

# Singular Values of Thompson Series\*

*Imin Chen and Noriko Yui*

---

This is an extended version of a talk presented by Noriko Yui at the Monster Bash, May 20—22, 1993 at the Mathematical Research Institute of the Ohio State University.

## Contents

Introduction

1. Hauptmoduln
2. Modular equations
3. Class fields
4. Class polynomials
5. Gross–Zagier type formulae for resultants and discriminants of class polynomials
6. Postscripts

Appendix : Tables

- A1. Modular relations for  $\Gamma_0(N)+$
- A2. Modular equations
- A3. Class polynomials
- A4. Discriminants of class polynomials
- A5. Resultants of class polynomials

References

---

\* This work was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and by the Royal Society of London.

## Introduction

Let  $\mathfrak{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$  be the upper half complex plane and let  $\Gamma = PSL_2(\mathbb{Z})$  be the modular group. Then  $\Gamma$  acts on  $\mathfrak{H}$  by the fractional linear transformation :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d} \quad \text{where} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \quad \text{and} \quad z \in \mathfrak{H}.$$

The quotient  $\mathfrak{H}/\Gamma$  is an open Riemann surface of genus zero. We compactify it by adding the point at infinity, the cusp of  $\Gamma$ . This compact Riemann surface will be denoted by  $\mathfrak{H}^*/\Gamma$ .

Let  $j(z)$  be the elliptic modular function. Then  $j$  defines a complex analytic isomorphism of compact Riemann surfaces

$$j : \mathfrak{H}^*/\Gamma \rightarrow \mathbb{P}^1(\mathbb{C}), \quad z \mapsto j(z),$$

that is,  $j$  is the uniformizer of  $\mathfrak{H}^*/\Gamma$ , and it generates the function field of  $\mathfrak{H}^*/\Gamma$  over  $\mathbb{C}$ . Furthermore, at  $z = \infty$  the function  $j(z)$  has a  $q$ -expansion of the form

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \quad \text{where} \quad q = e^{2\pi iz}.$$

We normalize it by subtracting the constant term

$$J(z) := j(z) - 744 = q^{-1} + \sum_{n \geq 1} c_j(n)q^n \quad \text{with} \quad c_j(n) \in \mathbb{Z} \quad \text{for all} \quad n \geq 1.$$

We may call  $J$  having the above properties a *canonical Hauptmodul* for the ‘‘genus zero group’’  $\Gamma$ .

More generally, let  $G$  be any discrete subgroup of  $PSL_2(\mathbb{R})$  such that  $\mathfrak{H}^*/G = \mathfrak{H}/G \cup \{\text{cusps of } G\}$  is a compact Riemann surface of genus zero. We may call such a group  $G$  a *genus zero subgroup* of  $PSL_2(\mathbb{R})$ . A *Hauptmodul*  $f$  for the genus zero subgroup  $G$  is then:

- (1) a meromorphic function on  $\mathfrak{H}^*/G$ ,
- (2) a generator of the function field of  $\mathfrak{H}^*/G$  over  $\mathbb{C}$ , or equivalently,
- (2') a uniformizer

$$f : \mathfrak{H}^*/G \rightarrow \mathbb{P}^1(\mathbb{C}), \quad z \mapsto f(z).$$

In all cases considered in this paper,  $G$  contains the transformation  $z \rightarrow z + 1$  so that  $f$  has a  $q$ -expansion in terms of  $q = e^{2\pi iz}$ . Furthermore, if  $f$  has a  $q$ -expansion of the following form with the constant term normalized to 0:

$$f(z) = q^{-1} + \sum_{n \geq 1} c_f(n)q^n \quad \text{with} \quad c_f(n) \in \mathbb{Z} \quad \text{for all} \quad n \geq 1,$$

$f$  is called a *canonical Hauptmodul* for a genus zero subgroup  $G$ .

(The reason for normalizing constant terms in the  $q$ -expansion of Hauptmoduln to 0 is that constant terms are not a well-defined concept in Monstrous Moonshine, i.e., they are not characters or even necessarily integers).

Let  $N \geq 1$  be an integer and let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N} \right\}.$$

Then  $\Gamma_0(N)$  is a subgroup of  $\Gamma$  of finite index. The cusps of  $\Gamma_0(N)$  consist of the finite set  $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$  and they are all defined over  $\mathbb{Q}$ . Let

$$X_0(N) = \mathfrak{H}^*/\Gamma_0(N) \quad \text{and} \quad X_0(N)+ = X_0(N)/\langle W_N \rangle$$

where  $\langle W_N \rangle$  denotes the group of Atkin–Lehner involutions on  $X_0(N)$  (of order  $2^r$  if  $r$  distinct primes divide  $N$ ). Associated to  $X_0(N)+$  there is a subgroup  $G$  of  $PSL_2(\mathbb{R})$ , which contains  $\Gamma_0(N)$  as a normal subgroup. We denote such a group by  $\Gamma_0(N)+$ . (If  $N$  is prime, then  $\Gamma_0(N)+ = \Gamma_0(N) + w_N$  where  $w_N = \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$

is the Fricke involution, and  $X_0(N)$  is a double covering of  $X_0(N)+$ .) There are only finitely many values of  $N$  for which  $X_0(N)$  or  $X_0(N)+$  has genus zero. Let  $\mathfrak{S}$  denote the set of prime values for  $N$  giving rise to genus zero Riemann surfaces  $X_0(N)+$ , then

$$\mathfrak{S} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\} \quad (\text{Fricke [13,14]; Ogg [23]}).$$

Suppose that  $G$  is a subgroup of  $PSL_2(\mathbb{R})$  which contains  $\Gamma_0(N)$  for some  $N$ .  $G$  is said to have *level*  $N$  if  $N$  is the smallest positive integer for which  $\Gamma_0(N) \subseteq G$ .

Now we bring in the Monster,  $\mathbb{M}$ , into our consideration. The Monster  $\mathbb{M}$  is the largest of the sporadic simple groups, of order

$$2^{46} 3^{20} 5^9 7^6 11^2 13^3 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \sim 8 \cdot 10^{53}.$$

Ogg [23] noticed that the primes dividing the order of  $\mathbb{M}$  are exactly those in the set  $\mathfrak{S}$ . The monster  $\mathbb{M}$  acts on a graded vector algebra  $V = V_{-1} \oplus_{n \geq 1} V_n$  constructed by Frenkel, Lepowsky and Meurman [12]. It was first shown by the same team that for each  $n \neq 0$ , the dimension of an  $\mathbb{M}$ -module  $V_n$  is equal to the  $n$ -th coefficient  $c_j(n)$  of the  $q$ -expansion of  $J$ , the characteristic defining property of  $V$ . For any element  $g \in \mathbb{M}$ , let  $\text{Tr}(g|V_n)$  denote the trace of  $g$  acting on  $V_n$  for each  $n$ . Then  $\text{Tr}(g|V_{-1}) = 1$  and  $\text{Tr}(g|V_n) \in \mathbb{Z}$  for every  $n \geq 1$ . Packaging together all these data, the Thompson series was defined:

$$T_g(z) = q^{-1} + \sum_{n \geq 1} \text{Tr}(g|V_n) q^n \quad \text{where } q = e^{2\pi iz}.$$

If  $g = 1_{\mathbb{M}}$  is the identity element of  $\mathbb{M}$ , then  $\text{Tr}(1_{\mathbb{M}}|V_n) = \dim(V_n) = c_j(n)$ , so one gets  $T_1(z) = J(z) = j(z) - 744$ , the canonical Hauptmodul for  $\Gamma$ . Furthermore, it was conjectured (*Monstrous Moonshine*) by Conway and Norton [8] on a suggestion of Thompson that *for any element  $g \in \mathbb{M}$  the Thompson series  $T_g(z)$  is a Hauptmodul for a genus zero subgroup of level  $N = N(g)$  divisible by the order of  $g$ . Moreover, this genus zero subgroup lies between  $\Gamma_0(N)$  and its normalizer in  $PSL_2(\mathbb{R})$ .*

This conjecture has recently been proved by Borcherds [5] using generalized Kac-Moody algebras and a no-ghost theorem from string theory.

The main purpose of this paper is to study Thompson series evaluated at imaginary quadratic arguments (*singular moduli*), and the fields they generate over imaginary quadratic fields, and  $\mathbb{Q}$ .

We shall first recall the classical results (*Kronecker's Jugendtraum*) on singular moduli of the elliptic modular function  $j$  for  $\Gamma$  evaluated at imaginary quadratic arguments. (The standard references on this subject are “Complex Multiplication” by Borel, et al. [4], Cox [9], Lang [19] and Shimura [25].)

Let  $K$  be an imaginary quadratic field over  $\mathbb{Q}$  of discriminant  $d_K$  and let  $\mathcal{O} \subset K$  be an order of conductor  $f$ , discriminant  $f^2 d_K$  and class number  $h(\mathcal{O})$ . Let  $\tau \in \mathfrak{H} \cap \mathcal{O}$  be an imaginary quadratic argument. Then  $j(\tau)$  is an algebraic integer (*singular modulus*). This was proved by constructing the modular equation. A singular modulus  $j(\tau)$  generates over  $K$  the ring class field,  $L$ , of  $\mathcal{O}$  (the Hilbert class field if  $\mathcal{O}$  is the maximal order of  $K$ ). The Galois group  $\text{Gal}(L/\mathbb{Q})$  is isomorphic to a generalized dihedral group  $\text{Pic}(\mathcal{O}) \rtimes C_2$ , where  $\text{Pic}(\mathcal{O})$  is the ideal class group of  $\mathcal{O}$  of order  $h(\mathcal{O})$  (=the class number of  $\mathcal{O}$ ). Moreover, any generalized dihedral extension of  $\mathbb{Q}$  is obtained in this way.

The ring class field  $L$  can be constructively realized over  $\mathbb{Q}$  as the splitting field of the minimal polynomial of  $j(\tau)$ , called a *class polynomial* of  $\mathcal{O}$ . Furthermore, discriminants of class polynomials and resultants of two class polynomials are highly divisible numbers and their decomposition laws were described by the formulae due to Gross and Zagier [16].

A similar theory should exist for any Thompson series, and we shall specifically look into the following questions:

- (a) Thompson series evaluated at imaginary quadratic arguments (“singular moduli” of Thompson series);
- (b) Explicit construction of “modular equations” associated to Thompson series;
- (c) Explicit description of the “class fields” generated by singular moduli of Thompson series, e.g., Galois group structure, class field structure;
- (d) Explicit construction of “class polynomials” satisfied by singular moduli of Thompson series;
- (e) Gross-Zagier type formulae for the discriminants of class polynomials (more generally, for the resultants of two class polynomials) determined in (d);
- (f) Singular moduli of “roots” of some Thompson series.

A Thompson series  $T_g(z)$  is said to be *fundamental* if it is a Hauptmodul for a genus zero subgroup of level  $N$  when  $N$  is exactly equal to the order,  $o(g)$ , of  $g \in \mathbb{M}$ . (This corresponds to the condition  $h = 1$  in Conway and Norton [8].)

Our results are formulated for fundamental Thompson series  $T_g$  for genus zero subgroups  $\Gamma_0(N) + e, f, g, \dots$ .

The questions (a) and (c) may be answered if we work out the Shimura Reciprocity Law (Shimura [25], Theorem (6.31)) explicitly in our context.

For (e) we simply observe that discriminants and resultants of class polynomials factor very highly, and that they seem to be governed by Gross–Zagier type formulae.

For (f) we discuss the illuminating examples considered in Yui–Zagier [30], that is, singular values of Weber functions, which are the 24–th roots of a Hauptmodul for  $\Gamma_0(2)$ , and then formulate a conjecture for singular moduli of “roots” of some fundamental Thompson series.

Now we are ready to state our main results.

**Theorem I.** Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$  with a fixing group  $G$  of the form  $\Gamma_0(N) + e, f, \dots$ . Then for each imaginary quadratic number  $\tau \in \mathfrak{H}$  satisfying  $az^2 + bz + c = 0$ ,  $(a, N) = 1$ ,  $T_g(\tau)$  is an algebraic integer.

In order to prove Theorem I, we shall construct “modular equations” associated to Thompson series. Our proof is a direct analogue of the classical proof for singular moduli of  $j$ .

**Theorem II.** For any positive integer  $m$  such that  $(m, N) = 1$ , there exists an irreducible symmetric polynomial  $\Phi_m^T(X, Y) \in \mathbb{Z}[X, Y]$  in two variables  $X, Y$  satisfying the following properties:

- (1)  $\Phi_m^T(T_g, T_g \circ m) = 0$ , and
- (2)  $\Phi_m^T(X, X)$  has leading coefficient  $\pm 1$  if  $m$  is square-free.

