Arithmetic of Modular Curves and Applications

Gerhard Frey and Michael Müller
Institut für Experimentelle Mathematik
Universität (GH) Essen, Ellernstr. 29, 45326 Essen (Germany)
email: {frey, mdm}@exp-math.uni-essen.de

August 25, 1998

Abstract

The aim of this article is to describe a computational approach to the study of the arithmetic of modular curves $X_0(N)$ and to give applications of these computations.

1 Introduction

Let K be a number field and C/K be a (projective irreducible regular) curve defined over K. The most challenging question of computational Diophantine geometry is to determine the set $C(K)$ of $K-$rational points of C. The most general theoretical result one has at ones disposition is Faltings' celebrated theorem that $C(K)$ is a finite set if the genus of C is larger than one. Unfortunately until now there is no effective version of this result available. There are two major tools to achieve a solution of the stated problem at least in concrete cases. First one can use the theory of minimal models for surfaces to extend C to a surface $\mathcal{C}$ over the ring $\mathcal{O}_K$, the integers of K, with best possible properties. The special fibers $\mathcal{C}_\mathfrak{p}$ of this surface at primes $\mathfrak{p}$ of $\mathcal{O}_K$, the reductions of $C \bmod \mathfrak{p}$, are not necessarily regular curves. They can be used to extract further information from C. As an example we mention the global $L-$series $L(C,s)$ related to C which is defined as the Euler product of the local $L-$series related to $\mathcal{C}_\mathfrak{p}$. Results of Hasse and Weil imply that $L(C,s)$ is a Dirichlet-series which converges for complex numbers with sufficiently large real part.

There is the central **Conjecture of Hasse and Weil:**

$\mathbf{L(C,s)}$ has an analytic continuation to $\mathbb{C}$ which satisfies a (well–determined) functional equation.

This conjecture is closely related to the second tool we shall discuss to study the arithmetic of C, its *Jacobian variety* J_C.

J_C is an abelian variety with a principal polarization induced by C defined over K. The theorem of *Torelli* states that J_C together with this polarization determines C up to $K-$isomorphism.

Question: Can one make this relation explicit?

A more precise version of this question is the following: If one knows that a complex torus given by its period matrix together with a principal polarization is the Jacobian of a curve C over a given number field (e.g. $\mathbb{Q}$) can one write down an equation for C?

Let us assume that $C(K)$ contains a point P_0. Using the fact that J_C is isomorphic to $Pic^0(C)$, we get a morphism of C (or more generally of symmetric products of C) to J_C with P_0 as base point.

This relation between C and J_C makes it obvious that information about $C(K)$ can be obtained from $J_C(K)$ and vice versa. It is important to note that due to results of Grothendieck and Raynaud the arithmetic surface $\mathcal{C}$ is closely related to the canonical extension of J_C to a group scheme over $\mathcal{O}_K$, its Néron model. The $L-$series of C is equal to the $L-$series of J_C which can be interpreted as an Euler product where the local factor at ℓ is the characteristic polynomial of Frobenius automorphisms acting on the first ℓ–adic cohomology group of J_C, the Tate module of J_C at ℓ. Hence we get a relation between diophantine problems and $\ell-$adic Galois representations of the Galois group G_K of K which is of greatest importance (cf. the proof of the theorem of Faltings).

Another important aspect of the $L-$series is the connection with rational points on $Pic^0(C)$. The local factors $L_{\mathfrak{p}}(t)$ take the value $\#Pic^0(\mathcal{C}_{\mathfrak{p}})(\mathcal{O}_K/\mathfrak{p})$ at $t=1$. Globally one knows by the *Theorem of Mordell-Weil* that $J_C(K)$ is a finitely generated $\mathbb{Z}$–module which has a natural euclidean structure given by the Néron-Tate pairing. The *Conjecture of Birch and Swinnerton-Dyer* assumes the truth of the conjecture of Hasse-Weil and predicts that the arithmetic data of this euclidean module can be deduced from the analytical behavior of $L(C,s)$ at $s=1$. Manin used this conjecture to construct a conditional algorithm to determine generators of $J_C(K)$.

The purpose of this paper is to give a report on possibilities to solve a good part of the algorithmic problems described above in special cases:
We take $K=\mathbb{Q}$ and assume that J_C is isogenous to a factor of the Jacobian of a modular curve X.
In fact we restrict ourselves to the simplest case and assume that X is one of the modular curves $X_0(N)$ parameterizing elliptic curves with cyclic isogenies of degree N. We remark that nearly all algorithms could be applied to the curves $X=X_1(N)$ or intermediate curves, too.

The origin of our algorithms is the concrete knowledge of the holomorphic differentials as cusp forms resp. their dual space, the singular homology, of $X_0(N)$ over $\mathbb{Z}$ together with the action of a big part of the endomorphism ring of the Jacobian given by the ring $\mathbb{T}_N$ of Hecke operators. Moreover the geometric $L-$series of $X_0(N)$ can be defined analytically and the conjecture of Hasse-Weil is true. For the convenience of the reader we describe this theory in the next section.

In the third section we develop the basic algorithms which depend on results of Manin, Merel and Zagier. They use the theory of Manin resp. modular symbols with explicit action of $\mathbb{T}_N$ to decompose the space of cusp forms into eigenspaces w.r.t. the action of the group ring $\mathbb{T}_N[G_{\mathbb{Q}}]$. This determines the $\mathbb{Q}$–factors of $J_0(N)$, the Jacobian of $X_0(N)$, up to isogeny. Moreover we can construct $\mathbb{Z}$–bases of these spaces by expanding modular forms into Fourier series. There are other methods to compute the space of modular, respectively cusp forms, for example the algorithm of Birch ([Bir91]) which uses ternary quadratic forms. This is a special case of the method of Brandt matrices developed by M. Eichler (see [Eic72]) and generalized by Pizer. Another possibility is Mestre's 'graph'–method [Mes86] to compute the space of cusp forms. The modular symbol method works for every level N and the whole space of cusp forms. The other methods are restricted to special levels or they compute only a subspace of the space of modular forms in general.

In the last section we shall give applications of these calculations. They include the computation of modular forms of weight 1 and weight 3/2 and their application to Artin's conjecture and to the determination of Selmer groups of twists of elliptic curve, the computation of the intersection pairing inside of $J_0(N)$ with applications to congruence primes and interesting diophantine conjectures like the ABC–conjecture, the computation of period matrices of factors of $J_0(N)$ and the explicit construction of curves up to genus 5 which are hyperelliptic with Jacobians equal to one of these factors. Since we can compute the characteristic polynomial of Hecke operators T_l for rather large prime numbers l we can use the Eichler-Shimura relation to compute local factors of the $L-$series corresponding to such curves over large finite field. This is of interest for the construction of public key crypto systems based on discrete logarithms.

Finally we want to mention that using the modular theory and assuming the correctness of Manin's conditional algorithm, it is possible to determine the Mordell-Weil group of the Jacobian of hyperelliptic curves over $\mathbb{Q}$ obtained above, at least in principle. For curves of genus 2 we give some results.

Acknowledgments
The algorithms and results described in this report rely on work of many members of our research group in number theory at the IEM in Essen during the last years. Especially J. Basmaji, Ch. Hahne, L. Merel (who was a visitor at the IEM on several occasions), X. Wang and H.-J. Weber provided many valuable and essential contributions. The authors would like to thank them very much.
The cooperation in our group at the IEM was to a large part made possible by the support given by the DFG in the frame of the Schwerpunkt. We are very thankful for this.

2 The Modular Curve $X_0(N)$

In this section we fix notations and summarize the basic facts on modular curves. The reference for this section is Shimura's book [Shi71].

2.1 Basic Definitions

Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of integral 2×2 matrices with determinant one. $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ and } R = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

For a positive integer N, denote by

$$\Gamma_0(N) = \{\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \bmod N\}$$

the Hecke subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of *level* N. $\mathrm{SL}_2(\mathbb{R})$ and hence $\Gamma_0(N)$ act via fractional linear transformations given by

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z \mapsto \tfrac{az+b}{cz+d}$$

on the upper half plane

$$\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

and, by the same formula, on the extended upper half plane

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$$

obtained from $\mathbb{H}$ by adjoining the set of *cusps* $\mathbb{Q} \cup \{\infty\}$ to $\mathbb{H}$. We denote the orbits of this action by

$$Y_0(N) := \Gamma_0(N)\backslash\mathbb{H} \subseteq \Gamma_0(N)\backslash\mathbb{H}^* =: X_0(N)$$

and call $X_0(N)$ the *modular curve of* $\Gamma_0(N)$.

The modular curve $X_0(N)$ ($Y_0(N)$, resp.) is equipped with a complex analytic structure coming from the projection map

$$\pi : \mathbb{H}^* \longrightarrow \Gamma_0(N)\backslash\mathbb{H}^* \, (\pi : \mathbb{H} \longrightarrow \Gamma_0(N)\backslash\mathbb{H}, \mathrm{resp.}).$$

(Special attention has to be given to the complex structure at the cusps, see [Shi71] Chap. 1.) With this structure $Y_0(N)$ is a connected one dimensional complex manifold. It is a Riemann surface with π as a covering map unramified outside of elliptic points which are conjugate to $z = i$ and $z = \zeta_3$ under the action of $\mathrm{SL}_2(\mathbb{Z})$. $X_0(N)$ is the compactification of $Y_0(N)$ which we get by adjoining the cusps of $\Gamma_0(N)$ to $Y_0(N)$. Therefore we can view $X_0(N)$ as a projective algebraic curve defined over $\mathbb{C}$.

Example 2.1

1. $N = 1$: $X_0(1)$ has genus 0 and therefore $X_0(1) \cong \mathbb{P}^1(\mathbb{C})$.

2. $N = 11$: $X_0(11)$ is a elliptic curve with Weierstraß model
$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

For any function $f(z)$ on $\mathbb{H}$, a positive integer k and matrices $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{R})$ with positive determinant we define:

$$f|_k(\alpha)(z) := \det(\alpha)^{-k/2}(cz + d)^{-k} f(\alpha z). \tag{1}$$

If $k = 2$, we omit the $|_2$ on the left hand side of (1). Let

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

be a Dirichlet character with conductor f dividing the level N.

Definition 2.2 *A modular form of level N, weight k and nebentypus χ is a function $f(z)$ on $\mathbb{H}$ such that:*

1. *$f(z)$ is holomorphic in $\mathbb{H}$,*

2. *$f|_k(\alpha)(z) = \chi(d)f(z) \quad \forall\, z \in \mathbb{H}, \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$,*

3. *$f(z)$ is holomorphic at the cusps.*

If in addition f vanishes at the cusps, then f is called a cusp form. We denote the space of modular (cusps, resp.) forms of weight k and nebentypus χ by $M_k(N, \chi)$ ($S_k(N, \chi)$, resp.). If the nebentypus is trivial, we write $M_k(N)$ ($S_k(N)$, resp.).

For a precise definition of holomorphicity and vanishing at the cusps see [Shi71] Chap. (2.1). The pull-back of a holomorphic differential form $\omega \in \Omega^1(X_0(N))$ under the covering map π has locally the form $f(z)dz$ with complex parameter z. It is easy to see, but crucial, that $f(z)$ is a cusp form of weight 2 and level N.

Lemma 2.3 *The map $f(z) \mapsto 2\pi i f(z)dz$ induces an isomorphism between the space of cusp forms $S_2(N)$ and the holomorphic differentials $\Omega^1(X_0(N))$ of $X_0(N)$. The dimension of $S_2(N)$ as a complex vector space is equal to the genus of the modular curve $X_0(N)$.*

Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ belongs to $\Gamma_0(N)$, property (2) of Definition (2.2) implies that a cusp form is a periodic function on $\mathbb{H}$ with period 1. Therefore $f(z)$ has a Fourier expansion near infinity:

$$f(z) = \sum_{n=1}^{\infty} a_n q^n \text{ with } q := e^{2\pi i z},\ a_n \in \mathbb{C}.$$

2.2 The Hecke Algebra $\mathbb{T}_N$

The points of $Y_0(N)$ can be interpreted in the following way:

Let τ be an element of $\mathbb{H}$. There is a one to one correspondence between the orbits $\Gamma_0(N)\tau$ and the isomorphism classes of pairs (E, C_N) consisting of an elliptic curve $E = \mathbb{C}/L$ with period lattice $L = \mathbb{Z} + \mathbb{Z}\tau$ and a cyclic subgroup C_N of order N of $E[N]$, the group of N–torsion points. We call this the *modular interpretation of* $Y_0(N)$. By $(E, C_N)_\sim$ we denote the isomorphism class of a pair (E, C_N).

As a consequence of the modular interpretation of $Y_0(N)$ one finds a canonical minimal proper model of $X_0(N)$ over Spec($\mathbb{Z}$). We shall denote this model by $X_0(N)_\mathbb{Z}$. One can show that $X_0(N)_\mathbb{Z}$ has good reduction at all primes p not dividing the level N. At the bad fibers there are partial but deep results about the type of reduction due to Igusa, Deligne–Rapoport and Katz–Mazur (see [DR73] and ([KM85]).

Therefore we get a $\mathbb{Z}$–structure on the space of modular and cusp forms, and we see that $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ has a basis of modular and cusp forms with integral Fourier coefficients. Thus it makes sense to define $M_k(\Gamma_0(N))(R) := M_k(\Gamma_0(N)) \otimes R$ for any commutative ring R (with an analogous definition for cusp forms.) The *q–expansion principle* states that a modular form f of $M_k(N, \chi)(R)$ is uniquely determined by its Fourier coefficients and these coefficients lie in R.

