Shimura Curve Computations

Noam D. Elkies

Harvard University

Abstract. We give some methods for computing equations for certain Shimura curves, natural maps between them, and special points on them. We then illustrate these methods by working out several examples in varying degrees of detail. For instance, we compute coordinates for all the rational CM points on the curves $\mathcal{X}^*(1)$ associated with the quaternion algebras over $\mathbf{Q}$ ramified at $\{2,3\}$, $\{2,5\}$, $\{2,7\}$, and $\{3,5\}$. We conclude with a list of open questions that may point the way to further computational investigation of these curves.

1 Introduction

1.1 Why and how to compute with Shimura curves

The classical modular curves, associated to congruence subgroups of $\mathrm{PSL}_2(\mathbf{Q})$, have long held and repaid the interest of number theorists working theoretically as well as computationally. In the fundamental paper [S2] Shimura defined curves associated with other quaternion algebras other over totally real number fields in the same way that the classical curves are associated with the algebra $M_2(\mathbf{Q})$ of 2×2 matrices over $\mathbf{Q}$. These Shimura curves are now recognized as close analogues of the classical modular curves: almost every result involving the classical curves generalizes with some more work to Shimura curves, and indeed Shimura curves figure alongside classical ones in a key step in the recent proof of Fermat's "last theorem" [Ri].

But computational work on Shimura curves lags far behind the extensive effort devoted to the classical modular curves. The 19th century pioneers investigated some arithmetic quotients of the upper half plane which we now recognize as Shimura curves (see for instance [F1, F2]) with the same enthusiasm that they applied to the $\mathrm{PSL}_2(\mathbf{Q})$ curves. But further inroads proved much harder for Shimura curves than for their classical counterparts. The $\mathrm{PSL}_2(\mathbf{Q})$ curves parametrize elliptic curves with some extra structure; the general elliptic curve has a simple explicit formula which lets one directly write down the first few modular curves and maps between them. (For instance, this is how Tate obtained the equations for the first few curves $\mathrm{X}_1(N)$ parametrizing elliptic curves with an N-torsion point; see for instance [Kn, pp.145–148].) Shimura showed that curves associated with other quaternion algebras also parametrize geometric objects, but considerably more complicated ones (abelian varieties with quaternionic endomorphisms); even in the first few cases beyond $M_2(\mathbf{Q})$, explicit formulas for these objects were obtained only recently [HM], and using such formulas to get at the Shimura curves seems a most daunting task. Moreover, most modern computations with modular curves (e.g. [C, E5]) sidestep the elliptic interpretation and instead rely heavily on q-expansions, i.e. on the curves' cusps. But arithmetic subgroups of $\mathrm{PSL}_2(\mathbf{R})$ other than those in $\mathrm{PSL}_2(\mathbf{Q})$ contain no parabolic elements, so their Shimura curves have no cusps, and thus any method that requires q-expansions must fail.

But while Shimura curves pose harder computational problems than classical modular curves, efficient solutions to these problems promise great benefits. These curves tempt the computational number theorist not just because, like challenging mountainpeaks, "they're there", but because of their remarkable properties, direct applications, and potential for suggesting new ideas for theoretical research. Some Shimura curves and natural maps between them provide some of the most interesting examples in the geometry of curves of low genus; for instance each of the five curves of genus $g \in [2, 14]$ that attains the Hurwitz bound $84(g-1)$ on the number of automorphisms of a curve in characteristic zero is a Shimura curve. Shimura curves, like classical and Drinfeld modular curves, reduce to curves over the finite field $\mathbf{F}_{q^2}$ of q^2 elements that attain the Drinfeld-Vlăduţ upper bound $(q-1+o(1))g$ on the number of points of a curve of genus $g \to \infty$ over that field [I3]. Moreover, while all three flavors of modular curves include towers that can be given by explicit formulas and thus used to construct good error-correcting codes [Go1, Go2, TVZ], only the Shimura curves, precisely because of their lack of cusps, can give rise to totally unramified towers, which should simplify the computation of the codes; we gave formulas for several such towers in [E6]. Finally, the theory of modular curves indicates that CM (complex multiplication) points on Shimura curves, elliptic curves covered by them, and modular forms on them have number-theoretic significance. The ability to efficiently compute such objects should suggest new theoretical results and conjectures concerning the arithmetic of Shimura curves. For instance, the computations of CM points reported in this paper should suggest factorization formulas for the difference between the coordinates of two such points analogous to those of Gross and Zagier [GZ] for j-invariants of elliptic curves, much as the computation of CM values of the Weber modular functions suggested the formulas of [YZ]. Also, as in [GS], rational CM points on rational Shimura curves with only three elliptic points (i.e. coming from arithmetic triangle groups $G_{p,q,r}$) yield identities $A + B = C$ in coprime integers A, B, C with many repeated factors; we list the factorizations here, though we found no example in which A, B, C are perfect p, q, r-th powers, nor any new near-record ABC ratios. Finally, CM computations on Shimura curves may also make possible new Heegner-point constructions as in [E4].

So how do we carry out these computations? In a few cases (listed in [JL]), the extensive arithmetic theory of Shimura curves has been used to obtain explicit equations, deducing from the curves' p-adic uniformizations Diophantine conditions on the coefficients of their equations stringent enough to determine them uniquely. But we are interested, not only in the equations, but in modular covers and maps between Shimura curves associated to the same quaternion algebra, and in CM points on those curves. The arithmetic methods may be able to provide this information, but so far no such computation seems to have been done. Our approach relies mostly on the uniformization of these curves *qua* Riemann surfaces by the hyperbolic plane, and uses almost no arithmetic. This approach is not fully satisfactory either; for instance it probably cannot be used in practice to exhibit all natural maps between Shimura curves of low genus. But it will provide equations for at least a hundred or so curves and maps not previously accessible, which include some of the most striking examples and should provide more than enough data to suggest further theoretical and computational work.

When a Shimura curve C comes from an arithmetic subgroup of $\mathrm{PSL}_2(\mathbf{R})$ contained in a triangle group $G_{p,q,r}$, the curve $\mathcal{H}/G_{p,q,r}$ has genus 0, and C is a cover of that curve branched only above three points, so may be determined from the ramification data. (We noted in [E5, p.48] that this method was available also for classical modular curves comings from subgroups of $\mathrm{PSL}_2(\mathbf{Z}) \cong G_{2,3,\infty}$, though there better methods are available thanks to the cusp. Subgroups of $\mathrm{PSL}_2(\mathbf{R})$ commensurate with[1] but not contained in $G_{p,q,r}$ may be handled similarly via the common subgroup of finite index.) The identification of $\mathcal{H}/G_{p,q,r}$ with $\mathbf{P}^1$ is then given by a quotient of hypergeometric functions on $\mathbf{P}^1$, which for instance lets us compute the $\mathbf{P}^1$ coordinate of any CM point on C as a complex number to high precision and thus recognize it at least putatively as an algebraic number.

Now it is known [T] that only nineteen commensurability classes of arithmetic subgroups of $\mathrm{PSL}_2(\mathbf{R})$ contain a triangle group. These include some of the most interesting examples — for instance, congruence subgroups of arithmetic triangle groups account for several of the sporadic "arithmetically exceptional functions" (rational functions $f(X) \in \mathbf{Q}(X)$ which permute $\mathbf{P}^1(\mathbf{F}_p)$ for infinitely many primes p) of [Mü]; but an approach that could only deal with those nineteen classes would be limited indeed. When there are more than three elliptic points, a new difficulty arises: even if $C = \mathcal{H}/\mathcal{G}$ still has genus 0, we must first determine the relative locations of the elliptic points, and to locate other CM points we must replace the hypergeometric functions to solutions of more general "Schwarzian differential equations" in the sense of [I1]. We do both by in effect using nontrivial elements of the "commensurator" of the group $G \in \mathrm{PSL}_2(\mathbf{R})$, i.e. transformations in $\mathrm{PSL}_2(\mathbf{R})$ which do not normalize G but conjugate G to a group commensurable with G. Ihara had already used these commensurators in [I1] theoretically to prove that both C and its Schwarzian equation are defined over a number field, but this method has apparently not been actually used to compute such equations until now.

1.2 Overview of the paper

We begin with a review of the necessary definitions and facts on quaternion algebras and Shimura curves, drawn mostly from [S2] and [V]. We then give

[1] Recall that two subgroups H, K of a group G are said to be *commensurate* if $H \cap K$ is a subgroup of finite index in both H and K.

extended computational accounts of Shimura curves and their supersingular and rational CM points for the two simplest indefinite quaternion algebras over $\mathbf{Q}$ beyond the classical case of the matrix algebra $M_2(\mathbf{Q})$, namely the quaternion algebras ramified at $\{2,3\}$ and $\{2,5\}$. In the final section we more briefly treat some other examples which illustrate features of our methods that do not arise in the $\{2,3\}$ and $\{2,5\}$ cases, and conclude with some open questions suggested by our computations that may point the way to further computational investigation on these curves.

1.3 Acknowledgements

Many thanks to B.H. Gross for introducing me to Shimura curves and for many enlightening conversations and clarifications on this fascinating topic. Thanks also to Serre for a beautiful course that introduced me to three-point covers of $\mathbf{P}^1$ among other things ([Se], see also [Mat]); to Ihara for alerting me to his work [I1, I2] on supersingular points on Shimura curves and their relation with the curves' uniformization by the upper half-plane; and to C. McMullen for discussions of the uniformization of quotients of $\mathcal{H}$ by general co-compact discrete subgroups of $\mathrm{PSL}_2(\mathbf{R})$. A. Adler provided several references to the 19th-century literature, and C. Doran informed me of [HM]. Finally, I thank B. Poonen for reading and commenting on a draft of this paper, leading to considerable improvements of exposition in several places.

The numerical and symbolic computations reported here were carried out using the GP/PARI and MACSYMA packages, except for (70), for which I thank Peter Müller as noted there.

This work was made possible in part by funding from the David and Lucile Packard Foundation.

2 Review of quaternion algebras over Q and their Shimura curves

2.1 Quaternion algebras over Q; the arithmetic groups $\Gamma(1)$ and $\Gamma^*(1)$

Let K be a field of characteristic zero; for our purposes K will always be a number field or, rarely, its localization, and usually the number field will be $\mathbf{Q}$. A *quaternion algebra over* K is a simple associative algebra A with unit, containing K, such that K is the center of A and $\dim_K \mathsf{A} = 4$. Such an algebra has a *conjugation* $a \leftrightarrow \bar{a}$, which is a K-linear anti-involution (i.e. $\bar{\bar{a}} = a$ and $\overline{a_1 a_2} = \bar{a}_2 \bar{a}_1$ hold identically in A) such that $a = \bar{a} \Leftrightarrow a \in K$. The *trace* and *norm* are the additive and multiplicative maps from A to K defined by

$$\mathrm{tr}(a) = a + \bar{a}, \qquad \mathrm{N}(a) = a\bar{a} = \bar{a}a; \tag{1}$$

every $a \in \mathsf{A}$ satisfies its characteristic equation

$$a^2 - (\mathrm{tr}(a))a + \mathrm{N}(a) = 0. \tag{2}$$

The most familiar example of a quaternion algebra is $M_2(K)$, the algebra of 2×2 matrices over K, and if K is algebraically closed then $M_2(K)$ is the only quaternion algebra over K up to isomorphism. The other well-known example is the algebra of Hamilton quaternions over $\mathbf{R}$. In $M_2(K)$ the trace is the usual trace of a square matrix, so the conjugate of $a \in M_2(K)$ is $\mathrm{tr}(a)I_{2\times 2} - a$, and the norm is just the determinant. Any quaternion algebra with zero divisors is isomorphic with $M_2(K)$. An equivalent criterion is that the algebra contain a nonzero element whose norm and trace both vanish. Now the trace-zero elements constitute a K-subspace of A of dimension 3, on which the norm is a homogeneous quadric; so the criterion states that $\mathsf{A} \cong M_2(K)$ if and only if that quadric has nonzero K-rational points. The Hamilton quaternions have basis $1, i, j, k$ satisfying the familiar relations

$$i^2 = j^2 = k^2 = 1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j; \qquad (3)$$

the conjugates of $1, i, j, k$ are $1, -i, -j, -k$, so a Hamilton quaternion $\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k$ has trace $2\alpha_1$ and norm $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$. Thus the Hamilton quaternions over K are isomorphic with $M_2(K)$ if and only if -1 is a sum of two squares in K.

In fact it is known that if $K = \mathbf{R}$ then every quaternion algebra over K is isomorphic with either $M_2(\mathbf{R})$ or the Hamilton quaternions. In general if K is any local field of characteristic zero then there is up to isomorphism exactly one quaternion algebra over K other than $M_2(K)$ — with the exception of the field of complex numbers, which being algebraically closed admits no quaternion algebras other than $M_2(\mathbf{C})$. If A is a quaternion algebra over a number field K then a finite or infinite place v of K is said to be *ramified* in A if $\mathsf{A} \otimes K_v$ is not isomorphic with $M_2(K_v)$. There can only be a finite number of ramified places, because a nondegenerate quadric over K has nontrivial local zeros at all but finitely many places of K. A less trivial result (the case $K = \mathbf{Q}$ is equivalent to Quadratic Reciprocity) is that the number of ramified places is always even, and to each finite set of places Σ of even cardinality containing no complex places there corresponds a unique (again up to isomorphism) quaternion algebra over K ramified at those places and no others. In particular an everywhere unramified quaternion algebra over K must be isomorphic with $M_2(K)$.

An *order* in a quaternion algebra over a number field (or a non-Archimedean local field) K is a subring containing the ring O_K of K-integers and having rank 4 over O_K. For instance $M_2(O_K)$ and $O_K[i,j]$ are orders in the matrix and quaternion algebras over K. Any order is contained in at least one *maximal* order, that is, in an order not properly contained in any other. Examples of maximal orders are $M_2(O_K) \in M_2(K)$ and the Hurwitz order $\mathbf{Z}[1, i, j, (1+i+j+k)/2]$ in the Hamilton quaternions over $\mathbf{Q}$. It is known that if K has at least one Archimedean place at which A is *not* isomorphic with the Hamilton quaternions then all maximal orders are conjugate in A.

Now let[2] $K = \mathbf{Q}$. A quaternion algebra $\mathsf{A}/\mathbf{Q}$ is called *definite* or *indefinite* according as $\mathsf{A} \otimes \mathbf{R}$ is isomorphic with the Hamilton quaternions or $M_2(\mathbf{R})$,

[2] Most of our examples, including the two that will occupy us in the next two sections,

i.e. according as the infinite place is ramified or unramified in A. [These names allude to the norm form on the trace-zero subspace of A, which is definite in the former case, indefinite in the latter.] We shall be concerned only with the indefinite case. Then Σ consists of an even number of finite primes. Fix such a Σ and the corresponding quaternion algebra A. Let $\mathcal{O}$ be a maximal order in A; since A is indefinite, all its maximal orders are conjugate, so choosing a different maximal order would not materially affect the constructions in the sequel.

Let $\mathcal{O}_1^*$ be the group of units of norm 1 in $\mathcal{O}$. We then define the following arithmetic subgroups of $\mathsf{A}^*/\mathbf{Q}^*$:

$$\Gamma(1) := \mathcal{O}_1^*/\{\pm 1\}, \tag{4}$$
$$\Gamma^*(1) := \{[a] \in \mathsf{A}^*/\mathbf{Q}^* : a\mathcal{O} = \mathcal{O}a,\ \mathrm{N}(a) > 0\}. \tag{5}$$

[In other words $\Gamma^*(1)$ is the normalizer of $\Gamma(1)$ in the positive-norm subgroup of $\mathsf{A}^*/\mathbf{Q}^*$. Takeuchi [T] calls these groups $\Gamma^{(1)}(\mathsf{A}, \mathcal{O}_1)$ and $\Gamma^{(*)}(\mathsf{A}, \mathcal{O}_1)$; we use $\Gamma(1)$ to emphasize the analogy with the classical case of $\mathrm{PSL}_2(\mathbf{Z})$, which makes $\Gamma^*(1)$ a natural adaptation of Takeuchi's notation. Vignéras [V, p. 121ff.] calls the same groups Γ and G, citing [Mi] for the structure of their quotient.] As noted, $\Gamma(1)$ is a normal subgroup of $\Gamma^*(1)$. In fact $\Gamma^*(1)$ consists of the classes mod $\mathbf{Q}^*$ of elements of $\mathcal{O}$ whose norm is $\prod_{p\in\Sigma'} p$ for some (possibly empty) subset $\Sigma' \subseteq \Sigma$, and $\Gamma^*(1)/\Gamma(1)$ is an elementary abelian 2-group with $\#\Sigma$ generators.

2.2 The Shimura modular curves $\mathcal{X}(1)$ and $\mathcal{X}^*(1)$

The group $\Gamma(1)$, and thus any other group commensurable with it such as $\Gamma^*(1)$, is a discrete subgroup of $(A \otimes \mathbf{R})_+^*/\mathbf{R}^*$ (the subscript "+" indicating positive norm), with compact quotient unless $\Sigma = \emptyset$, and of finite covolume even in that case. Since $A \otimes \mathbf{R} \cong M_2(\mathbf{R})$, the group $(A \otimes \mathbf{R})_+^*/\mathbf{R}^*$ is isomorphic with $\mathrm{PSL}_2(\mathbf{R})$ and thus with $\mathrm{Aut}(\mathcal{H})$, the group of automorphisms of the hyperbolic upper half plane

$$\mathcal{H} := \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}. \tag{6}$$

Explicitly, a unimodular matrix $\pm\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on $\mathcal{H}$ via the fractional linear transformation $z \mapsto (az + b)/(cz + d)$. We may define the Shimura curves $\mathcal{X}(1)$ and $\mathcal{X}^*(1)$ *qua* compact Riemann surfaces by

$$\mathcal{X}(1) := \mathcal{H}/\Gamma(1), \qquad \mathcal{X}^*(1) := \mathcal{H}/\Gamma^*(1). \tag{7}$$

[More precisely, the Riemann surfaces are given by (7) unless $\Sigma = \emptyset$, in which case the quotient only becomes compact upon adjoining a cusp.] The hyperbolic area of these quotients of $\mathcal{H}$ is given by the special case $k = \mathbf{Q}$ of a formula of Shimizu [S1, Appendix], quoted in [T, p.207]. Using the normalization

involve quaternion algebras over $\mathbf{Q}$. In [S2] Shimura associated modular curves to a quaternion algebra over any totally real number field K for which the algebra is ramified at all but one of the infinite places of K. Since the special case $K = \mathbf{Q}$ accounts for most of our computations, and is somewhat easier to describe, we limit our discussion to quaternion algebras over $\mathbf{Q}$ from here until section 5.3. At that point we briefly describe the situation for arbitrary K before working out a couple of examples with $[K : \mathbf{Q}] > 1$.

$\pi^{-1} \iint dx\, dy/y^2$ for the hyperbolic area (with $z = x+iy$; this normalization gives an ideal triangle unit area), that formula is

$$\operatorname{Area}(\mathcal{X}(1)) = \frac{1}{6} \prod_{p \in \Sigma} (p-1), \tag{8}$$

from which

$$\operatorname{Area}(\mathcal{X}^*(1)) = \frac{1}{[\Gamma^*(1) : \Gamma(1)]} \operatorname{Area}(\mathcal{X}(1)) = \frac{1}{6} \prod_{p \in \Sigma} \frac{p-1}{2}. \tag{9}$$

It is known (see for instance Ch.IV:2,3 of [V] for the following facts) that, for any discrete subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbf{R})$ of finite covolume, the genus of $\mathcal{H}/\Gamma$ is determined by its area together with with information on elements of finite order in Γ. All finite subgroups of Γ are cyclic, and there are finitely many such subgroups up to conjugation in Γ. There are finitely many points P_j of $\mathcal{H}/\Gamma$ with nontrivial stabilizer, and the stabilizers are the maximal nontrivial finite subgroups of Γ modulo conjugation in Γ. If the order of the stabilizer of P_j is e_j then P_j is said to be an "elliptic point of order e_j". Then if $\mathcal{H}/\Gamma$ is compact then its genus $g = g(\mathcal{H}/\Gamma)$ is given by

$$2g - 2 = \operatorname{Area}(\mathcal{H}/\Gamma) - \sum_j (1 - \frac{1}{e_j}). \tag{10}$$

Moreover Γ has a presentation

$$\Gamma = \langle \alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g, s_j | s_j^{e_j} = 1,\ \prod_j s_j \prod_{i=1}^{g} [\alpha_i, \beta_i] = 1 \rangle, \tag{11}$$

in which s_j generates the stabilizer of a preimage of P_j in $\mathcal{H}$ and rotates a neighborhood of that preimage by an angle $2\pi/e_j$ (i.e. has derivative $e^{2\pi i/e_j}$ at its fixed point), and $[\alpha, \beta]$ is the commutator $\alpha\beta\alpha^{-1}\beta^{-1}$. [This group is sometimes called $(g; e_1, \ldots, e_g)$.] If $\mathcal{H}/\Gamma$ is not compact then we must subtract the number of cusps from the right-hand side of (10) and include a generator s_j of Γ of infinite order for each cusp, namely a generator of the infinite cyclic stabilizer of the cusp. This generator is a "parabolic element" of $\mathrm{PSL}_2(\mathbf{R})$, i.e. a fractional linear transformation with a single fixed point; there are two conjugacy classes of such elements in $\mathrm{PSL}_2(\mathbf{R})$, and s_j will be in the class of $z \mapsto z+1$. We assign $e_j = \infty$ to a cusp. For both finite and infinite e_j, the trace and determinant of s_j are related by

$$\operatorname{Tr}^2(s_j) = 4\cos^2 \frac{\pi}{e_j} \det(s_j). \tag{12}$$

Since we are working in quaternion algebras over $\mathbf{Q}$, this means that $e_j \in \{2, 3, 4, 6, \infty\}$, and only $2, 3, \infty$ are possible if $\Gamma \subseteq \Gamma(1)$. Moreover $e_j = \infty$ occurs only in the classical case $\Sigma = \emptyset$.

