Computing modular curves via quaternions

David R. Kohel
National University of Singapore
January 1997

Based on a talk given at the Fourth CANT Conference
NUMBER THEORY AND CRYPTOGRAPHY
University of Sydney, 3-5 December 1997.

§1. Introduction.

Modular curves are of central interest for both the theoretical and computational investigation of elliptic curves. In the course of proving Fermat's "Last Theorem", Wiles [18] and Taylor–Wiles [17] established that a large class of elliptic curves are parameterized by a modular curve. Cremona has developed effective algorithms and performed extensive computations of these parametrizations [3]. In a different direction, Elkies [7] has used explicit models for modular curves to make significant practical improvements to a theoretical polynomial time algorithm of Schoof [15] for computing the trace of Frobenius on an elliptic curve over a finite field. This has made it possible to compute the number of points on elliptic curves over finite fields whose cardinality measures hundreds of decimal digits [10]. In order to apply this algorithm, one must precompute a large number of explicit models for modular curves.

One approach to the problem of computing models for modular curves is to produce a basis for the space of weight two cusp forms. Such forms correspond to differentials on the curve, by which one can construct the canonical morphism to projective space. When a curve is of genus greater than two and not hyperelliptic, the canonical morphism is an embedding and gives a nonsingular model for the curve.

For the purposes of computation, it serves to have the additional information of the Hecke module structure on differentials. This gives information on the decomposition of the Jacobian and on curves covered by the modular curve. In particular, we exploit the explicit action of the canonical involution to decompose the cusp forms into invariant and anti-invariant eigenspaces. The investigation of parametrizations of curves of higher genus is aided by a Hecke module decomposition of the space of differentials.

It will be the purpose of this article to discuss certain isomorphisms of Hecke modules, defined in very different contexts, and to describe isomorphisms among them. The relation between supersingular elliptic curves and the ideal theory in a quaternion algebra appears in the classical work of Deuring [4], which in the modern theory is properly stated as an equivalence of categories. The basis problem of Eichler [5] provides the means of relating the ideal theory to modular forms. Using this theory Pizer [12] describes an algorithm for computing modular forms. The method of graphs of Oesterlé and Mestre [9] rephrases the theory of quaternion ideals in terms of supersingular elliptic curves. This gives an intuitive method for relating the Hecke module, defined as a subgroup of the divisor group of a modular curve, with the space of modular forms of weight two. In this work they express the Hecke operator $T(n)$ in terms of the adjacency operator of a graph of supersingular elliptic curves. Via the above mentioned equivalence of categories, the ideas of Oesterlé and Mestre translate into the computationally simpler world of the ideal theory of a quaternion algebra. Using a method which is in essence that of Pizer [12], one can compute an array of quadratic forms determining the Brandt morphism. For any n, the Hecke operator $T(n)$ can be extracted as the Brandt matrix of n-th representation numbers of these quadratic forms.

In section two, we discuss quaternion algebras and their ideal theory, and follow in section three with a discussion of the equivalence between supersingular elliptic curves and certain ideals over a maximal order. In section four we recall the main ideas of the method of graphs of Mestre and Oesterlé. Section five introduces the Brandt morphism, given in terms of the Brandt matrix of theta functions for quadratic forms associated to the module of homomorphisms of a basis of ideals. We conclude with a discussion in section six of the computational aspects of computing modular curves using the ideal theory of quaternions.

As an appendix to this article we give a table of characteristic polynomials of the Hecke operators, which suffice to determine the decomposition of the Jacobian of corresponding modular curve. We further give examples of computations of the ring of modular functions, combining several ideas from the article of Elkies [7]. For any given level, one can make improvements to this approach. A significant advantage, however, is that this approach is systematic, thus suitable for implementation or for proving bounds for the computational complexity.

§2. Quaternion algebras over $\mathbb{Q}$.

A quaternion algebra $\mathfrak{A}$ over $\mathbb{Q}$ is a central simple algebra of dimension four over $\mathbb{Q}$. The number theory of these algebras is analogous to that of number fields. In particular we have an noncommutative theory for each of the following objects and concepts from commutative number theory.

1. Maximal orders. There exist infinitely many maximal orders of any quaternion algebra, however they fall in finitely many isomorphism classes.

2. Ideal theory. We can study the one-sided and two-sided ideals of a given maximal order in a quaternion algebra. Again, these fall into finitely many classes.

3. Ramification and splitting. The quaternion algebra $\mathfrak{A}$ is said to *split* at the rational prime l if $\mathfrak{A}_l = \mathfrak{A} \otimes \mathbb{Q}_l$ is isomorphic to $\mathbb{M}_2(\mathbb{Q}_l)$. Otherwise

$\mathfrak{A}$ is said to *ramify* at l and $\mathfrak{A}_l$ is a division algebra. Likewise $\mathfrak{A}$ is said to split or ramify at infinity if $\mathfrak{A} \otimes \mathbb{R}$ is a matrix algebra or a division algebra.

Quaternion algebras are analogous to quadratic extensions of $\mathbb{Q}$. In fact the analogy goes further: every element x of $\mathfrak{A}$ not in the center generates a quadratic extension of $\mathbb{Q}$.

Example 1. The matrix algebra $\mathbb{M}_2(\mathbb{Q})$ is a quaternion algebra, which we call the *split* quaternion algebra over $\mathbb{Q}$. Let x be the element

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

and set $K = \mathbb{Q}[x]$. Then K is isomorphic to the ring $\mathbb{Q}[X]/(X^2 - X)$. Every maximal order is conjugate to the order $\mathbb{M}_2(\mathbb{Z})$.

Example 2. Let $\mathfrak{A} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ be the quaternion algebra defined by the relations

$$i^2 = j^2 = -1, \quad k = ij = -ji.$$

Then $\mathfrak{A}$ ramifies at 2 and at infinity, and $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$, where $\omega = (1 + i + j + k)/2$, is the unique maximal order up to isomorphism.

§3. Supersingular elliptic curves.

Let k be an algebraically closed field of characteristic l. An elliptic curve E is supersingular if and only if its endomorphism ring $\mathcal{O} = \mathrm{End}(E)$ is an order in a quaternion algebra. Moreover, $\mathfrak{A} = \mathcal{O} \otimes \mathbb{Q}$ is ramified at l and at infinity, and $\mathcal{O}$ is a maximal order in $\mathfrak{A}$.

Let E be a fixed supersingular elliptic curves over k. Then the map $F \longmapsto \mathrm{Hom}(E, F)$ determines a bijection of the set of isomorphism classes of supersingular elliptic curves with the isomorphism classes of locally free rank one right $\mathcal{O}$-modules. This is properly stated as an equivalence of categories as follows.

Theorem 1 *Let k be an algebraic closure of a finite field, let $\mathcal{S}$ be the category of supersingular elliptic curves over k, and let E be an object in $\mathcal{S}$. Then the functor $\mathrm{Hom}_{\mathcal{S}}(E, -)$ to the category of locally free rank one right modules over $\mathcal{O} = \mathrm{End}(E)$ is an equivalence of categories.*

Consequences. We note a few consequences of the theorem.

1. Under the equivalence, isogenies of elliptic curves correspond to nonzero $\mathcal{O}$-module homomorphisms. Isomorphism of objects is functorial, thus the finite set of isomorphism classes in each category are in bijective correspondence.

2. Given any right $\mathcal{O}$-module of the form $\mathrm{Hom}(E,F)$ we can choose any element φ. Then the dual determines an embedding

   $$\widehat{\varphi} : \mathrm{Hom}(E,F) \longrightarrow \mathcal{O} = \mathrm{End}(E),$$

   as an ideal of $\mathcal{O}$. By the equivalence of categories every locally free rank one right module over $\mathcal{O}$ is isomorphic to one of the form $\mathrm{Hom}(E,F)$ and all of its embeddings in $\mathcal{O}$ are determined in this way.

3. The *degree* of a morphism $\varphi : I \longrightarrow J$ of right $\mathcal{O}$-modules is defined, which we refer to as the norm $\mathrm{N}(\varphi)$ in the category $\mathcal{I}$. The norm may be defined locally or as the squareroot of $|J/\varphi I|$.

4. For finite extensions $k/\mathbb{F}_l$ the functor $F \longmapsto (\mathrm{Hom}(E,F), \pi_*)$, where π is the Frobenius morphism, gives an equivalence of supersingular elliptic curves over k with an appropriately defined category of pairs.