Using the modular interpretation of the points on $X_0(N)_\mathbb{Z}$ we define a group of automorphisms of the algebraic curve $X_0(N)_\mathbb{Z}$: Let n be a positive divisor of N with $\gcd(n, N/n) = 1$ and $P = (E, C_N)_\sim$. Then

$$w_n(P) := (E/C_n, (C[n] \times C_{N/n})/C_n)_\sim$$

defines an involution on $X_0(N)$, i.e. $w_n^2 = id$. The w_n are called **Atkin–Lehner involutions**.

Remark 2.4 It is a result due to Ogg [Ogg78] that for square-free level $N > 37$

$$\mathrm{Aut}(X_0(N)) = \{w_n \mid n|N \text{ and } \gcd(n, N/n) = 1\}.$$

Next we look at the restriction map

$$\alpha_n : X_0(nN)_\mathbb{Z} \longrightarrow X_0(N)_\mathbb{Z};\quad (E, C_{nN})_\sim \mapsto (E, C_N)_\sim$$

for every positive integer n coprime to the level N. By combining the restriction map α_n with the involutions w_n:

$$\begin{tikzcd} X_0(nN)_{\mathbb{Z}} \arrow[r, "w_n"'] \arrow[d, "\alpha_n"] & X_0(nN)_{\mathbb{Z}} \arrow[d, "\alpha_n"] \\ X_0(N)_{\mathbb{Z}} & X_0(N)_{\mathbb{Z}} \end{tikzcd}$$

we find a $\mathbb{Z}$–rational correspondence on $Pic^0(X_0(N))$, the divisor classes of degree 0 of $X_0(N)$:

Definition 2.5 *For* $\gcd(n, N) = 1$

$$T_n := \alpha_{n*} \circ w_n \circ \alpha_n^*$$

is the n-th Hecke operator.

As a consequence, w_n and T_n act on

1. the Jacobian variety $J_0(N)$,
2. the (co-) tangent space, the differential forms $\Omega^1(X_0(N)_{\mathbb{Z}})$ and its dual,
3. the cusp forms $S_2(N)(\mathbb{Z})$,
4. the homology group $H_1(X_0(N), \mathbb{Z})$. We remark that this action is compatible with the natural action of the complex conjugation on paths. This is important for the computation of a basis of cusp forms over $\mathbb{Z}$ (see Sec. (3)).

Definition 2.6 *The Hecke algebra $\mathbb{T}_N$ of level N is the $\mathbb{Z}$–subalgebra of the endomorphism ring $\mathrm{End}_{\mathbb{Z}}(\Omega^1(X_0(N)_{\mathbb{Z}}))$ generated by*

$$w_n \textit{ with } n|N, \gcd(n, \tfrac{N}{n}) = 1 \textit{ and } T_k \textit{ with } \gcd(k, N) = 1.$$

The Hecke algebra $\mathbb{T}_N$ is commutative, see [Shi71].
Let us give an explicit description of the action of $\mathbb{T}_N$ on modular forms:

Definition 2.7 *For $f(z) \in M_k(N, \chi)$ and m a natural number, we define*

$$V_m(f(z)) := f(mz), \quad U_m(f(z)) := \frac{1}{m} \sum_{k=0}^{m-1} f\left(\frac{z+k}{m}\right). \tag{2}$$

Proposition 2.8 *Let $f \in M_k(N, \chi)$ be a modular form and n be a positive integer. Then*

$$T_n(f(z)) = \left(\sum_{d|n} \chi(d) d^{k-1} V_d \circ U_{n/d} \right) (f(z)). \tag{3}$$

If p is a prime number with $\gcd(p, N) = 1$, we get the well known formula

$$T_p(f(z)) := \chi(p)p^{k-1}f(pz) + \frac{1}{p}\sum_{k=0}^{p-1} f\left(\frac{z+k}{p}\right)$$

If we express the Hecke operator by its action on the q–expansion we get

Lemma 2.9 *Let $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_k(N, \chi)$ and p be a prime number. Then*

$$b_n := a_{pn} + \chi(p)p^{k-1}a_{n/p}$$

is the n–th Fourier coefficient of $T_p(f(z)) = \sum_{n=0}^{\infty} b_n q^n$ where $a_{n/p}$ is defined as zero if p does not divide n.

We shall study the decomposition of the space of cusp forms into eigenspaces under the Hecke algebra $\mathbb{T}_N$.

Definition 2.10 *A modular form $f(z) \in M_k(N, \chi)$ is a (Hecke-) eigenfunction, if $f(z)$ satisfies*

$$T(f(z)) \;\; = \;\; \lambda_T f(z) \textit{ for all } T \in \mathbb{T}_N.$$

The λ_T are the (Hecke-) eigenvalues with respect to T. By E_{λ_T} we denote the λ_T-eigenspace, i.e.

$$E_{T_\lambda} := \{f(z) \in M_k(N, \chi) \mid T(f(z)) = \lambda_T \cdot f(z)\}$$

where $T \in \mathbb{T}_N$ is fixed.

We shall restrict our attention to the case of weight 2 cusp forms with trivial nebentypus. We are interested in 'natural' subspaces of the vector space of cusp forms.

It is easy to see that, if $g(z) \in S_2(M)$ and $M|N$, then $g(dz) \in S_2(N)$ for $d|\frac{N}{M}$. So we define the space of *old forms* of $S_2(N)$ as:

$$S_2^{old}(N) := \left\langle g(dz) \mid g(z) \in S_2(M) \text{ with } M|N; M \neq N; d|\tfrac{N}{M} \right\rangle. \tag{4}$$

Definition 2.11 *The orthogonal complement of $S_2^{old}(N)$ with respect to the Petersson inner product*

$$\langle f, g\rangle := \int_{\Gamma_0(N)\backslash\mathbb{H}^*} f(z)\overline{g(z)}dxdy \textit{ with } f, g \in S_2(N),\;\; z = x + iy$$

is denoted by $S_2^{new}(N)$, the space of new forms. $f(z) \in S_2^{new}(N)$ is called a new form, if $f(z) = q + \sum_{n\geq 2} a_n q^n$ and $f(z)$ is a Hecke eigenform.

The Hecke operator T_n with $\gcd(n, N) = 1$ maps $S_2^{new}(N)$ ($S_2^{old}(N)$, resp.) to itself and is selfadjoint with respect to the Petersson inner product. Hence $S_2(N)$ decomposes into a direct sum of simultaneous eigenspaces and all eigenvalues are real.
For elements in $S_2^{new}(N)$ we get more: Let E be a simultaneous eigenspace of $S_2^{new}(N)$ under the Hecke algebra. Then $\dim(E) = 1$ (Multiplicity one theorem) [AL70].

Theorem 2.12 *Let R be an commutative ring. The pairing*

$$\mathbb{T}_N \times S_2(N)(R) \longrightarrow R, \quad (T_n, f) \mapsto a_1(T_n(f)) = \textit{first Fourier coeff. of } T_n(f)$$

has no left and right radical.

Since we know that $S_2(N)(\mathbb{C}) = S_2(N)(\mathbb{Z}) \otimes \mathbb{C}$ we get

Corollary 2.13 *$Hom(\Omega^1(X_0(N)), \mathbb{C})$ is a free rank one $\mathbb{T}_N \otimes \mathbb{C}$- module and $\mathbb{T}_N$ is a free $\mathbb{Z}$–module of rank $g(X_0(N))$.*

Moreover we get a construction principle for cusp forms over R:

Proposition 2.14 *Let $\Phi \in Hom(\mathbb{T}_N, R)$. Then*

$$\sum_{n=1}^{\infty} \Phi(T_n) q^n \in S_2(N)(R). \tag{5}$$

(See [DDT95] or [Mer94] for a proof.) We use this property to compute the Fourier expansion of cusp forms (see Sec. 3).
Since $\mathbb{T}_N$ is a free $\mathbb{Z}$–module of finite rank acting on $S_2(N)$ we get

Lemma 2.15 *Let $f = q + \sum_{n=2}^{\infty} a_n q^n \in S_2(N)$ be a Hecke eigenform and $T \in \mathbb{T}_N$. Then the eigenvalue λ_T is a totally real integral algebraic integer and the field*

$$K_f := \mathbb{Q}(\lambda_T \mid T \in \mathbb{T}_N) \tag{6}$$

is a finite extension of $\mathbb{Q}$.

By definition $\mathbb{T}_N$ is a subring of $\mathrm{End}(J_0(N))$.If N is square–free then

$$\mathbb{T}_N \otimes \mathbb{Q} = \mathrm{End}(J_0(N)) \otimes \mathbb{Q}$$

(Ribet), and if N is a prime we even get

$$\mathbb{T}_N = \mathrm{End}(J_0(N))$$

(cf. [Maz77]).

Remark 2.16

1. The explicit description of the Atkin–Lehner involutions on cusp forms is as follows: Let p a prime number and $\mathrm{ord}_p(N) = \alpha$, i.e. $p^\alpha || N$. Set

$$W_r := \left(\begin{smallmatrix} ra & b \\ Nc & rd \end{smallmatrix}\right), \text{ with } a, b, c, d \in \mathbb{Z}, r := p^\alpha, \det(W_r) = r. \tag{7}$$

   Then the *Atkin–Lehner operator*

$$S_2(N) \longrightarrow S_2(N); \quad f(z) \mapsto f(W_r)(z) \tag{8}$$

   is an involution on the space of cuspforms and

$$\prod_{p|N, p \text{ prime}} W_r = \left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right) := W_N$$

   is the *Fricke involution.*

2. One can define the Hecke and Atkin–Lehner operators for cuspforms with nebentype and higher weights (see [AL70]).

3. Without using the modular interpretation, but the theory of parabolic cohomology Shimura [Shi71] proved the existence of a basis of modular (cusp) forms with rational Fourier coefficients. For $S_2(N)$ this follows from the existence of a non-degenerate pairing

$$H_1^+(X_0(N),\mathbb{Z}) \times S_2(N) \longrightarrow \mathbb{C};\ \langle \sigma, f(z)\rangle \mapsto \int_\sigma f(z)dz \text{ (see (14))}$$

of the integral homology with the cusp forms. This pairing is compatible with the action of the Hecke operators, see [DDT95].

4. A second way to define Hecke operators T_n is via the double coset

$$\Gamma_0(N)\backslash\Delta/\Gamma_0(N),$$

with $\Delta = \{\alpha \in M^{2\times 2}(\mathbb{Z}) \mid \det(\alpha) = n\}$. This is the point of view in [Shi71], Chap. (3).

2.3 The Arithmetic of $J_0(N)$

Let $f = q + \sum_{n\geq 2} a_n q^n \in S_2(N)$ be a new form of weight 2 and $K_f = \mathbb{Q}(a_1, a_2, \dots)$ the field generated by the coefficients of f. As we have seen in the previous section, $K_f/\mathbb{Q}$ is a totally real field of degree d.
Let $I_f := \{\sigma_1, \dots, \sigma_d\}$ be the set of all distinct embeddings of K_f into $\mathbb{C}$. Following a construction due to Shimura ([Shi71] and [Shi73b]) we associate to f an abelian variety:

The cusp form f induces an algebra homomorphism

$$\lambda_f : \mathbb{T}_N \otimes \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}};\ T \mapsto a_1(T(f)).$$

Let $\mathcal{I}_f := \mathrm{kern}(\lambda_f) \cap \mathbb{T}_N$. The image $\mathcal{I}_f(J_0(N))$ is a subgroup scheme of the Jacobian of $X_0(N)$. Define:

$$A_f := J_0(N)/\mathcal{I}_f(J_0(N)). \tag{9}$$

Fact: A_f is an abelian variety.

It is easy to see that A_f is defined over $\mathbb{Q}$ and has good reduction at prime numbers not dividing the level N (since the same holds for $X_0(N)$).
The description of A_f as complex torus is due to Shimura, too. It is a special case of the following construction. Let $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$ and V a d–dimensional $G_\mathbb{Q}$–invariant subspace of $S_2(N)$ with a basis $\{f_1, \dots, f_d\}$. The image of the Abel–Jacobi map

$$\phi:\ H_1(X_0(N),\mathbb{Z}) \longrightarrow \mathbb{C}^d;\ \tau \mapsto (\textstyle\int_\tau f_1, \dots, \int_\tau f_d)^t$$

is a full lattice Λ_V, i.e a discrete free $\mathbb{Z}$-module of rank $2d$ in $\mathbb{C}^d$. The complex torus $\widetilde{A}_V := \mathbb{C}^d/\Lambda_V$ has the structure of an abelian variety. For a proof see [Shi71] or [Shi73b]. Especially, given a new form f we construct the d–dimensional $G_\mathbb{Q}$–invariant space

$$V_f := \langle f^{\sigma_i} \mid \sigma_i \in I_f\rangle$$

and the abelian variety $\widetilde{A}_{V_f}$ which we shall denote by $\widetilde{A}_f$. Shimura proved that

$$\widetilde{A}_f \text{ is the dual abelian variety of } A_f \otimes \mathbb{C}$$

(See [Shi71] or [DDT95]).