Here  $T_g \circ m$  means the composition of  $T_g$  and the multiplication by  $m$  map.

The essential point of Theorem II is the construction of a modular equation enjoying the property (2), from which the algebraic integrality of  $T_g(\tau)$  for  $\tau$  would be derived.

Our results on the algebraic structures of the fields generated by singular moduli of Thompson series are formulated in the following theorem. We restrict ourselves to those singular moduli of Thompson series evaluated at the imaginary quadratic arguments specified in Theorem I.

**Theorem III.** Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . Let  $K$  be an imaginary quadratic field of discriminant  $d_K$ . Let  $\mathcal{O}$  be an order of  $K$  of discriminant  $N^2 d_K$  and class number  $h(\mathcal{O})$ . Let  $\text{Pic}(\mathcal{O})$  be the ideal class group of  $\mathcal{O}$ . There is a bijection  $\psi : \text{Pic}(\mathcal{O}) \rightarrow I_K(N)/P_{K, \mathbb{Z}}(N)$  where the latter is the generalized ideal class group of  $K$  with modulus  $N$ . Then following assertions hold:

- (1) For any ideal class  $\mathfrak{a} \in \text{Pic}(\mathcal{O})$ ,  $T_g(\psi(\mathfrak{a}))$  generates the ring class field,  $L$ , of  $\mathcal{O}$ .
- (2) For any ideal classes  $\mathfrak{a}, \mathfrak{b} \in \text{Pic}(\mathcal{O})$ , define  $\sigma_{\mathfrak{b}}(T_g(\psi(\mathfrak{a})))$  by

$$\overline{\sigma_{\mathfrak{b}}(T_g(\psi(\mathfrak{a})))} = T_g(\psi(\bar{\mathfrak{b}}\mathfrak{a}))$$

where  $\bar{\phantom{x}}$  denotes complex conjugation. Then  $\sigma_{\mathfrak{b}}$  is a well-defined element of the Galois group  $\text{Gal}(L/K)$ , and  $\sigma \mapsto \sigma_{\mathfrak{b}}$  induces an isomorphism  $\text{Pic}(\mathcal{O}) \cong \text{Gal}(L/K)$ .

A constructive version of Theorem III can be derived if we translate the ideal formulation to quadratic forms. Let  $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$  denote the group of primitive positive definite quadratic forms  $[a, b, c]$ ,  $a > 0$ ,  $(a, N) = 1$  of discriminant  $d_K$  modulo  $\Gamma_0(N)$ . Then there is a bijection between  $\text{Pic}(\mathcal{O})$  and this group.

**Theorem IV.** For each  $Q \in \mathcal{Q}_{d_K}(N)/\Gamma_0(N)$ , let  $\tau_Q$  denote the root of  $Q(z, 1) = 0$  in  $\mathcal{O} \cap \mathfrak{H}$ . Define the polynomial

$$M(X) = \prod_{i=1}^{h(\mathcal{O})} (X - T_g(\tau_Q)).$$

Then

- (1)  $M(X)$  is the minimal polynomial of  $T_g(\tau_Q)$  over  $\mathbb{Q}$ ,

- (2)  $M(X) \in \mathbb{Z}[X]$  and is irreducible over  $\mathbb{Q}$ ,  
 (3) The splitting field of  $M(X)$  over  $\mathbb{Q}$  is the ring class field  $L$  of  $K$ , and  
 (4)  $\text{Gal}(M/\mathbb{Q}) \cong \text{Pic}(\mathcal{O}) \rtimes C_2$ .

**Observation.** The resultants and discriminants of class polynomials are highly divisible numbers with small prime factors. There are conjectural Gross–Zagier type formulae describing the decomposition law of discriminants and resultants.

**Conjecture.** Let  $T_g$  be a fundamental Thompson series for  $\Gamma_0(N) + e, f, \dots$ , which has shape:

$$T_g(z) = \left\{ \frac{\eta(az)^\alpha \eta(bz)^\beta \cdots}{\eta(cz)^\gamma \eta(dz)^\delta \cdots} \right\}^r \quad \text{with some } r \in \mathbb{Z}^+.$$

Then the assertions of Theorem I–IV hold true also for “roots” of  $T_g$ .

Yui–Zagier [30] discussed singular moduli of Weber functions, which are the 24–th roots of Hauptmoduln for  $\Gamma_0(2)$ , in the context of Theorem I–IV, and the conjectural Gross–Zagier type formulae for resultants and discriminants were described.

Similar results should also hold for any fundamental Thompson series having shape as in Conjecture. For instance, consider  $T_g$  for  $\Gamma_0(N)$  with  $N - 1 \mid 24$  and their  $N/m$ -th roots where  $m = (N - 1, 24)$ , or  $T_{6+3}(z) = \{\eta(z)\eta(3z)/\eta(2z)\eta(6z)\}^6$  for  $\Gamma_0(6) +$  and its  $r$ -th roots where  $r \in \{2, 3, 6\}$ . However, we are not going into a detailed discussion on singular moduli of “roots” of Thompson series here, but will study them in a subsequent paper.

Previously, several authors (Fricke [13,14], Weber [29], Schertz [24], Birch [2, 3], Cohn [7], and Cox [9], among others) considered singular moduli problem for a rather limited class of modular functions such as  $j, \gamma_2, \gamma_3$  and for the Weber functions  $f, f_1$  and  $f_2$ . The methods used were rather ad hoc and non-uniform.

In this paper, we have considered singular moduli problem for a large class of new modular functions (Thompson series arising from the Monstrous Moonshine) in a unified manner.

## Acknowledgments

During the course of this work, N. Yui was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Royal Society of London, as well as Fellowships at Newnham College, the Department of Pure Mathematics and Mathematical Statistics (DPMMS), and the Newton Institute, University of Cambridge.

I. Chen held NSERC Summer Research Awards at Queen’s University for the summer of 1991 and 1992, under the supervision of N. Yui, and a NSF Summer Research Award at Rensselaer Polytechnic Institute in the summer of 1991, under the supervision of E. Kalfoten.

We thank J. G. Thompson for his interest and encouragement during the preparation of this paper. We thank also B. Birch, R. Borcherds, K. Harada and J. McKay for many helpful discussions. We are especially indebted to S. Norton for making available to us his

computer programs of Hauptmoduln of genus zero and for his many helpful discussions and comments.

## 1. Hauptmoduln

The full modular group  $PSL_2(\mathbb{Z})$  is the most distinguished genus zero subgroup of  $PSL_2(\mathbb{R})$ , and is denoted by  $\Gamma$ .  $\Gamma$  is a group generated by two elements  $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,

and  $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  with relations  $S^2 = (TS)^3 = 1$ .

Thompson [28] has shown that there are only finite number of conjugacy classes of genus zero congruence subgroups of  $\Gamma$  which are commensurable with  $\Gamma$ .

In this section, we will be concerned with genus zero subgroups  $G$  of  $PSL_2(\mathbb{R})$  of the special form, and Hauptmoduln for  $G$ . We denote by  $\mathfrak{M}_0(G)$  the complex vector space consisting of all Hauptmoduln for  $G$ .

**(1.1) Hauptmodul for  $\Gamma$ .** The most classical example of Hauptmoduln is the elliptic modular  $j$ -function for  $G = \Gamma$ . It is a transcendental function defined as follows:

$$j(z) = 12^3 \frac{E_2(z)^3}{E_2^3(z) - 27E_3^2(z)} \quad \text{for } z \in \mathfrak{H}$$

where

$$E_k(z) := \sum_{(m,n) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(mz+n)^{2k}}$$

is the Eisenstein series of weight  $2k$  ( $k \geq 1$ ).  $j$  is a modular function for  $\Gamma$ . It has simple pole at  $z = \infty$ , and it has a  $q$ -expansion of the form:

$$j(z) = \frac{(1 + 240 \sum_{n>0} \sigma_3(n)q^n)^3}{q \prod_{n>0} (1 - q^n)^{24}} \quad \text{where } \sigma_3(n) = \sum_{\substack{d|n \\ d>0}} d^3.$$

Expanding it out, we obtain the well known series for  $j$  (and for  $J$ ):

$$\begin{aligned} J(z) &= j(z) - 744 = q^{-1} + 196884q + 21493760q^2 + \dots \\ &= q^{-1} + \sum_{n \geq 1} c_j(n)q^n \quad \text{with } c_j(n) \in \mathbb{Z}. \end{aligned}$$

The space  $\mathfrak{M}_0(\Gamma)$  is of dimension 1 and generated by  $j$ . Furthermore, any holomorphic modular function for  $\Gamma$  is a polynomial of  $j$  over  $\mathbb{Z}$ .

**(1.2) Genus zero involutory subgroups of the normalizer of  $\Gamma_0(N)$ .** (For details confer Conway and Norton [8], p. 311.) We now introduce a class of subgroups of the normalizer of  $\Gamma_0(N)$  in  $PSL_2(\mathbb{R})$ , with the purpose of describing relevant genus zero subgroups of  $PSL_2(\mathbb{R})$ .

Let  $h$  be the largest positive divisor of 24 for which  $h^2|N$  and put  $n = N/h$ . Let  $e$  be a Hall divisor of  $n/h$ , that is,  $e$  is a positive divisor of  $n/h$  for which  $(e, n/h) = 1$ .

remain = 68.1157pt  
pagetotal=463.8843pt  
pagegoal=540.0pt

We denote by  $\left\{ \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right\}_e$  a matrix of the form

$$\begin{pmatrix} ae & b/h \\ cn & de \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Q})^+ \quad \text{with determinant } e.$$

Then the normalizer of  $\Gamma_0(N)$  in  $PSL_2(\mathbb{R})$  is

$$N_{PSL_2(\mathbb{R})}(\Gamma_0(N)) := \left\{ \left\{ \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right\}_e \mid a, b, c, d, e \in \mathbb{Z} \text{ and } e > 0 \text{ a Hall divisor of } n/h \right\}.$$

With this description of the normalizer, we can now describe certain involutory subgroups of the normalizer. For any positive divisor  $h$  (not necessarily the largest) of 24 satisfying the above properties, we define the following subgroup of  $N_{PSL_2(\mathbb{R})}(\Gamma_0(N))$ :

$$\Gamma_0(n|h) = \left\{ \left\{ \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right\}_1 \mid a, b, c, d \in \mathbb{Z} \right\}$$

An *Atkin–Lehner involution* of  $\Gamma_0(n|h)$  is a matrix of the form

$$\left\{ \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right\}_e$$

where  $a, b, c, d, e \in \mathbb{Z}$  and  $e > 0$  is a Hall divisor of  $n/h$ . Such an element normalizes  $\Gamma_0(n|h)$ , and the normalizer of  $\Gamma_0(N)$  can also be obtained by adjoining to  $\Gamma_0(n|h)$  all its Atkin–Lehner involutions. If we let  $W_{e,h}$  denote the set of all such matrices with a fixed  $e$ , then  $W_{e,h}$  forms a  $\Gamma_0(n|h)$  coset.

In particular, if  $h = 1$ , we have that  $\Gamma_0(n|h) = \Gamma_0(N)$ . The set  $W_{e,1}$  of all Atkin–Lehner involutions with fixed  $e$  shall be denoted simply by  $W_e$ . These sets are  $\Gamma_0(N)$  cosets and satisfy the multiplication rule:

$$(1.2.1) \quad W_e W_f \equiv W_f W_e \equiv W_k \pmod{\Gamma_0(N)} \quad \text{where } k := \frac{e}{(e,f)} \cdot \frac{f}{(e,f)}.$$

(Notice that  $k$  is a Hall divisor of  $N$  if  $e$  and  $f$  are Hall divisors of  $N$ .)

The class of subgroups in question are then the groups  $\Gamma_0(n|h) + e, f, \dots$ , where  $e, f, \dots$  are Atkin–Lehner involutions of  $\Gamma_0(n|h)$ . We shall adopt the convention that  $\Gamma_0(n|h) +$  is the group obtained by adjoining to  $\Gamma_0(n|h)$  all its Atkin–Lehner involutions.

For a specific example, take  $N$  to be a prime. In this case,  $h = 1$  and the only non-trivial Atkin–Lehner involutions of  $\Gamma_0(N)$  lie in the coset of the Fricke involution,

$$w_N = \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$$

which (as a linear fractional transformation) sends  $z \in \mathfrak{H}$  to  $-1/Nz$ . The group  $\Gamma_0(N) +$  is thus the full normalizer of  $\Gamma_0(N)$  in  $PSL_2(\mathbb{R})$ .