5. One can define the *j-invariant* of an ideal I. To make the latter well-defined, we must specify an *orientation* $\mathcal{O} \longrightarrow k$ as described in Ribet [13]. An orientation is a homorphism to k, with the kernel equal to the unique prime ideal containing p. The image is a quadratic extension over the prime field, in which the j-invariant of I lies.

6. In its full generality, we take a category of supersingular elliptic curves with level N-structure and ideals of an *Eichler* order of index N in the maximal order.

In terms of computations, the two categories are quite different. The j-invariant of an elliptic curve is trivial to compute, while the endomorphism ring and isogenies are generally difficult. In contrast, determining homomorphisms and the endomorphism ring is easy for ideals, and determining the j-invariant of an $\mathcal{O}$-ideal is presumably of comparable difficulty to that of determining the j-invariant modulo l of a binary quadratic lattice.

§4. Method of graphs.

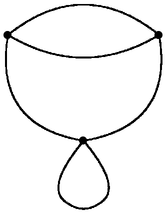
Following Mestre [9] we associate a graph to a set S of representatives of the isomorphism classes of $\mathcal{S}$. Fix an integer n. Let S be the set of *vertices* and let the *edges* $\mathcal{E}$ be the isogenies $\varphi : E \longrightarrow F$ of degree n with cyclic kernel, up to isomophism of F. Define

$$\begin{tikzcd} \mathcal{E} \arrow[r, "i \times t"] & S \times S \\ \varphi \arrow[r, mapsto] & (i(\varphi), t(\varphi)) = (E, F) \end{tikzcd}$$

This defines a directed multigraph. For an edge $\varphi : E \longrightarrow F$ the curve $E = i(\varphi)$ is called the *initial* vertex, and $F = t(\varphi)$ is called the *terminal* vertex.

For a prime $n = p$, the number of edges with initial vertex E are $p+1$ in number, in bijection with the $p+1$ cyclic subgroups of $E[p] = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Due to automorphisms of E, fewer edges may terminate at E.

Example. Let $l = 37$. There are three supersingular elliptic curves over the algebraic closure of $\mathbb{F}_{37}$. Since none of these curves has automorphisms group larger than $\{\pm 1\}$, we can view the graph as undirected. For $p = 2$, we have the graph:



Up to isomorphism there is exactly one supersingular elliptic curve defined over the prime field, and two curves, one conjugate to the other, defined over a quadratic extension. The necessary 3-regularity of the graph and the automorphism induced by the Frobenius morphism completely determine the above graph of 2-isogenies. The adjacency matrix of the graph is the matrix

$$T(2) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix},$$

with characteristic polynomial $(X-3)(X+2)X$. We will see that $T(2)$ can be interpretted as a Hecke operator on the space $M_2(\Gamma_0(37), \mathbb{Q})$ of modular forms of weight two for $\Gamma_0(37)$. The rational roots of the characteristic polynomial for $T(2)$ imply that the Jacobian of the modular curve $X_0(37)$ splits as a product of elliptic curves over $\mathbb{Q}$.

We construct a Hecke module associated to a graph of n-isogenies as follows. Let $\mathfrak{M}$ be the free abelian group with basis S. Define $T(n) : \mathfrak{M} \longrightarrow \mathfrak{M}$ to be the adjacency operator on $\mathfrak{M}$:

$$T(n)E = \sum_{\varphi \in i^{-1}(E)} t(\varphi).$$

We define $T(n)$ to be the n-th *Hecke operator* on $\mathfrak{M}$. Define an inner product on $\mathfrak{M}$ by

$$\langle E, F \rangle = \begin{cases} |\operatorname{Aut}(E)| & \text{if } E = F, \\ 0 & \text{otherwise}, \end{cases}$$

extending by linearity. Then $T(n)$ is self-adjoint with respect to the inner product:

$$\langle E, T(n)F \rangle = \langle T(n)E, F \rangle,$$

and this number equals the count of cyclic isogenies of degree p from E to F. Define an operator $A(n)$ by

$$A(n) = \sum_{r^2 m = n} T(m),$$

the adjacency operator of the graph of all n-isogenies.

In terms of the basis $S = \{E_i\}$ for $\mathfrak{M}$, the operators $T(n)$ and $A(n)$ have matrix representations where $|\operatorname{Aut}(E_j)|A(n)[i,j]$ is the number of isogenies of degree n from E_i to E_j.

For all relatively prime integers n and m, we obtain $T(n)T(m) = T(nm)$, and $T(n)D$ is a symmetric matrix, where D is the diagonal matrix with entries $D[i,i] = |\operatorname{Aut}(E_i)|$. The operators $A(n)$ satisfy the relations

$$A(np^2) = A(p)A(np) - pA(n).$$

The Hecke algebra $\mathbb{T}$ is defined to be the algebra over $\mathbb{Q}$ generated by the operators $T(n)$.

§5. Brandt morphism.

Let $\mathfrak{M}_{\mathbb{Q}} = \mathfrak{M} \otimes \mathbb{Q}$. We define the *Brandt morphism*

$$\Theta : \mathfrak{M}_{\mathbb{Q}} \times \mathfrak{M}_{\mathbb{Q}} \longrightarrow M_2(\Gamma_0(l), \mathbb{Q})$$

by $\Theta(E,F) = \sum q^{\deg \varphi} = \sum \langle A(n)E, F\rangle q^n$, where the first sum is over all elements φ of $\operatorname{Hom}(E,F)$, then extending Θ linearly to $\mathfrak{M}_{\mathbb{Q}}$. That the images lies in $M_2(\Gamma_0(l), \mathbb{Q})$ is a well-known result for theta functions [14]. Eichler proved, as part of his work on the *basis problem* [5], that $\mathfrak{M}_{\mathbb{Q}}$ and $M_2(\Gamma_0(l), \mathbb{Q})$ are isomorphic as Hecke modules. We state this result in the form of the following theorem.

Theorem 2 *The map $T(n) \longmapsto T_2(n)$ of Hecke operators defines an isomorphism of Hecke algebras on $\mathfrak{M}_{\mathbb{Q}}$ and $\mathbb{M}_2(\Gamma_0(l), \mathbb{Q})$ such that the Brandt morphism Θ is a nondegenerate Hecke bilinear map:*

$$\Theta(T(n)E, F) = \Theta(E, T(n)F) = T_2(n)\Theta(E,F),$$

and such that the traces of $T(n)$ on $\mathfrak{M}_{\mathbb{Q}}$ and $T_2(n)$ on $M_2(\Gamma_0(l), \mathbb{Q})$ agree.

We compute the Brandt morphism as follows. The degree map

$$\deg : \operatorname{Hom}_{\mathcal{S}}(F_1, F_2) \longrightarrow \mathbb{Z}$$

is a quadratic map: $\deg(n\varphi) = n^2 \deg(\varphi)$, and by means of a choice of basis, gives a quadratic form. By the equivalence of categories of Theorem 1, we can identify the module $\mathrm{Hom}_{\mathcal{S}}(F_1, F_2)$ with a module $\mathrm{Hom}_{\mathcal{O}}(I_1, I_2)$ of $\mathcal{O}$-homomorphisms of ideals. For a choice of basis we call the associated quadratic form the *norm form.*

Example. Let $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$, defined above. $\mathcal{O}$ is a right principal ideal ring, thus any right ideal I is isomorphic to $\mathcal{O}$ itself, and the ring of $\mathcal{O}$-endomorphisms of I is isomorphic to $\mathcal{O}$, acting by left multiplication. In the above basis, the norm form is given by

$$\begin{aligned} N(x_1 + x_2 i + x_3 j + x_4 \omega) &= f(x_1, x_2, x_3, x_4) \\ &= x_1^2 + x_2^2 + x_3^2 + (x_1 + x_2 + x_3 + x_4)x_4. \end{aligned}$$

We represent a quadratic form f by its Gram matrix M. In this case we write f as the product:

$$f(x_1, x_2, x_3, x_4) = \frac{1}{2} X M X^t = \frac{1}{2} X \left[\begin{array}{cccc} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{array} \right] X^t,$$

where $X = (x_1, x_2, x_3, x_4)$. Therefore the series $\sum_{\varphi \in \mathcal{O}} q^{\mathrm{N}(\varphi)}$ is equal to the theta series

$$\sum_{x_1, \ldots, x_4} q^{f(x_1, x_2, x_3, x_4)} = \sum_n a_n q^n,$$

where a_n is the n-th representation number of f. For the above example, we obtain the Eisenstein series

$$\theta(q) = 1 + 24(q + q^2 + 4q^3 + q^4 + 6q^5 + 4q^6 + 8q^7 + q^8 + 13q^9 + 6q^{10} + \cdots)$$

which generates the module $M_2(\Gamma_0(2), \mathbb{Q})$.