We shall need to numerically compute for several such Γ the identification of $\mathcal{H}/\Gamma$ with an algebraic curve $X/\mathbf{C}$, i.e. to compute the coordinates on X of a point corresponding to (the Γ-orbit of) a given $z \in \mathcal{H}$, or inversely to obtain z corresponding to a point with given coordinates. In fact the two directions are essentially equivalent, because if we can efficiently compute an isomorphism between two Riemann surfaces then we can compute its inverse almost as easily. For classical modular curves one usually uses q-expansions to go from z to rational coordinates; but this method is not available for our groups Γ, which have no parabolic ($e_j = \infty$) generator. We can, however, still go in the opposite direction, computing the map from X to $\mathcal{H}/\Gamma$ by solving differential equations on X. The key is that while the function z on X is not well defined due to the Γ ambiguity, its Schwarzian derivative is. In local coordinates the *Schwarzian derivative* of a nonconstant function $z = z(\zeta)$ is the meromorphic function defined by

$$S_\zeta(z) := -4z'^{1/2}\frac{d^2}{d\zeta^2}\frac{1}{z'^{1/2}} = \frac{2z'z''' - 3z''^2}{z'^2}. \tag{13}$$

This vanishes if and only if z is a fractional linear transformation of ζ. Moreover it satisfies a nice "chain rule": if ζ is in turn a function of η then

$$S_\eta(z) = \left(\frac{d\zeta}{d\eta}\right)^2 S_\zeta(z) + S_\eta(\zeta). \tag{14}$$

Thus if we choose a coordinate ζ on X then $S_\zeta(z)$ is the same for each lift of z from $\mathcal{H}/\Gamma$ to $\mathcal{H}$, and thus gives a well-defined function on the complement in X of the elliptic points; changing the coordinate from ζ to η multiples this function by $(d\zeta/d\eta)^2$ and adds a term $S_\eta(\zeta)$ that vanishes if ζ is a fractional linear transformation of η. In particular if X has genus 0 and we choose only rational coordinates (i.e. η, ζ are rational functions of degree 1) then these terms $S_\eta(\zeta)$ always vanish and $S_\zeta(z)\,d\zeta^2$ is a well-defined quadratic differential σ on X. Near an elliptic point ζ_0 of index e_j, the function z has a branch point such that $(z - z_0)/(z - \bar{z}_0)$ is $(\zeta - \zeta_0)^{1/e_j}$ times an analytic function; for such z the Schwarzian derivative is still well-defined in a neighborhood of ζ_0 but has a double pole there with leading term $(1 - e_j^{-2})/(\zeta - \zeta_0)^2$ [or $(1 - e_j^{-2})/\zeta^2$ if $\zeta_0 = \infty$ — note that this too has a double pole when multiplied by $d\zeta^2$]. So $\sigma = S_\zeta(z)\,d\zeta^2$ is a rational quadratic differential on X, regular except for double poles of known residue at the elliptic points, and independent of the choice of rational coordinate when X has genus 0. Knowing σ we may recover z from the differential equation

$$S_\zeta(z) = \sigma/d\zeta^2, \tag{15}$$

which determines z up to a fractional linear transformation over $\mathbf{C}$, and can then remove the ambiguity if we know at least three values of z (e.g. at elliptic points, which are fixed points of known elements of Γ).

Because $S_\zeta(z)$ is invariant under fractional linear transformations of z, the third-order nonlinear differential equation (15) can be linearized as follows (see e.g. [I1, §1–5]). Let (f_1, f_2) be a basis for the solutions of the linear second-order equation

$$f'' = af' + bf \tag{16}$$

for some functions $a(\zeta), b(\zeta)$. Then $z := f_1/f_2$ is determined up to fractional linear transformation, whence $S_\zeta(z)$ depends only on a, b and not the choice of basis. In fact we find, using either of the equivalent definitions in (13), that

$$S_\zeta(f_1/f_2) = 2\frac{da}{d\zeta} - a^2 - 4b. \tag{17}$$

Thus if a is any rational function and $b = -\sigma/4d\zeta^2 + a'/2 - a^2/4$ then the solutions of (15), and thus a map from X to $\mathcal{H}/\Gamma$, are ratios of linearly independent pairs of solutions of (16). In the terminology of [I1], (16) is then a *Schwarzian equation* for $\mathcal{H}/\Gamma$. We shall always choose a so that $a\,d\zeta$ has at most simple poles at the elliptic points and no other poles; the Schwarzian equation then has regular singularities at the elliptic points and no other singularities. The most familiar example is the case that Γ is a triangle group, i.e. X has genus 0 and three elliptic points (if $g = 0$ there must be at least three elliptic points by (10)). In that case σ is completely determined by its poles and residues: if two different σ's were possible, their difference would be a nonzero quadratic differential on $\mathbf{P}^1$ with at most three simple poles, which is impossible. If we choose the coordinate on X that puts the elliptic points at $0, 1, \infty$, and require that a be chosen of the form $a = C_0/\zeta + C_1/(\zeta - 1)$ so that b has only simple poles at $0, 1$, then there are four choices for (C_0, C_1), each giving rise to a *hypergeometric equation* upon multiplying (16) by $\zeta(1-\zeta)$:

$$\zeta(1-\zeta)f'' = [(\alpha+\beta+1)\zeta - \gamma]f' + \alpha\beta f. \tag{18}$$

Here α, β, γ are related to the indices e_1, e_2, e_3 at $\zeta = 0, 1, \infty$ by

$$\frac{1}{e_1} = \pm(1-\gamma), \quad \frac{1}{e_2} = \pm(\gamma - \alpha - \beta), \quad \frac{1}{e_3} = \pm(\alpha - \beta); \tag{19}$$

then $F(\alpha, \beta; \gamma; \zeta)$ and $(1-\zeta)^\gamma F(\alpha - \gamma + 1, \beta - \gamma + 1; 2 - \gamma; \zeta)$ constitute a basis for the solutions of (16), where $F = {}_2F_1$ is the hypergeometric function defined for $|\zeta| < 1$ by

$$F(\alpha, \beta; \gamma; \zeta) := \sum_{n=0}^{\infty} \left[\prod_{k=0}^{n-1} \frac{(\alpha+k)(\beta+k)}{(\gamma+k)} \right] \frac{\zeta^n}{n!}, \tag{20}$$

and by similar power series in neighborhoods of $\zeta = 1$ and $\zeta = \infty$ (see for instance [GR, 9.10 and 9.15]). In general, knowing σ we may construct and solve a Schwarzian equation in power series, albeit series less familiar than ${}_2F_1$, and numerically compute the map $X \to \mathcal{H}/\Gamma$ as the quotient of two solutions. But once Γ is not a triangle group — that is, when X has more than three elliptic points or positive genus — the elliptic points and their orders no longer determine σ but only restrict it to an affine space of finite but positive dimension. In general it is a refractory problem to find the "accessory parameters" that tell where σ lies in that space. If Γ is commensurable with a triangle group Γ' then we obtain σ from the quadratic differential on $\mathcal{H}/\Gamma'$ via the correspondence between that curve and $\mathcal{H}/\Gamma$; but this only applies to Shimura curves associated with the nineteen quaternion algebras listed by Takeuchi in [T], including only two over $\mathbf{Q}$, the matrix algebra and the algebra ramified at $\{2,3\}$. One of the advances in the present paper is the computation of σ for some arithmetic groups not commensurable with any triangle group.

We now return to the Shimura curves $\mathcal{X}(1)$, $\mathcal{X}^*(1)$ obtained from arithmetic groups $\Gamma = \Gamma(1), \Gamma^*(1)$. These curves also have a modular interpretation that gives them the structure of algebraic curves over $\mathbf{Q}$. To begin with, $\mathcal{X}(1)$ is the modular curve for principally polarized abelian surfaces (ppas) A with an embedding $O \hookrightarrow \mathrm{End}(A)$. (In the classical case $\mathcal{O} = M_2(\mathbf{Z})$, corresponding to $\Sigma = \emptyset$, such an abelian surface is simply the square of an elliptic curve and we recover the familiar picture of modular curves parametrizing elliptic ones, but for nonempty Σ the surfaces A are simple except for those associated to CM points on $\mathcal{X}(1)$; we shall say more about CM points later.) The periods of these surfaces satisfy a linear second-order differential equation which is a Schwarzian equation for $\mathcal{H}/\Gamma(1)$, usually called a "Picard-Fuchs equation" in this context. [This generalizes the expression for the periods of elliptic curves (a.k.a. "complete elliptic integrals") as ${}_2F_1$ values, for which see e.g. [GR, 8.113 1.].] The group $\Gamma^*(1)/\Gamma(1)$ acts on $\mathcal{X}(1)$ with quotient curve $\mathcal{X}^*(1)$. For each $p \in \Sigma$ there is then an involution $\mathsf{w}_p \in \Gamma^*(1)/\Gamma(1)$ associated to the class in $\Gamma^*(1)/\Gamma(1)$ of elements of $\mathcal{O}$ of norm p, and these involutions commute with each other. (We chose the notation w_p to suggest an analogy with the Atkin-Lehner involutions w_l, which as we shall see have a more direct counterpart in our setting when $l \notin \Sigma$.)

In terms of abelian surfaces these involutions w_p of $\mathcal{X}(1)$ may be explained as follows. Let $I_p \subset \mathcal{O}$ consist of the elements whose norm is divisible by p. Then I_p is a two-sided prime ideal of $\mathcal{O}$, with $\mathcal{O}/I_p \cong \mathbf{F}_{p^2}$ and $I_p^2 = p\mathcal{O}$. Given an action of $\mathcal{O}$ on a ppas A, the kernel of I_p is a subgroup of A of size p^2 isotropic under the Weil pairing, so the quotient surface $A' := A/\ker I_p$ is itself principally polarized. Moreover, since I_p is a two-sided ideal, A' inherits an action of $\mathcal{O}$. Thus if A corresponds to some point $P \in \mathcal{X}(1)$ then A' corresponds to a point $P' \in \mathcal{X}(1)$ determined algebraically by P; that is, we have an algebraic map $\mathsf{w}_p : P \mapsto P'$ from $\mathcal{X}(1)$ to itself. Applying this construction to A' yields $A/\ker I_p^2 = A/\ker p\mathcal{O} = A/\ker p \cong A$; thus $\mathsf{w}_p(P') = P$ and w_p is indeed an involution. The quotient curve $\mathcal{X}^*(1)$ then parametrizes surfaces A up to the identification of A with $A/\ker I$ where $I = \cap_{p \in \Sigma'} I_p = \prod_{p \in \Sigma'} I_p$ for some $\Sigma' \subseteq \Sigma$.

Since $\mathcal{X}(1)$, $\mathcal{X}^*(1)$ have the structure of algebraic curves over $\mathbf{Q}$, they can be regarded as curves over $\mathbf{R}$. Now a real structure on any Riemann surface is equivalent to an anti-holomorphic involution of the surface. For surfaces $\mathcal{H}/\Gamma$ uniformized by the upper half-plane, we can give such an involution by choosing a group $(\Gamma : 2) \subset \mathrm{PGL}_2(\mathbf{R})$ containing Γ with index 2 such that $(\Gamma : 2) \not\subset \mathrm{PSL}_2(\mathbf{R})$. An element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\mathbf{R}^*$ of $\mathrm{PGL}_2(\mathbf{R}) - \mathrm{PSL}_2(\mathbf{R})$ (i.e. with $ad - bc < 0$) acts on $\mathcal{H}$ anti-holomorphically $z \mapsto (a\bar{z}+b)/(c\bar{z}+d)$. Such a fractional conjugate-linear transformation has fixed points on $\mathcal{H}$ if and only if $a + d = 0$, in which case it is an involution and its fixed points constitute a hyperbolic line. Thus $\mathcal{H}/\Gamma$, considered as a curve over $\mathbf{R}$ using $\Gamma : 2$, has real points if and only if

$(\varGamma : 2) - \varGamma$ contains an involution of $\mathcal{H}$. The real structures on $\mathcal{X}(1)$, $\mathcal{X}^*(1)$ are defined by

$$(\varGamma(1) : 2) := \mathcal{O}^* / \{\pm 1\}, \tag{21}$$

$$(\varGamma^*(1) : 2) := \{[a] \in \mathsf{A}^* / \mathbf{Q}^* : a\mathcal{O} = \mathcal{O}a\}. \tag{22}$$

That is, compared with (4,5) we drop the condition that the norm be positive. If $\Sigma \neq \emptyset$ then $\mathcal{X}(1)$ has no real points, because if $\varGamma(1) : 2$ contained an involution $\pm a$ then the characteristic equation of a would be $a^2 - 1 = 0$ and A would contain the zero divisors $a \pm 1$. This is a special case of the result of [S3]. But $\mathcal{X}^*(1)$ may have real points. For instance, we shall see that if $\Sigma = \{2, 3\}$ then $\varGamma^*(1)$ is isomorphic with the triangle group $G_{2,4,6}$. For general p, q, r with[3] $1/p + 1/q + 1/r < 1$ we can (and, if p, q, r are distinct, can only) choose $G_{p,q,r} : 2$ so that the real locus of $\mathcal{H}/G_{p,q,r}$ consists of three hyperbolic lines joining the three elliptic points in pairs, forming a hyperbolic triangle, with $G_{p,q,r} : 2$ generated by hyperbolic reflections in the triangle's sides; it is this triangle to which the term "triangle group" alludes.

2.3 The Shimura modular curves $\boldsymbol{\mathcal{X}(N)}$ and $\boldsymbol{\mathcal{X}^*(N)}$ (with $\boldsymbol{N}$ coprime to $\boldsymbol{\Sigma}$); the curves $\boldsymbol{\mathcal{X}_0(N)}$ and $\boldsymbol{\mathcal{X}_0^*(N)}$ and their involution $\boldsymbol{w_N}$

Now let l be a prime not ramified in A. Then $\mathsf{A} \otimes \mathbf{Q}_l$ and $\mathcal{O} \otimes \mathbf{Z}_l$ are isomorphic with $M_2(\mathbf{Q}_l)$ and $M_2(\mathbf{Z}_l)$ respectively. Thus $(\mathcal{O} \otimes \mathbf{Q}_l)_1^* / \{\pm 1\} \cong \mathrm{PSL}_2(\mathbf{Z}_l)$, with the subscript 1 indicating the norm-1 subgroup as in (4). We can thus define congruence subgroups $\varGamma(l)$, $\varGamma_1(l)$, $\varGamma_0(l)$ of $\varGamma(1)$ just as in the classical case in which $\Sigma = \emptyset$ and $\varGamma(1) = \mathrm{PSL}_2(\mathbf{Z})$. For instance, $\varGamma(l)$ is the normal subgroup

$$\{\pm a \in \mathcal{O}_+^* / \{\pm 1\} : a \equiv 1 \bmod l\} \tag{23}$$

of $\varGamma(1)$, with $\varGamma(1)/\varGamma(l) \cong \mathrm{PSL}_2(\mathbf{F}_l)$; once we choose an identification of the quotient group $\varGamma(1)/\varGamma(l)$ with $\mathrm{PSL}_2(\mathbf{F}_l)$ we may define $\varGamma_0(l)$ as the preimage in $\varGamma(1)$ of the upper triangular subgroup of $\mathrm{PSL}_2(\mathbf{F}_l)$. Likewise we have subgroups $\varGamma(l^r)$, $\varGamma_0(l^r)$ etc., and even $\varGamma(N)$, $\varGamma_0(N)$ for a positive integer N not divisible by any of the primes of Σ.

The quotients of $\mathcal{H}$ by these subgroups of $\varGamma(1)$ are then modular curves covering $\mathcal{X}(1)$, which we denote by $\mathcal{X}(l)$, $\mathcal{X}_0(l)$, etc. They parametrize ppas's A with an $\mathcal{O}$-action and extra structure: in the case of $\mathcal{X}(N)$, a choice of basis for the N-torsion points $A[N]$; in the case of $\mathcal{X}_0(N)$, a subgroup $G \subset A[N]$ isomorphic with $(\mathbf{Z}/N)^2$ and isotropic under the Weil pairing. In the latter case the surface $A' = A/G$ is itself principally polarized and inherits an action of $\mathcal{O}$ from A, and the image of $A[N]$ in A' is again a subgroup $G' \cong (\mathbf{Z}/N)^2$ isotropic under the Weil pairing. Thus if we start from some point P on $\mathcal{X}_0(N)$ and associate to it a pair (A, G) we obtain a new pair (A', G') of the same kind and a new point $P' \in \mathcal{X}_0(N)$ determined algebraically by P. Thus we have an algebraic

[3] If $1/p+1/q+1/r$ equals or exceeds 1, an analogous situation occurs with $\mathcal{H}$ replaced by the complex plane or Riemann sphere.

map $w_N : P \mapsto P'$ from $\mathcal{X}_0(N)$ to itself. As in the classical case — in which it is easy to see that the construction of A', G' from A, G amounts to (the square of) the familiar picture of cyclic subgroups and dual isogenies — this w_N is an involution of $\mathcal{X}_0(N)$ that comes from a trace-zero element of A of norm N whose image in $\mathsf{A}^*/\mathbf{Q}^*$ is an involution normalizing $\Gamma_0(N)$.

By abuse of terminology we shall say that a pair of points P, P' on $\mathcal{X}(1)$ are "cyclically N-isogenous"[4] if they correspond to ppas's A, A' with $A' = A/G$ as above, and call the quotient map $A \to A/G \cong A'$ a "cyclic N-isogeny". If we regard P, P' as $\Gamma(1)$-orbits in $\mathcal{H}$ then they are cyclically N-isogenous iff a point in the first orbit is taken to a point in the second by some $a \in \mathcal{O}$ of norm N such that $a \neq ma'$ for any $a' \in \mathcal{O}$ and $m > 1$; since in that case $\bar{a}$ also satisfies this condition and acts on $\mathcal{H}$ as the inverse of a, this relation on P, P' is symmetric. Then $\mathcal{X}_0(N)$ parametrizes pairs of N-isogenous points on $\mathcal{X}(1)$, and w_N exchanges the points in such a pair. The involutions w_p on $\mathcal{X}(1)$ lift to the curves $\mathcal{X}(N)$, $\mathcal{X}_0(N)$, etc., and commute with w_N on $\mathcal{X}_0(N)$.

The larger group $\Gamma^*(1)$ likewise has congruence groups such as $\Gamma^*(N)$, $\Gamma_0^*(N)$, etc., which give rise to modular curves covering $\mathcal{X}^*(1)$ called $\mathcal{X}^*(N)$, $\mathcal{X}_0^*(N)$, etc. The involution w_N on $\mathcal{X}_0(N)$ descends to an involution on $\mathcal{X}_0^*(N)$ which we shall also call w_N. We extend our abuse of terminology by saying that two points on $\mathcal{X}^*(1)$ are "cyclically N-isogenous" if they lie under two N-isogenous points of $\mathcal{X}(1)$, and speak of "N-isogenies" between the equivalence classes of ppas's parametrized by $\mathcal{X}^*(1)$. One new feature of the congruence subgroups of $\Gamma^*(1)$ is that, while $\Gamma^*(N)$ is still normal in $\Gamma^*(1)$, the quotient group may be larger than $\mathrm{PSL}_2(\mathbf{Z}/N)$, due to the presence of the w_p. For instance if $l \notin \Sigma$ is prime then $\Gamma^*(1)/\Gamma^*(l)$ is $\mathrm{PSL}_2(\mathbf{F}_l)$ only if all the primes in Σ are squares modulo l; otherwise the quotient group is $\mathrm{PGL}_2(\mathbf{F}_l)$. In either case the index of $\Gamma_0^*(N)$ in $\Gamma^*(1)$, and thus also the degree of the cover $\mathcal{X}_0^*(N)/\mathcal{X}^*(1)$, is $l+1$.

Since these curves are all defined over $\mathbf{Q}$, they can again be regarded as curves over $\mathbf{R}$ by a suitable choice of $(\Gamma : 2)$. For instance, if $\Gamma = \Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$ we obtain $(\Gamma : 2)$ by adjoining $a \in \mathcal{O}$ of norm -1 such that $a \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \bmod N$ under our identification of $\mathcal{O}/N\mathcal{O}$ with $M_2(\mathbf{Z}/N)$. Note however that most of the automorphisms $\mathrm{PSL}_2(\mathbf{Z}/N)$ of $\mathcal{X}(N)$ do not commute with $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and thus do not act on $\mathcal{X}(N)$ regarded as a real curve. Similar remarks apply to $\Gamma^*(N)$ etc.