To A_f we associate – in the usual way – a *geometric* L–series:
For a prime number ℓ we define the ℓ–adic Tate module as

$$T_\ell(A_f) := \lim_{\longleftarrow} A_f[\ell^n],$$

where $A_f[\ell^n]$ is the group of ℓ^n–torsion points of A_f. Set

$$V_\ell(A_f) := T_\ell(A_f) \otimes \mathbb{Q}_\ell.$$

The natural action of $G_\mathbb{Q}$ on the ℓ–adic Tate module induces an ℓ–adic representation:

$$\rho_\ell : G_\mathbb{Q} \longrightarrow \mathrm{Aut}(V_\ell) \simeq \mathrm{GL}_{2d}(\mathbb{Q}_\ell)$$

For a prime number $p \neq \ell$, we define the local Euler factor

$$L_p(A_f, t) := \det(1 - t\rho_l^*(\sigma_\mathfrak{p}^{-1}) \mid V_\ell(A_f)^{*I(\mathfrak{p})}) \tag{10}$$

where $\sigma_\mathfrak{p}$ is the *Frobenius automorphism* of a prime $\mathfrak{p}$ in $\overline{\mathbb{Q}}$ lying above p, $I(\mathfrak{p})$ the inertia group of $\mathfrak{p}$ and ρ_ℓ^* is the adjoint representation to ρ_ℓ on the dual $V_\ell^*(A_f)$ of $V_\ell(A_f)$. It is easy to prove that the local Euler factor depends only on p and not on the choice of $\mathfrak{p}$ or $\sigma_\mathfrak{p}$. A much deeper result is that the the right hand side of (10) does not dependent on ℓ and is an element of the polynomial ring $\mathbb{Z}[t]$ (see [Roh97]). Let

$$L_p(A_f, t) = \prod_{k=1}^{2d}(1 - \alpha_{k,p}t) \tag{11}$$

be the factorization of the local Euler factor over the complex numbers. Then the theorem of Hasse–Weil states that $|\alpha_{k,p}| \leq \sqrt{p}$ and that we have equality if A_f has good reduction at p (see [Mum74]). Furthermore $L_p(A_f, 1)$ is equal to the number of points of the abelian variety $A_f \otimes \mathbb{F}_p$ defined over the finite field $\mathbb{F}_p$. It follows that the L-series defined by

$$L(A_f, s) := \prod_p L_p(A_f, p^{-s})^{-1};\ s \in \mathbb{C}$$

is convergent for all s with $\mathrm{Re}(s) > \frac{3}{2}$.
Next we define the *analytic* $L-$series attached to the new form f again by an Euler product:
Take

$$L_p(f,t) := \begin{cases} 1 - a_p t + pt^2 & \text{if} \quad p \not| N \\ 1 - a_p t & \text{if} \quad p | N \end{cases}$$

and define

$$L(f, s) := \prod_p L_p(f, p^{-s})^{-1};\ s \in \mathbb{C}.$$

Using properties of cusp forms one shows that: $L(f,s)$ is a holomorphic function on $\mathrm{Re}(s) > \frac{3}{2}$ and has an analytic continuation to the entire complex plane, see [Roh97].
A fundamental result is

Theorem 2.17 *For a prime number p not dividing the level N, we have:*

$$L_p(A_f,t) = \prod_{\sigma \in I_f} L_p(f^\sigma,t) \tag{12}$$

and the conductor $N(A_f)$ of A_f is equal to N^d.

Corollary 2.18 *$L(A_f,s)$ is a holomorphic function for $Re(s) > \frac{3}{2}$ and can be extended to an entire function to the whole complex plane which satisfies a functional equation.*

The first statement, formula (12) of theorem (2.17), is a consequence of the all–important *Eichler-Shimura*-relation between Hecke operators and Frobenius elements acting on $J_0(N)_{|\mathbb{F}_\ell}$ and related objects. The second statement of the theorem (2.17) is a deep result of Carayol (see [Car86]).
The following theorem states the Eichler–Shimura–relation for the Tate module $T_\ell(A_f)$:

Theorem 2.19 *Let $p \neq \ell$ a prime number, $\mathfrak{p}$ a prime lying above p and $\sigma_\mathfrak{p}$ a Frobenius automorphism. Then*

$$T_p = \sigma_\mathfrak{p} + \sigma_\mathfrak{p}^t$$

as endomorphism of the Tate module $T_\ell(A_f)$ where $\sigma_\mathfrak{p}^t$ is the transposed Frobenius endomorphism.

For a proof and the definition of the transposed Frobenius endomorphism see [Shi71] or [Roh97].

Corollary 2.20 *The coefficients of new forms satisfy the inequality*

$$|a_p| \leq 2\sqrt{p} \tag{13}$$

We summarize further properties of the abelian subvariety A_f, see theorem 7.14 in [Shi71].

Theorem 2.21 *Let $f = q + \sum_{n=2}^{\infty} a_n q^n \in S_2(N)$ be a Hecke eigenform and let $K_f = \mathbb{Q}(a_n | n \in \mathbb{N})$ be the field generated by the Fourier coefficients of f. Then there exists an abelian subvariety A_f of $J_0(N)$ and an isomorphism Θ from K_f to $\mathrm{End}(J_0(N)) \otimes \mathbb{Q}$ with the properties:*

1. $\dim(A_f) = [K_f : \mathbb{Q}]$
2. *If $\gcd(n,N) = 1$, then $\Theta(a_n)$ coincides with the restriction of T_n to A_f.*
3. *A_f is defined over $\mathbb{Q}$.*

Moreover these properties determine the pair (A_f, Θ) uniquely and A_f is a simple abelian variety defined over $\mathbb{Q}$.

Theorem 2.22 *Let f and A_f be as above and let in addition N be a square–free integer. Then the abelian variety A_f is absolutely simple.*

A most important consequence of the Eichler–Shimura relation is that every cusp form induces a two–dimensional ℓ–adic representation. This result is due to Shimura [Shi71] and can be extended to arbitrary weight, c.f. [DS74] or [Ser77] for an overview.

Theorem 2.23 *Let $f = q + \sum_{n=2} a_n q^n$ be a new form of weight k and level N, ℓ a prime number not dividing N and $K_f := \mathbb{Q}(a_n | n \in \mathbb{N})$. Then there exists a unique semi–simple ℓ–adic representation*

$$\rho_\ell : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_f \otimes \mathbb{Q}_\ell)$$

such that ρ_ℓ is unramified outside ℓN and

$$\mathrm{tr}(\rho_\ell(\sigma_{\mathfrak{p}})) = a_p \ , \ \det(\rho_\ell(\sigma_{\mathfrak{p}})) = p^{k-1} \quad \forall\, p \not| \ell N,$$

where $\sigma_{\mathfrak{p}}$ is a Frobenius automorphism at p.

3 The Basic Algorithms

The aim of this section is to describe the algorithm which computes $S_2(N)$ as a $\mathbb{T}_N[G_{\mathbb{Q}}]$–module. The basic idea of the algorithm is to use $H_1^+(X_0(N), \mathbb{Z})$, the $(+1)$–eigenspace under the involution induced by $i : z \mapsto \overline{-z}$ on $H_1(X_0(N), \mathbb{Z})$, instead of $S_2(N)$. This is possible since we have a good description of the homology space $H_1^+(X_0(N), \mathbb{Z})$ by generators and relations and a non–degenerate pairing

$$H_1^+(X_0(N), \mathbb{Z}) \times S_2(N) \longrightarrow \mathbb{C};\ \langle \sigma, f(z) \rangle \mapsto \int_\sigma f(z) dz, \tag{14}$$

compatible with the action of the Hecke operators, i.e.

$$\langle T_p(\sigma), f \rangle = \langle \sigma, T_p(f) \rangle.$$

Remark 3.1 We restrict ourselves to the case of weight 2 cusp forms with trivial nebentype. For more general cases see [Mer94] and [Wan94]. Merel makes use of the Manin–Shokurov theory and Wang applied the Eichler–Shimura isomorphism relating the space of cusp forms to the parabolic cohomology group, see [Shi71].

3.1 Modular Symbols and Relative Homology

Let $H_1(X_0(N), \mathbb{Z})$ be the singular homology group of the Riemann surface $X_0(N)_{\mathbb{R}}$ which is the abelianization of the fundamental group $\pi_1(X_0(N), z)$ where z is any base point. With $H_1(X_0(N), cusp, \mathbb{Z})$ we denote the relative homology of $X_0(N)$ with respect to the set of cusps.
We get the exact sequence

$$0 \longrightarrow H_1(X_0(N), \mathbb{Z}) \longrightarrow H_1(X_0(N), cusp, \mathbb{Z}) \xrightarrow{\delta} \mathbb{Z}^{\nu_\infty} \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{15}$$

where ν_∞ is the number of cusps of $\Gamma_0(N)$. An element of $H_1(X_0(N), cusp, \mathbb{Z})$ is called a *modular symbol*. A modular symbol can be represented as the projection of a path in $\mathbb{H}^*$ beginning and ending at a cusp to the modular curve $X_0(N)$. Since $\mathbb{H}$ is simply connected all paths $[z_1, z_2]$ between two fixed points $z_1, z_2 \in \mathbb{H}^*$ are equivalent and therefore their homology class depends only on the endpoints. We denote the image of $[z_1, z_2]$ by $\{z_1, z_2\}$. The main properties of modular symbols are (see [Man72] or [Cre92]):

Remark 3.2 For all $x, y, z \in \mathbb{H}^*$

1. $\{z, z\} = 0$ and $\{x, y\} = -\{y, x\}$,
2. $\{x, y\} + \{y, z\} + \{z, x\} = 0$,
3. $\{\alpha x, \alpha y\} = \{x, y\}$ for all $\alpha \in \Gamma_0(N)$.

One can show that the relative homology group splits into three direct summands [Mer94]

$$H_1(X_0(N), cusp, \mathbb{Z}) = \mathcal{E}is(N) \oplus \mathcal{S}_2(N) \oplus \overline{\mathcal{S}}_2(N)$$

where $\mathcal{E}is(N)$ corresponds to the Eisenstein series of $\Gamma_0(N)$ and $\mathcal{S}_2(N)$ ($\overline{\mathcal{S}}_2(N)$) to the holomorphic (anti–holomorphic) cusp forms.

Denote by J the right cosets $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$. According to remark (3.2.3) the map

$$\Phi : J \longrightarrow H_1(X_0(N), cusp, \mathbb{Z}), j \mapsto \{g(0), g(\infty)\} \text{ with } g \in j$$

is well defined.
Manin [Man72] proved:

Theorem 3.3 *$H_1(X_0(N), cusp, \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $2g + \nu_\infty - 1$ generated by the modular symbols $\{\{g(0), g(\infty)\} \mid g \in \mathrm{SL}_2(\mathbb{Z})\}$.*

Recall: The projective line over $\mathbb{Z}/N$ is defined by

$$\mathbb{P}^1(\mathbb{Z}/N) := \{(c, d) \in (\mathbb{Z}/N)^2 \mid \gcd(c, d, N) = 1\}/\sim$$

where

$$(c, d) \sim (c', d') \text{ iff } cd' \equiv c'd \bmod N.$$

We denote the class of (c, d) by $(c : d)$. It is a simple exercise to show that the map

$$J \longrightarrow \mathbb{P}^1(\mathbb{Z}/N),\ j \mapsto (c : d) \bmod N \text{ with } j \ni g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \tag{16}$$

is a bijection between J and the projective line $\mathbb{P}^1(\mathbb{Z}/N)$. Extending this map by linearity we get the $\mathbb{Z}$–linear map

$$\delta : \mathbb{Z}[J] \longrightarrow H_1(X_0(N), cusp, \mathbb{Z})$$

Remark (3.2.3) yields that the elements

$$\begin{gathered} j + jS \\ j + jR + jR^2 \end{gathered}$$

belong to the kernel of the map δ.It can be shown that the kernel of the map δ is generated by these elements, see [Man72]. Therefore we get the isomorphism

$$\mathbb{Z}[J]/\langle j + jS, j + jR + jR^2 \mid j \in J\rangle \ \cong\ H_1(X_0(N), cusp, \mathbb{Z}). \tag{17}$$

Using the bijection (16) we get an explicit description of $H_1(X_0(N), cusp, \mathbb{Z})$ as the $\mathbb{Z}$–module generated by

$$\begin{gathered} \mathbb{P}^1(\mathbb{Z}/N) \\ \text{with the relations} \\ (c : d) + (c : d)S \\ (c : d) + (c : d)R + (c : d)R^2. \end{gathered} \tag{18}$$

The involution $i : z \mapsto \overline{-z}$ acts by

$$i((c:d)) = (c:d)\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Define

$$\mathcal{M} := \mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/N)] \,/ \langle u + uS, u + uR + uR^2 \mid u \in \mathbb{P}^1(\mathbb{Z}/N)\rangle .$$

The Hecke correspondences induce an action of $\mathbb{T}_N$ on the relative homology. It is easy to check that on modular symbols we get:

$$T_p(\{c,d\}) = \{pc, pd\} + \sum_{k=0}^{p-1} \left\{ \frac{c+k}{p}, \frac{d+k}{p} \right\}.$$

The next aim is to express this action on $\mathcal{M}$. We follow Manin and Merel [Mer94] and collect their results in

Theorem 3.4 *Let* $M_n := \{\alpha \in M^{2\times 2} \mid \det(\alpha) = n\}$ *and*

$$(c:d)M := \begin{cases} 0 & \text{if} \quad (c:d)M \notin \mathbb{P}^1(\mathbb{Z}/N) \\ (c:d)M & \text{if} \quad (c:d)M \in \mathbb{P}^1(\mathbb{Z}/N). \end{cases}$$

1. *For all integers* $n \in \mathbb{N}$ *there exists an element*

$$\Theta_n := \sum u_M M \in \mathbb{Z}[M_n]$$

such that

$$\sum u_n(M(\infty) - M(0)) = (\infty) - (0) \quad \text{(condition } (C_n))$$

holds.