In the previous example the Hecke operator $T(2)$ acted on $M_2(\Gamma_0(37), \mathbb{Z})$ with characteristic polynomial $(X - 3)(X + 2)X$. The eigenspace of 3 is that generated by the Eisenstein series, and the eigenspaces of the eigenvalues -2 and 0 are rational cusp forms, each defining an isogeny class of modular elliptic curves over $\mathbb{Q}$.

§6. Computational aspects of modular curves.

The modular curve $X_0(l)$ has a singular model $\Phi_l(j, j_l) = 0$ based on the map $X_0(l) \longrightarrow X(1) \times X(1)$ taking a moduli point for the isogeny $\varphi : E \longrightarrow F$ to the pair $(j(E), j(F))$. There exists a *Fricke* or *canonical* involution $w_l : X_0(l) \longrightarrow X_0(l)$ which takes φ to its dual, $\widehat{\varphi}$, determining the involution $(j, j_l) \longmapsto (j_l, j)$ on the singular model.

It is often convenient to compute first $X_0^+(l) = X_0(l)/w_l$, a curve of genus at most one half that of $X_0(l)$. The modular functions on $X_0^+(l)$ are just those functions on $X_0(l)$ invariant under w_l. Moreover, by means of a decomposition of modular functions into invariant and anti-invariant spaces under w_l, the order of the poles at each cusp coincide, so relations between functions can be reduced to linear algebra on the Fourier expansions around the single cusp at ∞.

The morphism $X_0(l) \longrightarrow X_0^+(l)$ has degree 2 and is ramified precisely at the points of complex multiplication by an order of discriminant $-l$, $-2l$, or $-4l$. Thus there are precisely $R = h(-l) + h(-2l) + h(-4l)$ ramification points, where $h(D)$ is the class number of an order of discriminant D, when such an order exists, or zero otherwise. By the Riemann-Hurwitz formula, we obtain

$$g_0^+(l) = \frac{g_0(l) + 1 - R/2}{2},$$

where $g_0(l)$ is the genus of $X_0(l)$ and $g_0^+(l)$ is the genus of $X_0^+(l)$. Moreover, $R/2$ is the number of supersingular elliptic curves which can be defined over $\mathbb{F}_l$ and $\dim M_2(\Gamma_0(l), \mathbb{Q}) = g_0(l) + 1$ is the total number.

For the finitely many curves for which $g_0^+(l)$ equals 0, we can compute a Hauptmodul for $X_0^+(l)$, then obtain the function field of $X_0(l)$ as a quadratic extension by a function anti-invariant under w_l. We will thus focus on methods applicable as $g_0^+(l)$ and $g_0(l)$ grow large.

Let $\{f_1, \ldots, f_g\}$ be a basis for the space $S_2(\Gamma_0(l), \mathbb{Q})$ of cusp forms. Then we define the *canonical morphism* to projective space by

$$\begin{tikzcd}
X_0(l) \arrow[r] & \mathbb{P}^{g-1}. \\
Q \arrow[r, mapsto] & (f_1(Q) : \cdots : f_g(Q))
\end{tikzcd}$$

When $X_0(l)$ is nonhyperelliptic of genus greater than two, the canonical morphism is an embedding. In practice we will take a special subset of a basis for $S_2(\Gamma_0(l), \mathbb{Q})$, consisting of forms with prescribed zeros at ∞. We treat some specific examples in Appendix II.

In order to efficiently compute $S_2(\Gamma_0(l), \mathbb{Q})$ and its subspaces of invariant and anti-invariant forms, we will make a detailed study of the Brandt morphism and the decomposition of $\mathfrak{M}_{\mathbb{Q}}$. We begin with the following corollaries of Theorem 2.

Corollary 3 *Let $\mathcal{U}$ be a Hecke submodule of $\mathfrak{M}_{\mathbb{Q}}$. Then the orthogonal decomposition $\mathfrak{M}_{\mathbb{Q}} = \mathcal{U} \oplus \mathcal{V}$ is a decomposition of Hecke modules. Moreover, v lies in $\mathcal{V}$ if and only if $\Theta(u, v) = 0$ for all u in $\mathcal{U}$.*

Proof. Let $u \in \mathcal{U}$ and $v \in \mathcal{V}$, and let T lie in $\mathbb{T}$. Since $Tu \in \mathcal{U}$, we have $\langle u, Tv \rangle = \langle Tu, v \rangle = 0$, so Tv lies in $\mathcal{V}$. Since the $T(n)$ span $\mathbb{T}$ as a $\mathbb{Q}$ vector space, the latter statement is clear from examination of the coefficients of $\Theta(u, v) = \sum_n \langle T(n)u, v \rangle q^n$. □

Corollary 4 $\Theta(-, v) : \mathfrak{M}_{\mathbb{Q}} \longrightarrow M_2(\Gamma_0(l), \mathbb{Q})$ *is an isomorphism of Hecke modules if and only if v is not contained in any proper $\mathbb{T}$-submodule of $\mathfrak{M}_{\mathbb{Q}}$.*

Proof. By Theorem 2 the map $\Theta(-,v)$ is a homomorphism of Hecke modules, and by the last statement of Corollary 3 it follows that $\Theta(-,v)$ is injective if and only if v lies in no proper Hecke submodule. It remains only to show that $\Theta(-,v)$ is surjective when $\mathbb{T}v = \mathfrak{M}_{\mathbb{Q}}$. By the trace condition of Theorem 2,

$$\dim \mathfrak{M}_{\mathbb{Q}} = \mathrm{Tr}(T(1)) = \mathrm{Tr}(T_2(1)) = \dim M_2(\Gamma_0(l), \mathbb{Q}),$$

so Θ is surjective. Let u and w lie in $\mathfrak{M}_{\mathbb{Q}}$, and write $w = Tv$. Then $\Theta(u,w) = \Theta(u,Tv) = \Theta(Tu,v)$, so the image of $\Theta(-,v)$ is all of $M_2(\Gamma_0(l),\mathbb{Q})$. □

$\mathfrak{M}_{\mathbb{Q}}$ has a decomposition as $\mathcal{E}_{\mathbb{Q}} \oplus \mathcal{S}_{\mathbb{Q}}$, where $\mathcal{E}_{\mathbb{Q}}$ is the *Eisenstein space* generated by

$$\mathbf{E} = \sum_{E \in S} |\operatorname{Aut}(E)|^{-1} E,$$

and the *cusp space* $\mathcal{S}_{\mathbb{Q}}$ is the orthogonal complement $\{\sum a_E E : \sum a_E = 0\}$.

From Pizer [11] we know that the canonical involution w_l acts as $-T(l)$ on $\mathfrak{M}$, thus we also have a decomposition $\mathfrak{M}_{\mathbb{Q}} = \mathfrak{M}_{\mathbb{Q}}^{+} \oplus \mathfrak{M}_{\mathbb{Q}}^{-}$, where $\dim \mathfrak{M}_{\mathbb{Q}}^{+} = g_0^{+}(l)$ and $\dim \mathfrak{M}_{\mathbb{Q}}^{-} = g_0(l) - g_0^{+}(l) + 1$. The canonical involution acts by sending E to $-E^{\sigma}$, where σ is the Frobenius automorphism, and E^{σ} is the representative in S of the curve σ-conjugate to E. Thus the spaces $\mathfrak{M}_{\mathbb{Q}}^{+}$ and $\mathfrak{M}_{\mathbb{Q}}^{-}$ are spanned by $\{E - E^{\sigma} : E \in S\}$ and $\{E + E^{\sigma} : E \in S\}$, respectively.

By taking the intersection with the previous decomposition, we obtain an orthogonal decomposition $\mathfrak{M}_{\mathbb{Q}} = \mathcal{E}_{\mathbb{Q}} \oplus \mathcal{S}_{\mathbb{Q}}^{+} \oplus \mathcal{S}_{\mathbb{Q}}^{-}$, where $\mathcal{S}_{\mathbb{Q}}^{+} = \mathfrak{M}_{\mathbb{Q}}^{+}$. Note that $\mathcal{S}_{\mathbb{Q}}^{+}$ is the kernel of $T(l)+1$ and $\mathcal{S}_{\mathbb{Q}}^{-}$ is the kernel of $T(l)-1$ on $\mathcal{S}_{\mathbb{Q}}$. Moreover $T(p)$ has eigenvalue $p+1$ on $\mathcal{E}_{\mathbb{Q}}$ for all primes $p \neq l$ and eigenvalue 1 for $p = l$. Since each such space is defined as the kernel of certain Hecke operators, so is the image. We thus have the following corollary.