**(1.2.2) Theorem.** (Fricke [13,14]; Ogg [23])

- (1)  $\Gamma_0(N)$  is a genus zero subgroup of  $\Gamma$  exactly for  $N = 1, 2, \dots, 10, 12, 13, 16, 18, 25$ . ■
- (2) If  $N$  is prime,  $\Gamma_0(N) +$  is of genus zero exactly for 15 values of  $N$  in the set  $\mathfrak{S}$  defined in the Introduction.

(Incidentally, the set  $\mathfrak{S}$  is also the set of primes  $p$  for which supersingular elliptic curves  $E$  in characteristic  $p > 0$  have the absolute  $j$ -invariants in the prime field  $\mathbb{F}_p$ .)

**(1.3) The Monster  $\mathbb{M}$ .** Let  $\mathbb{M}$  denote the Monster, the largest of the finite sporadic simple groups. Its order,  $\#\mathbb{M}$  is about  $8 \times 10^{53}$ , but is highly factorizable. In fact, the primes dividing  $\#\mathbb{M}$  are exactly those in the set  $\mathfrak{S}$  (cf. Introduction). The smallest non-trivial representation of the Monster is of degree 196883. McKay first noticed that the coefficient of  $q$  in the  $q$ -expansion of  $J(z)$  is exactly 1 more than this number, and Thompson found that the next few coefficients of  $J(z)$  were also linear combinations of the character degrees of  $\mathbb{M}$ . Based on these findings, Thompson conjectured that the Monster  $\mathbb{M}$  acts on a naturally defined infinite dimensional graded vector space

$$V = V_{-1} + \sum_{n \geq 1} V_n$$

where  $\dim V_{-1} = 1$ , and for each  $n \geq 1$ ,  $V_n$  is a  $\mathbb{M}$ -module of dimension equal to  $c_j(n)$ , the coefficient of  $q^n$  in the  $q$ -expansion of  $J(z) = j(z) - 744$ . Such a vector space  $V$  was constructed by Frenkel, Lepowsky and Meurman [12].

Noticing that the function  $J(z)$  corresponds to the identity  $1_{\mathbb{M}}$  of  $\mathbb{M}$ , Thompson further proposed that if one replaces  $1_{\mathbb{M}}$  and the coefficients  $c_j(n)$ , by an arbitrary element  $g \in \mathbb{M}$  and the corresponding characters of  $\mathbb{M}$ , one should get a formal power series having similar properties to  $J(z)$ . The exact conjecture was formulated by Conway and Norton [8], based on experimental data.

**(1.4) Monstrous Moonshine.** (Conway and Norton [8]) *For any element  $g \in \mathbb{M}$ , let  $\text{Tr}(g|V_n)$  be the trace of  $g$  in  $V_n$  for each  $n$ . Define the Thompson series of  $g$  by*

$$T_g(z) = q^{-1} + \sum_{n \geq 1} \text{Tr}(g|V_n) q^n \quad \text{where } q = e^{2\pi iz}.$$

*Then we have the following assertions:*

- (1)  $\text{Tr}(g|V_{-1}) = 1$  and  $\text{Tr}(g|V_n) \in \mathbb{Z}$  for any  $n \geq 1$ . (In fact, this is the character value of the  $n$ -th head representation of  $\mathbb{M}$ .)
- (2)  $T_g$  is a canonical Hauptmodul for a certain genus zero subgroup  $G$  having level  $N$  divisible by the order  $o(g)$  of  $g$ . This subgroup lies between  $\Gamma_0(N)$  and its normalizer in  $PSL_2(\mathbb{R})$ .

**(1.4.1) A description of the genus zero subgroups  $G$ .** Conway and Norton [8] gave more a specific description for this genus zero subgroup  $G$ . First we need some definitions: The *fixing group* of  $T_g$  is the subgroup of  $PSL_2(\mathbb{R})$  that fixes  $T_g$ , and the *eigengroup* of  $T_g$  is the subgroup of  $PSL_2(\mathbb{R})$  which multiplies  $T_g$  by a  $h$ -th root of unity where  $h$  is a certain fixed positive integer. If we put  $N = h \cdot o(g)$ , then  $h|24$ ,  $h^2|N$  and the eigengroup of  $T_g$  is equal to  $\Gamma_0(o(g)|h) + e, f, \dots$  for some Atkin-Lehner involutions  $e, f, \dots$  of  $\Gamma_0(o(g)|h)$ . The genus zero subgroup  $G$  that we are after is the fixing group of  $T_g$ , and it is a subgroup of index  $h$  in the eigengroup.

We call a Thompson series  $T_g$  *fundamental* if  $h = 1$ . In this case,  $N = o(g)$ , and the fixing group which coincides with the eigengroup has the form  $G = \cup_{e \in \mathcal{S}} W_e$  where  $\mathcal{S}$  is a subset of the Hall divisors of  $N = o(g)$  closed under the multiplication rule of

remain = 128.2109pt  
 pagetotal=403.7891pt  
 pagegoal=540.0pt

(1.2.1). In particular,  $G$  is equal to the group  $\Gamma_0(N)$  extended by some Atkin–Lehner involutions of  $\Gamma_0(N)$ . (If  $N$  is prime in the set  $\mathfrak{S}$ , then  $G = \Gamma_0(N) + = \Gamma_0(N) + w_N$ .)

(When  $h > 1$ , Conway and Norton [8] gave a description of the fixing group  $G$  for  $T_g$ . But we are not discussing these non-fundamental Thompson series in this paper.)

The Monstrous Moonshine (conjecture) has recently been proved by Borcherds using generalized Kac–Moody algebras and the no-ghost theorem from string theory.

**(1.4.2) Theorem.** (Borcherds [5]) *Monstrous Moonshine holds true.*

**Remarks.** (1) If  $g$  has prime order  $N \in \mathfrak{S}$ , and if  $T_g$  is a canonical Hauptmodul for  $\Gamma_0(N) +$ , then  $\text{Tr}(g|V_n)$  is always a positive integer for every  $n \geq 1$ . There is a formula due to Reidemeister which describes the coefficient of  $q^n$  in  $T_g$ , as a sum of the dominant term and the rest.  $T_g$  has a simple pole at  $z = \infty$ . The Fricke involution  $w_N$  interchanges two cusps  $0$  and  $\infty$  of  $\Gamma_0(N) +$ . So  $T_g$  has also a simple pole at  $z = 0$ . In this case, Borcherds shows that the sign of the coefficient of  $q^n$  should be the same as the sign of the dominant term, which is always positive when  $n$  is sufficiently large (in fact  $n \geq 1$  in this situation). However, if  $T_g$  is a canonical Hauptmodul for  $\Gamma_0(N)$ , the coefficients of its  $q$ -expansion are not necessarily positive integers. Borcherds has a conjectural interpretation for these negative coefficients in terms of dimensions of supervector spaces associated to  $V_n$  for  $n \geq 1$ .

(2) Norton suggests that the coefficients of  $T_g(-1/z)$  are always non-negative and correspond to character degrees of a cover of  $C_{\mathbb{M}}(g)$  (=the centralizer of  $g$  in  $\mathbb{M}$ ). Furthermore, the corresponding character values give rise to modular functions  $T_{g,h}(z)$  associated to a commuting pair  $(g, h) \in \mathbb{M} \times \mathbb{M}$ , which are either (scaled) Hauptmoduln or identically zero, and the action of  $\Gamma$  on the pair  $(g, h)$  and on  $z$  is equivalent up to multiplication by a root of unity. For details, see *Generalized Moonshine* by Norton [22].

**(1.5) Description of Hauptmoduln.** Let  $G$  denote a genus zero subgroup of  $PSL_2(\mathbb{R})$  obtained by adjoining to  $\Gamma_0(N)$  a certain number of Atkin–Lehner involutions. Let  $T_g$  be the Thompson series for  $g \in \mathbb{M}$ . Then the validity of Monstrous Moonshine implies, in particular, that  $T_g$  has a  $q$ -expansion of the form

$$q^{-1} + c_1q + c_2q^2 + \cdots, \quad c_n \in \mathbb{Z} \quad \text{for all } n \geq 1$$

where  $q = e^{2\pi iz}$ . We may simply write  $[1, 0, c_1, c_2, \dots]$  for this power series. The constant terms are normalized to 0 as they are not characters (or, even necessarily integers).

**(1.5.1) Examples.** Many (but not all) of the canonical Hauptmoduln corresponding to Thompson series can be expressed as products of eta-functions with constant terms removed. First we recall the definition of the eta-function. The eta-function  $\eta$  is defined by the  $q$ -expansion

$$\eta(q) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n) \quad \text{where } q = e^{2\pi iz}, \quad z \in \mathfrak{H}.$$

It satisfies the transformation formulae :

$$\eta(z + 1) = e^{\frac{2\pi i}{24}} \eta(z) \quad ; \quad \eta\left(-\frac{1}{z}\right) = \sqrt{-iz} \eta(z).$$

Here are some examples. All Thompson series in these examples are fundamental, i.e.,  $h = 1$ .

(a) Let  $G = \Gamma_0(N)$  where  $N$  is a positive integer such that  $N - 1 \mid 24$ . Then

$$f(z) = \left\{ \frac{\eta(q)}{\eta(q^N)} \right\}^{24/m} \quad \text{where } m = (N - 1, 24)$$

gives rise to a Hauptmodul for  $\Gamma_0(N)$ . (cf. Fricke [13, 14], Gross [15] and Shimura [25].)

(b) Let  $G = \Gamma_0(13)_+$ . Then

$$f(z) = \frac{\eta(q)^2}{\eta(q^{13})^2} + 13 \frac{\eta(q^{13})^2}{\eta(q)^2}$$

is a Hauptmodul for  $\Gamma_0(13)_+$ .  $f - 12$  has a  $q$ -expansion of the form

$$[1, 0, 12, 28, 66, 132, 258, 468, 843, 1428, 2406, 3900, 6253, 9780, 15144, \dots].$$

This is the Thompson series 13A in Conway and Norton [8].

(c) Let  $G = \Gamma_0(50) + 50$ . Then  $\mathfrak{H}^*/\Gamma_0(50)_+$  is of genus zero. Construction of a Hauptmodul for this group was illustrated by Birch [3]. Let

$$f(z) = \frac{\eta(q^2)\eta(q^{25})}{\eta(q)\eta^2(q^{50})} = q^{-1} \prod_{n=1}^{\infty} \frac{1+q^n}{1+q^{25n}}.$$

Then the first 24 coefficients of its  $q$ -expansion are

$$[1, 1, 1, 2, 2, 3, 4, 5, 6, 8, 10, 12, 15, 18, 22, 27, 32, 38, 46, 54, 64, 76, 89, 104, 122, \dots].$$

Note that  $f - 1$  corresponds to the Thompson series 50a in the table given in Ford, McKay and Norton [11].

(d) Let  $G = \Gamma_0(71)_+$ . Then the Thompson series (71A) is given by

$$T_g(z) = \frac{\theta(4, 2, 18) - \theta(6, 2, 12)}{2\eta(q)\eta(q^{71})} - 1 \quad (\text{cf. Conway and Norton [8]}).$$

Here  $\theta$  is the theta function defined by

$$\theta(a, b, c) = \sum q^{(ax^2 + bxy + cy^2)/2}$$

where the sum runs over all pairs  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ . The constant term is  $1/3$ , and the first 24 terms of the  $q$ -expansion are

$$[1, 0, 1, 1, 1, 1, 2, 2, 3, 3, 4, 4, 6, 6, 7, 8, 10, 11, 13, 14, 17, 19, 22, 24, 29, \dots].$$

(e) Let  $G = \Gamma_0(6)+2$  (resp.  $\Gamma_0(6)+6$ ), and we consider the fundamental Thompson series  $T_{6+2}$  (resp.  $T_{6+6}$ ). It is expressed as a rational function of eta-functions:

$$T_{6+2}(z) = \left\{ \frac{\eta(q)\eta(q^2)}{\eta(q^3)\eta(q^6)} \right\}^4 + 4 \quad (\text{resp. } T_{6+6}(z) = \left\{ \frac{\eta(q^2)\eta(q^3)}{\eta(q)\eta(q^6)} \right\}^{12} - 12).$$

The first 10 coefficients of the  $q$ -expansion are

$$T_{6+2}(z) = [1, 0, -2, 28, -27, -52, 136, -108, -162, 620, -486, -760, \dots]$$

(resp.  $T_{6+6}(z) =$   
 $= [1, 0, 78, 364, 1365, 4380, 12520, 32772, 80094, 185276, 409578, 871272, \dots].$ )

**(1.5.2) Modular relations.** There is a relation called *modular relation* between any Hauptmodul  $f$  associated to a genus zero subgroup  $G \subset \Gamma$  and  $j$ . Such a relation describes  $j$  as a rational function of  $f$  of degree equal to the index  $[\Gamma : G]$ . It is possible to obtain such relations explicitly for the subgroups  $\Gamma_0(N)$  such that  $N - 1 \mid 24$ , i.e.,  $N = 2, 3, 4, 5, 7, 9, 13$  and  $25$ . Put  $m = (N - 1, 24)$ . We tabulate modular relations for these non-normalized Hauptmoduln  $f$  (cf. Table below). Under the remark, we list the corresponding Thompson series from Conway and Norton [8], for instance, in the first row,  $f + 24$  is the canonical Thompson series 2B.