2. *For any* Θ_n *satisfying condition* (C_n) *and for* $\gcd(n,N) = 1$ *the* n*–th Hecke operator acts on* $\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/N)]$ *by*

$$T_n((c:d)) = (c:d)\Theta_n = \sum u_M (c:d)M$$

Regarding the complexity of computations it is important that Θ_n is "not too long":

Refinement 3.5 There is a Θ_n such that $\#\{M \mid u_M \neq 0\} \leq O(n\log(n))$.

Example 3.6
Let R_n the set of all integral 2×2 matrices of the form $A = \left(\begin{smallmatrix} x & -y \\ y' & x' \end{smallmatrix}\right)$ where $\det(A) = n$ and one of the following three properties holds

- $x > |y| > 0$, $x' > |y'| > 0$, and $yy' > 0$
- $y = 0$, and $|y'| \leq \frac{1}{2}x'$
- $y' = 0$, and $|y| \leq \frac{1}{2}x$.

Then $\Theta_n = \sum_{A\in R_n} A$ satisfies the condition (C_n) (cf. [Mer94]).[1]

[1] This description of Hecke operators can also be found in the paper of Zagier [Zag90]. We thank the referee for this information.

Example 3.7

$$\Theta_2 = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

Remark 3.8

1. Θ_n does not depend on the level N and the weight k.

2. The 'classical' method of computing the Hecke operator on $\mathcal{M}$ is to use the isomorphism (17) to compute the Hecke operator on $H_1(X_0(N), cusp, \mathbb{Z})$ and to map the result back to the space $\mathcal{M}$. To do this explicitly one has to calculate a continued fraction expansion of some rational numbers (see [Cre92] or [Man72]). The complexity of this method is equal to the complexity of the method due to Merel.

3. The same formula holds if we replaces $\mathcal{M}$ by $\mathcal{M}^+$ corresponding to the +1-eigenspace under complex conjugation (see below).

Here is a small numerical example:

Example 3.9
Take $N = 31$. Then 0 and ∞ are the only cusps of $\Gamma_0(31)$ and $H_1(X_0(N), cusp, \mathbb{Z})$ is a free $\mathbb{Z}$–module of rank 5. The Hecke operator T_2 on $H_1(X_0(N), cusp, \mathbb{Z})$ is

$$T_2 = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & -1 & 0 \\ -1 & 0 & -1 & 1 & 0 \\ -1 & -1 & 0 & 0 & 1 \end{pmatrix}$$

and the characteristic polynomial $\chi_{T_2}(t)$ is

$$\chi_{T_2}(t) = \underbrace{(t-3)}_{\text{Eisenstein part}} \underbrace{(t^2-t-1)}_{\text{cusp form part}} \underbrace{(t^2-t-1)}_{\text{anti holomorphic cusp form part}} .$$

Next we compute the space $H_1^+(X_0(N), \mathbb{Z})$. The map δ in the exact homology sequence (15) is:

$$\begin{gathered} H_1(X_0(N), cusp, \mathbb{Z}) \xrightarrow{\delta} \mathbb{Z}^{\nu_\infty} \\ \left\{\tfrac{a}{b}, \tfrac{c}{d}\right\} \mapsto \left[\tfrac{c}{d}\right] - \left[\tfrac{a}{b}\right] \end{gathered} \tag{19}$$

where a, b, c, d are integers and $\left[\frac{a}{b}\right]$, $\left[\frac{c}{d}\right]$ are cusps of $\Gamma_0(N)$. We divide out the additional relation induced by the condition that the complex conjugation acts trivial. (Of course, we can do this at the same time as we deal with the other relations.) The quotient is denoted by $\mathcal{M}^+$. Via the isomorphism (17) we get the map corresponding to δ and we can compute the kernel of the boundary map δ.
Result: This kernel is dual to the space of cusp forms $S_2(N)$.

Remark 3.10

1. There is a different method to identify the cusp form part in $\mathcal{M}^+$. It is well known (see [Shi71]) that there exists a basis $\{f_1, \ldots, f_{\nu_\infty - 1}\}$ of Hecke eigenforms in the space of Eisenstein series which can be described explicitly. Especially there are easy to compute formulas for the Fourier coefficients of the f_i. Therefore we know the operation of T_p on $\mathcal{E}is(N)$ and so its characteristic polynomial on this subspace of $H_1(X_0(N), cusp, \mathbb{Z})$. We use this to find an element f in $\mathcal{M}$ which lies in the subspace $\mathcal{S}_2(N)$, see [Mül98].

2. With a similar trick as above we even find a vector f which lies in the 'new part' of $\mathcal{M}$ or in the ± 1 eigenspaces of the various Atkin–Lehner operators. This speeds up the computation of the minimal (characteristic, resp.) polynomial which we have to determine.

3. One problem to calculate in the $\mathbb{Z}$–module $\mathcal{M}$ (see (18)) is to find a basis for this space. To do this one has to use Gauß elimination or sparse matrix techniques to find a basis which can be rather painful since the matrices are very large. But with a nice trick due to X. Wang (see [Mül98]) we have a very efficient implementation which avoids entirely such matrix operations.

4. We described the algorithm over $\mathbb{C}$ but we have a $\mathbb{Z}$–structure on the symbols and on the Hecke algebra $\mathbb{T}_N$. Therefore we can use the algorithm over $\mathbb{Z}$ *and* over finite fields.

5. It turned out that for large n (about 10^9) and medium sized level N ($\leq 10^3$) a rearrangement of the matrices can speed up the computation. For this result and the implementation see [Bas96].

Example 3.11

The modular curve $X_0(41)$ has genus 3 and the matrix for the Hecke operator T_p with $p = 10^9 + 7$ is:

$$A_{T_p} = \begin{pmatrix} -15916 & -19368 & -2773 \\ -52558 & 22820 & 35963 \\ 30417 & -2773 & -35284 \end{pmatrix}.$$

The characteristic polynomial is:

$$\chi_{T_p}(t) = t^3 + 28380t^2 - 1440675460t - 27479384514602.$$

For a larger example see table (5.2).

Since the action of the Hecke operator is compatible with the pairing

$$\mathcal{S}_2(N) \times S_2(N) \longrightarrow \mathbb{C} \tag{20}$$

we calculate the integral matrices representing T_n on $\mathcal{S}_2(N)$. They coincide with the transpose of the corresponding matrix acting on the dual w.r.t. this pairing. Therefore we can split the space of cusp forms into simple $\mathbb{T}_N[G_{\mathbb{Q}}]$-invariant spaces and compute the splitting of $J_0(N)$ into simple abelian subvarieties as we have seen in theorem (2.21). Below one finds a small table for the splitting of $J_0(N)$ with large prime levels N. For a table for levels $11 \leq N \leq 80$ we refer to the appendix, table (5.1).

N	$\dim(S_2(N))$	Splitting
10009	833	393 440
10037	836	398 438
10039	836	384 452
10061	838	383 454
10067	839	399 440
10069	838	406 432
10079	840	1 353 486
10091	841	1 382 458
10093	840	410 430
10099	841	1 1 396 443

The description of the table is as follows: The first column is the level, the second the dimension of the space of cusp forms. In the third column one finds the dimensions of the $\mathbb{T}_N[G_{\mathbb{Q}}]$ invariant subspaces of $S_2(N)$. For example, for $N = 10099$ the space $S_2(N)$ splits into two one dimensional subspaces, one 396 dimensional and one 443 dimensional subspace as $\mathbb{T}_N[G_{\mathbb{Q}}]-$module. Since this splitting induces a decomposition of $J_0(N)$ in $\mathbb{Q}$–simple abelian subvarieties (see theorem (2.21)) we get:

$$J_0(N) \simeq E_1 \times E_2 \times A_{396} \times A_{443}.$$

The subvarieties E_1 and E_2 are *modular* elliptic curves.

3.2 Computation of Fourier Expansions of Bases of $S_2(N)$

In the last section we have determined the structure of $S_2(N)$ (or equivalently of $\Omega^1(X_0(N))$) as $\mathbb{T}_N[G_{\mathbb{G}}]$–module.

Now we want to compute explicitly a basis of $S_2(N)(\mathbb{Z})$ respectively a basis consisting of eigenforms. The elements f of these bases will be given by the Fourier expansion of such forms. To identify them it is sufficient to compute "enough" coefficients: If the level is N then f is determined by the first $\lfloor \frac{N}{6} \prod_{p|N}(1 + \frac{1}{p}) \rfloor$ coefficients.

Later on we want to get finer information. For instance we want to compute linear subspaces with special properties inside of the cusp forms and then we shall need much more coefficients. So the performance of our algorithm will be of great importance.

Here is the procedure: Choose an element e in $\mathcal{S}_2(N)$ found by the method described above. We know by proposition 2.14 that

$$\sum_{n=1}^{\infty} \Phi(T_n e) q^n \in S_2(N)(\mathbb{Z}) \text{ for } \Phi \in \mathrm{Hom}(\mathcal{S}_2(N), \mathbb{Z}). \tag{21}$$

By varying the random element e and the linear form Φ we get a $\mathbb{Z}$–basis of $S_2(N)$. (cf. [Mer94]). More precisely: We use a sequence $e_1 := e,\ e_{i+1} = T_m(e_i)$ with $\gcd(m, N) = 1$

and m as small as possible. This speeds up the computations since we have to compute fewer matrices, see (3.4) and (3.5). We find with Gauß elimination or the Wiedemann algorithm (see [KS91]) an integer d such that the set $B_1 := \{e_i \mid 1 \le i \le d\}$ is linearely independent. If $d = \dim(\mathcal{S}_2(N))$ we have found a basis of $\mathcal{S}_2(N)$ and we can use (21) to find the coefficients in the q–expansion for each e_i. In the case that $d < \dim(\mathcal{S}_2(N))$ we choose another random element e' or – alternatively – we take another Hecke operator T_n and compute a second sequence e'_i. We add the new elements to the set B_1 and test linear independence again. We repeat this until we have a basis of $\mathcal{S}_2(N)$ and then we use (21) to find the Fourier coefficients of the corresponding cusp forms and therefore a basis of $S_2(N)$. In practice we have only to choose 2 or 3 random elements e to find a basis of $\mathcal{S}_2(N)$.

Example 3.12
Take $N = 45$. The dimension of $S_2(45)$ is equal to 3 and

$$\begin{aligned}\{f_1 &= q - q^4 - q^{10} - 2q^{13} - q^{16} + 4q^{19} + 4q^{22} + \dots ,\\ f_2 &= q^2 - q^5 - 3q^8 + 4q^{11} - 2q^{17} + q^{20} + \dots ,\\ f_3 &= q^3 - q^6 - q^9 - q^{12} + q^{15} + q^{18} + \dots\}\end{aligned}$$

is a basis of $S_2(45)(\mathbb{Z})$.

As said above an analogous algorithm works in the case of higher weight (cf. [Mer94] or [Wan94]).

We give an example for the weight $k = 4$ and level $N = 22$:

$$\begin{aligned}\{f_1 &= q + 10q^6 - 6q^7 - 24q^8 - 13q^9 - 30q^{10} - 100q^{11} + 64q^{12} + 292q^{13} - 14q^{14}\\ &\quad +130q^{15} + 464q^{16} - 286q^{18} - 804q^{19} \dots ,\\ f_2 &= q^2 - 2q^6 + 8q^7 - 16q^8 - 32q^9 + 15q^{10} + 16q^{11} + 64q^{13} + 98q^{14} - 40q^{15}\\ &\quad -64q^{16} - 32q^{18} - 95q^{19} \dots ,\\ f_3 &= q^3 - 2q^6 - 5q^7 + 8q^8 - 12q^9 - 10q^{10} + 26q^{11} + 16q^{12} + 20q^{13} - 42q^{14}\\ &\quad -15q^{15} + 16q^{16} + 20q^{17} + 52q^{18} - 100q^{19} \dots ,\\ f_4 &= q^4 - q^6 - 4q^7 - 6q^8 + 16q^9 + 5q^{10} - 8q^{11} - 4q^{12} - 32q^{13} + 47q^{14} + 20q^{15}\\ &\quad -28q^{16} + 16q^{17} - 66q^{18} + 40q^{19} \dots ,\\ f_5 &= q^5 - 2q^6 + 2q^7 - 8q^8 + 10q^9 + 6q^{10} - 8q^{11} - 38q^{13} + 54q^{14} + 14q^{15}\\ &\quad -16q^{16} - 32q^{17} - 44q^{18} + 88q^{19} \dots\}\end{aligned}$$

is a basis of $S_4(22)(\mathbb{Z})$.

To obtain bases of simultaneous eigenfunctions we have to decompose $\mathcal{S}_2^{new}(N)$ w.r.t. all Hecke operators. We pick a T_n and decompose $\mathcal{S}_2(N)$ into a sum of T_n eigenspaces. If the eigenvalue λ_n has multiplicity one we find (up to scalars) an unique eigen vector e with $T_n e = \lambda_n e$. This must be an simultaneous eigenvector for all Hecke operators $T \in \mathbb{T}_N$. As a consequence of (20) we get:

$$\sum_{n=1}^{\infty} \lambda_n q^n \in S_2(N) \text{ with } \begin{cases} T_n(e) = \lambda_n e & & n \nmid N \\ w_n(e) = \lambda_n e & \text{for} & n|N \text{ and } \gcd(n, \frac{N}{n}) = 1 \\ \quad 0 & & \gcd(n, \frac{N}{n}) > 1. \end{cases}$$

If the eigenspace E_{λ_n} is not one–dimensional we apply another Hecke operator T_m to E_{λ_n} and refine the decomposition until we find a decomposition into one–dimensional factors. This procedure must terminate after a finite number of steps. To make the computation fast we use reduction modulo a prime p which splits totally in the totally real field extension $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3, ...)$ over $\mathbb{Q}$ and use the Hasse–Weil bound to determine the Fourier coefficients.