Corollary 5 *Let $v \in \mathfrak{M}_{\mathbb{Q}}$. Then $\Theta(\mathcal{E}_{\mathbb{Q}}, v)$, $\Theta(\mathcal{S}_{\mathbb{Q}}^{+}, v)$, and $\Theta(\mathcal{S}_{\mathbb{Q}}^{-}, v)$, are contained in the space of Eisenstein series, invariant cusp forms, and anti-invariant cusp forms, respectively.*

It is clear from Corollary 4 that for general v, equality will hold with the respective image space. We can thus exploit the structure of $\mathfrak{M}_{\mathbb{Q}}$ to decompose the Hecke module before mapping to the respective submodules of $M_2(\Gamma_0(l),\mathbb{Q})$.

Remark. A supersingular elliptic curve E is S lies in $\mathfrak{M}_{\mathbb{Q}}^{-}$ whenever E can be defined over the prime field. This is the basis of the observation of Pizer [12, Remark 2.16] that in the matrix of Θ with respect to the basis S, not every row or column can span $M_2(\Gamma_0(l),\mathbb{Q})$.

Using the equivalence of categories of Theorem 1 we find a basis for $\mathfrak{M}$ in terms of right ideal classes for a fixed maximal order $\mathcal{O}$ in the quaternion algebra ramified at l and ∞. For each pair (I,J), we determine the reduced quadratic norm form of the module $\mathrm{Hom}_{\mathcal{O}}(I,J) = JI^{-1}$. For the resulting positive definite quaternary quadratic forms over $\mathbb{Z}$ there exits a unique reduced form. Beginning with the ideal $\mathcal{O}$, we construct a basis for $\mathfrak{M}$, by choosing neighboring ideals in the graph of homormorphisms of small degree, in analogy with elliptic curves. For two ideals ideals I and J we test for identity via the reduced Gram matrix of $\mathrm{Hom}_{\mathcal{O}}(I, J)$.

By means of an implementation of the arithmetic of quaternion algebras using the computer algebra package Magma V 2.3 [1] we have computed the Hecke module of modular forms of weight two and small level. For instance, for prime level 73, the array of reduced Gram matrices of the ideal forms is the following.

$$\begin{bmatrix}
\begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 4 & 2 & 1 \\ 0 & 2 & 22 & 11 \\ 0 & 1 & 11 & 42 \end{bmatrix} &
\begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 8 & 3 & -2 \\ 2 & 3 & 12 & 5 \\ 1 & -2 & 5 & 22 \end{bmatrix} &
\begin{bmatrix} 6 & 2 & 3 & -1 \\ 2 & 8 & 3 & 4 \\ 3 & 3 & 12 & 4 \\ -1 & 4 & 4 & 16 \end{bmatrix} &
\begin{bmatrix} 6 & 2 & 3 & -1 \\ 2 & 8 & 3 & 4 \\ 3 & 3 & 12 & 4 \\ -1 & 4 & 4 & 16 \end{bmatrix} &
\begin{bmatrix} 6 & 2 & -1 & 0 \\ 2 & 10 & 4 & 3 \\ -1 & 4 & 10 & 4 \\ 0 & 3 & 4 & 14 \end{bmatrix} &
\begin{bmatrix} 6 & 2 & -1 & 0 \\ 2 & 10 & 4 & 3 \\ -1 & 4 & 10 & 4 \\ 0 & 3 & 4 & 14 \end{bmatrix} \\
\begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 8 & 3 & -2 \\ 2 & 3 & 12 & 5 \\ 1 & -2 & 5 & 22 \end{bmatrix} &
\begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 6 & 2 & 1 \\ 0 & 2 & 14 & 7 \\ 0 & 1 & 7 & 40 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 0 \\ 1 & 8 & 4 & 3 \\ -1 & 4 & 12 & 4 \\ 0 & 3 & 4 & 20 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 0 \\ 1 & 8 & 4 & 3 \\ -1 & 4 & 12 & 4 \\ 0 & 3 & 4 & 20 \end{bmatrix} &
\begin{bmatrix} 6 & 1 & 2 & -2 \\ 1 & 8 & 0 & -3 \\ 2 & 0 & 10 & 1 \\ -2 & -3 & 1 & 14 \end{bmatrix} &
\begin{bmatrix} 6 & 1 & 2 & -2 \\ 1 & 8 & 0 & -3 \\ 2 & 0 & 10 & 1 \\ -2 & -3 & 1 & 14 \end{bmatrix} \\
\begin{bmatrix} 6 & 2 & 3 & -1 \\ 2 & 8 & 3 & 4 \\ 3 & 3 & 12 & 4 \\ -1 & 4 & 4 & 16 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 0 \\ 1 & 8 & 4 & 3 \\ -1 & 4 & 12 & 4 \\ 0 & 3 & 4 & 20 \end{bmatrix} &
\begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 10 & 3 & -1 \\ 1 & 3 & 16 & 7 \\ 0 & -1 & 7 & 22 \end{bmatrix} &
\begin{bmatrix} 4 & 2 & 1 & 1 \\ 2 & 6 & 2 & 3 \\ 1 & 2 & 8 & 1 \\ 1 & 3 & 1 & 38 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 1 \\ 1 & 10 & 2 & 3 \\ -1 & 2 & 12 & 6 \\ 1 & 3 & 6 & 16 \end{bmatrix} &
\begin{bmatrix} 6 & 3 & 1 & -2 \\ 3 & 8 & 2 & 1 \\ 1 & 2 & 8 & 2 \\ -2 & 1 & 2 & 20 \end{bmatrix} \\
\begin{bmatrix} 6 & 2 & 3 & -1 \\ 2 & 8 & 3 & 4 \\ 3 & 3 & 12 & 4 \\ -1 & 4 & 4 & 16 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 0 \\ 1 & 8 & 4 & 3 \\ -1 & 4 & 12 & 4 \\ 0 & 3 & 4 & 20 \end{bmatrix} &
\begin{bmatrix} 4 & 2 & 1 & 1 \\ 2 & 6 & 2 & 3 \\ 1 & 2 & 8 & 1 \\ 1 & 3 & 1 & 38 \end{bmatrix} &
\begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 10 & 3 & -1 \\ 1 & 3 & 16 & 7 \\ 0 & -1 & 7 & 22 \end{bmatrix} &
\begin{bmatrix} 6 & 3 & 1 & -2 \\ 3 & 8 & 2 & 1 \\ 1 & 2 & 8 & 2 \\ -2 & 1 & 2 & 20 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 1 \\ 1 & 10 & 2 & 3 \\ -1 & 2 & 12 & 6 \\ 1 & 3 & 6 & 16 \end{bmatrix} \\
\begin{bmatrix} 6 & 2 & -1 & 0 \\ 2 & 10 & 4 & 3 \\ -1 & 4 & 10 & 4 \\ 0 & 3 & 4 & 14 \end{bmatrix} &
\begin{bmatrix} 6 & 1 & 2 & -2 \\ 1 & 8 & 0 & -3 \\ 2 & 0 & 10 & 1 \\ -2 & -3 & 1 & 14 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 1 \\ 1 & 10 & 2 & 3 \\ -1 & 2 & 12 & 6 \\ 1 & 3 & 6 & 16 \end{bmatrix} &
\begin{bmatrix} 6 & 3 & 1 & -2 \\ 3 & 8 & 2 & 1 \\ 1 & 2 & 8 & 2 \\ -2 & 1 & 2 & 20 \end{bmatrix} &
\begin{bmatrix} 2 & 1 & 0 & 1 \\ 1 & 8 & 2 & 1 \\ 0 & 2 & 20 & 5 \\ 1 & 1 & 5 & 20 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & 0 & 2 \\ 1 & 4 & 1 & 1 \\ 0 & 1 & 10 & 5 \\ 2 & 1 & 5 & 40 \end{bmatrix} \\
\begin{bmatrix} 6 & 2 & -1 & 0 \\ 2 & 10 & 4 & 3 \\ -1 & 4 & 10 & 4 \\ 0 & 3 & 4 & 14 \end{bmatrix} &
\begin{bmatrix} 6 & 1 & 2 & -2 \\ 1 & 8 & 0 & -3 \\ 2 & 0 & 10 & 1 \\ -2 & -3 & 1 & 14 \end{bmatrix} &
\begin{bmatrix} 6 & 3 & 1 & -2 \\ 3 & 8 & 2 & 1 \\ 1 & 2 & 8 & 2 \\ -2 & 1 & 2 & 20 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & -1 & 1 \\ 1 & 10 & 2 & 3 \\ -1 & 2 & 12 & 6 \\ 1 & 3 & 6 & 16 \end{bmatrix} &
\begin{bmatrix} 4 & 1 & 0 & 2 \\ 1 & 4 & 1 & 1 \\ 0 & 1 & 10 & 5 \\ 2 & 1 & 5 & 40 \end{bmatrix} &
\begin{bmatrix} 2 & 1 & 0 & 1 \\ 1 & 8 & 2 & 1 \\ 0 & 2 & 20 & 5 \\ 1 & 1 & 5 & 20 \end{bmatrix}
\end{bmatrix}$$

