algorithm described above for a group* $G = \pi_M^{-1}(G_M) \cap \pi_K^{-1}(G_K)$ *with* $B_1(M) \subseteq G_M \subseteq B_0(M)$ *of genus* g *is given by*

$$\widetilde{O}\left([G_M : B_1(M)](M^3K^6 + MK^4g^2)\right).$$

For a group of Shimura type $G = G(H, t)$*, it is given by* $\widetilde{O}\left(\frac{\phi(N)}{|H|}Nt^2g^2\right)$.

Proof We note that the complexity of the algorithm is dominated by the linear algebra operations performed in these spaces of modular forms. Specifically, since the algorithm requires computing the Hecke decomposition, to obtain the modular symbols corresponding to the eigenform, our complexity is dominated by $\widetilde{O}(d^3 + dL^2)$, where $d = \dim S_2(\Gamma_0(MK^2), \chi)$ is the dimension of the space and L is the precision required for the q-expansions, see [10, Table 5.2.3]. By Corollary 3.3, as the cusp width h is bounded by K, we see that the required precision to ascertain our linear relations indeed hold is bounded by $L \leq KB(\Gamma, \kappa)_c$, where κ is the maximal weight in which we look for an equation and Γ is the pullback of G to $\mathrm{SL}_2(\mathbb{Z})$. By Theorem 3.1, $\kappa \in \{4, 6\}$ in all considered cases, with $\kappa = 6$ occurring only if $g \leq 6$. Finally, by [47, Theorem 2.3], the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = O(g)$, hence $L = O(Kg)$. As $d = O(MK^2)$ (see [34] for a more precise and detailed asymptotic analysis), it follows that the running time complexity of the algorithm on the space corresponding to each Dirichlet character χ is $\widetilde{O}(M^3K^6 + MK^4g^2)$, and summing over all Dirichlet characters we obtain the result. For a group of Shimura type, we can simply compute for each of the direct summands the Hecke operators up to the required precision, which now satisfies $L = O(tg)$, as the cusp width at ∞ is precisely $h = t$. □

As a result, when looking for smooth plane models of general congruence subgroups, we will have to restrict ourselves to reasonable ranges of the parameter MK^2. We therefore treat in this paper only groups that are of Shimura type or such that $MK^2 \leq 500$. We further note that different representatives in the conjugacy class of Γ, and different groups G which pull back to Γ give rise to different values of M, K. We find for each conjugacy class of the congruence subgroup Γ, a corresponding group G with the maximal value of M (and so the minimal for MK^2). Moreover, by their definition, for groups of Shimura type we may choose $M = N/t$ and $K = t$, making them the easiest to compute using this method as well.

4 From a canonical model to a smooth plane model

In this section we propose an algorithm to check whether a smooth irreducible projective curve C of genus g and defined over a perfect field k does not admits a smooth plane model over $\bar{k}$. In the case where we cannot rule out this possibility, we propose a strategy

to compute such smooth plane model. We do not focus on the minimal fields of definitions for these models, but we point the interested reader to [4].

4.1 The low genus cases

For $g = 0, 1$ there is always a smooth plane model. For genus 2, or more generally, for hyperelliptic curves, there is never one. For genus 3 non-hyperelliptic there is always a smooth plane model and it is given by the canonical model. The next genus to check is 6, for which we have another necessary condition in order to have a smooth plane model of degree 5: the canonical ideal I_C defining $\phi_K(C)$ is not generated only by degree 2 elements, see Theorem 3.1. Still in this situation we need to distinguish between trigonal curves and smooth plane quintics, see Sect. 5.3 for a detailed example. Let us recall the following classical result, coming from the description of the regular differential forms of a smooth plane curve: The canonical model of a degree d smooth plane curve is given by the composition of $C \hookrightarrow \mathbb{P}^2$ with the $(d-3)$-Veronese embedding $\mathbb{P}^2 \hookrightarrow \mathbb{P}^{g-1}$.

Lemma 4.1 *Let C be a smooth plane quintic curve. Then the degree 2 elements of the canonical ideal I_C defining $\phi_K(C)$ define a $\mathbb{P}^2$. A bijective parametrization of it, evaluated at a degree 3 non-trivial generator of I_C, gives the smooth plane quintic model.*

Proof In the quintic case $C : F(x, y, z) = 0 \subseteq \mathbb{P}^2$ with $\deg(F) = 5$ and the Canonical model is given by the composition with the 2-Veronese embedding $\mathbb{P}^2 \hookrightarrow \mathbb{P}^5$. The canonical image $\phi_K(C)$ is generated by the equations defining $\phi_K(\mathbb{P}^2)$ that can all be taken of degree 2 and the 3 degree 3 equations, corresponding to $xF(x, y, z) = 0$, $yF(x, y, z) = 0$ and $zF(x, y, z) = 0$. □

We deal next with the higher genus situations.