Example 3.13
Let $N = 88$. Then $\dim(S_2(N)) = 9$, the dimension of $S_2^{new}(N)$ is 3 and $S_2^{new}(N)$ decomposes over $\mathbb{Q}$ into a a two–dimensional and one–dimension factors related to the eigenforms:

$$\begin{aligned} f_i &= q + \alpha_i q^3 + (2-\alpha_i)q^5 - 2\alpha_i q^7 + (\alpha_i+1)q^9 - q^{11} + (2\alpha_i - 2)q^{13} \\ &\quad +(\alpha_i - 4)q^{15} + 2q^{17} - 4q^{19} - (8+2\alpha_i)q^{21} + (4+\alpha_i)q^{23} + \cdots \end{aligned}$$

with $i \in \{1, 2\}$ and $\alpha_i^2 - \alpha_i - 4 = 0$.

$$\begin{aligned} f_3 &= q - 3q^3 - 3q^5 - 2q^7 + 6q^9 - q^{11} + 9q^{15} - 6q^{17} + 4q^{19} + 6q^{21} + q^{23} + 4q^{25} \\ &\quad -9q^{27} - 8q^{29} - 7q^{31} + 3q^{33} + 6q^{35} - q^{37} + 4q^{41} + 6q^{43} - 18q^{45} + \cdots \end{aligned}$$

3.3 Some Remarks about the Implementations

The main tool is a fast program which computes the module $\mathcal{M}$ and the action of the Hecke operators on the elements of $\mathcal{M}$. For the decomposition of the Hecke operator T_n we have to calculate the minimal (characteristic, resp.) polynomial of T_n. If n is small w.r.t. the level N it turned out that the representation matrix of T_n is a sparse matrix and so we can use an algorithm due to Wiedemann [KS91] to compute the minimal polynomial of T_n over various finite prime fields $\mathbb{F}_p$ (with $p \approx 2^{31}$) and apply the Chinese remainder theorem to lift the coefficients to $\mathbb{Z}$. The Hasse–Weil bound for the eigenvalues gives a bound for the coefficients of the minimal polynomial. Then we have to factor the minimal (characteristic, resp.) polynomial over $\mathbb{Z}$ to get informations on the decomposition of $S_2(N)$ into simultaneous eigenspaces. The problem is that the degree of the polynomials is approximately $N/12$. If we want, for example, to compute the minimal polynomial of T_n acting on $S_2(12007)$ we have to factor a polynomial of degree 1000 over $\mathbb{Z}$. At this point we use the C++-library `ntl` (the author is V. Shoup) which is a very fast public domain package to factor polynomials over prime fields and over $\mathbb{Z}$. As additional libraries we used `cln`, an efficient package for multi-precision and polynomial arithmetic (author B. Haible) [2]. The other parts of the program were written by X.Wang and the second author. For the computation of integral bases we used `gp` due to H. Cohen.

Actually we used some more tricks like using the Atkin–Lehner involutions to decompose $S_2(N)$ and factoring the minimal polynomial of an Hecke operator T_n over $\mathbb{F}_p$ and we combined this with our knowledge about the degree of the factors of the polynomial over $\mathbb{Z}$ (here again the Hasse–Weil bound plays a helpful role). More details can be found in [Mül98].

---

[2]We want to thank V. Shoup and B. Haible for providing us with `ntl` resp. `cln`

4 Applications

4.1 Cusp Forms of Weight 1 and $\frac{3}{2}$

In the previous section we described how one can compute cusp forms of weight greater equal 2. The algorithm depends on the geometric interpretation of these forms. Such an interpretation is not available for cusp forms of weight one and weight 3/2.

Cusp forms of weight $\frac{3}{2}$:
We define

$$\left(\frac{c}{d}\right) := \begin{cases} -\left(\dfrac{c}{|d|}\right); & c<0, d<0 \\ \left(\dfrac{c}{|d|}\right); & \text{else} \end{cases}$$

$$\varepsilon_d := \begin{cases} 1; & d \equiv 1 \bmod 4 \\ \sqrt{-1}; & d \equiv 3 \bmod 4 \end{cases}$$

and take $(cz+d)^{1/2}$ as square root of $cz+d$ with non negative imaginary part.

Definition 4.1 *Let $N \in 4\mathbb{N}$. For $k \in \frac{1}{2}+\mathbb{Z}$ define $M_k(N,\chi)$ ($S_k(N,\chi)$, resp.) as the set of holomorphic functions on $\mathbb{H}$ bounded near the cusps (vanishing at the cusps, resp.) such that for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ we have:*

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)\left(\frac{c}{d}\right)^{2k} \varepsilon_d^{-2k}\left((cz+d)^{1/2}\right)^{2k} f(z)$$

(cf. [Shi73a]).

In loc. cit. one can find the definition of the "Shimura–Shintani" lift φ_k which maps these forms into forms of weight $2k-1$.

In the frame of elliptic curves the case $k=3/2$ is of special interest: Due to the beautiful theorem of Waldspurger [Wal81] one can compute the value of the L–series at $s=1$ of twists E_D of a modular elliptic curve E with corresponding modular form f_E by the Fourier coefficients of a form F_E of weight 3/2 with $\varphi_{\frac{3}{2}}(F_E) = f_E$. (For the precise formulation see [ABF90].)

By multiplying with Θ–functions one maps $S_{\frac{3}{2}}(N)$ into a product of spaces $S_2(N')$ and then one describes the image as linear subspace ("Tate's trick"). For example:
If $16|N$, then the map

$$\begin{array}{rccc} \varphi: S_{\frac{3}{2}}(N) & \longrightarrow & S_2(N) \times S_2(N) \\ f(z) & \mapsto & (f(z)\Theta_2(z), f(z)\Theta_3(z)) \end{array} \tag{22}$$

where

$$\Theta_2(z) := \sum_{m=1, m \text{ odd}}^{\infty} q^{m^2} \text{ and } \Theta_3(z) := 1 + 2\sum_{m=1}^{\infty} q^{m^2}$$

is injective. Having an element $(f_2, f_3) = \varphi(F)$ in $\mathrm{Im}(\varphi)$, one finds easily F by the formula

$$F(z) = \frac{f_2(z)}{\Theta_2(z)}.$$

J. Basmaji implemented this algorithm in his thesis [Bas96] and computed the form F_E for many elliptic curves E. He uses this to get a lot of empirical material concerning the distribution of values of L–series at $s = 1$ (and so, according to the conjecture of Birch–Swinnerton-Dyer, of orders of Selmer groups) of families of twists of modular elliptic curves. It would be very interesting to have a better theoretical understanding of these data.

Cusp forms of weight 1:
Another weight which is not accessible directly is $k = 1$.

Cusp forms of weight 1 are very interesting since they are related to irreducible complex odd two–dimensional Galois representation of $G_{\mathbb{Q}}$ for which Artin's conjecture holds. See [Ser77] or [Fre94] for this topic.

Using again Tate's trick one can find the space of cusp forms of weight one as an (explicitly describable) subspace of cusp forms of higher weights and levels. This is used in [KW94] to determine a of the space $S_1(N, \chi)$, the cusp forms of level N, weight 1 and nebentypus χ for $N = 2^\alpha \cdot n$, n odd square–free, $\mathrm{lcm}(N, 4N) \le 10^4$ and χ a quadratic character. By computing all odd representations of $G_{\mathbb{Q}}$ with corresponding Artin conductors and determinants one can verify Artin's conjecture numerically in these cases.

4.2 The Degree of Modular Elliptic Curves

Let X be a compact Riemann surface. We denote by $(\cdot,\cdot)_X$ the intersection pairing on $H_1(X, \mathbb{Z})$ which takes values in $\mathbb{Z}$.

In the case of $X = X_0(N)$ Wang [Wan95] gives an explicit description of a pairing on the cuspidal cohomology group $H^1_p(\Gamma_0(N), \mathbb{Z})$ which comes from the cup product on the cohomology (see also Hida [Hid81] and Haberland [Hab83]). We use this and the knowledge of $H_1(X_0(N), \mathbb{Z})$ to calculate the intersection pairing on $X_0(N)$ (c.f. [Mül98]).

First we apply this to modular elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N associated to a new form $f \in S_2^{new}(N)$ (this is the special case that $\dim(A_f) = 1$ in (9)). Then we have a modular parameterization, i.e. a non–constant morphism

$$\varphi: \; X_0(N) \longrightarrow E \tag{23}$$

of the elliptic curve E. We want to calculate the degree of φ. The map φ induces a homomorphism

$$\overline{\varphi}: \; H_1(E, \mathbb{Z}) \longrightarrow H_1(X_0(N), \mathbb{Z}).$$

Since $\dim(H_1(E, \mathbb{Z})) = 2$ it has two generators $\omega, \widetilde{\omega}$ as $\mathbb{Z}$–module. A simple calculation shows:

$$(\overline{\varphi}(\omega), \overline{\varphi}(\widetilde{\omega}))_{X_0(N)} = \deg(\varphi)(\omega, \widetilde{\omega})_E$$

and furthermore $2|(\omega, \widetilde{\omega})_E| = c$ with $c = 1$ if $E(\mathbb{R})$ has one real connected component and $c = 2$ in the other case. This implies

$$\deg(\varphi) = \frac{2}{c}|(\overline{\varphi}(\omega), \overline{\varphi}(\widetilde{\omega}))_{X_0(N)}|$$

and so the degree can be computed if we know the intersection pairing.

Example 4.2
Let $X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$. Then $\deg(\varphi) = 1$. For the two modular elliptic curves of level $N = 132$

$$E_1 : y^2 = x^3 + x^2 + x$$
$$E_2 : y^2 = x^3 - x^2 - 77x + 330$$

we find $\deg(\varphi) = 6$ for E_1 and $\deg(\varphi) = 30$ for E_2.
For more informations and tables see [Zag85], [Cre95] or [Mül98].

There is another way to interpret $\deg(\varphi)$:
Assume that E is a "strong" modular curve, i.e. it does not factor through an intermediate elliptic curve, and let φ_* (φ^*) be the induced maps from $J_0(N)$ to E (to it's dual, resp.). Then φ^* is injective and the kernel of φ_* is an abelian variety A_φ. It is easy to see that

$$|A_\varphi \cap \varphi^*(E)| = \deg(\varphi)^2.$$

Hence $\deg(\varphi)^2$ describes the order of the largest group of torsion points which $\varphi^*(E)$ and A_φ have in common, and this group is $G_{\mathbb{Q}}$–invariant by definition. In other words:
There is an abelian variety A defined over $\mathbb{Q}$ which has no factor isogenous to E but which contains a $G_{\mathbb{Q}}$–invariant subspace of order $\deg(\varphi)^2$ Galois isomorphic to $E_{\deg(\varphi)}$, the kernel of the multiplication by $\deg(\varphi)$ on E.

Let us give a third interpretation of $\deg(\varphi)$. Since

$$||f||^2 = \deg(\varphi)\mathrm{Vol}(E),$$

where $||f||^2 = \langle f, f\rangle$ is the Petersson inner product and $\mathrm{Vol}(E)$ is the volume of the fundamental discriminant of E we get a relation with the Faltings height, see [Fre97]:
Let $h_{\mathbb{Q}}(E)$ be the Faltings height of E. Then

$$h_{\mathbb{Q}}(E) = \frac{1}{2}\log(\deg(\varphi)) - \log(|c_\varphi|) - \frac{1}{2\pi}\log(||f||)$$

where c_φ is the Manin constant (conjecturally $|c_\varphi| = 1$). The height conjecture for elliptic curves predicts that

$$h_{\mathbb{Q}}(E) \leq c \log N + d \tag{24}$$

with constants c and d. It is well known that this conjecture implies the ABC–conjecture. Estimates for $||f||$ (c.f. [Fre87] and [MM94]) give: (24) holds if and only if

$$\log(\deg(\varphi)) \leq O(\log(N)).$$

Therefore it is of great interest to know more about the degree of the modular parameterization.

One can regard analogous questions in the theory of cusp forms. This is the subject of the very interesting theory of *congruence primes* which played a crucial role in Wiles' proof of a large part of the Taniyama–Shimura conjecture. Let f be a normalized cusp form of level N with integer coefficients. $L := \langle f\rangle^\perp \cap S_2(N)(\mathbb{Z})$ where the orthogonal complement is taken with respect to the Petersson inner product. Define r as the largest positive integer such that there exists a cusp form $g \in L$, with

$$g \equiv f \bmod r.$$

Definition 4.3 *A prime number p is called a congruence prime, if p divides r.*

Question 4.4 *Let E_f be a strong modular curve, $\varphi : X_0(N) \longrightarrow E_f$ be the modular parameterization of E_f: Does the identity*

$$r = \deg(\varphi)$$

hold?

It was proved by Ribet [Rib83] (see also Zagier's paper [Zag85]) that

$$r | \deg(\varphi) | rN^i$$

for some positive integer i. Furthermore if N is a prime number then the answer of question (4.4) is yes, see [Zag85].