Now fix a prime $l \notin \Sigma$ and consider the sequence of modular curves $X_r = \mathcal{X}_0(l^r)$ or $X_r = \mathcal{X}_0^*(l^r)$ $(r = 0, 1, 2, \ldots)$. The r-th curve parametrizes l^r-isogenies, which is to say sequences of l-isogenies

$$A_0 \to A_1 \to A_2 \to \cdots \to A_n \tag{24}$$

such that the composite isogeny $A_{j-1} \to A_{j+1}$ is a *cyclic* l^2-isogeny for each j with $0 < j < n$. Thus for each $m = 0, 1, \ldots, n$ there are $n + 1 - m$ maps $\pi_j : X_n \to X_m$ obtained by extracting for some $j = 0, 1, \ldots, n - m$ the cyclic

[4] This qualifier "cyclically" is needed to exclude cases such as the multiplication-by-m map, which as in the case of elliptic curves would count as an "m^2-isogeny" but not a cyclic one.

l^m-isogeny $A_j \to A_{j+m}$ from (24). Each of these maps has degree l^{n-m}, unless $m = 0$ when the degree is $(l+1)l^{n-1}$. In particular we have a tower of maps

$$X_n \overset{\pi_0}{\to} X_{n-1} \overset{\pi_0}{\to} X_{n-2} \overset{\pi_0}{\to} \cdots \overset{\pi_0}{\to} X_2 \overset{\pi_0}{\to} X_1, \tag{25}$$

each map being of degree l. We observed in [E6, Prop. 1] that explicit formulas for X_1, X_2, together with their involutions w_l, w_{l^2} and the map $\pi_0 : X_2 \to X_1$, suffice to exhibit the entire tower (25) explicitly: For $n \geq 2$ the product map

$$\pi = \pi_0 \times \pi_1 \times \pi_2 \times \cdots \times \pi_{n-2} : X_n \to X_2^{n-1} \tag{26}$$

is a 1:1 map from X_n to the set of $(P_1, P_2, \ldots, P_{n-1}) \in X_2^{n-1}$ such that

$$\pi_0\big(w_{l^2}(P_j)\big) = w_l\big(\pi_0(P_{j+1})\big) \tag{27}$$

for each $j = 1, 2, \ldots, n-2$. Here we note that this information on X_1, X_2 is in turn determined by explicit formulas for X_0, X_1, together with the involution w_l and the map $\pi_0 : X_1 \to X_0$. Indeed $\pi_1 : X_1 \to X_0$ is then $\pi_0 \circ w_l$, and the product map $\pi_0 \times \pi_1 : X_2 \to X_1^2$ identifies X_2 with a curve in X_1^2 contained in the locus of

$$\{(Q_1, Q_2) \in X_1^2 \,:\, \pi_1(Q_1) = \pi_0(Q_2)\}, \tag{28}$$

which decomposes as the union of that curve with the graph of w_l.[5] This determines X_2 and the projections $\pi_j : X_2 \to X_1$ $(j = 0, 1)$; the involution w_{l^2} is

$$(Q_1, Q_2) \leftrightarrow (w_l Q_2, w_l Q_1). \tag{29}$$

Thus the equations we shall exhibit for certain choices of A and l suffice to determine explicit formulas for towers of Shimura modular curves $\mathcal{X}_0(l^r)$, $\mathcal{X}_0^*(l^r)$, towers whose reduction at any prime $l' \notin \Sigma \cup \{l\}$ is known to be asymptotically optimal over the field of l'^2 elements [I3, TVZ].

2.4 Complex-multiplication (CM) and supersingular points on Shimura curves

Let F be a quadratic imaginary field, and let O_F be its ring of integers. Assume that none of the primes of Σ split in F. Then F embeds in A (in many ways), and O_F embeds in $\mathcal{O}$. For any embedding $\iota : F \hookrightarrow \mathsf{A}$, the image of F^* in $\mathsf{A}^*/\mathbf{Q}^*$ then has a unique fixed point on $\mathcal{H}$; the orbit of this point under $\Gamma(1)$, or under any other congruence subgroup $\Gamma \subset \mathsf{A}^*/\mathbf{Q}^*$, is then a *CM point* on the Shimura curve $\mathcal{H}/\Gamma$. In particular, on $\mathcal{X}(1)$ such a point parametrizes a ppas with extra endomorphisms by $\iota(F) \cap \mathcal{O}$. For instance if $\iota(F) \cap \mathcal{O} = \iota(O_F)$ then this ppas is a product of elliptic curves each with complex multiplication by O_F (but not in the product polarization). In general $\iota^{-1}(\iota(F) \cap \mathcal{O})$ is called the *CM ring* of the CM point on $\mathcal{X}(1)$. Embeddings conjugate by $\Gamma(1)$ yield the same point

[5] This is where we use the hypothesis that l is prime. The description of X_n in (26,27) holds even for composite l, but the description of X_2 in terms of X_1 does not, because then (28) has other components.

on $\mathcal{X}(1)$, and for each order $O \subset F$ there are finitely many embeddings up to conjugacy, and thus finitely many CM points on $\mathcal{X}(1)$ with CM ring O; in fact their number is just the class number of O. In [S2] Shimura already showed that all points with the same CM ring are Galois conjugate over $\mathbf{Q}$, from which it follows that a CM point is rational if and only if its CM ring has unique factorization.

Thus far the description is completely analogous to the theory of complex multiplication for j-invariants of elliptic curves. But when $\Sigma \neq \emptyset$ a new phenomenon arises: CM points on the quotient curve $\mathcal{X}^*(1)$ may be rational even when their preimages on $\mathcal{X}(1)$ are not. For instance, a point with CM ring O_F is rational on $\mathcal{X}^*(1)$ if and only if the class group of F is generated by the classes of ideals $I \subset O_F$ such that I^2 is the principal ideal (p) for some rational prime $p \in \Sigma$. This has the amusing consequence that when $\Sigma = \{2, 3\}$ the number of rational CM points on $\mathcal{X}^*(1)$ is more than twice the number of rational CM points on the classical modular curve $X(1)$. [Curiously, already in the classical setting $X(1)$ does not hold the record: it has 13 rational CM points, whilst $X_0^*(6) = X_0(6)/\langle w_2, w_3\rangle$ has 14. The reason again is fields F with nontrivial class group generated by square roots of the ideals (2) or (3), though with a few small exceptions both 2 and 3 must ramify in F. In the $\mathcal{X}^*(1)$ setting the primes of Σ are allowed to be inert as well, which makes the list considerably longer.] In fact for each of the first four cases $\Sigma = \{2, 3\}, \{2, 5\}, \{2, 7\}, \{3, 5\}$ we find more rational CM points than on any classical modular curve.

A major aim of this paper is computation of the coordinates of these points. We must first list all possible O. The class number of O, and thus of F, must be a power of 2 no greater than $2^{\#\Sigma}$. In each of our cases, $\#\Sigma = 2$, so F has class number at most 4 and we may refer to the list of imaginary quadratic number fields with class group $(\mathbf{Z}/2)^r$ $(r = 0, 1, 2)$, proved complete by Arno [A].[6] Given F we easily find all possible O, and imbed each into $\mathcal{O}$ by finding $a \in \mathcal{O}$ such that $(a - \bar{a})^2 = \operatorname{disc}(O)$. This gives us the CM point on $\mathcal{H}$. But we want its coordinates on the Shimura curve $\mathcal{H}/\Gamma^*(1)$ as rational numbers. Actually only one coordinate is needed because $\mathcal{X}^*(1)$ has genus 0 for each of our four Σ. We recover the coordinate as a real number using our Schwarzian uniformization of $\mathcal{X}^*(1)$ by $\mathcal{H}$. (Of course a coordinate on $\mathbf{P}^1$ is only defined up to $\mathrm{PGL}_2(\mathbf{Q})$, but in each case we choose a coordinate once and for all by specifying it on the CM points.) We then recognize that number as a rational number from its continued fraction expansion, and verify that the putative rational coordinate not only agrees with our computations to as many digits as we want but also satisfies various arithmetic conditions such as those described later in this section.

Of course this is not fully satisfactory; we do not know how to prove that, for instance, $t = 13^2 67^2 109^2 139^2 157^2 163/2^{10} 5^6 11^6 17^6$ (see Tables 1,2 below) is the

[6] It might be possible to avoid that difficult proof for our application, since we are only concerned with fields whose class group is accounted for by ramified primes in a given set Σ, and it may be possible to provably list them all using the arithmetic of CM points on either classical or Shimura modular curves, as in Heegner's proof that $\mathbf{Q}(\sqrt{-163}\,)$ is the last quadratic imaginary field of class number 1.

CM point of discriminant -163 on the curve $\mathcal{X}^*(1)$ associated with the algebra ramified at $\{2,3\}$. But we can prove that above half of our numbers are correct, again using the modular curves $\mathcal{X}^*(l)$ and their involutions w_l for small l. This is because CM points behave well under isogenies: any point isogenous to a CM point is itself CM, and moreover a point on $\mathcal{X}(1)$ or $\mathcal{X}^*(1)$ is CM if and only if it admits a cyclic d-isogeny to itself for some $d > 1$. Once we have formulas for $\mathcal{X}_0^*(l)$ and w_l we may compute all points cyclically l-isogenous either with an already known CM points or with themselves. The discriminant of a new rational CM point can then be determined either by arithmetic tests or by identifying it with a real CM point to low precision.

The classical theory of *supersingular points* also largely carries over to the Shimura setting. We may use the fact that the ppas parametrized by a CM point has extra endomorphisms to define CM points of Shimura curves algebraically, and thus in any characteristic $\notin \Sigma$. In positive characteristic $p \notin \Sigma$, any CM point is defined over some finite field, and conversely every $\overline{\mathbf{F}_p}$-point of a Shimura curve is CM. All but finitely many of these parametrize ppas's whose endomorphism ring has $\mathbf{Z}$-rank 8; the exceptional points, all defined over $\mathbf{F}_{p^2}$, yield rank 16, and are called *supersingular*, all other $\overline{\mathbf{F}_p}$-points being *ordinary*. One may choose coordinates on $\mathcal{X}(1)$ (or $\mathcal{X}^*(1)$) such that a CM point in characteristic zero reduces mod p to a ordinary point if p splits in the CM field, and to a supersingular point otherwise. Conversely each ordinary point mod p lifts to a unique CM point (cf. [D] for the classical case). This means that if two CM points with different CM fields have the same reduction mod p, their common reduction is supersingular, and then as in [GZ] there is an upper bound on p proportional to the product of the two CM discriminants. So for instance if $\mathcal{X}^*(1) \cong \mathbf{P}^1$ then the difference between the coordinates of two rational CM points is a product of small primes. This remains the case, for similar reasons, even for distinct CM points with the same CM field, and may be checked from the tables of rational CM points in this paper. The preimages of the supersingular points on modular covers such as $\mathcal{X}_0(l)$ yield enough $\mathbf{F}_{p^2}$-rational points on these curves to attain the Drinfeld-Vlăduţ bound [I3]; these curves are thus “asymptotically optimal” over $\mathbf{F}_{p^2}$. Asymptotically optimal curves over $\mathbf{F}_{p^{2f}}$ $(f > 1)$ likewise come from Shimura curves associated to quaternion algebras over totally real number fields with a prime of residue field $\mathbf{F}_{p^f}$.

In the case of residue field $\mathbf{F}_p$ (so in particular for quaternion algebras over $\mathbf{Q}$) Ihara [I2] found a remarkable connection between the hyperbolic uniformization of a Shimura curve $\mathcal{X} = \mathcal{H}/\Gamma$ and the supersingular points of its reduction mod p. We give his result in the case that $\mathcal{X}$ has genus 0, because we will only apply it to such curves and the result can be stated in an equivalent and elementary form (though the *proof* is still far from elementary). Since we are working over $\mathbf{F}_p$, we may identify any curve of genus 0 with $\mathbf{P}^1$, and choose a coordinate (degree-1 function) t on $\mathbf{P}^1$ such that $t = \infty$ is an elliptic point. Let t_i be the coordinates of the remaining elliptic points.

First, the hyperbolic area of the curve controls the number of points, which is approximately $\frac{1}{2}(p+1)\mathrm{Area}(\mathcal{X})$ — “approximately” because $\frac{1}{2}(p+1)\mathrm{Area}(\mathcal{X})$

is not the number of points but their total mass. The mass of a non-elliptic supersingular point is 1, but an elliptic point with stabilizer G has mass $1/\#G$. If the elliptic point mod p is the reduction of only one elliptic point on $\mathcal{H}/\Gamma$ (which, for curves coming from quaternion algebras over $\mathbf{Q}$, is always the case once $p>3$), then its stabilizer is $\mathbf{Z}/e\mathbf{Z}$ and its mass is $1/e$ where e is the index of that elliptic point. [The mass formula also holds for $\mathcal{X}$ of arbitrary genus, and for general residue fields provided p is replaced by the size of the field.] Let d be the number of non-elliptic supersingular points, and choose a Schwarzian equation (16) with at most regular singularities at $t=\infty, t_i$ and no other singularities. Then the supersingular points are determined uniquely by the condition that their t-coordinates are the roots of a polynomial $P(t)$ of degree d such that for some $r_i \in \mathbf{Q}$ the algebraic function $\prod_i (t-t_i)^{r_i} \cdot P(t)$ is a solution of the Schwarzian differential equation (16)! For instance [I2, 4.3], if Γ is a triangle group we may choose $t_i = 0, 1$, and then $P(t)$ is a finite hypergeometric series mod p.

Given $t_0 \in \mathbf{Q}$ we may then test whether t_0 is ordinary or supersingular mod p for each small p. If t_0 is a CM point with CM field then its reduction is ordinary if p splits in F, supersingular otherwise. When we have obtained t_0 as a good rational approximation to a rational CM point, but could not prove it correct, we checked for many p whether t_0 is ordinary or supersingular mod p; when each prime behaves as expected from its behavior in F, we say that t_0 has "passed the supersingular test" modulo those primes p.

3 The case $\Sigma = \{2, 3\}$

3.1 The quaternion algebra and the curves $\mathcal{X}(1)$, $\mathcal{X}^*(1)$

For this section we let A be the quaternion algebra ramified at $\{2,3\}$. This algebra is generated over $\mathbf{Q}$ by elements b, c satisfying

$$b^2 = 2, \quad c^2 = -3, \quad bc = -cb. \tag{30}$$

The conjugation of A fixes 1 and takes b, c, bc to $-b, -c, -bc$; thus for any element $\alpha = \alpha_1 + \alpha_2 b + \alpha_3 c + \alpha_4 bc \in \mathsf{A}$ the conjugate and norm of α are given by

$$\bar{\alpha} = \alpha_1 - \alpha_2 b - \alpha_3 c - \alpha_4 bc, \quad \mathrm{N}(\alpha) = \alpha_1^2 - 2\alpha_2^2 + 3\alpha_3^2 - 6\alpha_4^2. \tag{31}$$

Since A is indefinite, all its maximal orders are conjugate; let $\mathcal{O}$ be the maximal order generated by b and $(1+c)/2$. Then $\Gamma^*(1)$ contains $\Gamma(1)$ with index $2^{\#\Sigma} = 4$, and consists of the classes mod $\mathbf{Q}^*$ of elements of $\mathcal{O}$ of norm 1, 2, 3, or 6. In row II of Table 3 of [T] (p.208) we find that $\Gamma^*(1)$ is isomorphic with the triangle group

$$G_{2,4,6} := \langle s_2, s_4, s_6 | s_2^2 = s_4^4 = s_6^6 = s_2 s_4 s_6 = 1 \rangle. \tag{32}$$

Indeed we find that $\Gamma^*(1)$ contains elements

$$s_2 = [bc + 2c], \quad s_4 = [(2+b)(1+c)], \quad s_6 = [3+c] \tag{33}$$

[NB $(2+b)(1+c), 3+c \in 2\mathcal{O}$] of orders $2,4,6$ with $s_2 s_4 s_6 = 1$. The subgroup of $\Gamma^*(1)$ generated by these elements is thus isomorphic with $G_{2,4,6}$. But a hyperbolic triangle group cannot be isomorphic with a proper subgroup (since the areas of the quotients of $\mathcal{H}$ by the group and its subgroup are equal), so $\Gamma^*(1)$ is generated by s_2, s_4, s_6. Note that these generators have norms $6,2,3 \bmod (\mathbf{Q}^*)^2$, and thus represent the three nontrivial cosets of $\Gamma^*(1)$ in $\mathcal{O}^*/\{\pm 1\}$.

Since $\Gamma^*(1)$ is a triangle group, $\mathcal{X}^*(1)$ is a curve of genus 0. Moreover $\mathcal{X}^*(1)$ has $\mathbf{Q}$-rational points (e.g. the three elliptic points, each of which must be rational because it is the only one of its index), so $\mathcal{X}^*(1) \cong \mathbf{P}^1$ over $\mathbf{Q}$. Let t be a rational coordinate on that curve (i.e. a rational function of degree 1). In general a rational coordinate on $\mathbf{P}^1$ is determined only up to the PGL_2 action on $\mathbf{P}^1$, but can be specified uniquely by prescribing its values at three points. In our case $\mathcal{X}^*(1)$ has three distinguished points, namely the elliptic points of orders $2,4,6$; we fix t by requiring that it assume the values $0,1,\infty$ respectively at those three points.

None of s_2, s_4, s_6 is contained in $\Gamma(1)$. Hence the $(\mathbf{Z}/2)^2$ cover $\mathcal{X}(1)/\mathcal{X}^*(1)$ is ramified at all three elliptic points. Thus s_2 lies under two points of $\mathcal{X}(1)$ with trivial stabilizer, while s_4 lies under two points of index 2 and s_6 under two points of index 3. By either the Riemann-Hurwitz formula or from (10) we see that $\mathcal{X}(1)$ has genus 0. This and the orders $2,2,3,3$ of the elliptic points do not completely specify $\Gamma(1)$ up to conjugacy in $\mathrm{PSL}_2(\mathbf{R})$: to do that we also need the cross-ratio of the four elliptic points. Fortunately this cross-ratio is determined by the existence of the cover $\mathcal{X}(1) \to \mathcal{X}^*(1)$, or equivalently of an involution s_4 on $\mathcal{X}(1)$ that fixes the two order-2 points and switches the order-3 points. This forces the pairs of order-2 and order-3 points to have a cross-ratio of -1, or to "divide each other harmonically" as the Greek geometers would say. The function field of $\mathcal{X}(1)$ is generated by the square roots of $c_0 t$ and $c_1(t-1)$ for some $c_0, c_1 \in \mathbf{Q}^*/\mathbf{Q}^{*2}$, but we do not yet know which multipliers c_0, c_1 are appropriate. If both c_0, c_1 were 1 then $\mathcal{X}(1)$ would be a rational curve with coordinate u with $t = ((u^2+1)/2u)^2 = 1 + ((u^2-1)/2u)^2$, the familiar parametrization of Pythagorean triples. The elliptic points of order 2 and 3 would then be at $u = \pm 1$ and $u = 0, \infty$. However it will turn out that the correct choices are $c_0 = -1, c_1 = 3$, and thus that $\mathcal{X}(1)$ is the conic with equation

$$X^2 + Y^2 + 3Z^2 = 0 \tag{34}$$

and no rational points even over $\mathbf{R}$. [That $\mathcal{X}(1)$ is the conic (34) is announced in [Ku, p.279] and attributed to Ihara; that there are no real points on the Shimura curve $\mathcal{X}(1)$ associated to any indefinite quaternion algebra over $\mathbf{Q}$ other than $M_2(\mathbf{Q})$ was already shown by Shimura [S3]. The equation (34) for $\mathcal{X}(1)$ does not uniquely determine c_0, c_1, but the local methods of [Ku] could probably supply that information as well.]