4.2 The minimal free resolution

A smooth curve C of genus g admits a smooth plane model if and only if it has a (unique up to linear equivalence) very ample complete g^2_d-linear series, i.e. a very ample divisor D such that $\deg(D) = d$ and $\ell(D) = 3$. Given a basis $\{x, y, z\}$ of $\mathcal{L}(D)$, the plane model is given by the image of $C \to \mathbb{P}^2 : P \mapsto (x(P) : y(P) : z(P))$.

Theorem 4.2 ([26, Appendix]) *If a smooth curve C of genus $g = \frac{(d-1)(d-2)}{2}$ with $d \geq 5$ and canonical divisor K, has a g^2_d-linear series then the Koszul cohomology group $\mathcal{K}_{\frac{(d-3)(d-2)}{2},1}(C, K) \neq 0$.*

This theorem proves a special case of one of the directions of Conjecture 5.1 in [26]. In terms of graded Betti numbers [41, p. 84] we have:

$$\dim(\mathcal{K}_{\frac{(d-3)(d-2)}{2},1}(C, K_C)) = \beta_{d-4,d-2}.$$

Let $C/\mathbb{C}$ be a smooth curve of genus g and $\phi_K(C)$ its image by the canonical map given by the ideal I_C in $S = \mathbb{C}[z_0, z_1, ..., z_{g-1}]$. Let $S_C = S/I_C$ be the homogeneous coordinate ring of $\phi_K(C)$. We consider the minimal free resolution:

$$0 \leftarrow S_C \leftarrow S \leftarrow F_1 \leftarrow F_2 \leftarrow ... \leftarrow F_{g-2} \leftarrow 0.$$

Noether proved that $F_i = S(-i-1)^{\beta_{i,i+1}} \oplus S(-i-2)^{\beta_{i,i+2}}$ for $i = 1, ..., g-3$, i.e. that F_i is a module generated by elements of degree $i+1$ and $i+2$. These Betti numbers can be

computed with `Magma` [12]. In order to speed up these calculations, we compute the Betti numbers for the reduction of the curve modulo a prime of good reduction: in this case the Betti numbers are the same for both curves, see [35, Thm. 20.5].

When $\beta_{d-4,d-2} \neq 0$, we still need to check whether a smooth plane model exists. As in the proof of Lemma 4.1, when $g \geq 6$ the ideal I_C is generated by the degree 2 equations defining $\mathbb{P}^2 \hookrightarrow \mathbb{P}^{g-1}$ by the $(d-3)$-Veronese embedding plus the (this time) degree 2 equations $x^a y^b z^c F(x, y, z) = 0$ with $a + b + c = d - 6$. In order to recover the putative smooth model we aim to determine the degree 2 equations defining the $\mathbb{P}^2$. Then we compute a bijective parametrization and plug it into any other equation of I_C, not defining the $\mathbb{P}^2$, and, therefore, we should obtain the smooth plane model we are looking for. If not such a model is found, it means that it does not exists. This strategy to recover the $\mathbb{P}^2$ is the one in the proof of Theorem 4.1 in [41] that gives a proof of the reverse implication of Conjecture 5.1 in [26] for $d = 6$. The idea is to recover the exceptional surface, so the $\mathbb{P}^2$, by finding relations with a certain shape and the standard basis techniques presented in the Appendix of [41]. We present an implementation of this algorithm in [2].

4.3 The algorithm

Following the discussion in the previous subsections, we present an algorithm, Algorithm 1, which allows to determine whether a curve admits a smooth plane model.

4.4 Other strategies

Sometimes, in order to prove that a certain curve does not admit a smooth plane model, we can try some less computationally expensive techniques. For instance, when the curves under considerations have some involutions:

Theorem 4.3 (Remark 2.1 (i) & Theorem 2.2 with $n = 2$ in [28]) *Let C be a smooth plane curve of degree d and σ an involution of C. Then the involution σ has $f = d + \frac{1-(-1)^d}{2}$ fixed points and the quotient $C/\langle\sigma\rangle$ has gonality $\lfloor \frac{d}{2} \rfloor$.*

Other ways of using the knowledge of some quotients to prove the non-existence of smooth plane models are the following results:

Lemma 4.4 *Let C be a smooth curve admitting a degree n morphism to a hyperelliptic curve. Then C does not admit a smooth plane model of degree greater than $2n + 1$.*

Proof The gonality of a smooth plane curve of degree d is $d - 1$ and the gonality of a hyperelliptic curve is 2. □

Theorem 4.5 *(Theorem 3.1 with $r = 1$ in [25]). A smooth plane curve of degree d does not admit any rational map to $\mathbb{P}^1$ of degree n such that*

$$(a-1)d + 1 \leq n \leq ad - (a^2 + 1)$$

for some $a \in \mathbb{N}$.