At the end of this section we come back to the interpretation of $\deg(\varphi)$ as order of $\varphi^*(E) \cap A_\varphi$ and ask whether a part of this intersection can be realized as an intersection between E and another elliptic curve E' defined over $\mathbb{Q}$ which is not isogenous to E. In the language of cusp forms this means that

$$f_E \equiv f_{E'} \bmod n$$

for some number $n > 1$. In the language of mod$n$ representations we have

$$E[n] \cong E'[n]$$

as $G_{\mathbb{Q}}$–modules.

The question concerning the existence of such pairs of elliptic curves was posed by Mazur, [Maz78], page 133. It gave rise to various conjectures (cf. [Fre97], (1b)). The strongest formulation (due to Kani-Darmon) predicts that for primes $l \geq 23$ the set of such pairs should be finite and even empty if l is large enough (see also Kani–Schanz [KS98] and Kraus–Oesterlé [KO92] for this topic). By checking Fourier coefficients of cusp forms corresponding to elliptic curves we find examples up to primes $l = 13$ (for composite numbers see [HK96]). In the appendix table (5.3) we give a list of these examples, see also [Mül98].

4.3 Finding Curve Equations

Again we use our knowledge of the intersection pairing and the holomorphic differential forms on $X_0(N)$ which we get by the Fourier expansion of cusp forms. We shall study simple abelian factors A of $J_0(N)$.
We want to calculate the period matrix and the invariants of such an abelian variety A. Furthermore we want to decide whether A is isogenous to the Jacobian of a hyperelliptic curve C. If this is the case we determine a model of this curve C over $\mathbb{Z}$.

First of all we collect some basic facts about abelian varieties defined over $\mathbb{C}$. We know that $\mathcal{A}_d$, the coarse moduli space of isomorphism classes of principally polarized abelian varieties of dimension d, can be parameterized by $\mathrm{Sp}_{2d}(\mathbb{Z})\backslash\mathbb{H}_d$ where

$$\mathbb{H}_d := \left\{ \Omega \in \mathbb{C}^{d\times d} \mid \Omega^t = \Omega; \mathrm{Im}(\Omega) \text{ positiv definite } \right\}.$$

The action of $\mathrm{Sp}_{2d}(\mathbb{Z})$ on $\mathbb{H}_d$ is given by:

$$\mathrm{Sp}_{2d}(\mathbb{Z}) \times \mathbb{H}_d \longrightarrow \mathbb{H}_d;\ \left(\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right), \Omega\right) \mapsto (A\Omega + B)(C\Omega + D)^{-1}$$

with $A, B, C, D \in \mathbb{Z}^{d\times d}$.

Remark 4.5 In the case of $d = 1$ (elliptic curves) we have $Y_0(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}_1$.

An abelian variety A of dimension d defined over the complex numbers can be viewed as a pair $(\mathbb{C}^d/\Lambda, H)$, where Λ is a full $\mathbb{Z}$–lattice in $\mathbb{C}^d$ and H is a non degenerated Hermitian form such that $\mathrm{Im}H(\Lambda, \Lambda) \subset \mathbb{Z}$. Furthermore there exists a $\{\omega_1, \dots, \omega_{2d}\}$ of $2d$ $\mathbb{R}$–linearly independ vectors of the lattice Λ, such that

$$(\mathrm{Im}H(\omega_i, \omega_j))_{i,j=1,\dots,2d} = \left(\begin{smallmatrix} 0 & \Delta \\ -\Delta & 0 \end{smallmatrix}\right) \in \mathbb{Z}^{2d\times 2d}$$

with the diagonal matrix

$$\Delta = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_d \end{pmatrix} \in \mathbb{Z}^{d\times d},\ e_i > 0 \text{ and } e_1|e_2|\dots|e_d. \tag{25}$$

$\{\omega_1, \dots, \omega_{2d}\}$ is called a *symplectic basis*. We form the two complex $d \times d$ matrices

$$\Omega_1 := (\omega_1, \dots, \omega_d),\ \ \Omega_2 := (\omega_{d+1}, \dots, \omega_{2d}).$$

It can be shown that

$$\begin{gathered} \Omega_2\Omega_1^t = \Omega_1\Omega_2^t \text{ and} \\ 2i(\Omega_2\overline{\Omega}_1^t - \Omega_1\overline{\Omega}_2^t) \text{ is positiv definite.} \end{gathered} \tag{26}$$

As a consequence of (26), Ω_2 is invertible. We call the matrix

$$\Omega := \frac{1}{e_d}\Omega_2^{-1}\Omega_1$$

the *period matrix* of the abelian variety A and the coset $\mathrm{Sp}_{2d}(\mathbb{Z})\Omega$ represents the isomorphism class of A in $\mathrm{Sp}_{2d}(\mathbb{Z})\backslash\mathbb{H}_d$.

Let f be a new form of level N. The corresponding A_f is a $\mathbb{Q}$–simple factor of $J_0(N)$ (see theorem (2.21)). In Wang ([Wan95]) it is shown that the pairing

$$\mathrm{Im}H(\Lambda, \Lambda) \to \mathbb{Z}$$

corresponds to the intersection pairing on $H_1(X_0(N), \mathbb{Z})$. In the same paper, Wang proves that one can compute the period matrix as

$$\begin{gathered} \Omega_f = e_d U_f^{-1} V_f\ \ (e_d \text{ as above}) \\ U_f := \left(\int_{\omega_i} f^{\sigma_j}\right)_{i,j=1,\dots,d} \in \mathbb{C}^{d\times d} \text{ and } V_f := \left(\int_{\omega_i} f^{\sigma_j}\right)_{\substack{j=1,\dots,d \\ i=d+1,\dots,2d}} \in \mathbb{C}^{d\times d}. \end{gathered}$$

The next step is to decide whether A_f is $\mathbb{Q}$–isogenous to a principally polarized abelian variety. A sufficient condition (see [Wan95]) is that

$$e_1 = \dots = e_d$$

holds. Let us assume now that this is the case.

In general there is no criterion to decide whether a principally polarized abelian variety is isogenous to the Jacobian of a curve (Schottky problem, see [Mum75]) but in the special case of hyperelliptic curves there is a result due to Mumford and Poor ([Poo94]): If A is simple over $\overline{\mathbb{Q}}$, principally polarized and certain Θ–series vanish, then A is isogenous to the Jacobian of an hyperelliptic curve. In the special case $d = 2$ this is always satisfied [Wei57].

Now we assume that A_f is isogenous to the Jacobian of an hyperelliptic curve C. We want to determine a affine model for this curve over the rational integers. The algorithm to do this depends mostly on results given in Mumford's Theta-lectures [Mum83]. To compute the equations over $\mathbb{Z}$ one uses a method due to Mestre [Mes91]. This was worked out and implemented by X. Wang for the case $d = 2$ and by H.-J. Weber in his thesis (see [Web97]) for $d \leq 5$.

We give an example for the simplest case $d = 2$. For the general case we refer the reader to [Web97].

Example 4.6
For $N = 87 = 3 \cdot 29$ the genus of $X_0(N)$ is 9 and the dimension of the space of new forms is 5. The Jacobian splits in

$$J_0(N) \simeq A_1^2 \times A_2 \times A_3$$

where A_1 arises from an old form coming of level 29, A_3 is a 3–dimensional factor and A_2 is isogenous to the Jacobian of a hyperelliptic curve of genus 2 associated to the cusp form of level 87 and weight 2, with Fourier coefficients:

$$\begin{array}{lllll} a_2 = \alpha, & a_3 = 1, & a_5 = -2\alpha + 2 & , a_7 = -2\alpha - 1, & a_{11} = 2\alpha + 1, \\ a_{13} = 4\alpha - 3, & a_{17} = 3, & \ldots\ldots & a_{2971} = -70\alpha + 57, & a_{2999} = -4\alpha + 12, \ldots \end{array}$$

with $\alpha^2 - \alpha - 1 = 0$.
We calculate the intersection matrices for a symplectic basis as

$$((\omega_i, \omega_j)_{X_0(N)})_{i,j=1,\ldots,4} = \left(\begin{smallmatrix} 0 & \Delta_f \\ -\Delta_f & 0 \end{smallmatrix} \right) \in \mathbb{Z}^{4\times 4} \text{ with } \Delta_f = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix} \right).$$

The period matrix is

$$\Omega_f = \begin{pmatrix} 0.63235869\ldots + 0.89156287\ldots i & -0.01791153\ldots + 0.5141950\ldots i \\ -0.01791153\ldots + 0.5141950\ldots i & -0.3085645\ldots + 1.21905454\ldots i \end{pmatrix}.$$

We find a model of the curve C over the complex numbers:

$$y^2 = x(x-1)(x-x_1)(x-x_2)(x-x_3)$$

with

$$\begin{aligned} x_1 &= -0.200591196\ldots - 0.027617620\ldots i \\ x_2 &= 0.404999977\ldots - 0.374771692\ldots i \\ x_3 &= 1.314698500\ldots - 0.312863721\ldots i \end{aligned}$$

and then we compute the absolute invariants as complex numbers

$$\begin{aligned} i_1 &= 243457.564392771\ldots - 0.38641\ldots \cdot 10^{-120} i \\ i_2 &= 2.855338295\ldots - 0.22809\ldots \cdot 10^{-122} i \\ i_3 &= 3676.120933706\ldots - 0.43387\ldots \cdot 10^{-122} i. \end{aligned}$$

Since we know by theoretical reasons that these complex numbers are rational numbers with denominators divisible at most by $2, 3, 29$, we guess that

$$i_1 = \frac{2^3 \cdot 73^5}{3^4 \cdot 29^2} \quad i_2 = \frac{73^3}{2 \cdot 3^4 \cdot 29^2} \quad i_3 = \frac{31 \cdot 67 \cdot 73^2 \cdot 181}{2^3 \cdot 3^4 \cdot 29^2}.$$

To determine the curve equation we follow Mestre and have to intersect a cubic with a quadric both defined over the rational numbers. In our case the quadric is:

$$-\frac{9417394}{48627125} z_1^2 + \frac{233886344942080}{9761465990744321} z_2^2 + \frac{24829251286245551330918 4}{1261638506225656595819776 25} z_3^2 = 0. \tag{27}$$

We have parameterize the quadric (27), and so we have to find an integral point on it. One solution is:

$$\begin{aligned} z_1 &= -857397781802345488594810074385500600 00 \\ z_2 &= -2750942355042629770002012722986101475 25 \\ z_3 &= 2306585430120386103068204884361466802 26 \end{aligned}$$

Now the intersection with the cubic is easily computed and gives a polynomial $f_6(x)$ of degree 6 in $\mathbb{Z}[x]$.

Result: $y^2 = f_6(x)$ is an equation for the curve C.
But the coefficients of $f_6(x)$ are rather huge. For example the smallest coefficient is:

$$145936780265720849968485226881259356486225191409816304571641352426792208059893706563334033746130944000.$$

An elementary reduction method due to Lagrange (connected to continued fractions) makes the coefficients much smaller and we get

$$C:\ y^2 = x^6 + 6x^5 + 13x^4 + 18x^3 + 10x^2 - 3. \tag{28}$$

Remark 4.7 We have to test the correctness of (28). We know the expected conductor of C ($= N^g = 87^2$) and the Euler factors of the L–series because of the Eichler–Shimura relation (see Sec. (4.4)). Therefore we compute the conductor of C and the local Euler factors for primes p by counting points on the curve C modulo p. If these data match (for sufficiently many Euler factors) we can be sure that the equation is the correct one (Theorem of Faltings).

With this method, Wang found hyperelliptic curves of genus 2 whose Jacobians are factors of $J_0(N)$. In the appendix 5 table (5.4) one finds a table computed by him and partly published in [Wan95].

E. Schaefer and V. Flynn used this table to verify the Birch–Swinnerton-Dyer conjecture in these cases.

In the appendix table (5.5) there are examples of curves of higher genus computed by H. -J. Weber.

4.4 Mordell–Weil Groups over Finite Fields

We consider the following task: Let $C_\mathfrak{p}$ be an irreducible projective regular curve of genus g over the finite field $k_\mathfrak{p}$. Let $J_{C_\mathfrak{p}}(k_\mathfrak{p})$ be the Jacobian variety of $C_\mathfrak{p}$. Determine $\#J_{C_\mathfrak{p}}(k_\mathfrak{p})$.

Of course one can try to do this by counting k'–rational points of extension fields k' of $k_\mathfrak{p}$. But since k' has to run through all extensions of degree $\leq g$ it is obvious that this is only possible for very small fields $k_\mathfrak{p}$ and small genus g. The alternative is to determine the L–series $L_\mathfrak{p}(C_\mathfrak{p}, t)$ of $C_\mathfrak{p}$ over $k_\mathfrak{p}$ by a more structural approach. Then one can use the identity

$$L_\mathfrak{p}(C_\mathfrak{p}, 1) = \# J_{C_\mathfrak{p}}(k_\mathfrak{p}).$$

In the case of hyperelliptic curves this can be done, at least in principle, by using the Schoof algorithm which computes $L_\mathfrak{p}(C_\mathfrak{p}, t)$ in polynomial time (see Schoof [Sch85] and Kampkötter [Kam91]). It turns out that despite of the "nice" complexity of this algorithm it is rather inefficient if one does not use further information about $C_\mathfrak{p}$. If the genus of $C_\mathfrak{p}$ is one this additional information is given by a careful study of modular curves $X_0(N)$ for suitable levels N. This approach goes back to Atkin and Elkies and was much refined by Morain and Couveignes as well as by the research group of J. Buchmann in Darmstadt.