From the representation numbers of the above quadratic forms, we find the first few Hecke operators act on this basis by the matrices:

$$T(2) = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 \end{bmatrix}, \quad T(3) = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}, \quad T(5) = \begin{bmatrix} 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 2 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 & 0 & 2 \\ 2 & 1 & 0 & 1 & 2 & 0 \end{bmatrix},$$

which have respective characteristic polynomials:

$$\begin{array}{rcl}
g_2(t) & = & (t-3)(t-1)(t^2-t-3)(t^2+3t+1), \\
g_3(t) & = & (t-4)(t)(t^2-t-3)(t^2+3t+1), \\
g_5(t) & = & (t-6)(t-2)(t^2+t-3)(t^2+3t+1).
\end{array}$$

In each case, the eigenvalue $p+1$ of $T(p)$ corresponds to the one dimensional space of Eisenstein series and the second linear factor to a one dimensional factor of $J_0(73)$. By calculating sufficiently many coefficients of the corresponding normalized eigenform,

$$\begin{array}{rcl}
f & = & q + q^2 - q^4 + 2q^5 + 2q^7 - 3q^8 - 3q^9 + 2q^{10} - 2q^{11} - 6q^{13} + 2q^{14} - q^{16} \\
 & & + 2q^{17} - 3q^{18} + 8q^{19} - 2q^{20} - 2q^{22} + 4q^{23} - q^{25} - 6q^{26} - 2q^{28} + \cdots
\end{array}$$

we can verify that this corresponds to the single isogeny class of conductor 73 of Cremona's tables [2].

Appendix I

We collect in the following tables the characteristic polynomials $\chi^+(T(p))$ and $\chi^-(T(p))$ of the Hecke operator $T(p)$ on $\mathcal{S}_\mathbb{Q}^+$ and $\mathcal{S}_\mathbb{Q}^-$ for $p = 2$, 3, and 5 and all primes l up to 139.

Characteristic polynomials of Hecke operators on $X_0(l)$.

l	p	$g_0(l)$	$g_0^+(l)$	$\chi^-(T(p))$	$\chi^+(T(p))$
2	2	0	0	–	–
	3			–	–
	5			–	–
3	2	0	0	–	–
	3			–	–
	5			–	–
5	2	0	0	–	–
	3			–	–
	5			–	–
7	2	0	0	–	–
	3			–	–
	5			–	–
11	2	1	0	$X+2$	–
	3			$X+1$	–
	5			$X-1$	–
13	2	0	0	–	–
	3			–	–
	5			–	–
17	2	1	0	$X+1$	–
	3			X	–
	5			$X+2$	–
19	5	1	0	X	–
	3			$X+2$	–
	5			$X-3$	–
23	2	2	0	X^2+X+1	–
	3			X^2-5	–
	5			X^2+2X-4	–
29	2	2	0	X^2+2X-1	–
	3			X^2-2X-1	–
	5			$(X+1)^2$	–
31	2	2	0	X^2-X-1	–
	3			X^2+2X-4	–
	5			$(X-1)^2$	–
37	2	2	1	X	$X+2$
	3			$X-1$	$X+3$
	5			X	$X+2$
41	2	3	0	X^3+X^2-5X-1	–
	3			X^3-4X+2	–
	5			X^3+2X^2-4X-4	–
43	2	3	1	X^2-2	$X+2$
	3			X^2-2	$X+2$
	5			X^2-4X+2	$X+4$
47	2	4	0	$X^4-X^3-5X^2+5X-1$	–
	3			X^4-7X^2+4X+1	–
	5			$X^4+2X^3-16X^2-16X+48$	–
53	2	4	1	X^3+X^2-3X-1	$X+1$
	3			X^3-3X^2-X+1	$X+3$
	5			X^3+2X^2-4X-4	X
59	2	5	0	$X^5-9X^3+2X^2+16X-8$	–
	3			$X^5+2X^4-8X^3-11X^2+13X-1$	–
	5			$X^5-2X^4-14X^3+23X^2+19X+1$	–
61	2	4	1	X^3-X^2-3X+1	$X+1$
	3			X^3-2X^2-4X+4	$X+2$
	5			$X^3+X^2-9X-13$	$X+3$
67	2	5	2	$(X-2)(X^2+X-1)$	(X^2+3X+1)
	3			$(X+2)(X^2-X-1)$	(X^2+3X+1)
	5			$(X-2)(X^2-4X-1)$	$(X+3)^2$
71	2	6	0	$(X^3-5X+3)(X^3+X^2-4X-3)$	–
	3			$(X^3-X^2-4X+3)(X^3+X^2-8X-3)$	–
	5			$(X^3-5X^2-2X+25)(X^3+3X^2-2X-7)$	–

l	p	$g_0(l)$	$g_0^+(l)$	$\chi^-(T(p))$	$\chi^+(T(p))$
73	2	5	2	$(X-1)(X^2-X-3)$	X^2+3X+1
	3			$X(X^2-X-3)$	X^2+3X+1
	5			$(X-2)(X^2+X-3)$	X^2+3X+1
83	2	7	1	$X^6-X^5-9X^4+7X^3+20X^2-12X-8$	$X+1$
	3			$X^6-X^5-10X^4+5X^3+30X^2-4X-25$	$X+1$
	5			$X^6-2X^5-20X^4+28X^3+104X^2-64X-160$	$X+2$
97	2	7	3	$X^4-3X^3-X^2+6X-1$	X^3+4X^2+3X-1
	3			X^4-5X^2-X+4	X^3+4X^2+3X-1
	5			$X^4-X^3-4X^2+X+2$	X^3+3X^2-4X+1
101	2	8	1	$X^7-13X^5+2X^4+47X^3-16X^2-43X+14$	X
	3			$X^7-4X^6-7X^5+38X^4+4X^3-96X^2+13X+68$	$X+2$
	5			$X^7+3X^6-13X^5-33X^4+48X^3+94X^2-43X-67$	$X+1$
103	2	8	2	$X^6-4X^5-X^4+17X^3-9X^2-16X+11$	X^2+3X+1
	3			$X^6-13X^4+40X^2-8X-16$	$(X+1)^2$
	5			$X^6-3X^5-11X^4+34X^3+12X^2-40X-16$	X^2+3X+1
107	2	9	2	$X^7+X^6-10X^5-7X^4+29X^3+12X^2-20X-8$	X^2+X-1
	3			$X^7-3X^6-9X^5+29X^4+14X^3-69X^2+12X+29$	X^2+3X+1
	5			$X^7-5X^6-9X^5+64X^4-28X^3-152X^2+192X-64$	X^2+3X+1
109	2	8	3	$(X-1)(X^4+X^3-5X^2-4X+3)$	X^3+2X^2-X-1
	3			$X(X^4-4X^3-X^2+15X-8)$	X^3+4X^2+3X-1
	5			$(X-3)(X^4-X^3-5X^2+4X+3)$	$X^3+6X^2+5X-13$
113	2	9	3	$(X+1)(X-1)^2(X^3+2X^2-5X-9)$	X^3+2X^2-X-1
	3			$(X-2)(X^2-2X-2)(X^3+X^2-4X-1)$	X^3+5X^2+6X+1
	5			$(X-2)(X^2-12)(X+1)^3$	X^3+X^2-9X-1
127	2	10	3	$X^7-2X^6-8X^5+15X^4+17X^3-28X^2-11X+15$	X^3+3X^2-3
	3			$X^7-3X^6-12X^5+39X^4+26X^3-128X^2+64X+16$	X^3+3X^2-3
	5			$X^7-8X^6+11X^5+53X^4-146X^3+32X^2+128X-48$	X^3+6X^2+9X+1
131	2	11	1	$X^{10}-18X^8+2X^7+111X^6-18X^5-270X^4+28X^3+232X^2+16X-32$	X
	3			$X^{10}-X^9-22X^8+24X^7+157X^6-184X^5-403X^4+533X^3+222X^2-390X+67$	$X+1$
	5			$X^{10}-4X^9-26X^8+116X^7+155X^6-988X^5+138X^4+2384X^3-763X^2-1856X+8$	$X+2$
137	2	11	4	$X^7-10X^5+28X^3+3X^2-19X-7$	X^4+3X^3-4X-1
	3			$X^7-3X^6-8X^5+26X^4+11X^3-58X^2+16X+14$	$X^4+5X^3+4X^2-10X-11$
	5			$X^7+2X^6-18X^5-21X^4+103X^3+26X^2-188X+88$	$X^4+2X^3-12X^2-23X+1$
139	2	11	3	$(X-1)(X^7-X^6-11X^5+8X^4+35X^3-10X^2-32X-8)$	X^3+2X^2-X-1
	3			$(X^7+2X^6-15X^5-25X^4+56X^3+52X^2-56X-16)$	X^3+2X^2-X-1
	5			$(X+1)(X^7-11X^6+36X^5+2X^4-211X^3+319X^2-55X-83)$	$X^3+8X^2+19X+13$