3.2 Shimura modular curves $\mathcal{X}_0^*(l)$ and $\mathcal{X}(l)$ for $l = 5, 7, 13$

Let l be a prime other than the primes $2,3$ of Σ. We determine the genus of the curve $\mathcal{X}_0^*(l)$ using the formula (10). Being a cover of $\mathcal{X}^*(1)$ of degree $l+1$, the curve $\mathcal{X}_0^*(l)$ has normalized hyperbolic area $(l+1)/12$. It has $1+(-6/l)$ elliptic points of order 2, $1+(-1/l)$ elliptic points of order 4, and $1+(-3/l)$ elliptic points of order 6. This is a consequence of our computation of s_2, s_4, s_6, which lift to elements of A that generate subfields isomorphic with $\mathbf{Q}(\sqrt{-6})$, $\mathbf{Q}(\sqrt{-1})$, and $\mathbf{Q}(\sqrt{-3})$. Actually the orders $2,4,6$ of the elliptic points suffice. Consider the images of s_2, s_4, s_6 in the Galois group ($\subseteq \mathrm{PGL}_2(\mathbf{F}_l)$) of the cover $\mathcal{X}_0^*(l)/\mathcal{X}^*(1)$, and the cycle structures of their actions on the $l+1$ points of $\mathbf{P}^1(\mathbf{F}_l)$. These images $\sigma_2, \sigma_4, \sigma_6$ are group elements of order $2,4,6$. For 4 and 6, the order determines the conjugacy class, which joins as many of the points of $\mathbf{P}^1(\mathbf{F}_l)$ as possible in cycles of length 4 or 6 respectively and leaves any remaining points fixed; the number of fixed points is two or none according to the residue of l mod 4 or 6. For σ_2 there are two conjugacy classes in $\mathrm{PGL}_2(\mathbf{F}_l)$, one with two fixed points and the other with none, but the choice is determined by the condition that the genus $g(\mathcal{X}_0^*(l))$ be an integer, or equivalently by the requirement that the signs of $\sigma_2, \sigma_4, \sigma_6$ considered as permutations of $\mathbf{P}^1(\mathbf{F}_l)$ be consistent with $s_2 s_4 s_6 = 1$. We readily check that this means that the image of s_2 has two fixed points if and only if $(-6/l) = +1$, as claimed. From (10) we conclude that

$$g(\mathcal{X}_0^*(l)) = \frac{1}{24}\left[l - 6\left(\frac{-6}{l}\right) - 9\left(\frac{-1}{l}\right) - 10\left(\frac{-3}{l}\right)\right]. \tag{35}$$

We tabulate this for $l < 50$:

l	5	7	11	13	17	19	23	29	31	37	41	43	47
$g(\mathcal{X}_0^*(l))$	0	0	1	0	1	1	2	1	1	1	2	2	3

It so happens that in the first seven cases $g(\mathcal{X}_0^*(l))$ coincides with the genus of the classical modular curve $\mathrm{X}_0(l)$, but of course this cannot go on forever because the latter genus is $l/12 + O(1)$ while the former is only $l/24 + O(1)$, and indeed $g(\mathcal{X}_0^*(l))$ is smaller for all $l > 23$. Still, as with $\mathrm{X}_0(l)$, we find that $\mathcal{X}_0^*(l)$ has genus 0 for $l = 5, 7, 13$, but not for $l = 11$ or any $l > 13$. For the three genus-0 cases we shall use the ramification behavior of the cover $\mathcal{X}_0^*(l)/\mathcal{X}^*(1)$ to find an explicit rational function of degree $l+1$ on $\mathbf{P}^1$ that realizes that cover and determine the involution w_l.

Now for any $l > 3$ the solution of $\sigma_2\sigma_4\sigma_6 = 1$ in elements $\sigma_2, \sigma_4, \sigma_6$ of orders $2,4,6$ in $\mathrm{PGL}_2(\mathbf{F}_l)$ is unique up to conjugation in that group. Thus we know from the general theory of [Mat] that the cover $\mathcal{X}_0^*(l)/\mathcal{X}^*(1)$ is determined by its Galois group and ramification data. Unfortunately the proof of this fact does not readily yield an efficient computation of the cover; for instance the Riemann existence theorem for Riemann surfaces is an essential ingredient. We use a method for finding the rational function $t : \mathcal{X}_0^*(l) \to \mathcal{X}^*(1)$ explicitly that amounts to solving for its coefficients, using the cycle structures of $\sigma_2, \sigma_4, \sigma_6$ to obtain algebraic conditions. In effect these conditions are the shape of the divisors $(t)_0$, $(t)_1$, $(t)_\infty$. But a rational function satisfying these conditions is not in general known to have the right Galois group: all we know is that the monodromy elements around $0, 1, \infty$ have the right cycle structures in the symmetric group S_{l+1}. Thus we obtain several candidate functions, only one of which has Galois group $\mathrm{PGL}_2(\mathbf{F}_l)$ (or $\mathrm{PSL}_2(\mathbf{F}_l)$ if $l \equiv 1 \bmod 24$). Fortunately for $l = 5, 7$ we can exclude the impostors by inspection, and for $l = 13$ the computation has already been done for us.

l=5. Here the cycle structures of s_2, s_4, s_6 are 2211, 411, 6. Curiously if the identity in the symmetric group S_6 is written as the product of three permutations $\sigma_2, \sigma_4, \sigma_6$ with these cycle structures then they can never generate all of S_6. This can be seen by considering their images $\sigma_2', \sigma_4', \sigma_6'$ under an outer automorphism of S_6: these have cycle structures 2211, 411, 321, and thus have too many cycles to generate a transitive subgroup (if two permutations of n letters generate a transitive subgroup of S_n then they and their product together have at most $n+2$ cycles). It turns out that the subgroup generated by $\sigma_2', \sigma_4', \sigma_6'$ can be either $A_4 \times S_2$ or the point stabilizer S_5. In the former case $\sigma_2, \sigma_4, \sigma_6$ generate a transitive but imprimitive subgroup of S_6: the six letters are partitioned into three pairs, and the group consists of all permutations that respect this partition and permute the pairs cyclically. In the latter case $\sigma_2, \sigma_4, \sigma_6$ generate $\mathrm{PGL}_2(\mathbf{F}_5)$; this is the case we are interested in. In each of the two cases the triple $(\sigma_2, \sigma_4, \sigma_6)$ is determined uniquely up to conjugation in the subgroup of S_6 generated by the σ's, each of which is in a rational conjugacy class in the sense of [Mat]. Thus each case corresponds to a unique degree-6 cover $\mathbf{P}^1 \to \mathbf{P}^1$ defined over $\mathbf{Q}$. We shall determine both covers.

Let t be a rational function on $\mathbf{P}^1$ ramified only above $t = 0, 1, \infty$ with cycle structures 2211, 411, 6. Choose a rational coordinate x on $\mathbf{P}^1$ such that $x = \infty$ is the sextuple pole of t and $x = 0$ is the quadruple zero of $t-1$; this determines x up to scaling. Then t is a polynomial of degree 6 in x with two double roots such that $t \equiv 1 \bmod x^4$. The double roots are necessarily the roots of the quadratic polynomial $x^{-3}dt/dx$. Thus t is a polynomial of the form $c_6x^6 + c_5x^5 + c_4x^4 + 1$ divisible by $6c_6x^2+5c_5x+4c_4$. We readily compute that there are two possibilities for c_4, c_5, c_6 up to scaling $(c_4, c_5, c_6) \to (\lambda^4 c_4, \lambda^5 c_5, \lambda^6 c_6)$. One possibility gives $t = 2x^6 - 3x^4 + 1 = (x^2 - 1)^2(2x^2 + 1)$; being symmetric under $x \leftrightarrow -x$ this must be the imprimitive solution. Thus the remaining possibility must give the $\mathrm{PGL}_2(\mathbf{F}_5)$ cover $\mathcal{X}_0^*(5)/\mathcal{X}^*(1)$. The following choice of scaling of $x = x_5$ seems simplest:

$$
\begin{aligned}
t &= 540x^6 + 324x^5 + 135x^4 + 1 \\
&= 1 + 27x^4(20x^2 + 12x + 5) = (15x^2 - 6x + 1)(6x^2 + 3x + 1)^2.
\end{aligned}
\tag{36}
$$

The elliptic points of order 2 and 4 on $\mathcal{X}_0^*(5)$ are the simple zeros of t and $t - 1$ respectively, i.e. the roots of $15x^2 - 6x + 1$ and $20x^2 + 12x + 5$. The involution w_5 switches each elliptic point with the other elliptic point of the same order; this suffices to determine w_5. The fact that two pairs of points on $\mathbf{P}^1$ switched by an involution of $\mathbf{P}^1$ determine the involution is well-known, but we have not found in the literature an explicit formula for doing this. Since we shall need this result on several occasion we give it in an Appendix as Proposition A. Using that formula (89), we find that

$$
w_5(x) = \frac{42 - 55x}{55 + 300x}. \tag{37}
$$

l=7. This time s_2, s_4, s_6 have cycle structures 22211, 44, 611. Again there are several ways to get the identity permutation on 8 letters as a product of three permutations with these cycle structures, none of which generate the full symmetric group S_8. There are two ways to get the imprimitive group $2^4 : S_4$; the corresponding covers are obtained from the S_4 cover $t = 4\xi^3 - 3\xi^4$ by taking $\xi = x^2 + \xi_0$ where ξ_0 is either root of the quadratic $3\xi^2 + 2\xi + 1 = (1-t)/(\xi-1)^2$. The remaining solution corresponds to our $\mathrm{PGL}_2(\mathbf{F}_7)$ cover.

To find that cover, let t be a rational function on $\mathbf{P}^1$ ramified only above $t = 0, 1, \infty$ with cycle structures 2211, 411, 6, and choose a rational coordinate x on $\mathbf{P}^1$ such that $x = \infty$ is the sextuple pole of t. This determines x up to an affine linear transformation. Then there is a cubic polynomial P and quadratic relatively prime polynomials Q_1, Q_2, Q_3 in x such that $t = P^2 Q_1/Q_3 = 1 + Q_2^4/Q_3$, i.e. such that $P^2 Q_1 - Q_2^4$ is quadratic. Equivalently, the Taylor expansion of $Q_2^2/\sqrt{Q_1}$ about $x = \infty$ should have vanishing x^{-1} and x^{-2} coefficients, and then $R(x)$ is obtained by truncating that Taylor expansion after its constant term. We assume without loss of generality that Q_1, Q_2 are monic. By translating x (a.k.a. "completing the square") we may assume that Q_1 is of the form $x^2 + \alpha$. If the same were true of Q_2 then t would be a rational function of x^2 and we would have an imprimitive cover. Thus the constant coefficient of Q_2 is nonzero, and by scaling x we may take $Q_2 = x^2 + x + \beta$. We then set the x^{-1}, x^{-2} coefficients of of $Q_2^2/\sqrt{Q_1}$ to zero, obtaining the equations

$$3\alpha^2 - 8\alpha\beta + 8\beta^2 - 4\alpha = 3\alpha^2 - 4\alpha\beta = 0. \tag{38}$$

Thus either $\alpha = 0$ or $\alpha = 4\beta/3$. The first option yields $\beta = 0$ which fails because then Q_1, Q_2 have the common factor x. The second option yields $\beta = 0$, which again fails for the same reason, but also $\beta = 2$ which succeeds. Substituting $-(2x+1)/3$ for x to reduce the coefficients we then find:

$$\begin{aligned} t &= -\frac{(4x^2+4x+25)(2x^3-3x^2+12x-2)^2}{108(7x^2-8x+37)} \\ &= 1 - \frac{(2x^2-x+8)^4}{108(7x^2-8x+37)}. \end{aligned} \tag{39}$$

The elliptic points of order 2 and 6 on $\mathcal{X}_0^*(7)$ are respectively the simple zeros and poles of t, i.e. the roots of $4x^2 + 4x + 25$ and $7x^2 - 38x + 7$. The involution w_7 is again by the fact that it switches each elliptic point with the other elliptic point of the same order: it is

$$w_7(x) = \frac{116 - 9x}{9 + 20x}. \tag{40}$$

l=13. Here the cycle structures are 2^7, 44411, 6611. The computation of the degree-14 map is of course much more complicated than for the maps of degrees 6, 8 for $l = 5, 7$. Fortunately this computation was already done in [MM, §4] (a paper concerned not with Shimura modular curves but with examples of rigid

$\mathrm{PSL}_2(\mathbf{F}_p)$ covers of the line). There we find that there is a coordinate $x = x_{13}$ on $\mathcal{X}_0^*(13)$ for which

$$t = 1 - \frac{27}{4}\frac{(x^2+36)(x^3+x^2+35x+27)^4}{(7x^2+2x+247)(x^2+39)^6} \tag{41}$$
$$= \frac{(x^7-50x^6+63x^5-5040x^4+783x^3-168426x^2-6831x-1864404)^2}{4(7x^2+2x+247)(x^2+39)^6}.$$

The elliptic points of order 4 and 6 on $\mathcal{X}_0^*(13)$ are respectively the simple zeros and poles of $t-1$, i.e. the roots of x^2+36 and $7x^2+2x+247$. Once more we use (89) to find the involution from the fact that it switches each elliptic point with the other elliptic point of the same order:

$$w_{13}(x) = \frac{5x+72}{2x-5}. \tag{42}$$

From an equation for $\mathcal{X}^*(l)$ and the rational map t on that curve we recover $\mathcal{X}_0(l)$ by adjoining square roots of $c_0 t$ and $c_1(t-1)$. For each of our three cases $l = 5, 7, 13$ the resulting curve has genus 1, and its Jacobian is an elliptic curve of conductor $6l$ — but only if we choose c_0, c_1 that give the correct quadratic twist. For $l=5$, $l=7$, $l=13$ it turns out that we must take a square root of $3t(1-t)$, $-t$, $3(t-1)$ respectively. Fortunately these are consistent and we obtain $c_0 = -1$ and $c_1 = 3$ as promised. The resulting curves $\mathcal{X}_0(5), \mathcal{X}_0(7), \mathcal{X}_0(13)$ have no rational or even real points (because this is already true of the curve $\mathcal{X}(1)$ which they all cover); their Jacobians are the curves numbered 30H, 42C, 78B in the Antwerp tables in [BK] compiled by Tingley et al., and and 30-A8, 42-A3, 78-A2 in Cremona [C].

3.3 Supersingular points on $\mathcal{X}^*(1)$ mod l

We have noted that Ihara's description of supersingular points on Shimura curves is particularly simple in the case of a triangle group: the non-elliptic supersingular points are roots of a hypergeometric polynomial, and the elliptic points are CM in characteristic zero so the Deuring test determines whether each one is supersingular or not.

In our case, The elliptic points $t=0$, $t=1$, $t=\infty$ are supersingular mod l if and only iff l is inert in $\mathbf{Q}(\sqrt{-6})$, $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$ respectively, i.e. iff -6, -1, -3 is a quadratic nonresidue of l. Thus the status of all three elliptic points depends on l mod 24, as shown in the next table:

t	e	l mod 24: 1	5	7	11	13	17	19	23
0	2					•	•	•	•
1	4			•	•			•	•
∞	6		•		•		•		•

(bullets mark elliptic points with supersingular reduction). This could also be obtained from the total mass $(l+1)/24$ of supersingular points, together with the fact that the contribution to this mass of the non-elliptic points is integral: in each column the table shows the unique subset of $1/2, 1/4, 1/6$ whose sum is congruent to $(l+1)/24$ mod 1. The hypergeometric polynomial whose roots are the non-elliptic supersingular points has degree $\lfloor l/24 \rfloor$, and depends on l mod 24 as follows:

$$\begin{cases} F(\frac{1}{24}, \frac{5}{24}; \frac{1}{2}; t), & \text{if } l \equiv 1 \text{ or } 5 \bmod 24; \\ F(\frac{7}{24}, \frac{11}{24}; \frac{1}{2}; t), & \text{if } l \equiv 7 \text{ or } 11 \bmod 24; \\ F(\frac{13}{24}, \frac{17}{24}; \frac{3}{2}; t), & \text{if } l \equiv 13 \text{ or } 17 \bmod 24; \\ F(\frac{19}{24}, \frac{23}{24}; \frac{3}{2}; t), & \text{if } l \equiv 19 \text{ or } 23 \bmod 24. \end{cases} \tag{43}$$

For example, for $l = 163 (\equiv 19 \bmod 24)$ we find

$$\begin{aligned} F(\frac{19}{24}, \frac{23}{24}; \frac{3}{2}; t) &= 43t^6 + 89t^5 + 97t^4 + 52t^3 + 149t^2 + 132t + 1 \\ &= (t+76)(t+78)(t+92)(t+127)(t^2+65t+74) \end{aligned} \tag{44}$$

in characteristic 163, so the supersingular points mod 163 are $0, 1$, and the roots of (44) in $\mathbf{F}_{163^2}$.

3.4 CM points on $\mathcal{X}^*(1)$ via $\mathcal{X}_0^*(l)$ and w_l

We noted already that the elliptic points $t = 0, 1, \infty$ on $\mathcal{X}^*(1)$ are CM points, with discriminants $-3, -4, -24$. Using our formulas for $\mathcal{X}_0(l)$ and w_l ($l = 5, 7, 13$) we can obtain fourteen further CM points: three points isogenous to one of the elliptic CM points, and eleven more points cyclically isogenous to themselves. This accounts for all but ten of the 27 rational CM points on $\mathcal{X}^*(1)$. The discriminants of the three new points isogenous to $t = 1$ or $t = \infty$ are determined by the isogenies' degrees. The discriminants of the self-isogenous points can be surmised by testing them for supersingular reduction at small primes: in each case only one discriminant small enough to admit a self-isogeny of that degree has the correct quadratic character at the first few primes, which is then confirmed by extending the test to all primes up to 200.

On $\mathcal{X}_0^*(5)$ the image of $x_5 = \infty$ under w_5 is $-11/60$, which yields the CM point $t = 152881/138240$; likewise from $w_5(0) = 42/55$ we recover the point $421850521/1771561$. These CM points are 5-isogenous with the elliptic points $t = \infty$, $t = 1$ respectively, and thus have discriminants $-3 \cdot 5^2$ and $-4 \cdot 5^2$. Similarly on $\mathcal{X}_0^*(7)$ we have $w_7(\infty) = -9/20$ at which $t = -1073152081/3024000000$, a CM point 7-isogenous with $t = \infty$ and thus of discriminant $-3 \cdot 7^2$.

For each of $l = 5, 7, 13$ the two fixed points of w_l on $\mathcal{X}_0^*(l)$ are rational and yields two new CM points of discriminants $-cl$ for some factors c of 24. For $\mathcal{X}_0^*(5)$ these fixed points are $x_5 = -3/5$ and $x_5 = 7/30$, at which $t = 2312/125$ and $t = 5776/3375$ respectively; these CM points have discriminants $-40, -120$ by the supersingular test. For $\mathcal{X}_0^*(7)$ we find $x_7 = 2$ and $x_7 = -29/10$, and thus $t = -169/27$, $t = -701784/15625$ of discriminants -84, -168 divisible by 7. For $\mathcal{X}_0^*(13)$ the fixed points $x_{13} = 9$, $x_{13} = -4$ yield $t = 6877/15625$ and $t = 27008742384/27680640625$, with discriminants $-52 = 4 \cdot 13$ and $-312 = 24 \cdot 13$.

Each of these new CM points admits an l-isogeny to itself. By solving the equation $t(x_l) = t(w_l(x_l))$ we find the remaining such points; those not accounted for by fixed points of w_l admit two self-isogenies of degree l, and correspond to a quadratic pair of x_l values over $\mathbf{Q}(t)$. As it happens all the t's thus obtained are rational with the exception of a quadratic pair coming from the quartic $167x_{13}^4 - 60x_{13}^3 + 12138x_{13}^2 - 1980x_{13} + 221607 = 0$. Those points are: from $\mathcal{X}_0^*(5)$, the known $t = 1$, $t = -169/25$, and the new $t = -1377/1024$, $t = 3211/1024$ of discriminants -51, -19; from $\mathcal{X}_0^*(7)$, the CM points $t = 0$, $152881/138240$, $3211/1024$, $2312/125$, $6877/15625$ seen already, but also $t = 13689/15625$ of discriminant -132; and from $\mathcal{X}_0^*(13)$, seven of the CM points already known and also the two new values $t = 21250987/16000000$, $15545888/20796875$ of discriminants -43, -88.

3.5 Numerical computation of CM points on $\mathcal{X}^*(1)$

If we could obtain equations for the modular cover of $\mathcal{X}^*(1)$ by the elliptic curve $\mathcal{X}^*(11)$, $\mathcal{X}^*(17)$ or $\mathcal{X}^*(19)$ we could similarly find a few more rational CM points on $\mathcal{X}^*(1)$. But we do not know how to find these covers, let alone the cover $\mathcal{X}^*(l)$ for l large enough to get at the rational CM point of discriminant -163; moreover, some applications may require irrational CM points of even higher discriminants. We thus want a uniform way of computing the CM points of any given discriminant as an algebraic irrationality. We come close to this by finding these points and their algebraic conjugates as real (or, in the irrational case, complex) numbers to high precision, and then using continued fractions to recognize their elementary symmetric functions as rational numbers. We say that this "comes close" to solving the problem because, unlike the case of the classical modular functions such as j, we do not know a priori how much precision is required, since the CM values are generally not integers, nor is an effective bound known on their height. However, even when we cannot prove that our results are correct using an isogeny of low degree, we are quite confident that the rational numbers we exist are correct because they not only match their numerical approximations to many digits but also pass all the supersingularity tests we tried as well as the condition that differences between pairs of CM values are products of small primes as in [GZ].

To do this we must be able to compute numerically the rational function $t : \mathcal{H}/\Gamma^*(1) \xrightarrow{\sim} \mathbf{P}^1$. Equivalently, we need to associate to each $t \in \mathbf{P}^1$ a representative of its corresponding $\Gamma^*(1)$-orbit in $\mathcal{H}$. We noted already that this is done, up to a fractional linear transformation over $\mathbf{C}$, by the quotient of two hypergeometric functions in t. To fix the transformation we need images of three points, and we naturally choose the elliptic points $t = 0, 1, \infty$. These go to fixed points of $s_2, s_4, s_6 \in \Gamma^*(1)$, and to find those fixed points we need an explicit action of $\Gamma^*(1)$ on $\mathcal{H}$.