5 Computations

We compute equations for all modular curves of Shimura type of genus 1, 3, 6, 10 and 15, i.e. possibly admitting a smooth plane model of degree 3, 4, 5, 6 or 7. We run the algorithm

Data: C/k a genus g curve given with its canonical model
Result: determining whether C admits a smooth plane model and, when possible, returning such model
$M \leftarrow 0$;
if *g is* 0 *or* 1 **then**
  $T \leftarrow$ *true*;
else
  if *g is* 3 **then**
    if $g(\phi_K(C)) = 3$ **then**
      $T \leftarrow$ *true*;
      $M \leftarrow \phi_K(C)$;
    else
      $T \leftarrow$ *false*;
    end
  else
    if *g is* 6 **then**
      if I_C *generated by quadrics* **then**
        $T \leftarrow$ *false*;
      else
        compute M with Lemma 4.1;
        if M *is a smooth plane quintic* **then**
          $T \leftarrow$ *true*;
        else
          $T \leftarrow$ *false*;
        end
      end
    else
      $T \leftarrow$ *false*;
      if $\exists d \in \mathbb{N}$ *with* $g = (d-1)(d-2)/2$ *and* $g(\phi_K(C)) \neq 0$ **then**
        Apply Theorem 4.2;
        if $\beta_{d-4,d-2} \neq 0$ **then**
          compute M with Schreyer's strategy [41];
          if M *is smooth* **then**
            $T \leftarrow$ *true*;
          end
        end
      end
    end
  end
end
return T, M

Algorithm 1: Existence of a smooth plane model

in previous section on all of them, in order to check which ones do admit a smooth plane model.

We also compute equations for modular curves of these genera which are not of Shimura type, when the congruence subgroup is $\Gamma = PG$, with $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfies $G = \pi_M^{-1}(G_M) \cap \pi_K^{-1}(G_K)$ with $B_1(M) \subseteq G_M \subseteq B_0(M)$ and $G_K \subseteq GL_2(\mathbb{Z}/K\mathbb{Z})$, and such that $MK^2 \leq 500$. Note that $(MK^2)^3$ is the dominant factor in the running time complexity, and indeed for larger values of MK^2, the linear algebra becomes the bottleneck.

Table 5 Hyperelliptic Shimura type modular curves of genus 3

Label	Name	Hyperelliptic model
12K3		$y^2 = x^8 + 14x^4 + 1$
20J3		$y^2 = x^8 + 8x^6 - 2x^4 + 8x^2 + 1$
21D3		$y^2 = x^8 - 6x^6 + 4x^5 + 11x^4 - 24x^3 + 22x^2 - 8x + 1$
24V3		$y^2 = x^8 + 14x^4 + 1$
30K3	$X_0(30)$	$y^2 = x^8 + 6x^7 + 9x^6 + 6x^5 - 4x^4 - 6x^3 + 9x^2 - 6x + 1$
33C3	$X_0(33)$	$y^2 = x^8 + 10x^6 - 8x^5 + 47x^4 - 40x^3 + 82x^2 - 44x + 33$
35A3	$X_0(35)$	$y^2 = x^8 - 12x^7 + 50x^6 - 108x^5 + 131x^4 - 76x^3 - 10x^2 + 44x - 19$
39A3	$X_0(39)$	$y^2 = x^8 - 6x^7 + 3x^6 + 12x^5 - 23x^4 + 12x^3 + 3x^2 - 6x + 1$
40F3	$X_0(40)$	$y^2 = x^8 + 8x^6 - 2x^4 + 8x^2 + 1$
41A3	$X_0(41)$	$y^2 = x^8 - 12x^7 + 48x^6 - 82x^5 + 60x^4 - 8x^3 - 27x^2 + 16x - 4$
48J3	$X_0(48)$	$y^2 = x^8 + 14x^4 + 1$

We discuss the results in the following subsections. We use the congruence subgroup labels introduced in [16]. All computations were done using `Magma` [12] and the full results are available online at [2].

5.1 Genus 1

In the case of modular curves of genus 1 they always admit a smooth plane model of degree 3. However, it is not given by the canonical model since they are not non-hyperelliptic. In this case we note that all groups of Shimura type give rise to elliptic curves, since the cusp at ∞ is rational. We may further compute models for some of the other congruence subgroups, using the methods in [40] to obtain the j-map and a model for the curve. For example, we see that for the congruence subgroups of level 6, the groups labeled 6A1, 6C1, 6D1 all yield elliptic curves, with equations $y^2 = x^3 - 27$, $y^2 = x^3 + 1$ and $y^2 = x^3 + 1$. We also find the q-expansion of the unique eigenform for all 98 congruence subgroups of genus 1 for which $MK^2 \leq 500$.

5.2 Genus 3

Among the 26 groups of Shimura type of genus 3, we find that there are 11 modular curves which are hyperelliptic, these are listed below. We note that 7 of these curves belong to the $X_0(N)$ family, and indeed we recover the models of Galbraith [23] for all these curves except for $X_0(35)$ and $X_0(41)$ that we find different ones. These, of course, give isomorphic curves to the Galbraith ones (Table 5).