$G$	Modular relation	Remark
$\Gamma_0(2)$	$j = \frac{(f+256)^3}{f^2}$	2B
$\Gamma_0(3)$	$j = \frac{(f+27)(f+243)^3}{f^3}$	3B
$\Gamma_0(4)$	$j = \frac{(f^2+256f+4096)^3}{(f+16)f^4}$	4C
$\Gamma_0(5)$	$j = \frac{(f^2+250f+3125)^3}{f^5}$	5B
$\Gamma_0(7)$	$j = \frac{(f^2+13f+49)(f^2+245f+2401)^3}{f^7}$	7B
$\Gamma_0(9)$	$j = \frac{(f+9)^3(f^3+243f^2+2187f+6561)^3}{(f^2+9f+27)f^9}$	9B
$\Gamma_0(13)$	$j = \frac{(f^2+5f+13)(f^4+247f^3+3380f^2+15379f+28561)^3}{f^{13}}$	13B
$\Gamma_0(25)$	$j = \frac{(f^{10}+250f^9+4375f^8+35000f^7+178125f^6+631250f^5+1640625f^4+3125000f^3+4296875f^2+3906250f+1953125)^3}{(f^4+5f^3+15f^2+25f+25)f^{25}}$	25b

**Remarks.** (1) In each modular relation in the table, the numerator is a monic integral polynomial which has an irreducible cubic factor over  $\mathbb{Z}$ . The presence of an irreducible factor to its cube power can be explained as follows: We know that the elliptic modular  $j$ -function has a zero of order 3 at  $\omega := \frac{-1+\sqrt{-3}}{2}$  in the standard fundamental domain for  $\mathfrak{H}/\Gamma$ . Now we determine the points in the fundamental domain for  $\mathfrak{H}/\Gamma_0(N)$  lying above the point  $\omega$ . First we note that no ramified points in  $\mathfrak{H}^*/\Gamma_0(N)$  over  $\omega$  are fixed by  $\Gamma_0(N)$ . Then the fact  $j$  has a triple zero at  $\omega$  implies that some of the points above  $\omega$  have ramification index 3. Evaluating  $f$  at these points, and using Galois theory, we obtain an integral irreducible polynomial to its cube power. (Integrality follows as singular values of  $f$  at these points are algebraic integers.) For instance, take  $N = 7$ . Then there are four points in  $\mathfrak{H}/\Gamma_0(7)$  above  $\omega$ : They are  $\omega(3)$ ;  $\frac{-1}{\omega+2}(3)$ ;  $\frac{-1}{\omega+3}(1)$  and  $\frac{-1}{\omega+5}(1)$ . (Here the number in parentheses denotes the ramification index of the preceding point.) Evaluate  $f$  at these points and form

$$(f - f(\omega))^3 (f - f(\frac{-1}{\omega+2}))^3 (f - f(\frac{-1}{\omega+3})) (f - f(\frac{-1}{\omega+5})).$$

Then this gives the numerator of the modular relation for  $\Gamma_0(7)$ .

(2) A similar argument as above at the cusp  $\infty$  gives information about the denominator of the modular relation.

For the genus zero subgroups  $\Gamma_0(N)_+$ , there is a “quadratic” modular relation between a Hauptmodul for  $\Gamma_0(N)_+$  and  $j$ . This follows from the following more general fact.

**(1.5.3) Remark.** Let  $G$  be a genus zero congruence subgroup of level  $N$  with Hauptmodul  $g$ . Then the minimal polynomial of  $j$  over  $\mathfrak{M}_0(G)$  has the form

$$A_0(g)j^t + A_1(g)j^{t-1} + \cdots + A_t(g) = 0$$

where  $t = [G : \Gamma_0(N)]$ , and  $A_i$  is a polynomial of  $g$  for each  $i$ .

We apply this to  $G = \Gamma_0(N)_+$  where  $N$  is a positive integer such that  $N - 1 \mid 24$ . Then  $[\Gamma_0(N)_+ : \Gamma_0(N)] = 2$ . Let  $f$  and  $f_+$  denote, respectively, Hauptmoduln corresponding to  $\Gamma_0(N)$  and  $\Gamma_0(N)_+$ . Then for each  $N$ , there is a “quadratic” modular relation between  $f_+$  and  $j$ .

Examples of modular relations for  $\Gamma_0(N)_+$  with  $N - 1 \mid 24$  are tabulated in Appendix 1.

## 2. Modular equations

The algebraic integrality of the elliptic modular  $j$  function at imaginary quadratic arguments and Kronecker’s Jugendtraum were classically proved by showing the existence of a modular equation  $\Phi_m(X, Y)$  giving the relation between  $j$  and  $j \circ m$ , where  $m$  is a positive integer and  $j \circ m(z) = j(mz)$ . This polynomial is symmetric, absolutely irreducible, and has integer coefficients. Furthermore, the modular equation  $\Phi_m(X, Y) = 0$  is an affine singular model of the modular curve  $X_0(m)$ , that is, there is a morphism over  $\mathbb{Q}$ :

$$X_0(m) \longrightarrow \mathbb{P}^1(\mathbb{C}) \times \mathbb{P}^1(\mathbb{C}) : z \mapsto (j(z), j(mz))$$

whose image is the correspondence defined by the locus of the modular polynomial. The affine curve  $\Phi_m(X, Y) = 0$  is a singular curve having only ordinary double points as singularities. (cf. Gross [15].)

The purpose of this section is to explicitly construct modular equations for *fundamental* Thompson series in a manner which generalizes the classical derivation for  $j$ . Although it is clear that there is some relation between  $T_g$  and  $T_g \circ m$  (the composition of  $T_g$  and the multiplication by  $m$  map), this explicit construction will allow us to deduce many important properties. For instance,  $\Phi_m(X, Y)$  lies in  $\mathbb{Z}[X, Y]$  and it is a symmetric polynomial whose diagonalization  $\Phi(X, X)$  has leading coefficient  $\pm 1$  if  $m$  is non-square.

Let  $m$  be a positive integer and define the set

$$\Omega(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad = m, a > 0, (a, b, d) = 1, 0 \leq b < d \right\}$$

whose cardinality we shall denote by  $\psi(m)$ .

Recall from the construction of the modular equation for  $j$  (Yui [31]; cf. Lang [16], p. 52) that the sets  $\Gamma\omega$ , where  $\omega \in \Omega(m)$ , are disjoint. In the classical formulation of this fact, one considers the group  $\Gamma$  acting on the set

$$\Delta_m^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}; (a, b, c, d) = 1; ad - bc = m \right\}$$

and one shows that  $\Omega(m)$  contains a complete set of representatives for the  $\Gamma \backslash \Delta_m^*$ .

The standard convention for describing Atkin-Lehner involutions involves working in  $PGL_2(\mathbb{Q})^+$ . Here, an Atkin-Lehner involution has the form

$$\begin{pmatrix} ae & b \\ cN & de \end{pmatrix}$$

where  $e \parallel N$ . To generalize the classical derivation of modular equations for Thompson series, we will regard Atkin-Lehner involutions as matrices in  $PSL_2(\mathbb{R})$ , that is to say, an Atkin-Lehner involution will have the form

$$\begin{pmatrix} a\sqrt{e} & b/\sqrt{e} \\ cN/\sqrt{e} & d\sqrt{e} \end{pmatrix}$$

where  $e \parallel N$ . The main reason for normalizing Atkin-Lehner involutions to determinant 1 is to avoid having to consider equality of matrices up to scalar equivalence. The second difference is that we will avoid considering group actions on  $\Delta_m^*$ . We will simply view  $G\omega$  as a set of matrices in  $PGL(\mathbb{R})^+$  with determinant  $m$ .

From the discussion in Section (1.2), we know that the fixing group  $G$  of a fundamental Thompson series  $T_g$  has a special form

$$G = \bigcup_{e \in \mathfrak{S}} W_e$$

where  $W_e$  is the set of all Atkin-Lehner involutions with a fixed Hall divisor  $e$  of  $N$ , and  $\mathfrak{S}$  is a subset of the Hall divisors of  $N$  closed under the multiplication rule given in (1.2.1).

**(2.1) Lemma.** *Let  $G$  be the fixing group of a fundamental Thompson series  $T_g$  of level  $N = o(g)$ . If  $(m, N) = 1$ , then the sets  $G\omega$  for  $\omega \in \Omega(m)$  are all disjoint.*

*Proof.* Suppose  $G\omega_1 \cap G\omega_2 \neq \emptyset$  where

$$\omega_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix} \in \Omega(m).$$

Then  $\omega_1 = \pi\omega_2$  for some Atkin-Lehner involution  $\pi \in W_e$ , where  $e \in \mathfrak{S}$ . So we have  $\omega_1\omega_2^{-1} = \pi$ . In terms of matrices, this equation is read :

$$\frac{1}{m} \begin{pmatrix} a_1d_2 & a_2b_1 - a_1b_2 \\ 0 & a_2d_1 \end{pmatrix} = \begin{pmatrix} w\sqrt{e} & x/\sqrt{e} \\ yN/\sqrt{e} & z\sqrt{e} \end{pmatrix}.$$

By equating entries on both sides, we see that  $y = 0$ . Since the determinant of both matrices is 1, we have  $wze = 1$  and therefore  $e = 1$  and  $wz = 1$ . Thus,  $a_1d_2 = a_2d_1 =$

$m$  and hence  $a_1 = a_2$ ,  $d_1 = d_2$ . It then follows that  $a_2b_1 - a_1b_2 = a_1(b_1 - b_2)$ . By equating entries again, we see that  $a_1(b_1 - b_2)/m = x \in \mathbb{Z}$ . However,  $m$  is prime to  $a_1$  so this implies that  $b_1 \equiv b_2 \pmod{m}$  and therefore  $b_1 = b_2$  by definition of  $\Omega(m)$ .  $\square$

Our next task is to show that multiplication on the right by a element in  $G$  induces a permutation of the sets  $G\omega$  where  $\omega \in \Omega(m)$ . For this, we first state the following elementary fact. In what follows, the notation and the hypothesis of Lemma (2.1) remain in force.

**(2.2) Lemma.** *Let  $\rho = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in M_2(\mathbb{Z})$  be a primitive matrix with determinant  $m$ . Suppose that  $(r, N) = 1$  and  $t$  is divisible by  $N$ . Then there exists a  $\gamma \in \Gamma_0(N)$  such that  $\rho = \gamma\omega$  for some  $\omega \in \Omega(m)$ .*

*Proof.* The numbers  $-t/(r, t)$  and  $r/(r, t)$  are relatively prime. Choose  $x, y$  such that  $xr/(r, t) + yt/(r, t) = 1$  and form the matrix

$$\gamma = \begin{pmatrix} x & y \\ -t/(r, t) & r/(r, t) \end{pmatrix}.$$

By the construction,  $\gamma \in \Gamma_0(N)$  and the matrix  $\gamma\rho$  is both upper triangular and primitive. Multiplying  $\gamma\rho$  on the left by a matrix of the form  $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$  we obtain a matrix in  $\Omega(m)$  as desired.  $\square$

**(2.3) Lemma.** *Multiplication on the right by an element  $\pi \in G$  induces a permutation of the sets  $G\omega$  where  $\omega \in \Omega(m)$ .*

*Proof.* We first show that if  $\pi \in G$  and  $\omega \in \Omega(m)$  then  $G\omega\pi = G\omega'$  for some  $\omega' \in \Omega(m)$ . It suffices to show that  $\omega\pi = \gamma\omega'$  for some  $\gamma \in \Gamma_0(N)$  and  $\omega' \in \Omega(m)$ . This occurs if and only if  $\pi^{-1}\omega\pi = \gamma\omega'$ . Write

$$\pi^{-1}\omega\pi = \begin{pmatrix} r & s \\ t & u \end{pmatrix}.$$

Expanding the product  $\pi^{-1}\omega\pi$  shows that  $r, s, t, u \in \mathbb{Z}$ ,  $r = zawe + zbyN - xdyN/e$  and  $t = -yNaw - y^2bN^2/e + dwyN$ .

A case by case analysis shows that  $r$  is relatively prime to  $N$ . Note also  $t$  is divisible by  $N$ . Thus  $\pi^{-1}\omega\pi$  satisfies the hypotheses of Lemma (2.2). Hence there exists a  $\gamma \in \Gamma_0(N)$  such that  $\pi^{-1}\omega\pi = \gamma\omega'$  for some  $\omega' \in \Omega(m)$ .