To obtain such an action we must imbed that group into $\mathrm{Aut}(\mathcal{H}) = \mathrm{PSL}_2(\mathbf{R})$. Equivalently, we must choose an identification of $\mathsf{A} \otimes \mathbf{R}$ with the algebra $M_2(\mathbf{R})$ of 2×2 real matrices. Having done this, to obtain the action of some $g \in \Gamma^*(1) \subset \mathsf{A}^*/\mathbf{Q}^*$ on $\mathcal{H}$ we will choose a representative of g in A^*, identify this representative with an invertible matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of positive determinant, and let g act on $z \in \mathcal{H}$ by $z \mapsto (az+b)/(cz+d)$. Identifying $\mathsf{A} \otimes \mathbf{R}$ with $M_2(\mathbf{R})$ is in turn tantamount to solving (30) in $M_2(\mathbf{R})$.

We choose the following solution:

$$b := \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}, \qquad c := \begin{pmatrix} 0 & \sqrt{3} \\ -\sqrt{3} & 0 \end{pmatrix}. \tag{45}$$

The elliptic points are then the $\Gamma^*(1)$ orbits of the fixed points in the upper half-plane of s_2, s_4, s_6, that is, of

$$P_2 := (1+\sqrt{2})i, \quad P_4 := \frac{1+\sqrt{2}}{\sqrt{3}}(-1+\sqrt{2}\,i), \quad P_6 := i. \tag{46}$$

Thus for $|t| < 1$ the point on $\mathcal{H}/\Gamma^*(1)$ which maps to t is the $\Gamma^*(1)$ orbit of z near P_2 such that

$$(z - P_2)/(z - \bar{P}_2) = F_1(t)/F_2(t) \tag{47}$$

for some solutions F_1, F_2 of the hypergeometric equation (18). Since the fractional linear transformation $z \mapsto (z - P_2)/(z - \bar{P}_2)$ takes the hyperbolic lines $\overline{P_2P_4}$ and $\overline{P_2P_6}$ to straight lines through the origin, F_2 must be a power series in t, and F_1 is such a power series multiplied by $\sqrt{t}$; that is,

$$(z - P_2)/(z - \bar{P}_2) = Ct^{1/2} F\left(\frac{13}{24}, \frac{17}{24}, \frac{3}{2}, t\right) \Big/ F\left(\frac{1}{24}, \frac{5}{24}, \frac{1}{2}, t\right)\right). \tag{48}$$

for some nonzero constant C. We evaluate C by taking $t = 1$ in (48). Then $z = P_4$, which determines the left-hand side, while the identity [GR, 9.122]

$$F(a, b; c; 1) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} \tag{49}$$

gives us the coefficient of C in the right-hand side in terms of gamma functions. We find $C = (.314837\ldots)i/(2.472571\ldots) = (.128545\ldots)i$. Likewise we obtain convergent power series for computing z in neighborhoods of $t = 1$ and $t = \infty$.

Now let D be the discriminant of an order O_D in a quadratic imaginary field $\mathbf{Q}(\sqrt{D})$ such that O_D has a maximal embedding in $\mathcal{O}$ (i.e. an embedding such that $O_D = (O_D \otimes \mathbf{Q}) \cap \mathcal{O}$) and the embedding is unique up to conjugation in $\Gamma^*(1)$. Then there is a unique, and therefore rational, CM point on $\mathcal{X}^*(1)$ of discriminant D. Being rational, the point is real, and thus can be found on one of the three hyperbolic line segments $\overline{P_2P_4}$, $\overline{P_2P_6}$, $\overline{P_4P_6}$. It is thus the fixed point of a positive integer combination, with coprime coefficients, of two of the elliptic elements $s_2 = bc + 2c$, $s_4 = (2+b)(1+c)/2$, $s_6 = (3+c)/2$ with fixed points P_2, P_4, P_6. In each case a short search finds the appropriate linear combination and thus the fixed point z. Using (48) or the analogous formulas near $t = 1$, $t = \infty$ we then solve for t as a real number with sufficient accuracy (60 decimals was more than enough) to recover it as a rational number from its continued-fraction expansion.

3.6 Tables of rational CM points on $\mathcal{X}^*(1)$

There are 27 rational CM points on $\mathcal{X}^*(1)$. We write the discriminant D of each of them as $-D_0D_1$ where $D_0|24$ and D_1 is coprime to 6. In Table 1 we give, for each $|D| = D_0D_1$, the integers A, B with $B \geq 0$ such that $(A : B)$ is the t-coordinate of a CM point of discriminant D. In the last column of this table we indicate whether the point was obtained algebraically (via an isogeny of degree 5, 7, or 13) and thus proved correct, or only computed numerically. The CM points are listed in order of increasing height $\max(|A|, B)$.

Table 1

$\|D\|$	D_0	D_1	A	B	proved?
3	3	1	1	0	Y
4	4	1	1	1	Y
24	24	1	0	1	Y
84	12	7	−169	27	Y
40	8	5	2312	25	Y
51	3	17	−1377	1024	Y
19	1	19	3211	1024	Y
120	24	5	5776	3375	Y
52	4	13	6877	15625	Y
132	12	11	13689	15625	Y
75	3	5^2	152881	138240	Y
168	24	7	−701784	15625	Y
43	1	43	21250987	16000000	Y
228	12	19	66863329	11390625	N
88	8	11	15545888	20796875	Y
123	3	41	−296900721	16000000	N
100	4	5^2	421850521	1771561	Y
147	3	7^2	−1073152081	3024000000	Y
312	24	13	27008742384	27680640625	Y
67	1	67	77903700667	1024000000	N
148	4	37	69630712957	377149515625	N
372	12	31	−455413074649	747377296875	N
408	24	17	−32408609436736	55962140625	N
267	3	89	−5766681714488721	1814078464000000	N
232	8	29	66432278483452232	56413239012828125	N
708	12	59	71475755554842930369	224337327397603890625	N
163	1	163	699690239451360705067	684178814003344000000	N

In Table 2 we give, for each except the first three cases, the factorizations of $|A|, B, |C|$ where $C = A - B$, and also the associated "ABC ratio" [E1] defined by $r = \log N(ABC)/\log\max(|A|, B, |C|)$. As expected, the A, B, C values are "almost" perfect squares, sixth powers, and fourth powers respectively: a prime at which at which the valuation of A, B, C is not divisible by $2, 6, 4$ resp. is either 2, 3, or the unique prime in D_1. When $D_1 > 1$ its unique prime factor is listed at the end of the $|A|$, B, or $|C|$ factorization in which it appears; otherwise the prime factors are listed in increasing order.

Table 2

$\lvert D\rvert$	D_0	D_1	$\lvert A\rvert$	B	$\lvert C\rvert$	r
84	12	7	13^2	3^3	$2^2 7^2$	1.19410
40	8	5	$2^3 17^2$	5^3	3^7	0.80487
51	3	17	$3^4 17$	2^{10}	7^4	0.84419
19	1	19	$13^2 19$	2^{10}	3^7	0.90424
120	24	5	$2^4 19^2$	$3^3 5^3$	7^4	0.95729
52	4	13	$23^2 13$	5^6	$2^2 3^7$	1.00276
132	12	11	$3^4 13^2$	5^6	$2^4 11^2$	0.87817
75	3	5^2	$17^2 23^2$	$2^{10} 3^3 5$	11^4	0.98579
168	24	7	$2^3 3^5 19^2$	5^6	$11^4 7^2$	0.79278
88	8	11	$2^5 17^2 41^2$	$5^6 11^3$	$3^7 7^4$	0.86307
43	1	43	$19^2 37^2 43$	$2^{10} 5^6$	$3^7 7^4$	0.92839
228	12	19	$13^2 17^2 37^2$	$3^6 5^6$	$2^6 7^4 19^2$	0.96018
123	3	41	$3^4 13^2 23^2 41$	$2^{10} 5^6$	$7^4 19^4$	0.90513
100	4	5^2	$19^2 23^2 47^2$	11^6	$2^4 3^7 7^4 5$	0.88998
147	3	7^2	$17^2 41^2 47^2$	$2^{10} 3^3 5^6 7$	$11^4 23^4$	0.96132
312	24	13	$2^4 3^5 17^2 43^2 13$	$5^6 11^6$	$7^4 23^4$	0.83432
67	1	67	$13^2 43^2 61^2 67$	$2^{16} 5^6$	$3^7 7^4 11^4$	0.89267
148	4	37	$13^2 47^2 71^2 37$	$5^6 17^6$	$2^2 3^7 7^4 11^4$	0.94008
372	12	31	$13^2 23^2 37^2 61^2$	$3^3 5^6 11^6$	$2^2 7^4 19^4 31^2$	0.99029
408	24	17	$2^6 13^2 19^2 43^2 67^2$	$3^6 5^6 17^3$	$7^4 11^4 31^4$	0.88352
267	3	89	$3^6 13^2 17^2 19^2 71^2 89$	$2^{16} 5^6 11^6$	$7^4 31^4 43^4$	0.87610
232	8	29	$2^3 13^2 17^2 41^2 89^2 113^2$	$5^6 23^6 29^3$	$3^7 7^4 11^4 19^4$	0.91700
708	12	59	$3^4 13^2 19^2 23^2 37^2 41^2 109^2$	$5^6 17^6 29^6$	$2^8 7^4 11^4 47^4 59^2$	0.91518
163	1	163	$13^2 67^2 109^2 139^2 157^2 163$	$2^{10} 5^6 11^6 17^6$	$3^{11} 7^4 19^4 23^4$	0.90013

In the factorization of the difference between the last two $t = A/B$ values in this table, the primes not accounted for by common factors in the last two rows of the table are 79, 127, 271, 907, 2287, 2971, 3547, each occurring once.

4 The case $\Sigma = \{2, 5\}$

4.1 The quaternion algebra and the curves $\mathcal{X}(1)$, $\mathcal{X}^*(1)$

For this section we let A be the quaternion algebra ramified at $\{2, 5\}$. This time A is generated over $\mathbf{Q}$ by elements b, e satisfying

$$b^2 + 2 = e^2 - 5 = be + eb = 0, \tag{50}$$

and the conjugate and norm of an element $\alpha = \alpha_1 + \alpha_2 b + \alpha_3 e + \alpha_4 be \in \mathsf{A}$ are

$$\bar{\alpha} = \alpha_1 - \alpha_2 b - \alpha_3 e - \alpha_4 be, \quad \alpha\bar{\alpha} = \bar{\alpha}\alpha = \alpha_1^2 + 2\alpha_2^2 - 5\alpha_3^2 - 10\alpha_4^2. \tag{51}$$

The elements b and $(1+e)/2$ generate a maximal order, which we use for $\mathcal{O}$.

By (9), the curve $\mathcal{X}^*(1)$ has hyperbolic area $1/6$. Since the algebra A is not among the nineteen algebras listed in [T] that produce arithmetic triangle groups, $\mathcal{X}^*(1)$ must have at least four elliptic points. On the other hand, by (10) a curve of area as small as $1/6$ cannot have more than four elliptic points, and if it has exactly four then their orders must be $2, 2, 2, 3$. Indeed we find in $\Gamma^*(1)$ the elements of finite order

$$s_2 = [b], s_2' = [2e + 5b - be], s_2'' = [5b - be], s_3 = [2b - e - 1] \tag{52}$$

[NB $2e + 5b - be, 5b - be, 2b - e - 1 \in 2\mathcal{O}$] of orders $2, 2, 2, 3$ with $s_2 s_2' s_2'' s_3 = 1$. As in the case of the $G_{2,4,6}$ we conclude that here $\Gamma^*(1)$ has the presentation

$$\langle s_2, s_2', s_2'', s_3 | s_2^2 = {s_2'}^2 = {s_2''}^2 = s_3^3 = s_2 s_2' s_2'' s_3 = 1 \rangle. \tag{53}$$

Of the four generators only s_3 is in $\Gamma(1)$; thus the $(\mathbf{Z}/2)^2$ cover $\mathcal{X}(1)/\mathcal{X}^*(1)$ is ramified at the elliptic points of order 2. Therefore $\mathcal{X}(1)$ is a rational curve with four elliptic points of order 3, and $\Gamma^(1)$ is generated by four 3-cycles whose product is the identity, for example by s_3 and its conjugates by s_2, s_2', s_2''. (The genus and number of elliptic points of $\mathcal{X}(1), \mathcal{X}^*(1)$, but not the generators of $\Gamma(1), \Gamma^*(1)$, are already tabulated in [V, Ch.IV:2].)

4.2 Shimura modular curves $\mathcal{X}_0^*(l)$, in particular $\mathcal{X}_0^*(3)$

The elliptic elements s_3, s_2, s_2', s_2'' have discriminants $-3, -8, -20, -40$. Thus the curve $\mathcal{X}_0^*(l)$ has genus

$$g(\mathcal{X}_0^*(l)) = \frac{1}{12}\left[l - 4\left(\frac{-3}{l}\right) - 3\left(\frac{-2}{l}\right) - 3\left(\frac{-5}{l}\right) - 3\left(\frac{-10}{l}\right)\right]. \tag{54}$$

Again we tabulate this for $l < 50$:

l	3	7	11	13	17	19	23	29	31	37	41	43	47
$g(\mathcal{X}_0^*(l))$	0	0	1	1	2	1	2	3	3	3	3	3	4

Since $g(\mathcal{X}_0^*(l)) \geq (l - 13)/12$, the cases $l = 3, 7$ of genus 0 occurring in this table are the only ones. We next find an explicit rational functions of degree 4 on $\mathbf{P}^1$ that realizes the cover $\mathcal{X}_0^*(3)/\mathcal{X}_0^*(1)$, and determine the involution w_3.

The curve $\mathcal{X}_0^*(3)$ is a degree-4 cover of $\mathcal{X}^*(1)$ with Galois group $\mathrm{PGL}_2(\mathbf{F}_3)$ and cycle structures 31, 211, 211, 22 over the elliptic points P_3, P_2, P_2', P_2''. Thus there are coordinates τ, x on $\mathcal{X}^*(1)$, $\mathcal{X}_0^*(3)$ such that $\tau(x) = (x^2 - c)^2/(x-1)^3$ for some c. To determine the parameter c, we use the fact that w_3 fixes the simple pole $x = \infty$ and takes each simple preimage of the 211 points P_2, P_2' to the other simple preimage of the same point. That is,

$$(x^2 - c)^{-1}(x-1)^4 \frac{dx}{dt} = x^2 - 4x + 3c \tag{55}$$

must have distinct roots x_i $(i = 1, 2)$ that yield quadratic polynomials

$$\frac{(x-1)^3(\tau(x) - \tau(x_i))}{(x - x_i)^2} \tag{56}$$

with the same x coefficient. We find that this happens only for $c = -5/3$, i.e. that $\tau = (3x^2 + 5)^2/9(x-1)^3$. For future use it will prove convenient to use

$$t = \frac{6^3}{9\tau + 8} = \frac{(6x-6)^3}{(x+1)^2(9x^2 - 10x + 7)}, \tag{57}$$

with $w_3(x) = \frac{10}{9} - x$. [Smaller coefficients can be obtained by letting $x = 1 + 2/x'$, $\tau = 2t'/9$, when $t' = (2x'^2 + 3x' + 3)^2/x'$ and $w_3(x') = -9x'/(4x' + 9)$. But our choice of x will simplify the computation of the Schwarzian equation, while the choice of t will turn out to be the correct one 3-adically.] The elliptic points are then $P_6 : t = 0$, $P_2'' : t = 27$, and $P_2, P_2' : t = \infty, 2$. In fact the information so far does not exclude the possibility that the pole of t might be at P_2' instead of P_2; that in fact $t(P_2) = \infty, t(P_2') = 2$ and not the other way around can be seen from the order of the elliptic points on the real locus of $\mathcal{X}^*(1)$, or (once we compute the Schwarzian equation) checked using the supersingular test.

4.3 CM points on $\mathcal{X}^*(1)$ via $\mathcal{X}_0^*(3)$ and w_3

From w_3 we obtain five further CM points. Three of these are 3-isogenous to known elliptic points: w_3 takes the triple zero $x = 1$ of t to $x = 1/9$, which gives us $t = -192/25$, the point 3-isogenous to P_3 with discriminant -27; likewise w_3 takes the double root $x = 5$ and double pole $x = -1$ of $t - 2$ to $x = -35/9, 19/9$ and thus to $t = -2662/169$ and $t = 125/147$, the points 3-isogenous to $t = 2$ and $t = \infty$ and thus (once these points are identified with P_2' and P_2) of discriminants -180 and -72. One new CM point comes from the other fixed point $x = 5/9$ of w_3, which yields $t = -27/49$ of discriminant -120. Finally the remaining solutions of $t(x) = t(w_3(x))$ are the roots of $9x^2 - 10x + 65$; the resulting CM point $t = 64/7$, with two 3-isogenies to itself, turns out to have discriminant -35.

4.4 The Schwarzian equation on $\mathcal{X}^*(1)$

We can take the Schwarzian equation on $\mathcal{X}^*(1)$ to be of the form

$$t(t-2)(t-27)f'' + (At^2 + Bt + C)f' + (Dt + E) = 0. \tag{58}$$

The coefficients A, B, C, D are then forced by the indices of the elliptic points. Near $t = 0$, the solutions of (58) must be generated by functions with leading terms 1 and $t^{1/3}$; near $t = 2$ ($t = 27$), by functions with leading terms 1 and $(t-2)^{1/2}$ (resp. $(t-27)^{1/2}$); and at infinity, by functions with leading terms t^{-e} and $t^{-e-1/2}$ for some e. The conditions at the three finite singular points $t = 0, 2, 27$ determine the value of the f' coefficient at those points, and thus yield A, B, C, which turn out to be $5/3, -203/6, 36$. Then $e, e + 1/2$ must be roots of an "indicial equation" $e^2 - 2e/3 + D = 0$, so $e = 1/12$ and $D = 7/144$.

Thus (58) becomes

$$t(t-2)(t-27)f'' + \frac{10t^2 - 203t + 216}{6} f' + (\frac{7t}{144} + E) = 0. \tag{59}$$

To determine the "accessory parameter" E, we again use the cover $\mathcal{X}_0^*(3)/\mathcal{X}^*(1)$ and the involution w_3. A Schwarzian equation for $\mathcal{X}_0^*(3)$ is obtained by substituting $t = (6x-6)^3/(x+1)^2(9x^2 - 10x + 17)$ in (59). The resulting equation will not yet display the w_3 symmetry, because it will have a spurious singular point at the double pole $x = -1$ of $t(x)$. To remove this singularity we consider not $f(t(x))$ but

$$g(x) := (x+1)^{-1/6} f(t(x)). \tag{60}$$

The factor $(x+1)^{-1/6}$ is also singular at $x = \infty$, but that is already an elliptic point of $\mathcal{X}_0^*(3)$ and a fixed point of w_3. Let $x = u + 5/9$, so w_3 is simply $u \leftrightarrow -u$. Then we find that the differential equation satisfied by g is

$$\begin{aligned} &4(81u^2+20)(81u^2+128)^2 g'' + 108u(81u^2+128)(405u^2+424)g' \\ &+(3^{11}u^4 - 163296u^2 + 170496 + 72(18E+7)(9u-4)(81u^2+128))g = 0. \end{aligned} \tag{61}$$

Clearly this has the desired symmetry if and only if $18E + 7 = 0$. Thus the Schwarzian equation is

$$t(t-2)(t-27)f'' + \frac{10t^2 - 203t + 216}{6} f' + (\frac{7t}{144} - \frac{7}{18}) = 0. \tag{62}$$

4.5 Numerical computation of CM points on $\mathcal{X}^*(1)$

We can now expand a basis of solutions of (62) in power series about each singular point $t = 0, 2, 27, \infty$ (using inverse powers of $t - \frac{27}{2}$ for the expansion about ∞ to assure convergence for real $t \notin [0, 27]$). As with the $\Sigma = \{2, 3\}$ case we need to identify $\mathsf{A} \otimes \mathbf{R}$ with $M_2(\mathbf{R})$, and use the solution

$$b := \begin{pmatrix} 0 & \sqrt{2} \\ -\sqrt{2} & 0 \end{pmatrix}, \qquad e := \begin{pmatrix} \sqrt{5} & 0 \\ 0 & -\sqrt{5} \end{pmatrix}. \tag{63}$$

of (50), analogous to (30). We want to proceed as we did for $\Sigma = \{2, 3\}$, but there is still one obstacle to computing, for given $t_0 \in \mathbf{R}$, the point on the hyperbolic quadrilateral formed by the fixed points of s_2, s_2', s_2'', s_3 at which $t = t_0$. In the $\Sigma = \{2, 3\}$ case, the solutions of the Schwarzian equation were combinations of hypergeometric functions, whose value at 1 is known. This let us determine two solutions whose ratio gives the desired map to $\mathcal{H}$. But here $\Gamma^*(1)$ is not a triangle group, so our basic solutions of (62 are more complicated power series and we do not know a priori their values at the neighboring singular points. In general this obstacle can be overcome by noting that for each nonsingular $t_0 \in \mathbf{R}$ its image in $\mathcal{H}$ can be computed from the power-series expansions about either of its neighbors and using the condition that the two computations agree for several choices of t_0 to determine the maps to $\mathcal{H}$. In our case we instead removed the obstacle using the non-elliptic CM points computed in the previous section. For example, we used the fact that $t_0 = 125/147$ is the CM point of discriminant 72, and thus maps to the unique fixed point in $\mathcal{H}$ of $(9b + 4e - be)/2$, to determine the correct ratio of power series about $t = 0$ and $t = 2$. Two or three such points suffice to determine the four ratios needed to compute our map $\mathbf{R} \to \mathcal{H}$ to arbitrary accuracy; since we actually had five non-elliptic CM points, we used the extra points for consistency checks, and then used the resulting formulas to numerically compute the t-coordinates of the remaining CM points.