Remark 5.1 The curves corresponding to the groups labeled 12K3, 24V3 and 48J3 are isomorphic. The curves corresponding to the groups labeled 20J3 and 40F3 are isomorphic. No other curves in Table 5 are isomorphic. This phenomenon is explained by the fact that the corresponding groups are conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

The other groups of Shimura type of genus 3 give rise to smooth plane quartics. In Table 6 we present the plane quartics obtained.

Remark 5.2 The curves corresponding to the groups labeled by 7A3 and 49A3 are isomorphic. The curves corresponding to the groups labeled by 8A3, 16H3, 32J3, 64B3 are isomorphic. The curves corresponding to the groups labeled by 12O3 and 36K3 are iso-

Table 6 Plane quartic Shimura type modular curves of genus 3

Label	Name	Plane quartic model
7A3	$X(7)$	$-xy^3 + x^3z + yz^3 = 0$
8A3		$x^3z + 4xz^3 - y^4 = 0$
12O3		$x^3z - 3x^2z^2 - xy^3 + 4xz^3 + 2y^3z - 2z^4 = 0$
15E3		$x^3z - x^2y^2 + xyz^2 - y^3z - 5z^4 = 0$
16H3		$-y^4 + x^3z + 4xz^3 = 0$
20S3	$X_1(20)$	$x^3z - x^2y^2 - 3x^2z^2 + xy^3 + 4xz^3 - 2z^4 = 0$
24X3		$x^3z - 2x^2yz - x^2z^2 - xy^3 + 2xy^2z$ $+6xyz^2 + 2y^3z - 2y^2z^2 - 4xz^3 = 0$
24Y3		$x^3z - x^2y^2 - x^2z^2 + xz^3 - xy^2z$ $-3xyz^2 + y^3z + 2y^2z^2 + yz^3 = 0$
32J3		$-y^4 + x^3z + 4xz^3 = 0$
34C3	$X_0(34)$	$-x^2y^2 + 2xy^3 - y^4 + x^3z + 3xy^2z + 4y^3z -$ $3x^2z^2 - 3xyz^2 - 6y^2z^2 + 4xz^3 + 4yz^3 - 2z^4 = 0$
36K3		$-xy^3 + x^3z + 2y^3z - 3x^2z^2 + 4xz^3 - 2z^4 = 0$
43A3	$X_0(43)$	$-2x^2y^2 + xy^3 - 9y^4 + x^3z + 2x^2yz + 3xy^2z + 24y^3z -$ $2x^2z^2 - 5xyz^2 - 28y^2z^2 + 3xz^3 + 16yz^3 - 4z^4 = 0$
45D3	$X_0(45)$	$-x^2y^2 + x^3z - y^3z + xyz^2 - 5z^4 = 0$
49A3		$-xy^3 + x^3z + yz^3 = 0$
64B3	$X_0(64)$	$-y^4 + x^3z + 4xz^3 = 0$

morphic. The curves corresponding to the groups labeled by 15E3 and 45D3 are isomorphic. No other curves in Table 6 are isomorphic. Again, the explanation for these isomorphisms is that the congruence subgroups are conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

We have also computed models for 92 out of the 105 congruence subgroups that are not of Shimura type and have $MK^2 \leq 500$. An example of a plane quartic occurs for the group labeled 9*A*3, cut out by the quartic $81x^4 - 54x^3y - 27x^2y^2 + 3xy^3 + y^4 - 729xz^3 + 486yz^3$.

5.3 Genus 6

Among the 8 groups of Shimura type occurring, none admits a smooth plane model. We have also computed models for 19 out of the 29 congruence subgroups that are not of Shimura type and have $MK^2 \leq 500$.

Except the curve corresponding to 18A6, all the other ones are of genus 6 and have a canonical model generated by quadrics, which means that they are non-hyperelliptic and that they do not admit a smooth plane model.

For the curve 18A6, we also need cubic equations to define its canonical model. According to Theorem 3.1, this implies that it does admit a smooth plane model or that it is a trigonal curve. We first found an explicit birational equivalence between $\mathbb{P}^2$ and the locus of the quadrics in the ideal generating the canonical model. This birational map gives a parametrization of the locus of the quadrics. We plugged it into the degree 3 equations, and, after a suitable scaling of the variables, we found the following equation:

$$y^3 = (x-3)(x+1)(x^2+3)(x+3)^2(x^2+6x+21)^2.$$

Interestingly, the curve (which is not a smooth plane quintic) is not only trigonal, but also superelliptic. Notice that this is a quite remarkable exception since the dimensions of the moduli space of curves of genus 6, and the locus of trigonal, plane and superelliptic

Table 7 Elliptic curves admitting a morphism from a Shimura type modular curve of genus 10