By disjointness of the sets  $G\omega$ , we see that  $G\omega\pi = G\omega'\pi$  implies  $\omega = \omega'$ . Therefore, multiplication on the right by a matrix  $\pi$  in  $G$  permutes the sets  $G\omega$ .  $\square$

We are ready to define the modular equation for a fundamental Thompson series  $T_g$  and prove some of its elementary properties.

**(2.4) Definition.** Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . For  $m$  prime to  $N$ , we define the *modular equation* for  $T_g$  by

$$\Phi_m^T(X) = \prod_{\omega \in \Omega(m)} (X - T_g \circ \omega).$$

Here  $T_g \circ \omega$  means the composition of  $T_g$  and  $\omega$ .

**Remark.** If  $g = 1_M$ , this just yields the classical modular equation for  $j$ .

Now we look into properties of the modular equations for Thompson series. They share similar properties enjoyed by the classical modular equation.

**(2.5) Proposition.**  $\Phi_m^T(X) \in \mathbb{Z}[X, T_g]$ .

The proof of Proposition (2.5) will be given by the following successive lemmas.

**(2.5.1) Lemma.** *A Thompson series  $T_g$  is analytic everywhere on  $\mathfrak{H}^*/G$  with the exception of a simple pole at the cusp  $z = \infty$ .*

*Proof.* This follows from  $T_g$  being a Hauptmodul. □

The coefficients of  $\Phi_m^T(X)$ , which we shall denote by  $E_i$  for  $0 \leq i < \psi(m)$ , are elementary symmetric polynomials in the functions  $T_g \circ \omega$ . By Lemma (2.3), multiplication on the right by an element in  $G$  induces a permutation of the sets  $G\omega$ . Hence, each  $E_i$  is invariant with respect to  $G$  and therefore each  $E_i$  is a modular function on  $\mathfrak{H}^*/G$ .

The Riemann surface  $\mathfrak{H}^*/G$  may have cusps other than  $\infty$ . In order to prove that each  $E_i$  is a polynomial in  $T_g$ , we will need to show that  $E_i$  is holomorphic at cusps different from  $\infty$ . To do this, let us first determine the  $G$  orbit of the cusp  $\infty$ .

**(2.5.2) Lemma.** *Let  $W_e$  be the set of Atkin-Lehner involutions of  $\Gamma_0(N)$  with a fixed Hall divisor  $e$  of  $N$ . Then the images of  $\infty$  under  $W_e$  are given by*

$$S_e := \left\{ \frac{w}{yN/e} \mid w, y \in \mathbb{Z} \text{ and } (we, yN/e) = 1 \right\}$$

*Proof.* Let  $\pi \in W_e$ . Now  $\pi(\infty) = \frac{w}{yN/e}$  and  $(we, yN/e) = 1$  since the determinant of  $\pi$  is  $e$ . Hence  $\pi(\infty) \in S_e$ . Conversely, let  $\frac{w}{yN/e}$  be an element of  $S_e$ . Choose  $z$  such that  $wz \equiv 1 \pmod{yN/e}$  and  $z \equiv 0 \pmod{e}$ . Choose  $x \in \mathbb{Z}$  satisfying  $wze - xyN/e = 1$ , and form the matrix

$$\pi = \begin{pmatrix} we & x \\ yN & ze \end{pmatrix}.$$

By construction,  $\pi$  lies in  $W_e$  and  $\pi(\infty) = \frac{w}{yN/e}$ . □

Let  $G_\infty$  denote the  $G$ -orbit of the cusp  $\infty$ . From Lemma (2.5.2) we see that  $G_\infty = \cup_{e \in \mathcal{S}} S_e$ .

**(2.5.3) Lemma.** *If  $\omega = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Omega(m)$ , then  $\omega^{-1}(G_\infty) \subseteq G_\infty$ .*

*Proof.* By Lemma (2.5.2), a point  $u \in G_\infty$  has the form  $\frac{w}{yN/e}$  where  $(we, yN/e) = 1$  and  $e \in S$ . Now,  $\omega^{-1}u = \frac{dw - byN/e}{mayN/e}$ . Note that if  $p$  is a prime dividing  $(dw - byN/e, mayN/e)$ , then  $p$  cannot divide  $N/e$ . (For otherwise  $p$  would divide  $dw$  and hence  $w$ , contradicting the fact that  $(we, yN/e) = 1$ .) Hence  $\omega^{-1}u$  has the reduced form  $\frac{w'}{y'N/e}$  where  $(w', y'N/e) = 1$ . In addition,  $mayN/e$  is prime to  $e$  so that  $y'N/e$  is also prime to  $e$ . Therefore  $(e, y'N/e) = 1$  and  $\omega^{-1}u$  lies in the  $G_\infty$ .  $\square$

**(2.5.4) Completing proof of (2.5).** By Lemma (2.5.1), we see that  $T_g$  is analytic on  $\mathfrak{H}^* - G_\infty$ . Thus,  $T_g \circ \omega$  is analytic on  $\mathfrak{H}^* - \omega^{-1}(G_\infty)$  and each  $E_i$  is analytic on  $\mathfrak{H}^* - \cup_{\omega \in \Omega(m)} \omega^{-1}(G_\infty)$ . By Lemma (2.5.3),  $\omega^{-1}(G_\infty)$  lies in the  $G_\infty$  so that each  $E_i$  is analytic on  $\mathfrak{H}^*/G$  with the exception of the point  $\infty$ .

Consider the  $q$ -expansion of  $T_g \circ \omega$ ,  $\omega \in \Omega(m)$ . Write

$$T_g(z) = \sum_{i \geq -1} c_i q^i \quad \text{with } c_{-1} = 1, c_0 = 0 \text{ and } c_i \in \mathbb{Z} \text{ for } i \geq 1.$$

The  $q$ -expansion of  $T_g \circ \omega$  has the form

$$(T_g \circ \omega)(z) = T_g\left(\frac{az + b}{d}\right) = \sum_{i \geq -1} \zeta_d^{bi} c_i q^{ai/d}$$

where  $\zeta_d^x = e^{2\pi i x/d}$ . Let  $\zeta = e^{2\pi i/m}$  be the principal  $m$ -th root of unity. Then the  $q$ -coefficients of  $T_g \circ \omega$  lie in the cyclotomic field  $\mathbb{Q}(\zeta)$ . Moreover, we see that there exists a positive integer  $t_i$  such that  $\lim_{q \rightarrow 0} q^{t_i} E_i = 0$ . Hence the functions  $E_i$  are meromorphic at  $\infty$ .

Write  $E_i = \sum e_{ij} q^j$ . We can find a polynomial  $A_i(x)$  with coefficients in the ring  $\mathcal{R}_i := \mathbb{Z}[e_{ij}; \text{Tr}(g|V_n)]$  such that the  $q$ -expansion of  $E_i - A_i(T_g)$  has no negative powers of  $q$ . This implies that  $E_i - A_i(T_g)$  is holomorphic on all of  $\mathfrak{H}^*/G$  and hence is a constant, say,  $B_i \in \mathcal{R}_i$ . Therefore  $E_i = A_i(T_g) + B_i$  for some polynomial  $A_i$  with coefficients in  $\mathcal{R}_i$ .

Finally, we claim that  $A_i$  has integer coefficients and that  $B_i \in \mathbb{Z}$ . As in the classical case, (cf. Shimura [25], p. 109), an element of the Galois group  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  acts as a permutation on the set  $T_g \circ \omega$ . From this we may conclude the coefficients  $e_{ij}$  and  $B_i$  are in fact in  $\mathbb{Z}$ . Therefore for each  $i$ ,  $A_i$  and hence  $E_i$  are integral polynomials. This concludes the proof of Proposition (2.5).  $\square$

**Remark.** As  $T_g$  is a non-constant analytic function, we see that  $\Phi_m^T(X)$  can be regarded as a two variable polynomial by substituting  $Y$  for  $T_g$  which we denote by  $\Phi_m^T(X, Y)$ . Mahler [20] has considered the construction of modular equations for so-called formal  $S_p$ -series where  $p$  is a prime. In his context, Proposition (2.5) asserts if  $(m, N) = 1$ , then the functions  $T_g$  are  $S_m$ -series. Hence, when  $m$  is a prime not dividing  $N$ , many of his results can be applied toward fundamental Thompson series. In particular, we shall have occasion to use his explicit description of the modular equation for  $S_p$  series where  $p = 2, 3$  to obtain our first examples of modular equations for Thompson series (See Appendix A2).

The most important properties (for the later applications) of the modular equations for  $T_g$  are formulated in the following theorem.

**(2.6) Theorem.** *Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . Let  $m$  be a positive integer such that  $(m, N) = 1$ . Let  $\Phi_m^T(X, Y)$  be the modular equation for  $T_g$  of level  $N$ . Then  $\Phi_m^T(X, Y)$  satisfies the following properties:*

- (1)  $\Phi_m^T(X, T_g)$  (regarded as an element of  $\mathbb{C}(T_g)[X]$ ) is irreducible over  $\mathbb{C}(T_g)$ .
- (2)  $\Phi_m^T(X, X)$  has leading coefficient  $\pm 1$  if  $m$  is square-free.
- (3)  $\Phi_m^T(X, Y) = \Phi_m^T(Y, X)$ .
- (4) If  $m$  is a prime  $p$ , then  $\Phi_p^T$  satisfies a generalized Kronecker congruence:

$$\Phi_p^T(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p\mathbb{Z}[X, Y]}.$$

*Proof.* The proofs are essentially the same as for the classical modular equation with  $T_g$  in place of  $j$  (Cox [9], p.232).

(1) We need to show that  $G$  acts transitively on the sets  $G\omega$  by multiplication on the right. In fact, we shall show the stronger result that  $\Gamma_0(N)$  acts transitively on the sets  $\Gamma_0(N)\omega$ . Let  $\omega = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$  be an element of  $\Omega(m)$ . Let  $\alpha$  to be the product of the primes dividing  $d$  but neither  $a$  nor  $b$ . Form the following matrix  $\pi = \begin{pmatrix} \alpha & \beta \\ N & \delta \end{pmatrix}$  where  $\beta$  and  $\delta$  are chosen so that  $\det(\pi) = \alpha\delta - N\beta = 1$ . Then it is easy to see that  $(a\alpha + bN, dN) = 1$ . Now

$$\omega\pi = \begin{pmatrix} a\alpha + bN & a\beta + b\delta \\ dN & d\delta \end{pmatrix}.$$

However, since  $(a\alpha + bN, dN) = 1$ , we have by Lemma (2.2)  $\omega\pi = \gamma \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$  for some  $\gamma \in \Gamma_0(N)$ . Hence every element in  $\Omega(m)$  can be sent to the set

$$\Gamma_0(N) \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$$

by multiplication on the right with an element of  $\Gamma_0(N)$ .

(3) The same as the classical case; Mahler [20](p. 71) has shown in the case that  $m$  is prime, (3) can be proved using only the fact that  $T_g$  is a  $S_m$ -series.

(2) and (4) Also the same as the classical proofs (cf. Lang [19]). □

**Remarks.** (a) Though the existence of a modular relation between  $T_g$  and  $T_g \circ m$  is clear, constructing modular equations explicitly in this way allows us to show the several important properties listed in Theorem (2.6). These properties, especially (2), will be used in the next section to show the algebraic integrality of singular moduli of Thompson series.

(b) Even when  $m$  is not relatively prime to  $N$ , an explicit construction of the modular equation for  $T_g$  may be also possible. In this case, the construction may involve generalized Hecke operators (cf. Ferenbaugh [10] and Koike [17]).

(c) As in the classical case, the modular equation of a Thompson series  $T_g$  defines an affine singular curve  $\Phi_m^T(X, Y) = 0$  over  $\mathbb{Z}$ . Natural geometric questions one may ask are:

- (1) Does it have only ordinary multiple points as singularities?
- (2) What are the possible relations to the classical modular equation?

### 3. Class fields

In this section, we shall generalize the theory of complex multiplication for the singular values of the elliptic modular function  $j$  to the singular values of fundamental Thompson series  $T_g$ . Explicit Shimura's reciprocity law will be the main tool in this investigation.

**(3.1) Lemma.** *For any  $g \in \mathbb{M}$ ,  $T_g(z)$  is a transcendental function for any algebraic number  $z \in \mathfrak{H}$  not belonging to an imaginary quadratic field.*

*Proof.* We know by Siegel [26] that  $j$  is transcendental for any algebraic number  $z \in \mathfrak{H}$  which is not imaginary quadratic. As  $j(z)$  is an algebraic function of  $T_g(z)$ , this implies  $T_g(z)$  cannot be algebraic for  $z \in \mathfrak{H}$  not imaginary quadratic.  $\square$

We can show, as an application of the existence of the "modular equation" for Thompson series, that Thompson series  $T_g$  evaluated at imaginary quadratic arguments are algebraic integers.