There are 21 rational CM points on $\mathcal{X}^*(1)$. We write the discriminant D of each of them as $-D_0 D_1$ where $D_0|40$ and D_1 is coprime to 10. Table 3 is organized in the same way as Table 1: we give, for each $|D| = D_0 D_1$, the integers A, B with $B \geq 0$ such that $(A : B)$ is the t-coordinate of a CM point of discriminant D. The last column identifies with a "Y" the nine points obtained algebraically from the computation of $\mathcal{X}_0^*(3)$ and w_3. Some but not all of the remaining twelve points would move from "N" to "Y" if we also had the equations for the degree-8 map $\mathcal{X}_0^*(7) \to \mathcal{X}^*(1)$ and the involution w_7 on $\mathcal{X}_0^*(7)$.

Table 3

$\lvert D\rvert$	D_0	D_1	A	B	proved?
3	1	1	0	1	Y
8	8	1	1	0	Y
20	20	1	2	1	Y
40	40	1	27	1	Y
52	4	13	-54	25	N
120	40	3	-27	49	Y
35	5	7	64	7	Y
27	1	3^3	-192	25	Y
72	8	3^2	125	147	Y
43	1	43	1728	1225	N
180	20	3^2	-2662	169	Y
88	8	11	3375	98	N
115	5	23	13824	3887	N
280	40	7	35937	7406	N
67	1	67	-216000	8281	N
148	4	37	71874	207025	N
340	20	17	657018	41209	N
520	40	13	658503	11257064	N
232	8	29	176558481	2592100	N
760	40	19	13772224773	237375649	N
163	1	163	-2299968000	6692712481	N

It will be seen that the factor 3^3 in our normalization (57) of t was needed[7] to make t a good coordinate 3-adically: 3 splits in the CM field iff t is not a multiple of 3.

[7] On the other hand the factor 2^3 in (57) was a matter of convenience, to make the four elliptic points integral.

In Table 4 we give the factorizations of $|A|, B, |A-2B|, |A-27B|$; as expected, $|A|$ is always "almost" a perfect cube, and $B, |A-2B|, |A-27B|$ "almost" a perfect square, any exceptional primes other than 2 or 5 being the unique prime in D_1, which if it occurs is listed at the end of its respective factorization.

Table 4

$\lvert D\rvert$	D_0	D_1	$\lvert A\rvert$	B	$\lvert A-2B\rvert$	$\lvert A-27B\rvert$
3	1	1	0	1	2	3^3
8	8	1	1	0	1	1
20	20	1	2	1	0	5^2
40	40	1	3^3	1	5^2	0
52	4	13	$2\cdot 3^3$	5^2	$2^3 13$	3^6
120	40	3	3^3	7^2	5^3	$2\cdot 3^3 5^2$
35	5	7	2^6	7	$2\cdot 5^2$	5^3
27	1	3^3	$2^6 3$	5^2	$2\cdot 11^2$	$17^2 3$
72	8	3^2	5^3	$7^2 3$	13^2	$2^2 31^2$
43	1	43	$2^6 3^3$	$5^2 7^2$	$2\cdot 19^2$	$3^6 43$
180	20	3^2	$2\cdot 11^3$	13^2	$2^3 5^3 3$	$5^2 17^2$
88	8	11	$3^3 5^3$	$2\cdot 7^2$	$17^2 11$	3^6
115	5	23	$2^9 3^3$	$13^2 23$	$2\cdot 5^2 11^2$	$3^6 5^3$
280	40	7	$3^3 11^3$	$2\cdot 23^2 7$	$5^3 13^2$	$3^8 5^2$
67	1	67	$2^6 3^3 5^3$	$7^2 13^2$	$2\cdot 11^2 31^2$	$3^8 67$
148	4	37	$2\cdot 3^3 11^3$	$5^2 7^2 13^2$	$2^5 17^2 37$	$3^8 29^2$
340	20	17	$2\cdot 3^3 23^3$	$7^2 29^2$	$2^3 5^2 13^2 7$	$3^6 5^4$
520	40	13	$3^3 29^3$	$2^3 7^2 47^2 13$	$5^4 11^2 17^2$	$3^8 5^2 43$
232	8	29	$3^3 11^3 17^3$	$2^2 5^2 7^2 23^2$	$13^2 19^2 53^2$	$3^6 71^2 29$
760	40	19	$3^3 17^3 47^3$	$7^2 31^2 71^2$	$5^2 11^2 13^2 37^2 19$	$2\cdot 3^8 5^3 67^2$
163	1	163	$2^9 3^3 5^3 11^3$	$7^2 13^2 29^2 31^2$	$2\cdot 19^2 59^2 79^2$	$3^6 17^2 73^2 163$

5 Further examples and problems

Our treatment here is briefer because most of the ideas and methods of the previous sections apply here with little change. Thus we only describe new features that did not arise for the algebras ramified at $\{2,3\}$ and $\{2,5\}$, and exhibit the final results of our computations of modular curves and CM points.

5.1 The case $\Sigma = \{2,7\}$

We generate A by elements b, g with

$$b^2 + 2 = g^2 - 7 = bg + gb = 0, \tag{64}$$

and a maximal order $\mathcal{O}$ by $\mathbf{Z}[b,g]$ together with $(1+b+g)/2$ (and $b(1+g)/2$). By (9), the curve $\mathcal{X}^*(1)$ has hyperbolic area $1/4$. Since $\Gamma^*(1)$ is not a triangle group (again by [T]), we again conclude by (10) that $\mathcal{X}^*(1)$ has exactly four elliptic points, this time of orders $2, 2, 2, 4$. We find in $\Gamma^*(1)$ the elements of finite order

$$s_2 = [b], s_2' = [7b - 2g - bg], s_2'' = [7b + 2g - bg], s_4 = [1 + 2b + g] \qquad (65)$$

[NB $7b \pm 2g - bg \in 2\mathcal{O}$] of orders $2, 2, 2, 4$ with $s_2 s_2' s_2'' s_4 = 1$, and conclude that s_2, s_2', s_2'', s_4 generate $\Gamma^*(1)$ with relations determined by $s_2^2 = {s_2'}^2 = {s_2''}^2 = s_4^4 = s_2 s_2' s_2'' s_4 = 1$. None of these is in $\Gamma^*(1)$: the representatives $b, 1 + 2b + g$ of s_2, s_4 have norm 2, while s_2', s_2'' have representatives $(7b \pm 2g - bg)/2$ of norm 14. The discriminants of s_4, s_2, s_2', s_2'' are $-4, -8, -56, -56$; note that -56 is *not* among the "idoneal" discriminants (discriminants of imaginary quadratic fields with class group $(\mathbf{Z}/2)^r$), and thus that the elliptic fixed points P_2', P_2'' of s_2', s_2'' are quadratic conjugates on $\mathcal{X}^*(1)$.

Again we use the involution w_3 on the modular curve $\mathcal{X}_0^*(3)$ to simultaneously determine the relative position of the elliptic points P_4, P_2, P_2', P_2'' on $\mathcal{X}^*(1)$ and the modular cover $\mathcal{X}_0^*(3) \to \mathcal{X}^*(1)$, and then to obtain a Schwarzian equation on $\mathcal{X}^*(1)$. Clearly P_4 is completely ramified in $\mathcal{X}_0^*(3)$. Since -8 and -56 are quadratic residues of 3, each of P_2, P_2', P_2'' has ramification type 211. Thus $\mathcal{X}_0^*(3)$ is a rational curve with six elliptic points all of index 2, and we may choose coordinates t, x on $\mathcal{X}^*(1), \mathcal{X}_0^*(3)$ such that $t(P_4) = \infty$, $t(P_2) = 0$, and $x = \infty$, $x = 0$ at the quadruple pole and double zero respectively of t.

We next determine the action of w_3 on the elliptic points of $\mathcal{X}_0^*(3)$. Necessarily the simple preimages of P_2 parametrize two 3-isogenies from P_2 to itself. On the other hand the simple preimages of P_2' parametrize two 3-isogenies from that point to P_2'' and vice versa, because the squares of the primes above 3 in $\mathbf{Q}(\sqrt{-14})$ are not principal. Therefore w_3 exchanges the simple preimages of P_2 but takes each of the two simple points above P_2' to one above P_2'' and vice versa.

So again we have a one-parameter family of degree-4 functions on $\mathbf{P}^1$, and a single condition in the existence of the involution w_3; but this time it turns out that there are (up to scaling the coordinates t, x) two ways to satisfy this condition:

$$t = \frac{1}{3}(x^4 + 4x^3 + 6x^2), \quad w_3(x) = \frac{1 - x}{1 + x}, \quad P_2', P_2'' : t^2 - 3t + 3 = 0 \qquad (66)$$

and

$$t = \frac{1}{27}(x^4 + 2x^3 + 9x^2), \quad w_3(x) = \frac{5 - 2x}{2 + x}, \quad P_2', P_2'' : 16t^2 + 13t + 8 = 0. \quad (67)$$

How to choose the correct one? We could consider the next modular curve $\mathcal{X}_0^*(5)$ and its involution to obtain a new condition that would be satisfied by only one of (66,67). Fortunately we can circumvent this laborious calculation by noting that the Fuchsian group associated with (66) is commensurable with a triangle group, since its three elliptic points of index 2 are the roots of $(1 - t)^3 = 1$ and are thus permuted by a 3-cycle that fixes the fourth elliptic point $t = \infty$. The quotient by that 3-cycle is a curve parametrized by $(1 - t)^3$ with elliptic points of order $2, 3, 12$ at $1, 0, \infty$. But by [T] there is no triangle group commensurable with an arithmetic subgroup of $\mathsf{A}^*/\mathbf{Q}^*$; indeed we find there that $G_{2,3,12}$ is associated with the quaternion algebra over $\mathbf{Q}(\sqrt{3})$ ramified at the prime above 2 and at one of the infinite places of that number field.[8] Therefore (67) is the correct choice. Alternatively, we could have noticed that since $\mathcal{X}(1)$ is a $(\mathbf{Z}/2)^2$ cover of $\mathcal{X}^*(1)$ ramified at all four elliptic points, it has genus 1, and then used the condition that this curve's Jacobian have conductor 14 to exclude (66). The function field of $\mathcal{X}^*(1)$ is obtained by adjoining square roots of $c_0 t$ and $c_1(16t^2+13t+8)$ for some c_0, c_1; for the Jacobian to have the correct conductor we must have $c_0 c_1 = 1$ mod squares. The double cover of $\mathcal{X}_0^*(3)$ obtained by adjoining $\sqrt{c_1(16t^2+13t+8)}$ also has genus 1, and so must have Jacobian of conductor at most 42; this happens only when $c_1 = -1$ mod squares, the Jacobian being the elliptic curve 42-A3 (42C). The curve $\mathcal{X}(1)$ then has the equation

$$y^2 = -16s^4 + 13s^2 - 8 \qquad (t = -s^2), \tag{68}$$

and its Jacobian is the elliptic curve 14-A2 (14D). Kurihara had already obtained in [Ku] an equation birational with (68). Let $\Gamma_0'(3^r)$ be the group intermediate between $\Gamma_0(3^r)$ and $\Gamma_0^*(3^r)$ consisting of the elements of norm 1 or 7 mod $\mathbf{Q}^{*2}$. Then the corresponding curves $\mathcal{X}_0'(3^r)$ $(r > 0)$ of genus $3^{r-1}+1$ are obtained from $\mathcal{X}_0^*(3^r)$ by extracting a square root of $t(16t^2+13t+8)$, and constitute an unramified tower of curves over the genus-2 curve

$$\mathcal{X}_0'(3) : y^2 = 3(4x^6 + 12x^5 + 75x^4 + 50x^3 + 255x^2 - 288x + 648) \tag{69}$$

whose reductions are asymptotically optimal over $\mathbf{F}_{l^2}$ $(l \neq 2,3,7)$ with each step in the tower being a cyclic cubic extension. (Of course when we consider only reductions to curves over $\mathbf{F}_{l^2}$ the factor of 3 in (69) may be suppressed.)

Using w_3 we may again find the coordinates of several non-elliptic CM points: $t = 4/3$ and $t = 75/16$ of discriminants -36 and -72, i.e. the points 3-isogenous to P_4 and P_2, other than P_4, P_2 themselves; $t = 4/9$ and $t = 200/9$ of discriminants -84 and -168, coming from the fixed points $x = 1$ and $x = -5$ of w_3; and the points $t = -1$, $t = -5$ of discriminants -11 and -35, coming from the remaining solutions of $t(x) = t(w_3(x))$ and each with two 3-isogenies to itself.

Even once the relative position of the elliptic points are known, the computation of the cover $\mathcal{X}_0^*(5)/\mathcal{X}^*(1)$ is not a trivial matter; I thank Peter Müller for performing this computation using J.-C. Faugere's Gröbner basis package GB. It turns out that there are eight $\mathrm{PGL}_2(\mathbf{F}_5)$ covers consistent with the ramification of which only one is defined over $\mathbf{Q}$:

$$t = -\frac{(256x^3 + 224x^2 + 232x + 217)^2}{50000(x^2+1)}, \quad w_5(x) = \frac{24 - 7x}{7 + 24x}. \tag{70}$$

[8] See [T], table 3, row IV. In terms of that algebra A', the triangle group $G_{2,3,12}$ is $\Gamma^*(1)$; the index-3 normal subgroup whose quotient curve is parametrized by the t of (66) is the normalized in $\Gamma^*(1)$ of $\{[a] \in \mathcal{O}^*/\{\pm 1\} : a \equiv 1 \bmod I_2\}$; and the intersection of this group with $\Gamma_0^*(3)$ yields as quotient curve the $\mathbf{P}^1$ with coordinate x.

This yields the CM points of discriminants -11, -35, -36, -84 already known from w_3, and new points of discriminants -91, -100, -280.

This accounts for eleven of the nineteen rational CM points on $\mathcal{X}^*(1)$; the remaining ones were computed numerically as we did for the $\Sigma = \{2, 5\}$ curve. We used the Schwarzian equation

$$t(16t^2 + 13t + 8)f'' + (24t^2 + 13t + 4)f' + \left(\frac{3}{4}t + \frac{3}{16}\right) f = 0, \tag{71}$$

for which the "accessory parameter" $3/16$ was again determined by pulling back to $\mathcal{X}_0^*(3)$ and imposing the condition of symmetry under w_3. We tabulate the coordinates $t = A/B$ and factorizations for all nineteen points:

Table 5

$\lvert D\rvert$	D_0	D_1	A	B	$16A^2 + 13AB + 8B^2$
4	4	1	1	0	2^4
8	8	1	0	1	2^3
11	1	11	-1	1	11
35	7	5	-5	1	7^3
36	4	3^2	$4 = 2^2$	3	$2^2 11^2$
84	28	3	$4 = 2^2$	$9 = 3^2$	$2^2 7^3$
72	8	3^2	$75 = 5^2 3$	$16 = 2^4$	$2^7 29^2$
91	7	13	-13	$81 = 3^4$	$7^3 11^2$
43	1	43	$-25 = -5^2$	$81 = 3^4$	$29^2 43$
168	56	3	$200 = 2^3 5^2$	$9 = 3^2$	$2^4 7^3 11^2$
88	8	11	$-200 = -2^3 5^2$	$81 = 3^4$	$2^5 37^2 11$
100	4	5^2	$-196 = -2^2 7^2$	$405 = 3^4 5$	$2^2 11^2 43^2$
67	1	67	$-1225 = -5^2 7^2$	$81 = 3^4$	$11^2 53^2 67$
280	56	5	$-845 = -13^2 5$	$1296 = 2^4 3^4$	$2^8 7^3 11^2$
148	4	37	$1225 = 5^2 7^2$	$5184 = 2^6 3^4$	$2^4 11^2 67^2 37$
532	28	19	$96100 = 2^2 5^2 31^2$	$29241 = 3^4 19^2$	$2^2 7^3 11^2 29^2 37^2$
232	8	29	$135200 = 2^5 5^2 13^2$	$194481 = 3^4 7^4$	$2^3 11^2 53^2 109^2 29$
427	7	61	$-3368725 = -5^2 47^2 61$	$6561 = 3^8$	$7^3 11^2 29^2 43^2 53^2$
163	1	163	$-2235025 = -5^2 13^2 23^2$	$1185921 = 3^4 11^4$	$37^2 107^2 149^2 163$

We see that t is also a good coordinate 3-adically: a point of $\mathcal{X}^*(1)$ is supersingular at 3 iff the denominator of its t-coordinate is a multiple of 3. (It is supersingular at 5 iff $5|t$.)

5.2 The case $\Sigma = \{3, 5\}$

Here the area of $\mathcal{X}^*(1)$ is $1/3$. This again is small enough to show that there are only four elliptic points, but leaves two possibilities for their indices: 2,2,2,6 or 2,2,3,3. It turns out that the first of these is correct. This fact is contained in the table of [V, Ch.IV:2]; it can also be checked as we did in the cases $\Sigma = \{2, p\}$ ($p = 3, 5, 7$) by exhibiting appropriate elliptic elements of $\Gamma^*(1)$ — which we need to do anyway to compute the CM points. We chose to write write $\mathcal{O} = \mathbf{Z}[\frac{1}{2}1+c,e]$ with

$$c^2+3 = e^2-5 = ce+ec = 0, \tag{72}$$

and found the elliptic elements

$$s_2 = [4c-3e], s_2' = [5c-3e-ce], s_2'' = [20c-9e-7ce], s_6 = [3+c] \tag{73}$$

[NB $20c-9e-7ce, 3+c \in 2\mathcal{O}$] of orders $2,2,2,6$ with $s_2s_2's_2''s_6 = 1$. The corresponding elliptic points P_2 , P_2', P_2'', P_6 have CM discriminants $-3,-12,-15,-60$. For the first time we have a curve $\mathcal{X}_0^*(2)$, and here it turns out that the elliptic points P_2' is not ramified in the cover $\mathcal{X}_0^*(2)/\mathcal{X}^*(1)$: it admits two 2-isogenies to itself, and one to P''. Of the remaining elliptic points, P_6 is complete ramified, and each of P_2, P_2'' has one simple and one double preimage. So we may choose coordinates x,t on $\mathcal{X}_0^*(2)$ and $\mathcal{X}^*(1)$ such that $t = x(x-3)^2/4$, with $t(P_6) = \infty$, $t(P_2) = 0$, $t(P_2'') = 1$. To determine $t(P_2')$ we use the involution w_2, which switches $x = \infty$ (the triple pole) with $x = 0$ (the simple zero), $x = 4$ (the simple preimage of P_2'') with one of the preimages x_1 of P_2' (the one parametrizing the isogeny from P_2' to P_2''), and the other two preimages of P_2' with each other. Then w_2 is $x \leftrightarrow 4x_1/x$, so the product of the roots of $(t(x_1)-t(x))/(x-x_1)$ is $4x_1$. Thus

$$x(x-3)^2 - 4t(P_2') = (x-x_1)(x^2+ax+4x_1) \tag{74}$$

for some a. Equating x^2 coefficients yields $a = x_1 - 6$, and equating the coefficients of x we find $9 = 10x_1 - x_1^2$. Thus $x_1 = 1$ or $x_1 = 9$; but the first would give us $t(P_2') = 1 = t(P_2'')$ which is impossible. Thus $x_1 = 9$ and $t(P_2') = 81$, with $w_2(x) = 36/x$. This lets us find six further rational CM points, of discriminants $-7,-28,-40,-48,-120,-240$; we can also solve for the accessory parameter $-1/2$ in the Schwarzian equation

$$t(t-1)(t-81)f'' + \left(\frac{3}{2}t^2 - 82t + \frac{81}{2}\right) f' + \left(\frac{1}{18}t - \frac{1}{2}\right) f = 0, \tag{75}$$

and use it to compute the remaining twelve rational CM points numerically. We tabulate the coordinates $t = A/B$ and factorizations for the twenty-two rational

CM points on $\mathcal{X}^*(1)$:

Table 6

$\lvert D\rvert$	D_0	D_1	A	B	$A-B$	$81B-A$
3	3	1	1	0	1	-1
12	3	2^2	0	1	-1	3^4
60	15	2^2	1	1	0	$2^4 5$
15	15	1	$81=3^4$	1	$2^4 5$	0
7	1	7	$-27=-3^3$	1	$-2^2 7$	$2^2 3^3$
40	5	2^3	$27=3^3$	2	5^2	$3^3 5$
43	1	43	$-27=-3^3$	$16=2^4$	-43	$3^3 7^2$
195	15	13	$81=3^4$	$16=2^4$	$5\cdot 13$	$3^3 5$
48	3	2^4	$243=3^5$	1	$11^2 2$	$-3^4 2$
120	15	2^3	$-243=-3^5$	2	$-7^2 5$	$3^4 5$
28	1	$2^2 7$	$-675=-3^3 5^2$	1	$-2^2 13^2$	$2^2 3^3 7$
115	5	23	$621=3^3 23$	$16=2^4$	$11^2 5$	$3^3 5^2$
147	3	7^2	$-729=-3^6$	$112=2^4 7$	-29^2	$3^4 11^2$
123	3	41	$2025=3^4 5^2$	$16=2^4$	$7^2 41$	-3^6
67	1	67	$-3267=-3^3 11^2$	$16=2^4$	$-7^2 67$	$3^3 13^2$
240	15	2^4	$9801=3^4 11^2$	1	$2^3 5^2 7^2$	$-2^3 3^5 5$
267	3	89	$7225=5^2 17^2$	$16=2^4$	$3^4 89$	$-7^2 11^2$
435	15	29	$21141=3^6 29$	$16=2^4$	$5^3 13^2$	$-3^4 5\cdot 7^2$
795	15	53	$-6413=-11^2 53$	$432=2^4 3^3$	$-5\cdot 37^2$	$5\cdot 7^2 13^2$
235	5	47	$1269=3^3 47$	$1024=2^{10}$	$5\cdot 7^2$	$3^3 5^2 11^2$
555	15	37	$23409=3^4 17^2$	$1024=2^{10}$	$5\cdot 11^2 37$	$3^5 5\cdot 7^2$
163	1	163	$-1728243=-3^3 11^2 23^2$	$1024=2^{10}$	$-103^2 163$	$3^3 7^2 37^2$

An equivalent coordinate that is also good 2-adically is $(t-1)/4$, which is supersingular at 2 iff its denominator is even.