At present we do not know such an efficient version of the Schoof algorithm for curves of genus larger than one. But if we know that $C_\mathfrak{p}$ is the special fiber of a curve C whose Jacobian A_f is a factor of $J_0(N)$ we can use the Eichler–Shimura relation (theorem (2.19)) to determine the L-series of $C_\mathfrak{p}$. To do this we only have to compute the characteristic polynomial χ_{T_p} of the Hecke operator T_p $(p \in \mathfrak{p})$ restricted to J_C. In the simplest case $k_\mathfrak{p} = \mathbb{Z}/p$ we get

$$\chi_{T_p}(p+1) = \# J_{C_\mathfrak{p}}(k_\mathfrak{p})$$

Therefore we can use the results of subsection 3.1 to compute $\# J_{C_\mathfrak{p}}(k_\mathfrak{p})$. This was implemented by J. Basmaji [Bas96]. We give one example:

Example 4.8
For $N = 284$ $J_0(N)$ has an 3–dimensional factor A_f which is isogenous to the Jacobian variety of

$$C: \ y^2 = x^7 + 3x^6 + 2x^5 - x^4 - 2x^3 - 2x^2 - x - 1.$$

For $p = 1000011149$ the characteristic polynomial is

$$\chi_{T_p}(t) = t^3 + 34755t^2 - 69189426t - 7700504141987$$

and therefore we find

$$\# J_{C_p}(\mathbb{F}_p) = \chi_{T_p}(p+1) = 1000068206078811809058120613$$

which is a prime.

Remark 4.9 The determination of $J_{C_\mathfrak{p}}(k_\mathfrak{p})$ has applications to public key cryptosystems based on the discrete logarithm problem. With the described method one finds interesting examples for this purpose if the genus of $C_\mathfrak{p}$ is ≥ 4.

4.5 Mordell–Weil Groups over $\mathbb{Q}$

We now come to the task of computing the Mordell–Weil group of the Jacobian of a curve C in the global case. Of course we have to restrict ourself to a very special situation. We assume that C is a hyperelliptic curve and that J_C is isogenous to a factor of $J_0(N)$.

We recall the theorem of Mordell–Weil: For a number field K and an abelian variety A defined over K $A(K)$ is a finitely generated $\mathbb{Z}$–module and hence

$$A(K) \cong A(K)_{\mathrm{tor}} \oplus \mathbb{Z}^{r_K}$$

where r_K is the (*geometric*) *rank* of the abelian variety A and $A(K)_{\text{tor}}$ is the subgroup of elements of finite order. Moreover $A(K) \otimes \mathbb{R}$ has a Euclidean structure induced by the Néron–Tate height h. We denote by

$$\langle P, Q \rangle := \frac{1}{2} \left(h(P+Q) - h(P) - h(Q) \right)$$

the corresponding bilinear form on $A(K)$ (see [Lan97]).

Definition 4.10 *Let $\{P_1, \ldots, P_r\}$ be elements in $A(K)$ which form a basis of $A(K) \otimes \mathbb{R}$. Then*

$$R(A(K)) := |\det \left(\langle P_i, P_j \rangle \right)|$$

is the regulator of A.

The regulator does not dependent of the choice of the elements $\{P_1, \cdots, P_r\}$.

The fundamental conjecture of Birch and Swinnerton-Dyer relates the arithmetic invariants of the abelian variety A to analytic properties of the corresponding L-series. In the following we restrict ourselves to the case $K = \mathbb{Q}$ and so we state this conjecture only in this case. We **assume** that $L(A, s)$ has an analytic continuation to $\mathbb{C}$.

Conjecture 4.11 *The rank r of $A(\mathbb{Q})$ is equal to the order of the L-series $L(A, s)$ at $s = 1$ and*

$$\frac{1}{r!} L^{(r)}(A, 1) = \frac{\# Ш \cdot R(A(\mathbb{Q})) \cdot c_\infty \cdot \prod_{p \text{ prime}} c_p}{\# A(\mathbb{Q})_{\text{tor}} \cdot \# \widehat{A}(\mathbb{Q})_{\text{tor}}}$$

holds. Here c_p are the Tamagawa numbers at the (finite) places p and c_∞ is the Tamagawa number at infinity, Ш denotes the Tate–Shafarevich group of $A(\mathbb{Q})$ and $\widehat{A}$ is the dual of A.

We mentioned in the introduction Manin's conditional algorithm for computing a basis of the Mordell–Weil group of an abelian variety A **assuming** the Birch–Swinnerton-Dyer conjecture. This algorithm reduces the search for base points to the computer search for points with Néron–Tate height bounded by an explicit estimate.
In our case A is a factor of $J_0(N)$ and isogenous to the Jacobian of an hyperelliptic curve C. Hence $L(C, s)$ satisfies the assumption on holomorphy. Even better: Since we can compute the Fourier expansions of the corresponding cusp forms we can determine its value at $s = 1$ very precisely. So the most difficult part of Manin's algorithm is to compute the height pairing. For elliptic curves there are several implementations available which do this very efficiently (e.g. in `SIMATH` or `APECS`.) For $g(C) \geq 2$ and C hyperelliptic Ch. Hahne developped a method to compute this height pairing by using Arakelov's intersection theory on the arithmetic surface associated to C (see [Hah98]). He implemented his algorithm for curves of genus 2 and applied it to the curves given in the table table (5.4). He succeeded to find a basis of $J_C(\mathbb{Q})$ in these cases. The results are:

Level	curve equation $C/$ generators	Tor/rank
67	$y^2 + (x^3 + x^2 + 1)y = 3x^5 + 9x^4 + 10x^3 + 6x^2 + 2x$ $[x^2 + 2x + 2, 4x + 3], [x^2 + 3x + 6, 10x + 7]$	$\#J_C(\mathbb{Q})_{\mathrm{tor}} = 1$ rank $= 2$
73	$y^2 + (x^3 + x^2 + 1)y = -3x^5 - 4x^4 - x^3 + x^2 + x$ $[x^2 + 2x - 1, 9x - 2], [x^2 + 2x - 2, 10x - 7]$	$\#J_C(\mathbb{Q})_{\mathrm{tor}} = 1$ rank $= 2$
93	$y^2 + (x^3 + x^2 + 1)y = -2x^5 + x^4 + x^3$ $[x^2 + 3x - 6, 24x - 29], [x^2 - 4x - 3, x + 2]$	$\#J_C(\mathbb{Q})_{\mathrm{tor}} = 1$ rank $= 2$
103	$y^2 + (x^3 + x^2 + 1)y = x^5 - 5x^4 + 5x^3 - 3x^2$ $[x^2 - 4x + 2, 18x - 11], [x^2 + 11x - 6, 72x - 37]$	$\#J_C(\mathbb{Q})_{\mathrm{tor}} = 1$ rank $= 2$
107	$y^2 + (x^3 + x^2 + 1)y = x^5 + 2x^4 + 4x^3 + 4x^2 + 2x$ $[x^2 + 3, x + 4], [x^2 - x + 1, x]$	$\#J_C(\mathbb{Q})_{\mathrm{tor}} = 1$ rank $= 2$
115	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + 2x^3$ $[x^2 + 1, x - 2], [x^2 + 6, 6x + 13]$	$\#J_C(\mathbb{Q})_{\mathrm{tor}} = 1$ rank $= 2$

The equations f_C of the curve C are changed in order to have minimality at $p = 2$. A point of $J_C(\mathbb{Q})$ corresponds to an ideal class of the integral closure of $\mathbb{Q}[x]$ in

$$F(x, y) := \mathbb{Q}[x, y] \,/\, \langle f_C \rangle$$

which is a free module of rank 2 over $\mathbb{Q}[x]$ with integral basis $\langle 1, \Delta_C \rangle$ (Δ_C is the discriminant of F). In the table a point is given by its coordinates w.r.t. this basis.

5 Appendix

Table 5.1

Splitting of $S_2^{new}(N)$

N	$\dim(S_2(N))$	$\dim(S_2^{new}(N))$	Splitting	N	$\dim(S_2(N))$	$\dim(S_2^{new}(N))$	Splitting
11	1	1	1(1)	46	5	1	1(1)
12	0	0		47	4	4	4(1)
13	0	0		48	3	1	1(1)
14	1	1	1(1)	49	1	1	1(1)
15	1	1	1(1)	50	2	2	1(2)
16	0	0		51	5	3	1(1), 2(1)
17	1	1	1(1)	52	5	1	1(1)
18	0	0		53	4	4	1(1), 3(1)
19	1	1	1(1)	54	4	2	1(2)
20	1	1	1(1)	55	5	3	1(1), 2(1)
21	1	1	1(1)	56	5	2	1(2)
22	2	0		57	5	3	1(3)
23	2	2	2(1)	58	6	2	1(2)
24	1	1	1(1)	59	5	5	5(1)
25	0	0		60	7	0	
26	2	2	1(2)	61	4	4	1(1), 3(1)
27	1	1	1(1)	62	7	3	1(1), 2(1)
28	2	0		63	5	3	1(1), 2(1)
29	2	2	2(1)	64	3	1	1(1)
30	3	1	1(1)	65	5	5	1(1), 2(2)
31	2	2	2(1)	66	9	3	1(3)
32	1	1	1(1)	67	5	5	1(1), 2(2)
33	3	1	1(1)	68	7	2	2(1)
34	3	1	1(1)	69	7	3	1(1), 2(1)
35	3	3	1(1), 2(1)	70	9	1	1(1)
36	1	1	1(1)	71	6	6	3(2)
37	2	2	1(2)	72	5	1	1(1)
38	4	2	1(2)	73	5	5	1(1), 2(2)
39	3	3	1(1), 2(1)	74	8	4	2(2)
40	3	1	1(1)	75	5	3	1(3)
41	3	3	3(1)	76	8	1	1(1)
42	5	1	1(1)	77	7	5	1(3), 2(1)
43	3	3	1(1), 2(1)	78	11	1	1(1)
44	4	1	1(1)	79	6	6	1(1), 5(1)
45	3	1	1(1)	80	7	2	1(2)

Explanation of the fourth column: The notation $a(b)$ means that $S_2^{new}(N)$ has b a–dimensional $\mathbb{T}_N[G_{\mathbb{Q}}]$–invariant subspaces.

Table 5.2

Large example of a Hecke operator

$N = 95, p = 1000002667, g = 9$

$$A_{T_p} = \begin{pmatrix} 23806 & -7956 & -4126 & -8456 & 20272 & -16620 & -8164 & 7070 & 474 \\ -7752 & 18882 & 594 & -13176 & 20272 & -21340 & -8164 & 7460 & 474 \\ -12482 & -5280 & 6330 & -7202 & 21232 & -18724 & -11522 & 16802 & 4694 \\ 10000 & 636 & -76 & 27152 & -11522 & 15542 & 1922 & -16328 & -3944 \\ 32756 & -2040 & 3000 & 12366 & 1050 & 17646 & 5280 & -26060 & -8164 \\ -960 & -20390 & -12366 & -3000 & 12482 & 5252 & -5280 & 2850 & 8164 \\ -27464 & -23466 & -12658 & -30758 & 26776 & -33640 & 10650 & 21944 & 19522 \\ 4330 & -13380 & 9050 & -9050 & 0 & -9050 & 0 & 22508 & 0 \\ 12484 & -10204 & -9108 & 258 & -3734 & 844 & 586 & -13202 & 25530 \end{pmatrix}$$

Characteristic polynomial of the Hecke operator T_p

$$\begin{aligned}\chi_{A_{T_p}}(x) = {} & (x^4 - 41852x^3 - 1705573680x^2 + 99715463270960x - 1145905723637314144) \\ & (x^3 - 72244x^2 + 1423292512x - 4544597778992)(x - 13532)^2\end{aligned}$$

Table 5.3

Congruences between elliptic curves

Examples for $p = 11$:

Weierstraß model	Conductor	$\deg\varphi$
$E_1 : y^2 = x^3 + x^2 + 2x + 2$	$N_1 = 190$	8
$E_2 : y^2 = x^3 + x^2 + 81710302x + 576603336052$	$N_2 = 2470 = 13 \cdot 190$	656656
$E_1 : y^2 = x^3 - 3x - 34$	$N_1 = 216$	24
$E_2 : y^2 = x^3 - 362988x + 82933524$	$N_2 = 1512 = 7 \cdot 216$	15840
$E_1 : y^2 = x^3 - 27x + 918$	$N_1 = 216$	72
$E_2 : y^2 = x^3 - 40332x - 3071612$	$N_2 = 1512 = 7 \cdot 216$	5280

Example for $p = 13$:

Weierstraß model	Conductor	$\deg\varphi$
$E_1 : y^2 = x^3 + x - 10$	$N_1 = 52$	3
$E_2 : y^2 = x^3 - 362249x + 165197113$	$N_2 = 988 = 19 \cdot 52$	13260

There are no congruences for $p > 13$ up to N = 3000.