Appendix II
Computations of modular curves

The modular curve $X_0(l)$ is defined in terms of generators and relations for the field of meromorphic modular functions of weight zero for $\Gamma_0(l)$. We define $Y_0(l)$ to be the affine open subset $\mathfrak{H}/\Gamma_0(l)$ of $X_0(l)$. The space of weight zero modular functions holomorphic on $\mathfrak{H}$ can be identified with the ring R of functions on $Y_0(l)$. In order to have a working model for computing with the curve, we require expressions for $j(q)$ and $j(q^l)$ in R. Moreover if we are to apply the ideas of Elkies [7] for efficiently computing isogenies of curves, we require a description of the five Eisenstein series

$$E_2^{(l)}(q), \quad E_4(q^l), \quad E_4(q), \quad E_6(q), \text{ and } E_6(q^l)$$

in the ring $M = \bigoplus M_k(\Gamma_0(l), \mathbb{Q})$ of modular forms for $\Gamma_0(l)$.

We thus collect here the definitions of standard modular functions as well as some calculations of the graded rings of modular forms for $\Gamma_0(l)$. For the present purposes we will restrict to prime level l.

Standard modular forms

The function $E_k(q)$ denotes the normalized Eisenstein series with Fourier series expansion

$$E_k(q) = 1 - \frac{2k}{B_k} \sum_n \frac{n^{k-1} q^n}{1 - q^n} = 1 - \frac{2k}{B_k} \sum_n \sigma_{k-1}(n) q^n,$$

where $\sigma_r(n)$ denotes the sum of the r-th power of the divisors of n, and B_k is the k-th Bernoulli number. We write

$$\begin{aligned} E_k^{(l)}(q) &= l^{k/2} E_k(q^l) - E_k(q), \\ E_k^{+}(q) &= l^{k/2} E_k(q^l) + E_k(q). \end{aligned}$$

Note that $w_l E_k(q) = l^{k/2} E_k(q^l)$, so that $E_k^{(l)}(q)$ is anti-invariant and $E_k^{+}(q)$ is invariant under w_l. While neither $E_2(q)$ nor $E_2(q^l)$ is a modular form, the function $E_2^{(l)}(q)$ is, generating the Eisenstein space of weight two for $\Gamma_0(l)$. The *delta* function $\Delta(q)$ is defined in terms of Eisenstein series as $(E_4(q)^3 - E_6(q)^2)/12^3$. The *Dedekind eta* function is a 24-th root of $\Delta(q)$, having q-expansion

$$\eta(q) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

It is well-known that $\Delta(q)$, hence also $\eta(q)$, has no zeros on the upper half plane $\mathfrak{H}$. Thus we will be able to invert $\eta(q)$ to produce new functions without introducing poles on $\mathfrak{H}$.

Genus zero curves

For $l = 2, 3, 5, 7$, and 13, the modular curve $X_0(l)$ has genus zero, hence we can find a degree one function on $X_0(l)$. For this purpose we take the *Hauptmodul*

$$h = \left(\frac{\eta(q)}{\eta(q^l)}\right)^{24/(l-1)},$$

defined as a degree one function having neither zeros nor poles on $\mathfrak{H}$. The function h is holomorphic outside of the cusps and transforms under the involution w as $w_l(h) = l^{12/(l-1)}h^{-1}$. We set u equal to h/l^n, for appropriate n, and find the following expressions for the j-invariant in terms of u.

$$l = 2: \quad u = 64^{-1}\left(\frac{\eta(q)}{\eta(q^2)}\right)^{24}, \quad w_l(u) = 1/u, \qquad j = \frac{64(u+4)^3}{u^2},$$

$$l = 3: \quad u = 27^{-1}\left(\frac{\eta(q)}{\eta(q^3)}\right)^{12}, \quad w_l(u) = 1/u, \qquad j = \frac{27(u+1)(u+9)^3}{u^3}.$$

$$l = 5: \quad u = 25^{-1}\left(\frac{\eta(q)}{\eta(q^5)}\right)^{6}, \quad w_l(u) = 1/5u, \qquad j = \frac{25(u^2+10u+5)^3}{u^5}.$$

$$l = 7: \quad u = 49^{-1}\left(\frac{\eta(q)}{\eta(q^7)}\right)^{4}, \quad w_l(u) = 1/49u,$$

$$j = \frac{(49u^2+13u+1)(u^2+5u+1)^3}{u^7}.$$

$$l = 13: \quad u = 13^{-1}\left(\frac{\eta(q)}{\eta(q^{13})}\right)^{2}, \quad w_l(u) = 1/169u,$$

$$j = \frac{(13u^2+5u+1)(u^4+19u^3+20u^2+7u+1)^3}{u^{13}}.$$

Similar functions can be found for curves $X_0^+(l)$, where l is one of the ten primes 11, 17, 19, 23, 29, 31, 41, 47, 59 and 71 for which $X_0^+(l)$ is of genus zero.

Graded rings of modular forms

In order to produce the graded ring of modular forms we must find modular forms of low weight such that for all k, monomials in the forms span the spaces $M_k(\Gamma_0(l), \mathbb{Q})$ over $\mathbb{Q}$. The ring of modular forms of level 1 is $M = \mathbb{Q}[E_4(q), E_6(q)]$. The dimension of the space $M_k(\Gamma_0(l), \mathbb{Q})$ is

$$1 - k/2 + [k/4] + [k/3].$$

From Theorem 2.23 in Shimura [16] we find that for $l \neq 2, 3$ and all even k greater than 2, that

$$\begin{aligned}\dim M_k(\Gamma_0(l)) &= (k-1)(g_0(l)-1) + k + \nu_2 \left[\frac{k}{4}\right] + \nu_3 \left[\frac{k}{3}\right] \\ \dim M_k^+(\Gamma_0(l)) &= (k-1)(g_0^+(l)-1) + k/2 + (R+\nu_2/2) \left[\frac{k}{4}\right] + (\nu_3/2) \left[\frac{k}{3}\right]\end{aligned}$$

where $g_0^+(l) = (g_0(l) + 1 - R/2)/2$ with $R = h(-l) + h(-4l)$, and where

$$\nu_2 = 1 + \left(\frac{-4}{l}\right) \quad \text{and} \quad \nu_3 = 1 + \left(\frac{-3}{l}\right).$$

Recall that $h(D)$ denotes the class number of a binary quadratic order of discriminant D, where such exists, and is zero otherwise. Let $K = \mathbb{Q}(X_0(l))$ be the function field of $X_0(l)$ and note that $KM = K[\omega]$ for any ω in $M_2(\Gamma_0(l), \mathbb{Q})$.

Level 2.