Label	Name	Image in $\mathbb{P}^2$
9A10	$X(9)$	$y^2 = x^3 + 16$
18E10		$y^2 = x^3 - 12x^2 + 48x$
27B10		$y^2 = x^3 + 16$
36Q10		$y^2 = x^3 - 12x^2 + 48x$
54A10		$y^2 = x^3 - 12x^2 + 48x$
81A10		$y^2 = x^3 + 16$
108F10	$X_0(108)$	$y^2 = x^3 - 12x^2 + 48x$

ones of degree 3 inside it are: $\dim(\mathcal{M}_6) = 15$, $\dim(\mathcal{M}_6^{trig}) = 13$, $\dim(\mathcal{M}_6^{plane}) = 12$ and $\dim(\mathcal{M}_6^{superell,3}) = 5$. Actually, we could have guessed the existence of an automorphism of order 3 of the curve, since $\mathrm{Aut}(G)$ contains an element σ of order 3, which induces an automorphism of the curve X_G. The induced action of the automorphism on the q-expansions is via $\sigma(f)(q) = f(\zeta_3 q)$. Therefore, we can readily compute its action on the curve, and observe that it corresponds to the action $x \mapsto x$ and $y \mapsto \zeta_3 y$ in the model we found.

5.4 Genus 10

We have checked all the 17 groups of Shimura type of genus 10. None of them admits a smooth plane model. This was verified by computing the graded Betti number $\beta_{2,4}$. In 15 out of the 17 cases we have $\beta_{2,4} = 0$. Therefore, by Theorem 4.2, these curves do not admit a g_6^2, or equivalently a smooth plane model. The remaining cases, of the groups 46A10 and 92A10, are both isomorphic to the curve $X_0(92)$. In this case, we obtain $\beta_{2,4} = 27$, which by [41, Corollary 4.2] implies either that the curve is a smooth plane curve or that it is a double cover of an elliptic curve. However, in this case one checks that the quotient of the curve by the Atkin–Lehner involution W_{23} yields an elliptic curve, hence by Lemma 4.4 it does not admit a smooth plane model.

In most cases, projecting to $\mathbb{P}^2$ using the three divisors of maximal valuation at the cusp at ∞, which is a flex, one obtains a singular curve of degree 10 or 11 with coefficients of large height. However, for the groups in Table 7 we obtain a smooth cubic (an elliptic curve).

5.5 Genus 15

We have not been able to check the existence of a smooth plane model for any of the 23 groups of Shimura type of genus 15 using Algorithm 1, as computing the corresponding Betti numbers $\beta_{3,5}$ turned out to be beyond our computational ability.

However, we can rule out the existence of smooth plane models for all these curves by looking at their Atkin–Lehner quotients. Indeed, any congruence subgroup $\Gamma(H, 1)$ of Shimura type of level N and parameter $t = 1$ satisfies $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, and a subset of the Atkin–Lehner operators on $\Gamma_0(N)$ normalize Γ as well. These induce automorphisms of the curve X_G (for $G = G(H, 1)$), and we denote the quotients by a subset W of them by X_G/W. Whenever $|W| = 4$ and X_G/W is hyperelliptic, we have a morphism $X_G \to \mathbb{P}^1$ of degree 8, and we can deduce from Theorem 4.5 that X_G does not admit a smooth plane model (which must be of degree $d = 7$).

Table 8 Atkin–Lehner quotients of modular curves of Shimura type of genus 15

Label	Name	W	$g(X_G/W)$
35C15, 175A15	$X_0(175)$	$\langle w_{25}, w_7\rangle$	3
40W15, 80R15		$\langle w_{16}, w_5\rangle$	1
40X15, 80T15		$\langle w_{16}, w_5\rangle$	1
43A15		$\langle w_{43}\rangle$	7
51A15, 153A15	$X_0(153)$	$\langle w_9, w_{17}\rangle$	2
60AC15		$\langle w_3, w_5\rangle$	1
60AD15		$\langle w_3, w_5\rangle$	1
67A15		$\langle w_{67}\rangle$	7
68D15, 136D15	$X_0(136)$	$\langle w_8, w_{17}\rangle$	3
85A15		$\langle w_5, w_{17}\rangle$	2
85B15		$\langle w_5, w_{17}\rangle$	2
102C15	$X_0(102)$	$\langle w_2, w_3, w_{17}\rangle$	1
110A15	$X_0(110)$	$\langle w_5, w_{11}\rangle$	1
141D15	$X_0(141)$	$\langle w_3, w_{47}\rangle$	1
155A15	$X_0(155)$	$\langle w_5, w_{31}\rangle$	1
161A15	$X_0(161)$	$\langle w_7, w_{23}\rangle$	2
179A15	$X_0(179)$	$\langle w_{179}\rangle$	3
193A15	$X_0(193)$	$\langle w_{193}\rangle$	7

Moreover, each of the congruence subgroups of Shimura type of genus 15 is isomorphic to a group of type $\Gamma(H, 1)$. Table 8 summarizes our findings, where for groups which are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ we have written down both labels.