The elliptic curve $\mathcal{X}(1)$ is obtained from $\mathcal{X}^*(1)$ by extracting square roots of At and $B(t-1)(t-81)$ for some $A, B \in \mathbf{Q}^*/\mathbf{Q}^{*2}$. Using the condition that the Jacobian of $\mathcal{X}(1)$, and any elliptic curve occurring in the Jacobian of $\mathcal{X}_0(2)$, have conductor at most 15 and 30 respectively, we find $A=B=-3$. Then $\mathcal{X}(1)$ has equation

$$y^2 = -(3s^2+1)(s^2+27) \tag{76}$$

(with $t=-3s^2$) and Jacobian isomorphic with elliptic curve 15C (15-A1); the curve intermediate between $\mathcal{X}^*(2)$ and $\mathcal{X}_0(2)$ whose function field is obtained from $\mathbf{Q}(\mathcal{X}^*(2))$ by adjoining $\sqrt{-3(t-1)(t-81)}$ has equation

$$y^2 = -3(x^4 - 10x^3 + 33x^2 - 360x + 1296) \tag{77}$$

and Jacobian 30C (30-A3). Fundamental domains for $\Gamma^*(1)$ and $\Gamma(1)$, computed by Michon [Mi] and drawn by C. Léger, can be found in [V, pp.123–127]; an equation for $\mathcal{X}(1)$ birational with (76) is reported in the table of [JL, p.235].

5.3 The triangle group $G_{2,3,7}$ as an arithmetic group

It is well-known that the minimal quotient area of a discrete subgroup of $\mathrm{Aut}(\mathcal{H}) = \mathrm{PSL}_2(\mathbf{R})$ is $1/42$, attained only by the triangle group $G_{2,3,7}$, and that the Riemann surfaces $\mathcal{H}/\Gamma$ with Γ a proper normal subgroup of finite index in $G_{2,3,7}$ are precisely the curves of genus $g > 1$ whose number of automorphisms attains Hurwitz's upper bound $84(g-1)$. Shimura observed in [S2] that this group is arithmetic.[9] Indeed, let K be the totally real cubic field $\mathbf{Q}(\cos 2\pi/7)$ of minimal discriminant 49, and let A be a quaternion algebra over K ramified at two of the three real places and at no finite primes of K. Now for any totally real number field of degree $n > 1$ over $\mathbf{Q}$, and any quaternion algebra over that field ramified at $n-1$ of its real places, the group $\Gamma(1)$ of norm-1 elements of a maximal order embeds as a discrete subgroup of $\mathrm{PSL}_2(\mathbf{R}) = \mathrm{Aut}(\mathcal{H})$, with $\mathcal{H}/\Gamma$ of finite area given by Shimizu's formula

$$\mathrm{Area}(\mathcal{X}(1)) \frac{d_K^{3/2}\zeta_K(2)}{4^{n-1}\pi^{2n}} \prod_{\wp\in\Sigma}(\mathrm{N}\wp - 1) \left[= \frac{(-1)^n}{2^{n-2}}\zeta_K(-1)\prod_{\wp\in\Sigma}(\mathrm{N}\wp - 1)\right] \tag{78}$$

(from which we obtained (8) by taking $K = \mathbf{Q}$). Thus, in our case of $K = \mathbf{Q}(\cos 2\pi/7)$, $\Sigma = \{\infty, \infty'\}$, the area of $\mathcal{H}/\Gamma(1)$ is $1/42$, so $\Gamma(1)$ must be isomorphic with $G_{2,3,7}$. From this Shimura deduced [S2, p.83] that for any proper ideal $I \subset O_K$ his curve $\mathcal{X}(I) = \mathcal{H}/\Gamma(I)$ attains the Hurwitz bound. For instance, if I is the prime ideal $\wp_7$ above the totally ramified prime 7 of $\mathbf{Q}$ then $\mathcal{X}(\wp_7)$ is the Klein curve of genus 3 with automorphism group $\mathrm{PSL}_2(\mathbf{F}_7)$ of order 168. The next-smallest example is the ideal $\wp_8$ above the inert prime 2, which yields a curve of genus 7 with automorphism group $[\mathrm{P}]\mathrm{SL}_2(\mathbf{F}_8)$ of order 504. This curve is also described by Shimura as a "known curve", and indeed it first appears in [Fr3]; an equivalent curve was studied in detail only a few years before Shimura by Macbeath [Mac], who does not cite Fricke, and the identification of Macbeath's curve with Fricke's and with Shimura's $\mathcal{X}(\wp_8)$ may first have been observed by Serre in a 24.vii.1990 letter to Abhyankar. At any rate, we obtain towers $\{\mathcal{X}(\wp_7^r)\}_{r>0}$, $\{\mathcal{X}(\wp_8^r)\}_{r>0}$ of unramified abelian extensions which are asymptotically optimal over the quadratic extensions of residue fields[10] of K other than $\mathbf{F}_{49}$ and $\mathbf{F}_{64}$ respectively, which are involved in the class field towers of exponents $7, 2$ of the Klein and Macbeath curves over those fields.

These towers are the Galois closures of the covers of $\mathcal{X}(1)$ by $\mathcal{X}_0(\wp_7^r)$, $\mathcal{X}_0(\wp_8^r)$, which again may be obtained from the curves $\mathcal{X}_0(\wp_7)$, $\mathcal{X}_0(\wp_8)$ together with their involutions. It turns out that these curves both have genus 0 (indeed the corresponding arithmetic subgroups $\Gamma_0(\wp_7)$, $\Gamma_0(\wp_8)$ of $\Gamma(1)$ are the triangle groups $G_{3,3,7}$, $G_{2,7,7}$ in [T, class X]). The cover $\mathcal{X}_0(\wp_7)/\mathcal{X}(1)$ has the same ramification

[9] Actually this fact is due to Fricke [F1, F2], over a century ago; but Fricke could not relate $G_{2,3,7}$ to a quaternion algebra because the arithmetic of quaternion algebras had yet to be developed.

[10] That is, over the fields of size p^2 for primes $p = 7$ or $p \equiv \pm 1 \bmod 7$, and p^6 for other primes p.

data as the degree-8 cover of classical modular curves $\mathrm{X}_0(7)/\mathrm{X}(1)$, and is thus given by the same rational function

$$t = \frac{(x_7^4 - 8x_7^3 - 18x_7^2 - 88x_7 + 1409)^2}{2^{13}3^3(9 - x_7)}$$
$$= 1 + \frac{(x_7^2 - 8x_7 - 5)^3(x_7^2 + 8x_7 + 43)}{2^{13}3^3(9 - x_7)} \tag{79}$$

(with the elliptic points of orders $2, 3, 7$ at $t = 0, 1, \infty$, i.e. t corresponds to $1 - 12^{-3}j$). The involution is different, though: it still switches the two simple zeros $x_7 = -4 \pm \sqrt{-27}$ of $t - 1$, but it takes the simple pole $x_7 = 0$ to itself instead of the septuple pole at $x_7 = \infty$. Using (89) again we find

$$w_{\wp_7}(x_7) = \frac{19x_7 + 711}{13x_7 - 19}. \tag{80}$$

For the degree-9 cover $\mathcal{X}_0(\wp_8)/\mathcal{X}(1)$ we find

$$t = \frac{(1 - x_8)(2x_8^4 + 4x_8^3 + 18x_8^2 + 14x_8 + 25)^2}{27(4x_8^2 + 5x_8 + 23)}$$
$$= 1 - \frac{4(x_8^3 + x_8^2 + 5x_8 - 1)^3}{27(4x_8^2 + 5x_8 + 23)}, \tag{81}$$

with the involution fixing the simple zero $x_8 = 1$ and switching the simple poles, i.e.

$$w_{\wp_8}(x_8) = \frac{51 - 19x_8}{19 + 13x_8}. \tag{82}$$

Note that all of these covers and involutions have rational coefficients even though a priori they are only known to be defined over K. This is possible because K is a normal extension of $\mathbf{Q}$ and the primes $\wp_7$, $\wp_8$ used to define our curves and maps are Galois-invariant. To each of the three real places of K corresponds a quaternion algebra ramified only at the other two places, and thus a Shimura curve $\mathcal{X}(1)$ with three elliptic points P_2, P_3, P_7 to which we may assign coordinates $0, 1, \infty$. Then $\mathrm{Gal}(K/\mathbf{Q})$ permutes these three curves; since we have chosen rational coordinates for the three distinguished points, any point on or cover of $\mathcal{X}(1)$ defined by a Galois-invariant construction must be fixed by this action of Galois and so be defined over $\mathbf{Q}$. The same applies to each of the triangle groups $G_{p,q,r}$ associated with quaternion algebras over number fields F properly containing $\mathbf{Q}$, which can be found in cases III through XIX of Takeuchi's list [T]. In each case, F is Galois over $\mathbf{Q}$, and the finite ramified places of the quaternion algebra are Galois-invariant. Moreover, even when $G_{p,q,r}$ is not $\Gamma(1)$, it is still related with $\Gamma(1)$ by a Galois-invariant construction (such as intersection with $\Gamma_0(\wp)$ or adjoining $\mathsf{w}_\wp$ or $w_\wp$ for a Galois-invariant prime $\wp$ of F). At least one of the triangle groups in each commensurability class has distinct indices p, q, r, whose corresponding elliptic points may be unambiguously identified with $0, 1, \infty$; this yields a model of the curve $\mathcal{H}/G_{p,q,r}$, and thus of all its commensurable triangle curves, that is defined over $\mathbf{Q}$.

This discussion bears also on CM points on $\mathcal{X}(1)$. There are many CM points on $\mathcal{X}(1)$ rational over K, but only seven of those are $\mathbf{Q}$-rational: a CM point defined over $\mathbf{Q}$ must come from a CM field K' which is Galois not only over K but over $\mathbf{Q}$. Thus K' is the compositum of K with an imaginary quadratic field, which must have unique factorization. We check that of the nine such fields only five retain unique factorization when composed with K. One of these, $\mathbf{Q}(\sqrt{-7})$, yields the cyclotomic field $\mathbf{Q}(e^{2\pi i/7})$, whose ring of integers is the CM ring for the elliptic point $P_7 : t = \infty$; two subrings still have unique factorization and yield CM points $\wp_7$- and $\wp_8$-isogenous to that elliptic point, which again are not only K- but even $\mathbf{Q}$-rational thanks to the Galois invariance of $\wp_7$, $\wp_8$. The other four cases are the fields of discriminant $-3, -4, -8, -11$, which yield one rational CM point each. The first two are the elliptic points $P_3, P_2 : t = 1, 0$. To find the coordinates of the CM point of discriminant -8, and of the two points isogenous with P_7, we may use the involutions (80,82) on $\mathcal{X}_0(\wp_7)$ and $\mathcal{X}_0(\wp_8)$. On $\mathcal{X}_0(\wp_7)$, the involution takes $x_7 = \infty$ to $19/13$, yielding the point $t = 3593763963/4015905088$ $\wp_7$-isogenous with P_7 on $\mathcal{X}(1)$; on $\mathcal{X}_0(\wp_8)$ the involution takes $x_8 = \infty$ to $-19/13$, yielding the point $t = 47439942003/8031810176$ $\wp_8$-isogenous with P_7. On the latter curve, the second fixed point of the involution (besides $x_8 = 1$) is $x_8 = -51/13$, which yields the CM point $t = 1092830632334/1694209959$ of discriminant -8. The two points isogenous with P_7 also arise from the second fixed point of $w_{\wp_7}$ and a further solution of $t(x_8) = t(w_{\wp_8}(x_8))$.

This still leaves the problem of locating the CM point of discriminant -11. We found it numerically using quotients of hypergeometric functions as we did for $G_{2,4,6}$. Let $c = 2\cos 2\pi/7$, so c is the unique positive root of $c^3 + c^2 - 2c - 1$. Consider the quaternion algebra over K generated by i, j with

$$i^2 = j^2 = c, \quad ij = -ji. \tag{83}$$

This is ramified at the two other real place of K, in which c maps to the negative reals $2\cos 4\pi/7$ and $2\cos 6\pi/7$, but not at the place with $c = 2\cos 2\pi/7$; since c is a unit, neither is this algebra ramified at any finite place with the possible exception of $\wp_8$, which we exclude using the fact that the set of ramified places has even cardinality. Thus $K(i, j)$ is indeed our algebra A. A maximal order $\mathcal{O}$ is obtained from $O_K[i, j]$ by adjoining the integral element $(1 + ci + (c^2 + c + 1)j)/2$. Then $\mathcal{O}^*$ contains the elements

$$\begin{gathered} g_2 := ij/c, \qquad g_3 := \frac{1}{2}(1 + (c^2 - 2)j + (3 - c^2)ij), \\ g_7 := \frac{1}{2}(c^2 + c - 1 + (2 - c^2)i + (c^2 + c - 2)ij) \end{gathered} \tag{84}$$

of norm 1, with $g_2^2 = g_3^3 = g_7^7 = -1$ and $g_2 = g_7 g_3$. Thus the images of g_2, g_3, g_7 in $\Gamma(1)$ are elliptic elements that generate that group. A short search finds the linear combination $(2 - c^2)g_3 + (c^2 + c)g_7 \in \mathcal{O}$ of discriminant -11; computing its fixed point in $\mathcal{H}$ and solving for t to high precision (150 decimals, which turned out to be overkill), we obtain a real number whose continued fraction matches that of

$$\frac{88983265401189332631297917}{45974167834557869095293} = \frac{7^3 43^2 127^2 139^2 207^2 659^2 11}{3^3 13^7 83^7}, \tag{85}$$

with numerator and denominator differing by $2^9 29^3 41^3 167^3 281^3$. Having also checked that this number differs from the t-coordinates of the three non-elliptic CM points by products of small ($< 10^4$) primes,[11] and that it passes the supersingular test, we are quite confident that (85) is in fact the t-coordinate of the CM point of discriminant -11.

5.4 An irrational example: the algebras over $\mathbf{Q}[\tau]/(\tau^3 - 4\tau + 2)$ with $\Sigma = \{\infty_i, \infty_j\}$

While our examples so far have all been defined over $\mathbf{Q}$, this is not generally the case for Shimura curves associated to a quaternion algebra over a totally number field K properly containing $\mathbf{Q}$. For instance, K may not be a Galois extension of $\mathbf{Q}$; or, K may be Galois, but the set of finite ramified places may fails to be Galois-stable; or, even if that set is Galois-stable, the congruence conditions on the subgroup of A^*/K^* may not be Galois-invariant, and the resulting curve would not be defined over $\mathbf{Q}$ even though $\mathcal{X}(1)$ would be. In each case different real embeddings of the field yield different arithmetic subgroups of $\mathrm{PSL}_2(\mathbf{R})$ and thus different quotient curves. We give here what is probably the simplest example: a curve $\mathcal{X}(1)$ associated to a quaternion algebra with no finite ramified places over a totally real cubic field which is not Galois over $\mathbf{Q}$. While the curve has genus 0, no degree-1 rational function on it takes $\mathbf{Q}$-rational values at all four of its elliptic points, and the towers of modular curves over this $\mathcal{X}(1)$ are defined over K but not over $\mathbf{Q}$.

Let K be the cubic field $\mathbf{Q}[\tau]/(\tau^3 - 4\tau + 2)$ and discriminant $148 = 2^2 37$, which is minimal for a totally real non-Galois field. Let A/K be a quaternion algebra ramified at two of the three real places and at no finite primes of K. Using GP/PARI to compute $\zeta_K(2)$, we find from Shimizu's formula (78) that the associated Shimura curve $\mathcal{X}(1) = \mathcal{X}^*(1)$ has hyperbolic area $.16666\ldots$; thus the area is $1/6$ and, since A is not in Takeuchi's list, the curve $\mathcal{X}(1)$ has genus 0 and four elliptic points, one of order 3 and three of order 2. The order-3 point P_3 has discriminant -3 as expected, but the order-2 points are a bit more interesting: their CM field is $K(i)$, but the ring of integers of that field is not $O_K[i]$! Note that the rational prime 2 is totally ramified in K, being the cube of the prime (τ); thus $(1+i)/\tau$ is an algebraic integer, and we readily check that it generates the integers of $K(i)$ over O_K. One of the elliptic points, call it P_2, has CM ring $O_K[(1+i)/\tau]$ and discriminant $-4/\tau^2$; of its three (τ)-isogenous points, one is

[11] If 10^4 does not seem small, remember that the factorizations are really over K, not $\mathbf{Q}$; the largest *inert* prime that occurs is 19, and the split primes are really primes of K of norm at most comparable with that of 19.

P_2 itself, and the others are the remaining elliptic points P_2', P_2'', with CM ring $O_K[i]$ of discriminant -4.

Thus the modular curve $\mathcal{X}_0((\tau))$ is a degree-3 cover of $\mathcal{X}(1)$ unramified above the elliptic point P_2, and ramified above the other three elliptic points with type 3 for P_3 and 21 for P_2', P_2''. This determines the cover up to $\bar{K}$-isomorphism — the curve $\mathcal{X}_0((\tau))$ has genus 0, and we can choose coordinates x on that curve and t on $\mathcal{X}(1)$ such that $t(P_3) = \infty$ and $t = x^3 - 3cx$ for some $c \neq 0$ — but not the location of the unramified point P_2 relative to the other three elliptic points. To determine that we once again use the involution, this time $w_{(\tau)}$, of $\mathcal{X}_0((\tau))$: this involution fixes the point above P_2 corresponding to its self-isogeny, and pairs the other two preimages of P_2 with the simple preimages of P_2', P_2''. We find that there are three ways to satisfy this condition:

$$t = x^3 - 3(\tau^2 - 3)x, \quad P_2 : t = 1300 - 188\tau - 351\tau^2, \quad P_2', P_2'' : t = \pm 2(\tau^2 - 3)^{3/2}, \tag{86}$$

and its Galois conjugates. The correct choice is determined by the condition that the Shimura curves must be fixed by the involution of the Galois closure of $K/\mathbf{Q}$ that switches the two real embeddings of K that ramify A: the image of τ under the the third (split) embedding must be used in (86). We find that the simple and double preimages of P_2', P_2'' are $x = \pm 2\sqrt{a^2 - 3}, \mp\sqrt{a^2 - 3}$, and the preimages of P_2 are $12 - 2\tau - 3\tau^2$ (fixed by $w_{(\tau)}$) and $(-12 + 2\tau + 3\tau^2 \pm (3a^2 - 12)\sqrt{a^2 - 3})/2$. From this we recover as usual the tower of curves $\mathcal{X}_0((\tau)^r)$, whose reductions at primes of K other than τ are asymptotically optimal over the quadratic extensions of the primes' residue fields, and which in this case is a tower of double (whence cyclic) covers unramified above the genus-3 curve $\mathcal{X}_0((\tau)^4)$ and thus involved in that curve's class-field tower.