First we state the following well known but rather useful fact (cf. Cox [9], p. 188).

**(3.2) Lemma.** *Let  $Q = [a, b, c]$  be a primitive positive definite quadratic form. Then  $Q(x, y) = ax^2 + bxy + cy^2$  with  $x, y \in \mathbb{Z}$  represents infinitely many primes.*

**(3.3) Proposition.** *Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . Let  $K$  be an imaginary quadratic field of discriminant  $d_K$ . Let  $\tau_0 \in \mathcal{O}_K$  be a root of a quadratic equation  $z^2 + \mathbf{T}(\tau_0)z + \mathbf{N}(\tau_0) = 0$  with  $\mathbf{T}(\tau_0)^2 - 4\mathbf{N}(\tau_0) = d_K$ . Then  $T_g(\tau_0)$  is an algebraic integer.*

(Here  $\mathbf{T}$  and  $\mathbf{N}$  denote, respectively, the trace and the norm from  $K$  to  $\mathbb{Q}$ .)

*Proof.* Let  $\tau_0 \in \mathcal{O}_K$ , and consider the quadratic form

$$Q = [\mathbf{N}(\tau_0)N^2, \mathbf{T}(\tau_0)N, 1]$$

of discriminant  $N^2(\mathbf{T}(\tau_0)^2 - 4\mathbf{N}(\tau_0)) = N^2d_K$ . Then Lemma (3.2) guarantees that there exist integers  $c, d \in \mathbb{Z}$  such that  $c$  is divisible by  $N$  and  $\lambda = cz + d$  has norm  $Q(c, d)$  which is equal to a prime  $\ell$  not dividing  $N$ . We also see that  $d$  must be prime to  $c$  in such a case. Now  $z = (c\mathbf{T}(\tau_0) + d)\tau_0 - c\mathbf{N}(\tau_0)$ , so that  $\tau_0 = \rho\tau_0$  where

$$\rho = \begin{pmatrix} c\mathbf{T}(\tau_0) + d & -c\mathbf{N}(\tau_0) \\ c & d \end{pmatrix}$$

has determinant  $\ell$ . Since  $\rho$  satisfies the conditions of Lemma (2.2), it can be written as  $\gamma\omega$  for some  $\gamma \in \Gamma_0(N)$  and  $\omega \in \Omega(\ell)$ . Whence,  $T_g(\tau_0) = (T_g \circ \omega)(\tau_0)$  and  $T_g(\tau_0)$  satisfies the equation  $\Phi_\ell(X, X) = 0$ , which by virtue of Proposition (2.5) and Theorem (2.6) is a monic integral polynomial. Thus  $T_g(\tau_0)$  is an algebraic integer.  $\square$

More generally, we have the following result for imaginary quadratic numbers which are not necessarily algebraic integers, and which therefore supersedes Proposition (3.3).

**(3.4) Theorem.** *Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . Let  $Q = [a, b, c]$  be a primitive positive definite quadratic form of discriminant  $d = N^2 d_K$  and  $(a, N) = 1$ . Let  $\tau$  a root of  $Q(z, 1) = az^2 + bz + c = 0$  in  $\mathfrak{H}$ . Then  $T_g(\tau)$  is an algebraic integer.*

*Proof.* Note that  $\tau$  is not necessarily an algebraic integer, but  $a\tau$  lies in  $\mathcal{O}_K$ , so that  $\tau = \omega_0\tau_0$  for  $\omega_0 = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \in \Omega(a)$  and  $\tau_0 \in \mathcal{O}_K$ . Since  $(a, N) = 1$ , there is a modular equation  $\Phi_a(X)$  which is monic and has roots  $T_g \circ \omega$  for  $\omega \in \Omega(a)$ . It has coefficients in  $\mathbb{Z}[T_g]$ . Thus  $(T_g \circ \omega_0)(\tau_0)$  is integral over  $\mathbb{Z}[T_g(\tau_0)]$ , so  $\mathbb{Z}[T_g(\tau_0)][(T_g \circ \omega_0)(\tau_0)]$  is finitely generated as a  $\mathbb{Z}[T_g(\tau_0)]$ -module. But Theorem (3.3) asserts that  $\mathbb{Z}[T_g(\tau_0)]$  is finitely generated as a  $\mathbb{Z}$ -module, and hence so is  $\mathbb{Z}[T_g(\tau_0)][(T_g \circ \omega_0)(\tau_0)]$ . Since the property “finitely generated” is transitive,  $\mathbb{Z}[T_g \circ \omega_0(\tau_0)]$  is finitely generated as a  $\mathbb{Z}$ -module. Therefore,  $T_g(\tau) = (T_g \circ \omega_0)(\tau_0)$  is integral over  $\mathbb{Z}$ .  $\square$

**Remark.** Proposition (3.3) and Theorem (3.4) are the complement of Siegel’s theorem: Lemma (3.1). We may call algebraic integers  $T_g(\tau)$  “singular moduli” of  $T_g$ .

Let  $K$  be an imaginary quadratic field of discriminant  $d_K$ , and let  $\mathcal{O}$  be an order of  $K$ . The results in Proposition (3.3) and Theorem (3.4) were stated without reference to the ideal class group  $\text{Pic}(\mathcal{O})$  of  $\mathcal{O}$ . Now we will discuss this point of view.

In the classical case, singular moduli of the elliptic modular  $j$  function generate Hilbert class fields of  $\mathcal{O}_K$  over  $\mathbb{Q}$ . In our situation, we will show that singular moduli of fundamental Thompson series  $T_g$  will generate certain class fields of  $K$ .

First we recall some facts from the class field theory of imaginary quadratic fields. Let  $I(\mathcal{O})$  denote the group of proper fractional  $\mathcal{O}$ -ideals, and  $P(\mathcal{O})$  the group of principal  $\mathcal{O}$ -ideals. Then  $\mathcal{O}$ -ideals prime to  $f$  form a subgroup of  $I(\mathcal{O})$  denoted by  $I(\mathcal{O}, f)$ . There is the subgroup,  $P(\mathcal{O}, f)$ , of  $I(\mathcal{O}, f)$  generated by the principal ideals  $(\alpha)$  where  $\alpha \in \mathcal{O}$  has norm  $N(\alpha)$  prime to  $f$ . If  $\mathcal{O}$  is the maximal order  $\mathcal{O}_K$ , we write  $I_K(f)$  and  $P_{K, \mathbb{Z}}(f)$  for  $I(\mathcal{O}_K, f)$  and  $P(\mathcal{O}_K, f)$ , respectively. The ideals in  $I(\mathcal{O}, f)$  are nicely related to ideals in  $I_K(f)$ . If  $\mathfrak{a}$  is an  $\mathcal{O}$ -ideal prime to  $f$ , then  $\mathfrak{a}\mathcal{O}_K$  is an ideal in  $I_K(f)$  with the same norm. This extends to ideal class groups  $\text{Pic}(\mathcal{O})$  and  $I_K(f)/P_{K, \mathbb{Z}}(f)$  (cf. Cox [9], p. 143).

**(3.5) Lemma.** *Let  $\mathcal{O} \subset \mathcal{O}_K$  be an imaginary quadratic order of conductor  $f$  in  $K$ . Then*

$$\text{Pic}(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K, \mathbb{Z}}(f).$$

*Here the first isomorphism is induced from the inclusion map  $I(\mathcal{O}, f) \hookrightarrow I(\mathcal{O})$ , and the second isomorphism  $\psi$  is induced from the map  $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ .*

Class field theory asserts that there exists a unique abelian extension,  $L$ , of  $K$  having  $\text{Pic}(\mathcal{O})$  as its Galois group  $\text{Gal}(L/K)$ , and with the property that all primes of  $K$  that ramify in  $L$  divide  $f\mathcal{O}_K$ . Such a field  $L$  is called the *ring class field* of  $\mathcal{O}$ .

Now we consider the fields over  $K$  (and also over  $\mathbb{Q}$ ) generated by singular moduli of fundamental Thompson series  $T_g$ , evaluated at the imaginary quadratic arguments as in Theorem (3.4).

**(3.6) Theorem.** *Let  $N$  be a positive integer listed in Theorem (1.2.2). Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . Let  $K$  be an imaginary quadratic field of discriminant  $d_K$ . Let  $\mathcal{O}$  be an order of  $K$  of discriminant  $N^2 d_K$  and class number  $h(\mathcal{O})$ . Let  $\text{Pic}(\mathcal{O})$  be the ideal class group of  $\mathcal{O}$ . Then the following assertions hold:*

- (1) *For any ideal class  $\mathfrak{a} \in \text{Pic}(\mathcal{O})$ ,  $T_g(\psi(\mathfrak{a}))$  generates the ring class field  $L$  of  $\mathcal{O}$ .*
- (2) *For any ideal classes  $\mathfrak{a}, \mathfrak{b} \in \text{Pic}(\mathcal{O})$ , define  $\sigma_{\mathfrak{b}}(T_g(\psi(\mathfrak{a})))$  by*

$$\overline{\sigma_{\mathfrak{b}}(T_g(\psi(\mathfrak{a})))} = T_g(\psi(\bar{\mathfrak{b}}\mathfrak{a}))$$

*where  $\bar{\phantom{x}}$  denotes complex conjugation. Then  $\sigma_{\mathfrak{b}}$  is a well-defined element of the Galois group  $\text{Gal}(L/K)$ , and  $\sigma \mapsto \sigma_{\mathfrak{b}}$  induces an isomorphism  $\text{Pic}(\mathcal{O}) \cong \text{Gal}(L/K)$ .*

A proof of assertion (2) will be given in section 4 (see the proof of Theorem (4.5)).

**(3.7) Proof of Theorem (3.6)(1).** Let  $\mathcal{L} = \mathbb{Z} + \mathbb{Z}\tau$  be a lattice in  $\mathbb{C}$  with  $\tau \in \mathfrak{H}$ . Let  $K = \mathbb{Q}(\tau)$  be an imaginary quadratic field. Let  $N$  be a positive integer and let  $\Gamma(N)$  be the principal congruence subgroup of  $\Gamma$  which is defined as the kernel of the reduction map mod  $N$ . The field of modular functions for  $\Gamma(N)$  is denoted by  $\mathfrak{F}_N$ , and its structure is well understood:  $\mathfrak{F}_N = \mathbb{Q}(j, f_{a,b})$  where for  $a, b \in \mathbb{Z}$  with  $a, b \pmod{N}$  not both 0,  $f_{a,b}$  denotes the Fricke function:

$$f_{a,b}(\tau) = -2^7 3^5 \frac{E_2(\tau) E_3(\tau)}{E_2^3(\tau) - 27 E_3^2(\tau)} \wp\left(\frac{a\tau + b}{N}; \tau\right).$$

Here  $\wp$  is the Weierstrass  $\wp$  function with respect to  $\mathcal{L}$ .

**(3.7.1) Lemma.** (Shöngen [27]; cf. Birch [2]) Let  $f \in \mathfrak{F}_N$ . Suppose that the coefficients of the Fourier expansion of  $f$  at every cusp of  $\Gamma(N)$  all lie in the cyclotomic field  $\mathbb{Q}(e^{2\pi i/N})$ . Then the value  $f(\tau)$  belongs to the ray class field of  $K$  with modulus  $N$ .

(By the ray class field with modulus  $N$  over  $K$ , we mean the class field corresponding to the ideal class group generated by principal ideals  $(\alpha)$  where  $\alpha \equiv 1 \pmod{N}$ . This ideal class group is called the *ray class group* and denoted by  $J_K^N$ .)

In our situation, Lemma (3.7.1) already implies that for any genus zero subgroup  $G$  of level  $N$  the values of modular functions at  $\tau$  will belong to the ray class field of  $K$  of modulus  $N$ . Furthermore we know that such values lie in smaller fields than the ray class field of  $K$ . Our purpose here is to determine such fields explicitly.

Theorem (3.6) should follow from working out the Shimura reciprocity law (Theorem (6.31) in Shimura [25]) explicitly in our context. This program is indeed carried out in depth by one of the authors, Imin Chen. A proof of Theorem (3.6) in full detail can be found in his Oxford “dissertation” *Shimura Reciprocity and Singular Values of Modular Functions*. The standard references on Shimura’s reciprocity law are Shimura [25] (and also Lang [19]); confer also Laing [18] for an explicit description of the Shimura reciprocity law for modular functions with rational Fourier coefficients.