Note that, with the exception of $X_0(102)$, $X_0(136)$, $X_0(175)$, $X_0(179)$, $X_0(193)$ and the two curves corresponding to labels 43A15 and 67A15, the genus of all Atkin–Lehner quotients is either 1 or 2, implying that they are hyperelliptic, and $|W| = 4$. By [29] we deduce that $X_0^*(136) = X_0(136)/W$ is also hyperelliptic and thus we are left with six curves for which we were not able to rule out the existence of a smooth plane model using Theorem 4.5, namely $X_0(102)$, $X_0(175)$, $X_0(179)$, $X_0(193)$ and the two curves corresponding to labels 43A15 and 67A15. Note that by [22] there is no quotient of either of $X_0(175)$, $X_0(179)$, $X_0(193)$ which is hyperelliptic.

In order to rule out the six remaining curves, we use Theorem 4.3 with a simple application of Riemann-Hurwitz as follows. If X_G admits a smooth plane model (of degree $d = 7$), and $w \in W$ is any Atkin–Lehner involution, by Theorem 4.3 w has 8 fixed points. Riemann-Hurwitz then implies that the genus of the quotient is $g(X_G/\langle w\rangle) = 6$. Therefore, if we find some $w \in W$ where the genus of the quotient is not 6, it does not admit a smooth plane model. Looking again at Table 8 we see that this rules out $X_0(179)$, $X_0(193)$ and the two curves corresponding to labels 43A15 and 67A15. Finally, for $X_0(102)$ we see that $g(X_0(102)/\langle w_2\rangle) = 7$, and for $X_0(175)$ we have $g(X_0(175)/\langle w_7\rangle) = 8$, showing that they also do not admit a smooth plane model.

The map to $\mathbb{P}^2$ obtained by using the cusp at ∞ as the flex point always yields a singular curve of degree 16, except the following cases. For the group 60AC15, we obtain the elliptic curve

$$y^2 = x^3 + 4x^2 - 16x.$$

Table 9 Atkin–Lehner quotients of modular curves of Shimura type of genus 21 indicating no smooth plane model

Label	Name	$W' \subseteq W$	$g(X_G/W')$
21C21, 147B21		$\langle w_3 \rangle$	10
24A21, 48CE21, 96BA21, 192P21	$X_0(192)$	$\langle w_{64} \rangle$	11
28M21, 56L21, 112E21		$\langle w_{112} \rangle$	10
30G21, 90O21		$\langle w_{10} \rangle$	11
33C21	$X_1(33)$	$\langle w_{33} \rangle$	10
34A21	$X_1(34)$	$\langle w_{34} \rangle$	10
35B21, 245A21	$X_0(245)$	$\langle w_{245} \rangle$	8
36F21, 72AC21		$\langle w_{72} \rangle$	10
39B21, 117A21		$\langle w_{13} \rangle$	11
42H21, 84Q21		$\langle w_3 \rangle$	10
45F21		$\langle w_{45} \rangle$	10
52C21, 104B21		$\langle w_{13} \rangle$	11
55B21		$\langle w_5 \rangle$	3
56M21		$\langle w_8 \rangle$	6
65A21		$\langle w_{13} \rangle$	6
69A21, 207A21	$X_0(207)$	$\langle w_{23} \rangle$	8
72AC21		$\langle w_{72} \rangle$	10
78C21		$\langle w_{26} \rangle$	8
92A21, 184A21	$X_0(184)$	$\langle w_{23} \rangle$	5
97A21		$\langle w_{97} \rangle$	10
111A21		$\langle w_{111} \rangle$	7
115A21		$\langle w_{23} \rangle$	6
119A21		$\langle w_7 \rangle$	6
133B21		$\langle w_{133} \rangle$	10
138A21	$X_0(138)$	$\langle w_{23} \rangle$	5
154B21	$X_0(154)$	$\langle w_{22} \rangle$	11
165B21	$X_0(165)$	$\langle w_3 \rangle$	11
178A21	$X_0(178)$	$\langle w_{89} \rangle$	8
201A21	$X_0(201)$	$\langle w_{67} \rangle$	11
215A21	$X_0(215)$	$\langle w_{43} \rangle$	11
247A21	$X_0(247)$	$\langle w_{247} \rangle$	8
251A21	$X_0(251)$	$\langle w_{251} \rangle$	4
257A21	$X_0(257)$	$\langle w_{257} \rangle$	7

For the groups 40W15 and 80R15 (which induce isomorphic curves) we obtain a septic with 3 singular points, namely

$$x^5y^2 - x^6z - 5x^4y^2z + x^2y^4z + 4x^5z^2 + 12x^3y^2z^2 - 4xy^4z^2 - 6x^4z^3 - 16x^2y^2z^3 + 4y^4z^3 + 4x^3z^4 + 12xy^2z^4 - x^2z^5 - 4y^2z^5 = 0.$$

5.6 Genus 21

We have not been able to check the existence of a smooth plane model for any of the 55 groups of Shimura type of genus 21 using Algorithm 1, as computing the corresponding Betti numbers $\beta_{4,6}$ turned out to be beyond our computational ability.