The graded ring of modular functions for $\Gamma_0(2)$ is $\mathbb{Q}[X, Y]$, with

$$X = E_2^{(2)}, \quad \text{and} \quad Y = E_4^{(2)}/3 = \frac{u-1}{u+1} X^2,$$

where u is the Hauptmodul defined above for $\Gamma_0(2)$. By means of an analysis of the ramification of $X_0(2) \longrightarrow X_0^+(2)$ we find the dimensions of the spaces of modular forms of even weight are given by

$$\begin{aligned}\dim M_k(\Gamma_0(2), \mathbb{Q}) &= 1 + [k/4], \\ \dim M_k^+(\Gamma_0(2), \mathbb{Q}) &= 1 - k/2 + [k/4] + [3k/8],\end{aligned}$$

and verify that this agrees with the dimensions of the graded components of $\mathbb{Q}[X, Y]$. We express the standard Eisenstein series in terms of X and Y as follows:

$$\begin{aligned} E_4^{(2)}(q) &= 3Y, & E_4^+(q) &= 5X^2, \\ E_6^{(2)}(q) &= 7X^3, & E_6^+(q) &= 3XY. \end{aligned}$$

Level 3.

The graded ring of modular functions for $\Gamma_0(3)$ is $\mathbb{Q}[X, Y, Z]/I$, where

$$X = E_2^{(3)}(q)/2, \quad Y = E_4^{(3)}(q)/8, \quad \text{and} \quad Z = (\eta\eta_3)^6,$$

and where I is the ideal $(X^4 - 108XZ - Y^2)$. The forms Y and Z can be expressed in the ring $\mathbb{Q}(u)[X]$ as

$$Y = \frac{u-1}{u+1} X^2, \quad \text{and} \quad Z = \frac{u}{27(u+1)^2} X^3,$$

where u is the Hauptmodul defined above for $\Gamma_0(3)$. As above we deduce from the ramification of $X_0(3) \longrightarrow X_0^+(3)$ and Theorem 2.23 of Shimura [16] that the dimensions of the spaces of modular forms of even weight are as follows:

$$\begin{aligned} \dim M_k(\Gamma_0(3), \mathbb{Q}) &= 1 + [k/3]\,, \\ \dim M_k^+(\Gamma_0(3), \mathbb{Q}) &= 1 - k/2 + [5k/12] + [k/4]\,, \end{aligned}$$

and verify that this coincides with the dimensions of the graded components of $\mathbb{Q}[X, Y, Z]/I$. We express the Eisenstein series for $\Gamma_0(3)$ in terms of X, Y, and Z, by the following relations:

$$\begin{array}{lll} E_2^{(3)}(q) = 2X, & E_4^{(3)}(q) = 8Y, & E_4^+(q) = 10X^2, \\ E_6^{(3)}(q) = 26X^3 - 432Z, & & E_6^+(q) = 28XY. \end{array}$$

Mapping forms to functions

Determining the full ring of modular forms of a given level is an impractical undertaking in general, as the size of a basis for $M_k(\Gamma_0(l), \mathbb{Q})$ grows in proportion to both k and l. Rather, following Elkies [7], we find a modular form λ of weight -2 with no poles on $\mathfrak{H}$ then map the spaces $M_{2m}(\Gamma_0(l))$ to meromorphic functions on $X_0(l)$ all of whose poles lie at the cusps, by $f \longmapsto \lambda^m f$.

For the purpose of constructing such a λ, we introduce certain generalized theta function of weight one. Let $\mathfrak{a}$ be an ideal in the quadratic imaginary order R of discriminant D. Then

$$\theta_{\mathfrak{a}}(q) = \sum_{x \in \mathrm{Hom}(R, \mathfrak{a})} q^{\mathrm{N}(x)},$$

where $\mathrm{N}(x)$ is the cardinality of the ideal quotient $\mathfrak{a}/x(R)$, is a modular form of weight one and level $|D|$. The product of any two such forms is a modular form of weight two and level $|D|$, which is anti-invariant under the canonical involution.

For $l \equiv 3 \bmod 4$ we can set $D = -l$ to obtain modular forms of level l. As in Elkies' manuscript [6] we can modify the construction for forms associated to discriminant $D = -4l$ to obtain forms with characters and level l, when $l \equiv 1 \bmod 4$.

Since 2 ramified in R, the ring $R/2R$ is isomorphic to $\mathbb{F}_2[\varepsilon]$, where $\varepsilon^2 = 0$. Fix an isomorphism $R/2R \cong \mathfrak{a}/2\mathfrak{a}$, and let $\chi : R/2R \longrightarrow \{-1, 0, 1\}$ be the unique character on $R/2R$. Then

$$\theta_{\mathfrak{a}}^{\chi}(q) = \sum_{x \in \mathrm{Hom}(R, \mathfrak{a})} \chi(x) q^{\mathrm{N}(x)/4},$$

where χ is defined on $\mathfrak{a}$ via the reduction to $\mathfrak{a}/2\mathfrak{a}$ and isomorphism with $R/2R$.

We may take λ to be the following function, according to the congruence class of l modulo 12.

$\underline{l \equiv 1 \bmod 4}$. Set $\lambda = \theta/(\eta\eta_l)^3$, where θ is a linear combination of functions $\theta_{\mathfrak{a}}^{\chi}$ having maximal zero at the cusps, and with each $\mathfrak{a}$ in the correct genus such that $\theta_{\mathfrak{a}}^{\chi}$ and $(\eta\eta_l)^3$ have the same character. There exists such an ideal with $\theta_{\mathfrak{a}}^{\chi} \neq 0$ for all primes $l \equiv 1 \bmod 4$ except for the three primes 5, 13, and 37 for which $\mathbb{Z}[\sqrt{-l}]$ has class number two.

$\underline{l \equiv 7 \bmod 12}$. Set $\lambda = \theta/(\eta\eta_l)^3$, for the linear combination θ of functions $\theta_{\mathfrak{a}}$ having the highest order zero at the cusps.

$\underline{l \equiv 11 \bmod 12}$. Set $\lambda = \omega^{-1}$, where $\omega = (\eta\eta_l)^2$, the unique anti-invariant cusp form with a zero of maximal order at the cusps.

In each case λ is a modular function of weight -2, holomorphic on $\mathfrak{H}$, which is anti-invariant under the canonical involution.

Level 73.

Using a decomposition of $S_2(\Gamma_0(73), \mathbb{Q})$ into invariant and anti-invariant forms, we set $\{f_1, f_2\}$ equal to the echelon basis

$$\begin{aligned} f_1 &= q - 3q^3 - 3q^4 + q^6 - 3q^7 + 3q^8 + 5q^9 - q^{10} - 3q^{11} + \cdots \\ f_2 &= q^2 - q^3 - 3q^4 + q^5 + 4q^8 + 3q^9 - 3q^{10} - q^{11} + 3q^{12} + \cdots \end{aligned}$$

for the space $S_2^+(\Gamma_0(73), \mathbb{Q})$ of invariant cusp forms, and let $\{g_1, g_2, g_3\}$ be the basis

$$\begin{aligned} g_1 &= q + q^3 - q^4 + 2q^5 - q^6 + q^7 - q^8 - q^9 + q^{10} - q^{11} + \cdots \\ g_2 &= q^2 - q^3 + q^4 - q^5 - q^9 - q^{10} + q^{11} - q^{12} + q^{13} + \cdots \\ g_3 &= q^4 - q^5 - q^6 - q^7 + 2q^8 + q^9 - 2q^{10} + 2q^{11} - q^{12} + \cdots \end{aligned}$$

for the anti-invariant forms such that $g_1/g_2 = f_1/f_2$. Note that both f_2 and g_3 are uniquely determined as the invariant and anti-invariant forms having zeros of maximum order at the cusps. By Chaper IV §5 of Hartshorne [8], the forms f_1 and f_2 define the degree 2 canonical morphism of $X_0^+(73)$ to a genus zero curve $C_0 = X_0^+(73)/\sim$, where $\sim$ is the hyperelliptic involution of $X_0^+(73)$. Set t and u equal to the invariant functions

$$\begin{aligned} t &= f_1/f_2 - 1 = q^{-1} + q + 2q^3 + 2q^4 + q^5 + q^6 + 3q^7 + \cdots \\ u &= g_1/g_3 = q^{-3} + q^{-2} + 3q^{-1} + 4 + 8q + 11q^2 + 19q^3 + \cdots \end{aligned}$$

satisfying the equation

$$u^2 - (t^3 + t^2 + 1)u - t(t-1)(t+1) = 0.$$

Then t is a generator for the function field of C_0, having poles only at the cusp of $X_0^+(73)$ and its image under $\sim$. Since the twist of u by the hyperelliptic involution

$$\sim u = (t^3 + t^2 + 1) - u = -1 + q + q^3 - 5q^4 - q^5 + 6q^6 + 3q^7 + \cdots$$

has value -1 at the cusp, we conclude that u is holomorphic on $\mathfrak{H}$. We eliminate the pole of t to find a degree 4 function $v = (u+1)t$ on $X_0^+(73)$.