Tables of equations of hyperelliptic curves whose Jacobians are factors of $J_0(N)$

Table 5.4

Hyperelliptic curves of genus 2 with real multiplication	
Level	Affine curve equations defined over $\mathbb{Z}[\frac{1}{2}]$
23	$y^2 = x^6 + 4x^5 - 18x^4 - 142x^3 - 351x^2 - 394x - 175$
29	$y^2 = x^6 + 2x^5 - 17x^4 - 66x^3 - 83x^2 - 32x - 4$
31	$y^2 = x^6 + 4x^5 - 14x^4 - 94x^3 - 159x^2 - 98x - 27$
63	$y^2 = x^5 + 27x^4 + 280x^3 + 1512x^2 + 7056x + 21168$
65	$y^2 = 3(5x^6 - 30x^5 + 63x^4 - 62x^3 + 9x^2 + 36x - 8)$
65	$y^2 = -x^6 + 10x^5 - 32x^4 + 20x^3 + 40x^2 + 6x - 1$
67	$y^2 = x^6 + 8x^5 - 18x^4 + 14x^3 - 3x^2 - 2x + 1$
73	$y^2 = x^6 - 10x^5 - 15x^4 - 2x^3 + 6x^2 + 4x + 1$
87	$y^2 = x^6 + 6x^5 + 13x^4 + 18x^3 + 10x^2 - 3$
93	$y^2 = x^6 - 6x^5 + 5x^4 + 6x^3 + 2x^2 + 1$
103	$y^2 = x^6 + 6x^5 - 19x^4 + 22x^3 - 10x^2 + 1$
107	$y^2 = x^6 - 4x^5 + 10x^4 - 18x^3 + 17x^2 - 10x + 1$
115	$y^2 = 25x^6 + 90x^5 + 137x^4 + 110x^3 + 50x^2 + 12x + 1$
117	$y^2 = 3x^5 + 150x^4 + 3250x^3 + 39000x^2 + 264147x + 799370$
117	$y^2 = -3(x^6 + 4x^4 + 6x^3 + 16x^2 + 12x + 9)$
125	$y^2 = x^6 + 4x^5 - 10x^4 - 90x^3 - 215x^2 - 230x - 95$
133	$y^2 = -3x^6 + 40x^5 - 190x^4 + 370x^3 - 251x^2 + 70x - 7$
133	$y^2 = x^6 - 4x^5 - 18x^4 - 26x^3 - 15x^2 - 2x + 1$
135	$y^2 = x^6 + 12x^5 + 66x^4 + 198x^3 + 333x^2 + 270x + 45$
147	$y^2 = x^6 + 30x^5 + 371x^4 + 2422x^3 + 8813x^2 + 16968x + 13524$
161	$y^2 = x^6 - 12x^5 + 26x^4 - 22x^3 + 17x^2 - 6x + 1$
167	$y^2 = x^6 - 10x^5 + 37x^4 - 70x^3 + 70x^2 - 32x + 1$
175	$y^2 = x^6 + 4x^5 + 2x^4 - 18x^3 - 55x^2 - 70x - 35$
177	$y^2 = x^6 + 6x^5 + 5x^4 + 6x^3 + 2x^2 + 1$
188	$y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$
189	$y^2 = 3x^5 + 96x^4 + 1498x^3 + 13356x^2 + 64827x + 132300$
191	$y^2 = x^6 - 18x^5 + 125x^4 - 402x^3 + 506x^2 + 144x - 607$

We remark that the models defined over $\mathbb{Z}[\frac{1}{2}]$ are calculated with a program of Liu [Liu94] and some corrections are made by E. Schaefer.

Table 5.5

Hyperelliptic curves of genus 3 with real multiplication	
N	41
Curve	$y^2 = x^8 + 4x^7 - 8x^6 - 66x^5 - 120x^4 - 56x^3 + 53x^2 + 36x - 16$
Δ_3	$(-1) \cdot 2^{16} \cdot 41^6$
N	$95 = 5 \cdot 19$
Curve	$y^2 = 19x^8 - 262x^7 + 1507x^6 - 4784x^5 + 9202x^4 - 10962x^3 + 7844x^2 - 3040x + 475$
Δ_3	$2^{16} \cdot 5^6 \cdot 19^4$
N	$284 = 2^2 \cdot 71$
Curve	$y^2 = x^7 + 3x^6 + 2x^5 - x^4 - 2x^3 - 2x^2 - x - 1$
Δ_3	$(-1) \cdot 71^3$
N	$385 = 5 \cdot 7 \cdot 11$
Curve	$y^2 = x^8 + 12x^7 + 68x^6 + 114x^5 + 282x^4 + 176x^3 - 123x^2 - 170x + 25$
Δ_3	$(-1) \cdot 2^{16} \cdot 5^4 \cdot 7^{19} \cdot 11^6$

Hyperelliptic curves of genus 4 with real multiplication	
N	47
Curve	$y^2 = x^{10} + 6x^9 + 11x^8 + 24x^7 + 19x^6 + 16x^5 - 13x^4 - 30x^3 - 38x^2 - 28x - 11$
Δ_4	$2^{20} \cdot 47^8$
N	$119 = 7 \cdot 17$
Curve	$y^2 = x^{10} + 2x^8 - 11x^6 - 14x^5 - 40x^4 - 42x^3 - 48x^2 - 28x - 7$
Δ_4	$2^{20} \cdot 7^6 \cdot 17^6$

References

[ABF90] J. Antoniadis, M. Bungert, and G. Frey. Properties of twists of elliptic curves. *J. Reine Angew. Math.*, 405:1–28, 1990.

[AL70] A. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.* , (185):134–160, 1970.

[Bas96] J. Basmaji. *Ein Algorithmus zur Berechnung von Hecke–Operatoren und Anwendung auf modulare Kurven.* PhD thesis, Universität (GH) Essen, 1996.

[Bir91] B. Birch. Hecke actions on classes of ternary quadratic forms. In A. Pethö et. al., editor, *Computational Number Theory*, pages 191–212, Berlin, New York, 1991. de-Gruyter.

[Car86] H. Carayol. Sur les representations ℓ-adiques associees aux formes modulaires de Hilbert. *Ann. Sci. Ec. Norm. Super.* , IV. Ser. 19, 409-468 (1986).

[Cre92] J. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, Cambridge, 1992.

[Cre95] J. E. Cremona. Computing the degree of modular parametrization of a modular elliptic curve. *Math. Comp.* , 64:1235–1250, 1995.

[DDT95] H. Darmon, F. Diamond, and R. Taylor. Fermat's Last Theorem. Current Development in Mathematics, pages 1–170, Boston, 1995. International Press.

[DR73] P. Deligne and M. Rapoport. Les schemas de modules de courbes elliptiques. In W. Kuyk and P. Deligne, editors, *Modular Functions in One Variable II*, number 349 in Lecture Notes in Mathematics, pages 143–316, Berlin, Heidelberg, 1973. Springer-Verlag.

[DS74] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Ann. sci. E.N.S.* 4^e *ser.* , pages 507–530, 1974.

[Eic72] M. Eichler. The Basis Problem for Modular Forms and Traces of the Hecke Operators. In *Modular Functions of one Variable I*, volume 320 of *Lecture Notes in Mathematics*, pages 75–152, Berlin, Heidelberg, 1972. Springer-Verlag.

[Fre87] G. Frey. Links between solutions of $A - B = C$ and elliptic curves. In *Number Theory (Ulm 1987)*, volume 1380 of *Lecture Notes in Mathematics*, pages 31–62, 1987.

[Fre94] G. Frey, editor. *On Artin's Conjecture for Odd 2-dimensional Representations*, volume 1583 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, Heidelberg, 1994.

[Fre97] G. Frey. On Ternary Equations of Fermat Type and Relations with Elliptic Curves. In G. Cornell, J. H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 527–548, Berlin, Heidelberg, 1997. Springer-Verlag.

[Hab83] K. Haberland. Perioden von Modulformen einer Variablen und Gruppencohomologie, I. *Math. Nachr.*., 112:245–282, 1983.

[Hah98] C. Hahne. *Die kanonische Höhe auf hyperelliptischen Jacobischen Varietäten und Erzeuger von modularen Mordell-Weil Gittern.* PhD thesis, Universität (GH) Essen, 1998. to appear.

[Hid81] H. Hida. Congruences of Cusp Forms and special values of their zeta functions. *Invent. math.* , 63:225–261, 1981.

[HK96] E. Halberstadt and A. Kraus. Sur la comparaison galoisienne des points de torsion des courbes elliptiques. *C. R. Acad. Sci., Paris Ser. I*, 322(4):313–316, 1996.

[Kam91] W. Kampkötter. *Explizite Gleichungen für Jacobische Varietäten hperelliptischer Kurven.* PhD thesis, Universität (GH) Essen, 1991.

[KM85] N. M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic curves.* Princeton University Press, Princeton, NJ, 1985.

[KO92] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.* , 293:259–275, 1992.

[KS91] E. Kaltofen and B. Saunders. On Wiedemann's Method of Solving Sparse Linear Systems. In *Proc. 9th Int. Symp., AAECC-9,*, number 539 in Lect. Notes Comput. Sci., pages 29–38, 1991.

[KS98] E. Kani and W. Schanz. Modular diagonal quotient surfaces. *Mathematische Zeitschrift*, 227:337–366, 1998.

[KW94] I. Kiming and X. Wang. Examples of 2–dimensional odd Galois repesentations of A_5–type over $\mathbb{Q}$ satisfying the Artin conjecture. In G. Frey, editor, *On Artin's Conjecture for Odd 2–dimensional Representations*, volume 1585 of *Lecture Notes in Mathematics*, pages 109–121, Berlin, Heidelberg, 1994. Springer-Verlag.

[Lan97] S. Lang. *Survey of Diophantine Geometry.* Springer-Verlag, Berlin, Heidelberg, 1997.

[Liu94] Q. Liu. Modèles minimaux des courbes de genre deux. *J. Reine Angew. Math.*, 453:127–164, 1994.

[Man71] J. Manin. Cyclotomic Fields and Modular Curves. *Russian Math. Surveys*, 26(6):7–78, 1971.

[Man72] J. Manin. Parabolic Points and Zeta-Functions of Modular Curves. *Math. USSR Izvestija*, 6(1):19–64, 1972.

[Maz77] B. Mazur. Modular Curves and the Eisenstein ideal. *Publ. Math. IHES*, 47:33–186, 1977.

[Maz78] B. Mazur. Rational Isogenes of Prime Degree. *Invent. math.* , 44:129–162, 1978.

[Mer93] L. Merel. *Quelques aspectes arithmétiques et géométriques de la théorie des symboles modulaires.* PhD thesis, Université Paris 6, 1993.

[Mer94] L. Merel. Universal Fourier expansions of modular forms. In G. Frey, editor, *On Artin's Conjecture for Odd 2–dimensional Representations*, volume 1585 of *Lecture Notes in Mathematics*, pages 59–94, Berlin, Heidelberg, 1994. Springer-Verlag.

[Mes86] J. F. Mestre. 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, Katata/Japan, 1986.

[Mes91] J. F. Mestre. Construction de courbes de genre 2 á partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 313–334. Birkhäuser Verlag, 1991.

[MM94] L. Mai and M. R. Murty. The Phragmén–Lindelöf theorem and modular elliptic curves. *Contemp. Math.*, 166:335–340, 1994.

[Mül98] M. Müller. *Arithmetik von Modulkurven.* PhD thesis, Universität (GH) Essen, 1998. to appear.

[Mum74] David Mumford. *Abelian Varieties.* Oxford University Press, Oxford, 2 edition, 1974.

[Mum75] David Mumford. *Curves and Their Jacobians.* University of Michigan Press, Ann Arbor, 1975.

[Mum83] D. Mumford. *Tata lectures on Theta I–III* . Birkhäuser Verlag, Zürich, 1983.

[Ogg78] A. Ogg. On the Weierstrass Points of $X_0(N)$. *Illinois J. Math.* , 22(1):31–35, 1978.

[Poo94] C. Poor. On the hyperelliptic locus. *Duke Math. J.* , 76(3):809–884, 1994.

[Rib83] K. Ribet. On mod p Hecke operators and congruences between modular forms. *Invent. math.* , 71:193–205, 1983.

[Roh97] D. Rohrlich. Modular Curves, Hecke Correspondences and L-Functions. In G. Cornell, J. H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 41–100, Berlin, Heidelberg, 1997. Springer-Verlag.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp.* , 43:483–494, 1985.

[Ser77] J. P. Serre. Modular forms of weight one and Galois representations. In A. Fröhlich, editor, *Algebraic Number Fields*, pages 193–268, New York, 1977. Academic Press.

[Shi71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, Princeton, New Jersey, 1971.

[Shi73a] G. Shimura. On modular forms of half integral weight. *Annals of Mathematics*, 97:440–481, 1973.

[Shi73b] G. Shimura. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan*, 25(3):523–544, 1973.

[Wal81] J.-L. Waldspurger. Sur les coéfficients de Fourier des formes modulaires de poids demi–entiers. *Journal de Mathématiques pures et appliquées*, 60:375–484, 1981.

[Wan94] X. Wang. The Hecke operators on the cusp forms of $\Gamma_0(N)$ with nebentype. In G. Frey, editor, *On Artin's Conjecture for Odd 2–dimensional Representations*, volume 1585 of *Lecture Notes in Mathematics*, pages 59–94, Berlin, Heidelberg, 1994. Springer-Verlag.

[Wan95] X. Wang. 2–dimensional simple factors of $J_0(N)$. *Manuscripta mathematica*, 87:179–197, 1995.

[Web97] H.-J. Weber. Hyperelliptic simple Factors of $J_0(N)$ with dimension at least 3. *Experimental Math.*, 1997. to appear.

[Wei57] A. Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen*, 2:33–53, 1957.

[Zag85] D. Zagier. Modular Parametrization of Elliptic Curves. *Can. Math. Bull.* , 28(3):372–384, 1985.

[Zag90] D. Zagier. Hecke operators and periods of modular forms. In S. Gelbart, R. Howe, and P. Sarnak, editors, *Festschrift in honor of I.I. Piatetski-Shapiro on the occasion of his sixtieth birthday*, volume 3 of *Isr. Math. Conf. Proc.*, pages 321–336. The Weizmann Science Press of Israel, 1990.