5.5 Open problems

Computing modular curves and covers. Given a nonempty even set Σ of rational primes, and thus a quaternion algebra $\mathsf{A}/\mathbf{Q}$, how to compute the curve $\mathcal{X}^*(1)$ together with its Schwarzian equation and modular covers such as $\mathcal{X}(1)$ and $\mathcal{X}_0^*(l)$? Even in the simplest case $\Sigma = \{2, 3\}$ where $\Gamma^*(1)$ is a triangle group and all the covers $\mathcal{X}_0^*(l)/\mathcal{X}^*(1)$ are in principle determined by their ramifications, finding those covers seems at present a difficult problem once l gets much larger than the few primes we have dealt with here. This is the case even when l is still small enough that $\mathcal{X}_0^*(l)$ has genus small enough, say $g \leq 5$, that the curve should have a simple model in projective space. For instance, according to 35 the curve $\mathcal{X}_0^*(73)$ has genus 1. Thus its Jacobian is an elliptic curve; moreover it must be one of the six elliptic curves of conductor $6 \cdot 73$ tabulated in [C]. Which one of those curves it is, and which principal homogeneous space of that curve is isomorphic with $\mathcal{X}_0^*(73)$, can probably be decided by local methods such as those of [Ku]; indeed such a computation was made for $\mathcal{X}_0(11)$ in D. Roberts' thesis [Ro]. But that still leaves the problem of finding the degree-74 map on that curve which realizes the modular cover $\mathcal{X}_0^*(73) \to \mathcal{X}^*(1)$. For classical modular curves (i.e. with $\Sigma = \emptyset$) of comparable and even somewhat higher levels, the equations and covers can be obtained via q-expansions as explained in [E5]; but what can we do here in the absence of cusps and thus of q-expansions? Can we do anything at all once the primes in Σ are large or numerous enough to even defeat the methods of the present paper for computing $\mathcal{X}^*(1)$ and the location of the elliptic points on this curve? Again this happens while the genus of $\mathcal{X}^*(1)$ is still small; for instance it seems already a difficult problem to locate the elliptic points on all curves $\mathcal{X}^*(1)$ of genus zero and determine their Schwarzian equations, let alone find equations for all curves $\mathcal{X}^*(1)$ of genus 1, 2, or 3. By [I2] the existence of the involutions w_l on $\mathcal{X}_0^*(l)$ always suffices in principle to answer these questions, but the computations needed to actually do this become difficult very quickly; it seems that a perspicuous way to handle these computations, or a new and more efficient approach, is called for. The reader will note that so far we have said nothing about computing with *modular forms* on Shimura curves. Not only is this an intriguing question in its own right, but solving it may also allow more efficient computation of Shimura curves and the natural maps between them, as happens in the classical modular setting.

In another direction, we ask: is there a prescription, analogous to (27), for towers of Shimura curves whose levels are powers of a ramified prime of the algebra? For a concrete example (from case III of [T]), let A be the quaternion algebra over $\mathbf{Q}(\sqrt{2}\,)$ with $\Sigma = \{\infty_1, \wp_2\}$, where ∞_1 is one of the two Archimedean places and $\wp_2$ is the prime ideal $(\sqrt{2}\,)$ above 2; let $\mathcal{O} \subset \mathsf{A}$ be a maximal order, $I = I_{\wp_2} \subset \mathcal{O}$ the ideal of elements whose norm is a multiple of $\sqrt{2}$, and

$$\Gamma_n = \{[a] \in O_1^*/\{\pm 1\} : a \equiv 1 \bmod I^n\} \tag{87}$$

for $n = 0, 1, 2, \ldots$. Then Γ_{n+1} is a normal subgroup of Γ_n with index $3, 2^2, 2$ according as $n = 0$, n is odd, or n is even and positive. Consulting [T], we find that Γ_0, Γ_1 are the triangle groups $G_{3,3,4}$ and $G_{4,4,4}$. Let X_n be the Shimura curve $\mathcal{H}/\Gamma_n$, which parametrizes principally polarized abelian fourfolds with endomorphisms by A and complete level-I^n structure. Then $\{X_n\}_{n>0}$ is a tower of $\mathbf{Z}/2$ or $(\mathbf{Z}/2)^2$ covers, unramified above the curve X_3. Moreover, X_n has genus zero for $n = 0, 1, 2$, while X_3 is isomorphic with the curve $y^2 = x^5 - x$ of genus 2 with maximal automorphism group. The reduction of this tower at any prime $\wp \neq \wp_2$ of $\mathbf{Q}(\sqrt{2}\,)$ is asymptotically optimal over the quadratic extension of the residue field of $\wp$. So we ask for explicit recursive equations for the curves in this tower. Note that unlike the tower (25), this one does not seem to offer a w_l or $\mathsf{w}_{\wp_2}$ shortcut.

CM points. Once we have found a Shimura modular curve together with a Schwarzian equation, we have seen how to compute the coordinates of CM points on the curve, at least as real or complex numbers to arbitrary precision. But this still leaves many theoretical and computational questions open. For instance, what form does the Gross-Zagier formula [GZ] for the difference between j-invariants of elliptic curves take in the context of Shimura curves such as $\mathcal{X}_0^*(1)$ or $\mathcal{X}(1)$? Note that a factorization theorem would also yield a rigorous proof that our tabulated rational coordinates of CM points are correct. Our tables also suggest that at least for rational CM points the heights increase more or less regularly with D_1; can this be explained and generalized to CM points of degree > 1? For CM points on the classical modular curve X(1) this is easy: a CM j-invariant is an algebraic integer, and its size depends on how close the corresponding point of $\mathcal{H}/\mathrm{PSL}_2(\mathbf{Z})$ is to the cusp; so for instance if $\mathbf{Q}(\sqrt{-D})$ has class number 1 then the CM j-invariant of discriminant $-D$ is a rational integer of absolute value $\exp(\pi\sqrt{D}) + O(1)$. But such a simple explanation probably cannot work for Shimura curves which have neither cusps nor integrality of CM points. Within a commensurability class of Shimura curves (i.e. given the quaternion algebra A), the height is inversely proportional to the area of the curve; does this remain true in some sense when A is varied?

As a special case we might ask: how does the minimal polynomial of a CM point of discriminant $-D$ factor modulo the primes contained in D_1? That the minimal polynomials for CM j-invariants are almost squares modulo prime factors of the discriminant was a key component of our results on supersingular reduction of elliptic curves [E2, E3]; analogous results on Shimura curves may likewise yield a proof that, for instance, for every $t \in \mathbf{Q}$ there are infinitely many primes p such that the point on the $(2,4,6)$ curve with coordinate t reduces to a supersingular point mod p.

Enumeration and arithmetic of covers. When an arithmetic subgroup of $\mathrm{PSL}_2(\mathbf{R})$ is commensurable with a triangle group $G = G_{p,q,r}$, as was the case for the $\Sigma = \{2,3\}$ algebra, any modular cover $\mathcal{H}/G'$ of $\mathcal{H}/G$ (for $G' \subset G$ a congruence subgroup) is ramified above only three points on the genus-0 curve $\mathcal{H}/G$. We readily obtain the ramification data, which leave only finitely many possibilities for the cover. We noted that, even when there is only one such cover, actually finding it can be far from straightforward; but much is known about covers of $\mathbf{P}^1$ ramified at three points — for instance, the number of such covers with given Galois group and ramification can be computed by solving equations in the group (see [Mat]), and the cover is known [Be] to have good reduction at each prime not dividing the size of the group. But when G, and any group commensurable with it, has positive genus or more than three elliptic points, we were forced to introduce additional information about the cover, namely the existence of an involution exchanging certain preimages of the branch points. In the examples we gave here (and in several others to be detailed in future work) this was enough to uniquely determine the cover $\mathcal{H}/G' \to \mathcal{H}/G$. But there is as yet no general theory that predicts the number of solutions of this kind of covering problem. The arithmetic of the solutions is even more mysterious: recall for instance that in our final example the cubic field $\mathbf{Q}[\tau]/(\tau^3 - 4\tau + 2)$ emerged out of conditions on the cover $\mathcal{X}_0((\tau))/\mathcal{X}(1)$ in which that field, and even its ramified prime 37, are nowhere to be seen.

6 Appendix: Involutions of $\mathbf{P}^1$

We collect some facts concerning involutions of the projective line over a field of characteristic other than 2. We do this from a representation-theoretic point of view, in the spirit of [FH]. That is, we identify a pair of points $t_i = (x_i : y_i)$ $(i = 1, 2)$ of $\mathbf{P}^1$ with a binary quadric, i.e. a one-dimensional space of homogeneous quadratic polynomials $Q(X,Y) = AX^2+2BXY+CY^2$, namely the polynomials vanishing at the two points; we regard the three-dimensional space V_3 of all such polynomials $AX^2 + 2BXY + CY^2$ as a representation of the group SL_2 acting on $\mathbf{P}^1$ by unimodular linear transformations of (X,Y).

An invertible linear transformation of a two-dimensional vector space V_2 over any field yields an involution of the projective line $\mathbf{P}^1 = \mathbf{P}(V_2^*)$ if and only if it is not proportional to the identity and its trace vanishes (the first condition being necessary only in characteristic 2). Over an algebraically closed field of characteristic other than 2, every involution of $\mathbf{P}^1$ has two fixed points, and any two points are equivalent under the action of PSL_2 on $\mathbf{P}^1$. It is clear that the only involution fixing $0, \infty$ is $t \leftrightarrow -t$; it follows that any pair of points determines a unique involution fixing those two points. Explicitly, if $B^2 \neq AC$, the involution fixing the distinct roots of $AX^2 + 2BXY + CY^2$ is $(X : Y) \leftrightarrow (BX+CY : -AX-BY)$. Note that the 2-transitivity of PSL_2 on $\mathbf{P}^1$ also means that this group acts transitively on the complement in the projective plane $\mathbf{P}V_3$ of the conic $B^2 = AC$ (and also acts transitively on that conic); indeed it is well-known that PSL_2 is just the special orthogonal group for the discriminant quadric $B^2 - AC$ on V_3.

Now let $Q_1, Q_2 \in V_3$ be two polynomials without a common zero. Then there is a unique involution of $\mathbf{P}^1$ switching the roots of Q_1 and also of Q_2. (If Q_i has a double zero the condition on Q_i means that its zero is a fixed point of the involution.) This can be seen by using the automorphism group $\mathrm{Aut}(\mathbf{P}^1) = \mathrm{PGL}_2$ to map Q_i to XY or Y^2 and noting that the involutions that switch $t = 0$ with ∞ are $t \leftrightarrow a/t$ for nonzero a, while the involutions fixing $t = \infty$ are $t \leftrightarrow a - t$ for arbitrary a. As before, we regard the involution determined in this way by Q_1, Q_2 as an element of $\mathbf{P}V_3$. This yields an algebraic map f from (an open set in) $\mathbf{P}V_3 \times \mathbf{P}V_3$, parametrizing Q_1, Q_2 without common zeros, to $\mathbf{P}V_3$. We next determine this map explicitly.

First we note that this map is covariant under the action of PSL_2: we have $f(gQ_1, gQ_2) = g(f(Q_1, Q_2))$ for any $g \in \mathrm{PSL}_2$. Next we show that f has degree 1 in each factor. Using the action of PSL_2 it is enough to show that if $Q_1 = XY$ or Y^2 then f is linear as a function of $Q_2 = AX^2+2BXY+CY^2$. In the first case, the involution is $t \leftrightarrow C/At$ and its fixed points are the roots of $AX^2 - CY^2$. In the second case, the involution is $t \leftrightarrow (-2B/A) - t$ with fixed points $t = \infty$ and $t = -B/A$, i.e. the roots of $AXY + BY^2$. In either case the coefficients of $f(Q_1, Q_2)$ are indeed linear in A, B, C.

But it turns out that these two conditions completely determine f: there is up to scaling a unique PSL_2-covariant bilinear map from $V_3 \times V_3$ to V_3; equivalently, V_3 occurs exactly once in the representation $V_3 \otimes V_3$ of PSL_2. In fact it is known (see e.g. [FH, §11.2]) that $V_3 \otimes V_3$ decomposes as $V_1 \oplus V_3 \oplus V_5$, where V_1 is the trivial representation and V_5 is the space of homogeneous polynomials of degree 4 in X, Y. The factor V_3 is particularly easy to see, because it is just the antisymmetric part $\bigwedge^2 V_3$ of $V_3 \otimes V_3$. Now the next-to-highest exterior power $\bigwedge^{\dim V - 1} V$ of any finite-dimensional vector space V is canonically isomorphic with $(\det V) \otimes V^*$, where $\det V$ is the top exterior power $\bigwedge^{\dim V} V$. Taking $V = V_3$, we see that $\det V_3$ is the trivial representation of PSL_2. Moreover, thanks to the invariant quadric $B^2 - AC$ we know that V_3 is self-dual as a PSL_2 representation. Unwinding the resulting identification $\bigwedge^2 V_3 \xrightarrow{\sim} V_3^* \xrightarrow{\sim} V_3$, we find:

Proposition A. *Let $Q_i = A_i X^2 + 2B_i XY + C_i Y^2$ $(i = 1, 2)$ be two polynomials in V_3 without a common zero. Then the unique involution of $\mathbf{P}^1$ switching the roots of Q_1 and also of Q_2 is the involution whose fixed points are the roots of*

$$(A_1 B_2 - A_2 B_1) X^2 + (A_1 C_2 - A_2 C_1) XY + (B_1 C_2 - B_2 C_1) Y^2, \tag{88}$$

i.e. the fractional linear transformation

$$t \longleftrightarrow \frac{(A_1 C_2 - A_2 C_1) t + 2(B_1 C_2 - B_2 C_1)}{2(B_1 A_2 - B_2 A_1) t + (C_1 A_2 - C_2 A_1)}. \tag{89}$$

Proof: The coordinates of $Q_1 \wedge Q_2$ for the basis of V_3^* dual to $(X^2, 2XY, Y^2)$ are $(B_1 C_2 - B_2 C_1,\, A_2 C_1 - A_1 C_2,\, A_1 B_2 - A_2 B_1)$. To identify V_3^* with V_3 we need a PSL_2-invariant element of $V_3^{\otimes 2}$. We could get this invariant from the invariant quadric $B^2 - AC \in V_3^{*\otimes 2}$, but it is easy enough to exhibit it directly: it is

$$X^2 \otimes Y^2 - \frac{1}{2} 2XY \otimes 2XY + Y^2 \otimes X^2, \tag{90}$$

the generator of the kernel of the multiplication map $\mathrm{Sym}^2(V_3) \to V_5$. The resulting isomorphism from V_3^* to V_3 takes the dual basis of $(X^2, 2XY, Y^2)$ to $(Y^2, -XY, X^2)$, and thus takes $Q_1 \wedge Q_2$ to (88) as claimed. □

Of course this is not the only way to obtain (89). A more "geometrical" approach (which ultimately amounts to the same thing) is to regard $\mathbf{P}^1$ as a conic in $\mathbf{P}^2$. Then involutions of $\mathbf{P}^1$ correspond to points $p \in \mathbf{P}^2$ not on the conic: the involution associated with p takes any point q of the conic to the second point of intersection of the line pq with the conic. Of course the fixed points are then the points q such that pq is tangent to the conic at q. Given Q_1, Q_2 we obtain for $i = 1, 2$ the secant of the conic through the roots of Q_i, and then p is the intersection of those secants.

From either of the two approaches we readily deduce

Corollary B. *Let $Q_i = A_i X^2 + 2B_i XY + C_i Y^2$ $(i = 1, 2, 3)$ be three polynomials in V_3 without a common zero. Then there is an involution of $\mathbf{P}^1$ switching the roots of Q_i for each i if and only if the determinant*

$$\begin{vmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \\ A_3 & B_3 & C_3 \end{vmatrix} \tag{91}$$

vanishes.

As an additional check on the formula (88), we may compute that the discriminant of that quadratic polynomial is exactly the resolvent

$$\det \begin{pmatrix} A_1 & 2B_1 & C_1 & 0 \\ 0 & A_1 & 2B_1 & C_1 \\ A_2 & 2B_2 & C_2 & 0 \\ 0 & A_2 & 2B_2 & C_2 \end{pmatrix} \tag{92}$$

of Q_1, Q_2 which vanishes if and only if these two polynomials have a common zero.

References

[A] Arno, S.: The imaginary quadratic fields of class number 4. *Acta Arith.* **60** (1992), 321–334.

[Be] Beckmann, S.: Ramified primes in the field of moduli of branches coverings of curves. *J. of Algebra* **125** (1989), 236–255.

[BK] Birch, B.J., Kuyk, W., ed.: *Modular Functions of One Variable IV.* Lect. Notes in Math. **476**, 1975.

[C] Cremona, J.E.: *Algorithms for modular elliptic curves.* Cambridge University Press, 1992.

[D] Deuring, M.: Die Typen die Multiplikatorenringe elliptische Funktionkörper, *Abh. Math. Sem. Hansischen Univ.* **14**, 197–272 (1941).

[E1] Elkies, N.D.: ABC implies Mordell, *International Math. Research Notices* 1991 #7, 99–109.

[E2] The existence of infinitely many supersingular primes for every elliptic curve over **Q**, *Invent. Math.* **89 (1987)**, 561–568.

[E3] Supersingular primes for elliptic curves over real number fields, *Compositio Math.* **72** (1989), 165–172.

[E4] Elkies, N.D.: Heegner point computations. Pages 122–133 in *Algorithmic number theory* (Ithaca, NY, 1994; L.M. Adleman and M.-D. Huang, eds.; Lect. Notes in Computer Sci. #877; Berlin: Springer, 1994).

[E5] Elkies, N.D.: Elliptic and modular curves over finite fields and related computational issues. Pages 21–76 in *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin* (D.A. Buell and J.T. Teitelbaum, eds.; AMS/International Press, 1998).

[E6] Elkies, N.D.: Explicit modular towers. Pages 23–32 in *Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing* (T. Başar and A. Vardy, eds.; Univ. of Illinois at Urbana-Champaign, 1998).

[F1] Fricke, R.: Über den arithmetischen Charakter der zu den Verzweigungen $(2,3,7)$ und $(2,4,7)$ gehörenden Dreiecksfunctionen, *Math. Ann.* **41** (1893), 443–468.

[F2] Fricke, R.: Entwicklungen zur Transformation fünfter und siebenter Ordnung einiger specieller automorpher Functionen, *Acta Mathematica* **17** (1893), 345–395.

[Fr3] Fricke, R.: Ueber eine einfache Gruppe von 504 Oprationen, *Math. Ann.* **52** (1899), 321–339.

[FH] Fulton, W., Harris, J.: *Representation Theory: A First Course.* New York: Springer, 1991 (GTM **129**).

[Go1] Goppa, V.D.: Codes on algebraic curves, *Soviet Math. Dokl.* **24** (1981), 170–172.
[Go2] Goppa, V.D.: Algebraico-geometric codes, *Math. USSR Izvestiya* **24** (1983), 75–91.
[GR] Gradshteyn, I.S., Ryzhik, I.M.: *Table of Integrals, Series, and Products.* New York: Academic Press 1980.
[GS] Granville, A., Stark, H.M.: abc implies no Siegel zeros, preprint 1997.
[GZ] Gross, B.H., Zagier, D.: On singular moduli, *J. für die reine und angew. Math.* **335** (1985), 191–220.
[HM] Hashimoto, K.-i., Murabayashi, N.: Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two, *Tohoku Math. Journal (2)* **47** (1995), #2, 271–296.
[I1] Ihara, Y.: Schwarzian equations, *J. Fac. Sci. Univ. Tokyo* **21** (1974), 97–118.
[I2] Ihara, Y.: On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations, *J. Fac. Sci. Univ. Tokyo* **21** (1974), 309–332.
[I3] Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo* **28** (1981), 721–724.
[JL] Jordan, B.W., Livné, R.A.: Local Diophantine properties of Shimura curves. *Math. Ann.* **270** (1985), 235–248.
[Kn] Knapp, A.W.: *Elliptic Curves.* Princeton Univ. Press, 1992 (*Mathematical Notes* **40**).
[Ku] Kurihara, A.: On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo* **25** (1979), 277–301.
[MM] Malle, G., Matzat, B.H.: Realisierung von Gruppen $PSL_2(\mathbf{F}_p)$ als Galoisgruppen über $\mathbf{Q}$, *Math. Ann.* **272** (1985), 549–565.
[Mac] Macbeath, A.M.: On a curve of genus 7, *Proc. LMS* **15** (1965), 527–542.
[Mat] Matzat, B.H.: *Konstruktive Galoistheorie*, Lect. Notes Math. **1284**, 1987.
[Mi] Michon, J.-F.: Courbes de Shimura hyperelliptiques, *Bull. Soc. math. France* **109** (1981), 217–225.
[Mü] Müller, P.: Arithmetically exceptional functions and elliptic curves. Preprint, 1998.
[Ri] Ribet, K.A.: On modular representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.
[Ro] Roberts, D.P.: *Shimura curves analogous to* $X_0(N)$. Harvard doctoral thesis, 1989.
[Se] Serre, J.-P.: *Topics in Galois Theory.* Boston: Jones and Bartlett 1992.
[S1] Shimizu, H.: On zeta functions of quaternion algebras, *Ann. of Math.* **81** (1965), 166–193.
[S2] Shimura, G.: Construction of class fields and zeta functions of algebraic curves, *Ann. of Math.* **85** (1967), 58–159.
[S3] Shimura, G.: On the Real Points of an Arithmetic Quotient of a Bounded Symmetric Domain, *Math. Ann.* **215** (1975), 135–164.
[T] Takeuchi, K.: Commensurability classes of arithmetic triangle groups, *J. Fac. Sci. Univ. Tokyo* **24** (1977), 201–212.
[TVZ] Tsfasman, M.A., Vlăduţ, S.G., Zink, T.: Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound. *Math. Nachr.* **109** (1982), 21–28.
[V] Vignéras, M.-F.: *Arithmétique des Algèbres de Quaternions.* Berlin: Springer, 1980 (SLN **800**).

[YZ] Yui, N., Zagier, D.: On the singular values of Weber modular functions. *Math. of Computation* **66** (1997), 1629–1644.