However, we can rule out the existence of smooth plane models for all but five of these curves by looking at their Atkin–Lehner quotients, and using Theorem 4.3 and Riemann-Hurwitz as before. In this case, if X_G admits a smooth plane model (of degree

$d = 8$), and $w \in W$ is any Atkin–Lehner involution, by Theorem 4.3 w has 8 fixed points. Riemann-Hurwitz then implies that the genus of the quotient is $g(X_G/\langle w\rangle) = 9$. Table 9 shows, for each of these curves, the chosen Atkin–Lehner involution and the genus of the corresponding quotient, where for groups which are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ we have written down all labels in a single line.

The curves left after this analysis are $X_0(256)$ and the curves corresponding to labels 41A21, 91A21, 91B21, 137A21. The modular curve $X_0(256)$ has a single Atkin–Lehner involution, and its quotient by that involution has genus 9. By Theorem 4.3, if this curve admitted a smooth plane model, the corresponding quotient would have gonality 4. However, by computing the Betti table of the quotient, we see that the $a(X_0(256)/\langle w\rangle)$ invariant of the table is 3. Then, Corollary 9.7 in [20] implies that $\mathrm{Cliff}(X_0(256)/\langle w\rangle) \geq 4$, so the gonality of $X_0(256)/\langle w\rangle$ is at least 6. On the other hand, it is also bounded by 6 because of the genus being 9. This proves that $X_0(256)$ does not admit a smooth plane model. For the other four curves, at the present time, no algorithm is implemented to compute their Atkin–Lehner quotients.

5.7 Proof of Theorem 1.1

We are ready to prove now our main theorem:

Proof The first claim is Theorem 2.1 and the second one is deduced from its proof. The last claim is a consequence of the computations in this section. □

Acknowledgements
We thank the organisers of the conference "Arithmetic Aspects of Explicit Moduli Problems" held in Banff in June 2017 where this project was first mentioned. We thank Peter Bruin, Bas Edixhoven and Noam Elkies for insightful discussions during the aforementioned conference. We also thank John Voight for putting us in contact with each other. Last but not least, we thank Wouter Castryck and all the referees that read our paper and helped us to improve its results and exposition; in particular, to the one detecting a crucial error in the first version of Sect. 4.
The research of the first and third author is partially funded by the Melodia ANR-20-CE40-0013 project. The second author was supported by a Simons Collaboration grant (550029, to John Voight).

Funding Open access funding provided by University of Neuchâtel.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Author details
[1] Aix-Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille case 907, 163 avenue de Luminy, 13288 Marseille Cedex 9, France, [2] Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA, [3] Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, 2000 Neuchâtel, Switzerland, [4] Univ Rennes, CNRS, IRMAR - UMR 6625, 35000 Rennes, France.

Received: 15 September 2022 Accepted: 10 October 2022 Published online: 18 March 2023

References

1. Assaf, E.: Computing classical modular forms for arbitrary congruence subgroups. In: Arithmetic Geometry, Number Theory and Computation, pp. 43–104 (2022)
2. Assaf, E.: Modular symbols package for arbitrary congruence subgroups. GitHub (2022). https://github.com/assaferan/ModFrmGL2. Accessed 3 Oct 2022
3. Baaziz, H.: Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. Math. Comp. **79**, 2371–2386 (2010)
4. Badr, E., Bars, F., García, E.L.: On twists of smooth plane curves. Math. Comp. **88**(315), 421–438 (2019)
5. Baker, M.H., González-Jiménez, E., González, J., Poonen, B.: Finiteness results for modular curves of genus at least 2. Am. J. Math. **127**(6), 1325–1387 (2005)
6. Banwait, B.S., Cremona, J.E.: Tetrahedral elliptic curves and the local-global principle for isogenies. Algebr. Number Theory **8**(5), 1201–1229 (2014)