We now recall the statement of the Shimura reciprocity law. Let  $\mathcal{L}$ ,  $\tau$  and  $K$  be as above. Let  $K_{\text{ab}}$  denote the maximal abelian extension of  $K$ , and let  $\text{Gal}(K_{\text{ab}}/K)$  denote its Galois group. Class field theory provides the Artin reciprocity map to describe this Galois group, via the following exact sequence:

$$1 \longrightarrow \mathcal{D}_K \longrightarrow \mathcal{C}_K \xrightarrow{[\cdot, K]} \text{Gal}(K_{\text{ab}}/K) \longrightarrow 1$$

where  $\mathcal{C}_K = \mathbb{A}_K/K^*$  is the idèle class group of  $K$ ,  $\mathcal{D}_K$  the norm group, and  $[\cdot, K]$  the Artin reciprocity map.

Shimura considers the field,  $\mathfrak{F} = \cup_{N \geq 1} \mathfrak{F}_N$ , of modular functions of all levels. He shows using the theory of complex multiplication that the field  $\mathfrak{F}(\tau) =: \{f(\tau) \mid f \in \mathfrak{F}\}$  is indeed isomorphic to  $K_{\text{ab}}$ . Consequently, the Galois group  $\text{Gal}(K_{\text{ab}}/K)$  can be described in terms of the automorphisms of  $\mathfrak{F}$ . Now the automorphism group  $\text{Aut}(\mathfrak{F})$  is determined by the Shimura exact sequence

$$0 \longrightarrow \mathbb{Q}^* \longrightarrow \text{GL}_2(\mathbb{A}_f) \xrightarrow{\sigma} \text{Aut}(\mathfrak{F}) \longrightarrow 0.$$

Here  $\mathbb{A}_f$  denotes the finite adeles. One can write  $\text{GL}_2(\mathbb{A}_f) = U \cdot \text{GL}_2^+(\mathbb{Q})$  where

$$U = \varprojlim \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_p \text{GL}_2(\mathbb{Z}_p),$$

and  $\text{GL}_2^+(\mathbb{Q})$  denotes the group of  $2 \times 2$  rational matrices with positive determinant (cf. Shimura (6.16) [25]). Hence, we see that every automorphism of  $\mathfrak{F}$  is represented by matrices of the form  $u \cdot \mathcal{A}$  where  $u \in U$  and  $\mathcal{A} \in \text{GL}_2^+(\mathbb{Q})$ .

The essential point of the Shimura reciprocity law is to represent the action of the idèle class group  $\mathcal{C}_K$ , or rather just the action of ideals in  $K$ , on singular values of modular functions by rational matrices. In our context, we know the level of modular functions, so by Lemma (3.7.1), we may just consider the action of ideals in the ray class group on singular values of modular functions. Furthermore, since all modular functions that concern us have rational Fourier coefficients, the Shimura reciprocity law will take a simpler form. However, we first state the full-fledged version of the Shimura reciprocity law. We need to embed  $\mathbb{A}_K$  into  $\text{GL}_2(\mathbb{A}_f) = \prod' \text{GL}_2(\mathbb{Q}_p)$ , where  $\prod'$  means the restricted product. We first define the embedding locally, and then extend it by continuity to the idèles. Locally, this embedding is given by a rational matrix  $q_{z,p} \in \text{GL}_2(\mathbb{Q}_p)$  which gives multiplication in  $K_p =: K^* \otimes \mathbb{Q}_p^*$  under the  $\mathbb{Q}_p$  basis  $\begin{pmatrix} z \\ 1 \end{pmatrix}$ , specifically, for  $\mu = r + tz \in K_p$ ,

$$q_{z,p}(\mu) = \begin{pmatrix} r + t\mathbf{T}(z) & -t\mathbf{N}(z) \\ t & r \end{pmatrix}$$

where  $\mathbf{T}$  and  $\mathbf{N}$  denote, respectively, the trace and the norm of  $z$  from  $K$  to  $\mathbb{Q}$ . We can extend this to idèles as follows: For an idèle  $t = (\cdots, t_p, \cdots) \in \mathbb{A}_K$ , we define

$$q_z(t) = (\cdots, q_{z,p}(t_p), \cdots) \in \text{GL}_2(\mathbb{A}_f),$$

ignoring the infinite components. Since  $q_z$  is an automorphism of  $\mathfrak{F}$ , we may write

$$q_z = u \cdot \mathcal{A} \quad \text{with } u \in U \text{ and } \mathcal{A} \in \text{GL}_2^+(\mathbb{Q}).$$

**(3.7.2) The Shimura reciprocity law.** Let  $K$  be an imaginary quadratic field, and let  $\tau \in K \cap \mathfrak{H}$ . Let  $\mathfrak{s}$  be an idèle of  $K$ , and let  $[\mathfrak{s}, K]$  denote the Artin map on  $K_{\text{ab}}$ . Then for every modular function  $f$  which is finite at  $\tau$ ,  $f(\tau)$  belongs to  $K_{\text{ab}}$ . Furthermore, we have

$$f(\tau)^{[\mathfrak{s}, K]} = f^\sigma(\tau),$$

where  $\sigma = \sigma(q_\tau(\mathfrak{s}^{-1})) = \sigma(u)\sigma(\mathcal{A})$ . Here  $\sigma(u)$  is the automorphism of  $\mathfrak{F}$  induced by permuting the Fricke functions  $f_{a,b}$  and  $\sigma(\mathcal{A})$  is the composition  $f \mapsto f \circ \mathcal{A}$ .

**(3.7.3) A digression: The Shimura reciprocity law.** Let  $f$  be a modular function of level  $N$  with rational Fourier coefficients. Let  $\tau \in \mathfrak{H}$  be an imaginary quadratic and let  $K = \mathbb{Q}(\tau)$ . Then for any ideal  $\mathfrak{a}$  in the ray class group  $J_K^N$  with modulus  $N$ , there exists a rational matrix  $\mathcal{A} \in \text{GL}_2^+(\mathbb{Q})$  such that

$$f(\tau)^\mathfrak{a} = f(\mathcal{A}\tau).$$

*Proof.* See Laing [18] for an alternative proof. Let  $\mathfrak{s}$  be the idèle associated to  $\mathfrak{a}$ . Write

$$q(\mathfrak{s}^{-1}) = u \cdot g \quad \text{where } u \in U \text{ and } g \in \text{GL}_2^+(\mathbb{Q}).$$

To obtain the action of  $\mathfrak{a}$  on  $f(\tau)$ , we first reduce  $u$  modulo  $N$  and get a matrix  $\tilde{U}_N \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ . Then the action is given by  $f^{\tilde{U}_N}(\tau)$ . But we know that every element of the Galois group  $\text{Gal}(\mathfrak{F}_N/\mathbb{Q}(j)) \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$  which is of the form  $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$  acts on  $f$  by the action of  $\sigma_d \in \text{Gal}(\mathbb{Q}(e^{2\pi i/N})/\mathbb{Q})$  sending  $e^{2\pi i/N}$  to its  $d$ -th power on the Fourier coefficients of  $f$ . In our case, the Fourier coefficients of  $f$  are all rational, so these matrices fix  $f$ . Hence, writing

$$\tilde{U}_N = \begin{pmatrix} 1 & 0 \\ 0 & \det(\tilde{U}_N) \end{pmatrix} \cdot \bar{u}_N \quad \text{with } \bar{u}_N \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

we can find a lifting  $u_N \in \text{SL}_2(\mathbb{Z})$  which gives the same action as  $\bar{u}_N$  on  $f(\tau)$ :

$$f^{\tilde{U}_N}(\tau) = f^{\bar{u}_N}(\tau) = f^{u_N}(\tau) = f(u_N\tau).$$

Therefore the matrix  $\mathcal{A} = u_N \cdot g \in \text{GL}_2^+(\mathbb{Q})$  represents the Galois action of  $\mathfrak{a}$  on  $f(\tau)$ .  $\square$

**(3.7.4) Remark.** A useful fact which we will use is that if  $f$  is a Hauptmodul for a genus zero group  $G$  then  $f(\mathcal{A}\tau) = f(\tau)$  if and only if  $\mathcal{A} \in G \cdot \text{GL}_2^+(\mathbb{Q})_\tau$ , where  $\text{GL}_2^+(\mathbb{Q})_\tau$  denotes the isotropy subgroup at  $\tau$ . In particular, we will take  $\mathcal{A}$  to be a rational matrix associated to an automorphism of  $\text{Gal}(K_{\text{ab}}/K)$  as obtained by Shimura reciprocity and use this criterion to check whether the automorphism fixes a particular singular value  $f(\tau)$ .

**(3.7.5) Theorem.** Let  $T_g$  be a fundamental Thompson series for a genus zero subgroup  $G$  of the form  $\Gamma_0(N) + \epsilon, f, \dots$ . Let  $\tau$  be a root of a quadratic equation  $az^2 + bz + c = 0$  such that  $a > 0$ ,  $(a, b, c) = 1$  and  $b^2 - 4ac = m^2 d_K < 0$ . Let  $K = \mathbb{Q}(\tau)$  and let  $\mathfrak{O}$  be an order in  $K$  of discriminant  $m^2 d_K$ . Then the following assertions hold:

- (1) Suppose that  $G = \Gamma_0(N)$  where  $N$  takes values in Theorem (1.2.2)(1). Then  $T_g(\tau)$  generates the ring class field  $L$  of an imaginary quadratic order  $\mathcal{O}'$  of discriminant  $f^2 d_K$  where  $f = m \cdot N/(a, N)$ , that is,  $L = K(T_g(\tau))$ .
- (2) Suppose that  $G = \Gamma_0(N)_+$  where  $N$  takes values in Theorem (1.2.2)(2). Assume that  $(a, N) = 1$ . Then  $T_g(\tau)$  generates the ring class field  $L$  of an imaginary quadratic order  $\mathcal{O}'$  of discriminant  $f^2 d_K$  where  $f = mN$ , that is,  $L = K(T_g(\tau))$ .

In both cases, if  $m = 1$ ,  $K(T_g(\tau))$  is the ring class field  $L$  of an imaginary quadratic order  $\mathcal{O}'$  of discriminant  $N^2 d_K$ .

(In case (2), the condition  $(a, N) = 1$  is rather essential. If we ease this condition, the assertion no longer holds true. In fact, if  $(a, N) > 1$ ,  $K(T_g(\tau))$  is strictly smaller than the ring class field  $L$  of  $\mathcal{O}'$ .)

*Proof.* (1):  $G = \Gamma_0(N)$ . Since  $j$  is a rational function of  $T_g$  with rational coefficients,  $K(f(\tau))$  is a finite extension of the ring class field  $K(j(\tau))$  of  $\mathcal{O}$ . Thus, it follows that the fixing group of  $T_g(\tau)$  is contained in the principal ideal group  $P(\mathcal{O})$ . Let  $(\alpha)$  be a principal ideal of  $\mathcal{O}$  relatively prime to  $N$ . The discriminant of  $(\alpha)$  is of the form  $M^2 d_K$  with some  $M$  divisible by  $m$ , say,  $M/m = n$ . The action of  $(\alpha)$  on  $f(\tau)$  is represented by a matrix of the form

$$\mathcal{A} = \begin{pmatrix} \frac{\mathbf{T}(\alpha)+bn}{2} & cn \\ -a n \mathbf{N}(\alpha)^{-1} & \frac{\mathbf{T}(\alpha)-bn}{2} \mathbf{N}(\alpha)^{-1} \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

where  $\mathbf{N}(\alpha)^{-1}$  is the inverse of  $\mathbf{N}(\alpha)$  modulo  $N$ , which is well defined since  $(\mathbf{N}(\alpha), N) = 1$ . (We will prove this in (3.7.6).)

Now by Lemma (3.7.4),  $\mathcal{A}$  fixes  $T_g(\tau)$  if and only if  $\mathcal{A} \in \Gamma_0(N) \cdot \mathbf{GL}_2(\mathbb{Q})_\tau^+$ . But the product decomposition of a matrix in  $\Gamma \cdot \mathbf{GL}_2^+(\mathbb{Q})_\tau$  is determined up to multiplication by  $\Gamma_\tau$ , and we know that  $\Gamma_\tau$  is trivial unless  $\tau$  is  $\Gamma$ -equivalent to  $e^{2\pi i/r}$  with  $r \in \{4, 6\}$ . Assuming that  $\Gamma_\tau$  is trivial,  $\mathcal{A} \in \Gamma_0(N)$  if and only if  $N$  divides  $a n$ . Therefore, the principal ideals in  $\mathcal{O}$  which fix  $T_g(\tau)$  are of the form  $(\alpha)$  with  $\text{disc}(\alpha)$  dividing  $((m \cdot N/(a, N))^2 d_K)$ . But these principal ideals are all in  $P(\mathcal{O}')$ .