Let R be the imaginary quadratic order of discriminant -292, and set $\mathfrak{a} = R$ and $\mathfrak{b}$ equal to a prime ideal of norm 7. We obtain two modified theta functions

$$\begin{array}{rcl} \theta_{\mathfrak{a}}^{\chi}(q) & = & q^{1/4}(1 + q^2 + q^6 + q^{12} - q^{18} - 2q^{19} + q^{20} - 2q^{22} + \cdots) \\ \theta_{\mathfrak{b}}^{\chi}(q) & = & q^{3/4}(q - q^2 - q^7 + q^{10} - q^{11} + q^{14} + q^{15} + q^{20} + \cdots) \end{array}$$

set $\lambda = \theta_{\mathfrak{b}}^{\chi}/(\eta\eta_{73})^3$, and find a degree 5 function

$$w = \lambda g_3 = \frac{u(u-1)}{t} = \frac{u(u-1)(u+1)}{v} = t(u+v) - 1,$$

holomorphic on $\mathfrak{H}$, and conclude that u, v, and w generate the ring of functions on $X_0^+(73)$ with poles only at the cusp.

To complete the calculation of modular functions for $X_0(73)$, we set x equal to the degree 3 function f_1/g_3 and y equal to the degree 5 function

$$y = \frac{\lambda(f_1 - f_2)}{u} = \frac{(1 - v + w)x}{u}.$$

We verify that x and y are holomorphic on $\mathfrak{H}$ by expressing their squares in terms of u, v, and w:

$$\begin{array}{rcl} x^2 & = & u^2 - 8v - 12u - 8 \\ y^2 & = & u^2v - u^3 - 7uw + 2uv + 3u^2 - 2w + 6v - u - 10 \end{array}$$

By the Riemann-Roch theorem, we see that these functions generate the ring of meromorphic functions on $X_0(73)$ with poles only at the cusps. Each of the functions $\lambda E_2^{(73)}$, $\lambda^2 E_4^{(73)}$, $\lambda^2 E_4^+$, $\lambda^3 E_6^{(73)}$, and $\lambda^3 E_6^+$ can thus be expressed in terms of u, v, w, x and y.

Level 239.

By computing the Hecke module of theta function we find the echelon basis $\{f_1, f_2, f_3\}$

$$\begin{array}{rcl} f_1 & = & q - q^4 - 2q^5 - q^6 - q^7 - q^9 - q^{11} - q^{12} - 3q^{13} + \cdots \\ f_2 & = & q^2 - q^4 - q^5 - q^6 - q^8 + q^9 - q^{11} - q^{13} - q^{14} + \cdots \\ f_3 & = & q^3 - q^4 - q^5 + q^8 + q^{10} - q^{11} - q^{12} - q^{13} - 2q^{15} + \cdots \end{array}$$

for the space $S_2^+(\Gamma_0(239))$ of cusp forms invariant under the canonical involution. Likewise we compute an echelon basis for the space of anti-invariant cusp forms in $S_2(\Gamma_0(239))$, and take the four forms

$$\begin{array}{rcl} g_1 & = & q^{14} - 3q^{17} - 6q^{18} + q^{19} + 23q^{21} + 11q^{22} - 17q^{23} + \cdots \\ g_2 & = & q^{15} - 2q^{17} - 3q^{18} + 12q^{21} + 7q^{22} - 10q^{23} + 6q^{26} + \cdots \\ g_3 & = & q^{16} - q^{17} - 2q^{18} + 6q^{21} + 2q^{22} - 4q^{23} - 3q^{24} + \cdots \\ g_4 & = & q^{20} - 2q^{21} - q^{22} + 2q^{23} + q^{24} + 2q^{25} - 2q^{26} + \cdots \end{array}$$

of highest zeros at the cusps. Necessarily g_4 is the form $(\eta\eta_{239})^2$, with no zeros on the upper half plane $\mathfrak{H}$.

We set $X = f_3$, $Y = f_2$, and $Z = f_1$, and find a nonsingular quartic relation

$$X^4 - X^3(Y+Z) + X^2Z^2 + XZ(Y^2 - Z^2) - Y^2(Y^2 + YZ - Z^2) = 0,$$

defining the canonical embedding of $X_0^+(239)$ as a plane curve. We set x, y, and z to be the modular functions f_3/g_4, f_2/g_4, and f_1/g_4, respectively.

Next we set u, v, and w equal to the functions on $X_0^+(239)$,

$$\begin{aligned}
u &= g_3/g_4 = q^{-4} + q^{-3} + q^{-2} + q^{-1} + 1 + 2q + 3q^2 + 3q^3 + 4q^4 + \cdots \\
v &= g_2/g_4 = q^{-5} + 2q^{-4} + 3q^{-3} + 3q^{-2} + 4q^{-1} + 3 + 7q + 9q^2 + 11q^3 + \cdots \\
w &= g_1/g_4 = q^{-6} + q^{-5} + 5q^{-4} + 6q^{-3} + 7q^{-2} + 8q^{-1} + 4 + 15q + 21q^2 + \cdots \\
&= (v^3 + 2u^3 + 31v + 11v^2 - 8uv + 5u^2 - 37u - 9)/(uv + u^2 + v + 8u + 9),
\end{aligned}$$

of degree 4, 5, and 6, respectively. By eliminating coefficients, we find a function $r = uw - v^2 + uv - u^2$ of degree 7, and the ring of modular functions for $X_0^+(239)$ is generated by u, v, and w, satisfying the relations

$$\begin{gathered}
w^2 - u^3 - vw - v^2 - 3uw + uv + 5w - 14v - 10u - 19 = 0 \\
w(uv + u^2 + v + 8u + 9) = v^3 + 2u^3 + 31v + 11v^2 - 8uv + 5u^2 - 37u - 9
\end{gathered}$$

By the relation $z = uy - vx + y - 4x$, we find that u, v, w, x, and y generate the ring of modular functions on $X_0(239)$ with poles only at the cusps. We verify that the gap sequence consists exactly of the $g(l)$ gaps accounted for by the Riemann-Roch theorem, so that these functions indeed generate the full ring of modular functions holomorphic on $\mathfrak{H}$.

To complete a working model for $X_0(l)$ we solve for x^2, xy, and y^2 in terms of u, v, and w, and find expressions for the five functions

$$\lambda E_2^{(239)}(q), \quad \lambda^2 E_4^{(239)}(q), \quad \lambda^2 E_4^+(q), \quad \lambda^3 E_6^{(239)}(q), \quad \text{and } \lambda^3 E_6^+(q),$$

with $\lambda = g_4^{-1}$, in $\mathbb{Q}[u, v, w, x, y]$.

References

[1] Wieb Bosma, John Cannon, Catherine Playoust, et al. *Magma reference manual.* Online reference document, 1997.

[2] John E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, 1992.

[3] John E. Cremona. Computing the degree of the modular parametrization of a modular elliptic curve. *Mathematics of Computation*, 64(211):1235–1250, 1995.

[4] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.

[5] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In W. Kuyk, editor, *Modular Functions of One Variable I*, volume 320 of *Lecture Notes in Mathematics*, pages 75–152. Springer–Verlag, 1973.

[6] N. Elkies. Explicit isogenies. Manuscript, 1991.

[7] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory A conference in honor of A.O.L. Atkin*, 1998.

[8] R. Hartshorne. *Algebraic Geometry*. Springer–Verlag, 1977.

[9] J.-F. Mestre. Sur la méthode des graphes, exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, pages 217–242. Nagoya University, 1986.

[10] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques. *J. Théorie des Nombres de Bordeaux*, 7:255–282, 1995.

[11] A. Pizer. The action of the canonical involution on modular forms of weight 2 on $\Gamma_0(N)$. *Math. Ann.*, 226:99–116, 1977.

[12] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *Journal of Algebra*, 64:340–390, 1980.

[13] K. Ribet. Bimodules and abelian surfaces. In *Algebraic number theory*, volume 17 of *Advanced Studies in Pure Mathematics*, pages 359–407. Academic Press, 1989.

[14] B. Schoeneberg. *Elliptic Modular Functions*. Springer-Verlag, 1974.

[15] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985.

[16] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1971.

[17] R. Taylor and A. Wiles. Ring-theoretic properties of certain hecke algebras. *Annals of Mathethematics (2)*, 141(3):553–572, 1995.

[18] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics (2)*, 141(3):443–551, 1995.