7. Baran, B.: Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. J. Number Theory **130**(12), 2753–2772 (2010)
8. Bars, F., Kontogeorgis, A., Xarles, X.: Bielliptic and hyperelliptic modular curves $X(N)$ and the group Aut($X(N)$). Acta Arith. **161**(3), 283–299 (2013)
9. Bassino, F., Nicaud, C., Weil, P.: Statistics of subgroups of the modular group. Int. J. Algebr. Comput. **31**(8), 1691–1751 (2021)
10. Best, A.J., Bober, J., Booker, A.R., Costa, E., Cremona, J., Derickx, M., Lowry-Duda, D., Lee, M., Roe, D., Sutherland, A.V.: Computing classical modular forms (2020). arXiv:2002.04717
11. Borisov, L., Gunnells, P., Popescu, S.: Elliptic functions and equations of modular curves. Math. Ann. **321**(3), 553–568 (2001)
12. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I The user language. J. Symbol. Comput. **24**(3-4), 235–265 (1997). Computational algebra and number theory (London, 1993)
13. Box, J.: Computing models for quotients of modular curves. Res. Number Theory **7**(3), 34 (2021)
14. Coppens, M., Kato, T.: The gonality of smooth curves with plane models. Manuscr. Math. **70**(1), 5–25 (1990)
15. Cox, David A., Parry, Walter R.: Genera of congruence subgroups in Q-quaternion algebras. J. Reine Angew. Math. **351**, 66–112 (1984)
16. Cummins, C.J., Pauli, S.: Congruence subgroups of PSL(2, $\mathbb{Z}$) of genus less than or equal to 24. Exp. Math. **12**(2), 243–255 (2003)
17. Derickx, M., Najman, F., Siksek, S.: Elliptic curves over totally real cubic fields are modular. Algebra Number Theory **14**(7), 1791–1800 (2020)
18. Diamond, F., Shurman, J.: A First Course in Modular Forms. Graduate Texts in Mathematics, vol. 228. Springer, New York (2005)
19. Dose, V., Mercuri, P., Stirpe, C.: Double covers of cartan modular curves (2017). arXiv:1706.03988
20. Eisenbud, D.: A second course in commutative algebra and algebraic geometry. In: The Geometry of Syzygies. Graduate Texts in Mathematics, vol. 229. Springer, New York (2005)
21. Enge, A., Schertz, R., Modular Curves of Composite Level: Modular curves of composite level. Acta Arithmetica **118**, 129–141 (2005)
22. Furumoto, M., Hasegawa, Y.: Hyperelliptic quotients of modular curves $X_0(N)$. Tokyo J. Math. **22**(1), 105–125 (1999)
23. Galbraith, S.D.: Equations for modular curves. Ph.D. Thesis (1996)
24. González-Jiménez, E., Oyono, R.: Non-hyperelliptic modular curves of genus 3. J. Number Theory **130**(4), 862–878 (2010)
25. Greco, S., Raciti, G.: The Lüroth semigroup of plane algebraic curves. Pac. J. Math. **151**(1), 43–56 (1991)
26. Green, M.L.: Koszul cohomology and the geometry of projective varieties. J. Differ. Geom. **19**(1), 125–171 (1984)
27. Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer, New York (1977)
28. Harui, T., Kato, T., Komeda, J., Ohbuchi, A.: Quotient curves of smooth plane curves with automorphisms. Kodai Math. J. **33**(1), 164–172 (2010)
29. Hasegawa, Y.: Hyperelliptic modular curves $X_0^*(N)$. Acta Arith. **81**(4), 369–385 (1997)
30. Hasegawa, Y., Shimura, M.: Trigonal modular curves $X_0^{+d}(N)$. Proc. Jpn. Acad. Ser. A **75**(9), 172–175 (1999)
31. Kim, H.H.: Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. J. Am. Math. Soc. **16**(1), 139–183 (2003). With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak. MR1937203
32. Kodrnja, I.: On a simple model of $x_0(n)$. **186**(4), 653–666 (2018). arXiv:1704.01098
33. Kohel, D.: Computing modular curves via quaternions (1997)
34. Martin, G.: Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$. J. Number Theory **112**(2), 298–331 (2005)
35. Milne, J.S.: Lectures on etale cohomology (v2.21) (2013). www.jmilne.org/math/
36. Muic, G.: On embeddings of curves in projective spaces. Monatshefte Math. **173**(2), 239–256 (2014)
37. Noether, M.: Ueber die invariante Darstellung algebraischer Functionen. Math. Ann. **17**(2), 263–284 (1880)
38. Poonen, B.: Gonality of modular curves in characteristic p. Math. Res. Lett. **14**(4), 691–701 (2007)
39. Rasmussen, J.B.: Higher congruences between modular forms. Ph.D. Thesis (2009)
40. Rouse, J., Zureick-Brown, D.: Elliptic curves over Q and 2-adic images of Galois. Res. Number Theory **1**, 34 (2015)
41. Schreyer, F.-O.: A standard basis approach to syzygies of canonical curves. J. Reine Angew. Math. **421**, 83–123 (1991)
42. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
43. Shimura, G.: Introduction to the arithmetic theory of automorphic functions, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, (1994). Reprint of the 1971 original, Kanô Memorial Lectures, 1
44. Stein, W.: Modular Forms, a Computational Approach. Graduate Studies in Mathematics, vol. 79. American Mathematical Society, Providence (2007). With an appendix by Paul E. Gunnells
45. Sturm, J.: On the congruence of modular forms. Number Theory (New York, 1984–1985) 275–280 (1987)
46. Zograf, P.G.: Small eigenvalues of automorphic Laplacians in spaces of cusp forms. Zapiski Nauchnykh Seminarov POMI **134**, 157–168 (1984). Automorphic functions and number theory, II
47. Zograf, P.G.: A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group. J. Reine Angew. Math. **414**, 113–116 (1991)
48. Zywina, D.: Computing actions on cusp forms (2021). arXiv:2001.07270

Publisher's Note