(The cases  $\tau \sim_\Gamma e^{2\pi i/r}$  with  $r = 4$  or  $6$  can be done similarly, but greater care must be taken.)

(2):  $G = \Gamma_0(N)_+$ . We first describe the action of an arbitrary prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  on  $T_g(\tau)$ . Take a rational prime  $p$  not dividing  $2 a b c m N$ . Suppose that  $p$  splits in  $K$ :  $(p) = \mathfrak{p}\mathfrak{p}'$  where  $\mathfrak{p} = [p, \frac{-r+\sqrt{d_K}}{2}]$ , and  $s := \frac{r^2-d_K}{4p} \in \mathbb{Z}$  with  $(s, N) = 1$ . Then a matrix representing the action of  $\mathfrak{p}$  on  $T_g(\tau)$  has the form

$$\mathcal{A} = \begin{pmatrix} 1 & \frac{rm+b}{2} N k \ell \\ 0 & p \end{pmatrix}$$

where  $k$  (resp.  $\ell$ ) is a solution of the congruence  $ak \equiv 1 \pmod{p}$  (resp.  $N\ell \equiv 1 \pmod{p}$ .) (Again we will prove this in (3.7.6).) Then the following holds true:

**(\*)**. Assume that  $(a, N) = 1$ . Then  $\mathcal{A}$  does not belong to any coset  $W_e \cdot \mathbf{GL}_2^+(\mathbb{Q})_\tau$  of non-trivial Atkin-Lehner involutions  $W_e$  of  $\Gamma_0(N)$ . However, if  $e = 1$ , (i.e.  $W_1 = \Gamma_0(N)$ ) and  $\mathcal{A} \in W_1 \cdot \mathbf{GL}_2^+(\mathbb{Q})_\tau$  then  $\mathfrak{p}$  is a principal ideal  $(\alpha)$  of  $\mathcal{O}$ .

(These two assertions are critical for our conclusion, and the proof will be given in (3.7.7) below. The condition  $(a, N) = 1$  is very subtle as if  $(a, N) > 1$  there may be a non-trivial coset which contains  $A$ .)

Now we are ready to prove the assertion of Theorem (3.6)(1) in the case (2). From the case (1), we know that  $P(\mathcal{O}')$  fixes  $T_g(\tau)$ . Let  $\mathfrak{a}$  be an ideal in  $J_K^N$  that fixes  $T_g(\tau)$ . Choose a prime  $p$  such that  $p \nmid 2abc m N$ . Suppose that  $p$  splits in  $K$  as  $\mathfrak{p}\mathfrak{p}'$  so that  $\mathfrak{p}$  belongs to the same ray class as  $\mathfrak{a}$ . Then a matrix  $A$  giving the action of  $\mathfrak{p}$  on  $T_g(\tau)$  must lie in one of the cosets  $W_e \cdot \mathrm{GL}_2^+(\mathbb{Q})_\tau$ . But as we noted above (\*), no non-trivial Atkin–Lehner involutions  $W_e$  contains this matrix, so it must lie in  $W_1 \cdot \mathrm{GL}_2^+(\mathbb{Q})$ . But then it follows that  $\mathfrak{p}$  is a principal ideal of  $\mathcal{O}$  with a generator  $\alpha$ . The same argument as in the case (1) then shows that  $\alpha \in \mathcal{O}'$  and the fixing group of  $T_g(\tau)$  is  $P(\mathcal{O}')$ .  $\square$

**(3.7.6) Completing the proof of Theorem (3.7.5)(1).** In order to complete our proof, we ought to show how we obtained matrices representing the action of principal ideals, and prime ideals on singular values of  $T_g$ . The procedure is rather computational, but is the essential point in our explicit realization of the Shimura reciprocity law. Here is an algorithm for finding such a matrix :

Step 1: Let  $\mathfrak{s} \in \mathbb{A}_K$ .

Step 2: Find the image of  $\mathfrak{s}^{-1}$  under the embedding  $q$ .

Step 3: Find a product decomposition  $q(\mathfrak{s}^{-1}) = u \cdot g$  where  $u \in U$  and  $g \in \mathrm{GL}_2^+(\mathbb{Q})$ .

Step 4: Find  $\tilde{U}_N := u \pmod{N} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  and define

$$\bar{u}_N := \begin{pmatrix} 1 & 0 \\ 0 & \det(\tilde{U}_N)^{-1} \end{pmatrix} \cdot \tilde{U}_N.$$

Step 5: Find a lifting  $u_N$  of  $\bar{u}_N$  to  $\mathrm{SL}_2(\mathbb{Z})$ . Then  $u_N \cdot g$  is the matrix  $A$  we want.

Case (1):  $G = \Gamma_0(N)$ . Let  $\mathfrak{s} = (1, \dots, \alpha, \dots) \in \mathbb{A}_K$  be an idèle where we put 1 on each place dividing  $N$ , and  $\alpha$  on other places. Under the embedding  $q : \mathbb{A}_K \rightarrow \mathrm{GL}_2(\mathbb{A}_f)$ ,  $\mathfrak{s}$  is sent to

$$q(\mathfrak{s}) = (\mathbb{I}_2, \dots; \begin{pmatrix} \frac{\mathbf{T}(\alpha)m+bM}{2} & cM \\ -aM & \frac{\mathbf{T}(\alpha)m-bM}{2} \end{pmatrix}, \dots)$$

where  $\mathbb{I}_2$  stands for the  $2 \times 2$  identity matrix. So we get

$$q(\mathfrak{s}^{-1}) = (\mathbb{I}_2, \dots; \frac{1}{\mathbf{N}(\alpha)m} \begin{pmatrix} \frac{\mathbf{T}(\alpha)m-bM}{2} & -cM \\ aM & \frac{\mathbf{T}(\alpha)m+bM}{2} \end{pmatrix}, \dots).$$

Further the latter matrix may be written as

$$\frac{1}{\mathbf{N}(\alpha)} \begin{pmatrix} \frac{\mathbf{T}(\alpha)-bn}{2} & -cn \\ an & \frac{\mathbf{T}(\alpha)+bn}{2} \end{pmatrix} \quad \text{with } n = M/m.$$

Next we decompose  $q(\mathfrak{s}^{-1})$  into a product  $u \cdot g$  where  $u \in U$  and  $g \in \mathrm{GL}_2^+(\mathbb{Q})$ :

$$\begin{aligned} q(\mathfrak{s}^{-1}) &= \left( \begin{pmatrix} \frac{\mathbf{T}(\alpha)+bn}{2} & cn \\ -an & \frac{\mathbf{T}(\alpha)-bn}{2} \end{pmatrix}, \dots; \mathbb{I}_2, \dots \right) \cdot \frac{1}{\mathbf{N}(\alpha)} \begin{pmatrix} \frac{\mathbf{T}(\alpha)-bn}{2} & -cn \\ an & \frac{\mathbf{T}(\alpha)+bn}{2} \end{pmatrix} \\ &= u \cdot g. \end{aligned}$$

(Note that  $\det \begin{pmatrix} \frac{\mathbf{T}(\alpha)+bn}{2} & cn \\ -an & \frac{\mathbf{T}(\alpha)-bn}{2} \end{pmatrix} = \mathbf{N}(\alpha)$  and hence the  $u$  we have chosen is indeed in  $U$  as its determinant is prime to  $N$  and its entries have no denominators in  $N$ .)

Now we reduce  $u$  modulo  $N$  to obtain  $\tilde{U}_N$ , and then multiply it on the left by

$$\begin{pmatrix} 1 & 0 \\ 0 & \det(\tilde{U}_N)^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \mathbf{N}(\alpha)^{-1} \end{pmatrix}.$$

The resulting matrix is

$$\bar{u}_N = \begin{pmatrix} \frac{\mathbf{T}(\alpha)+bn}{2} & cn \\ -an\mathbf{N}(\alpha)^{-1} & \frac{\mathbf{T}(\alpha)-bn}{2}\mathbf{N}(\alpha)^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

(Here  $\mathbf{N}(\alpha)^{-1}$  is the inverse of  $\mathbf{N}(\alpha)$  modulo  $N$ .) Lift  $\bar{u}_N$  to a matrix  $u_N \in \mathrm{SL}_2(\mathbb{Z})$ . Then the matrix representing the Galois action of  $(\alpha)$  on  $T_g(\tau)$  is given by  $u_N \cdot g$ . Notice however that  $g$  is in the isotropy group  $\mathrm{GL}_2^+(\mathbb{Q})_\tau$  of  $\tau$ , so we finally have

$$f(\tau)^{(\alpha)} = f^{u_N \cdot g}(\tau) = f(u_N \cdot g \tau) = f(u_N \tau).$$

Case (2):  $G = \Gamma_0(N)_+$ . In this case, we take an idèle  $\mathfrak{s}$  associated to the ideal  $\mathfrak{p} = [p, \frac{-r+\sqrt{d_K}}{2}]$ :

$$\mathfrak{s} = (1, \dots; \frac{-r+\sqrt{d_K}}{2}, \dots)$$

where we put 1 at all places but the place corresponding to  $p$ . Its image under the embedding  $q$  is

$$q(\mathfrak{s}) = (\mathbb{1}_2, \dots; \frac{1}{pm} \begin{pmatrix} \frac{r m+b}{2} & c \\ -a & \frac{r m-b}{2} \end{pmatrix}, \dots)$$

where  $s = \frac{r^2-d_K}{4p}$ . We now decompose  $q(\mathfrak{s}^{-1})$  as a product  $u \cdot g$  where  $u \in U$  and  $g \in \mathrm{GL}_2^+(\mathbb{Q})$ . We rewrite

$$q(\mathfrak{s}^{-1}) = \left( \begin{pmatrix} 1 & -\frac{r m+b}{2a} \frac{1}{p} \\ 0 & \frac{1}{p} \end{pmatrix}, \dots; \frac{1}{sm} \begin{pmatrix} \frac{r m-b}{2} & -\frac{s m^2}{a} \\ a & 0 \end{pmatrix}, \dots \right) \cdot \begin{pmatrix} 1 & \frac{r m+b}{2a} \\ 0 & p \end{pmatrix}.$$

(Here note that  $\frac{1}{sm} \begin{pmatrix} \frac{r m-b}{2} & -\frac{s m^2}{a} \\ a & 0 \end{pmatrix}$  is in  $\mathrm{GL}_2(\mathbb{Z}_p)$  as it contains no denominators in  $p$  and has determinant prime to  $p$ .)

Let  $p_a^{-1}, k \in \mathbb{Z}$  be such that  $ak = 1 - pp_a^{-1}$ . We further rewrite  $q(\mathfrak{s}^{-1})$  by factoring out the matrix  $\begin{pmatrix} 1 & -\frac{r m+b}{2a} p_a^{-1} \\ 0 & 1 \end{pmatrix}$  from each place. We obtain  $q(\mathfrak{s}^{-1}) =$

$$= \left( \begin{pmatrix} 1 & -\frac{r m+b}{2} \frac{k}{p} \\ 0 & \frac{1}{p} \end{pmatrix}, \dots; \frac{1}{sm} \begin{pmatrix} \frac{r m-b}{2} & -\frac{s m^2}{a} \\ a & 0 \end{pmatrix} \begin{pmatrix} 1 & \frac{r m+b}{2a} p_a^{-1} \\ 0 & 1 \end{pmatrix}, \dots \right) \cdot \begin{pmatrix} 1 & \frac{r m+b}{2} k \\ 0 & 1 \end{pmatrix} \blacksquare$$

(Here again we note that  $\begin{pmatrix} 1 & -\frac{r m+b}{2} \frac{k}{p} \\ 0 & \frac{1}{p} \end{pmatrix}$  lies in  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  for any  $\ell \neq p$  and  $\begin{pmatrix} 1 & \frac{r m+b}{2a} p_a^{-1} \\ 0 & 1 \end{pmatrix} \blacksquare$  is in  $\mathrm{GL}_2(\mathbb{Z}_p)$  so that the  $u$  we have chosen is indeed in  $U$ .)

Now we want to find a matrix  $u_N \in \text{SL}_2(\mathbb{Z})$ . Let  $p_N^{-1}, \ell \in \mathbb{Z}$  be such that  $N\ell = 1 - pp_N^{-1}$ , and put

$$u_N = \begin{pmatrix} 1 & -\frac{r m+b}{2} k p_N^{-1} \\ 0 & 1 \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).$$

Then the final matrix we want is

$$u_N \cdot g = \begin{pmatrix} 1 & -\frac{r m+b}{2} k p_N^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{r m+b}{2} k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{r m+b}{2} N k \ell \\ 0 & p \end{pmatrix}.$$

**(3.7.7) Completing the proof of Theorem (3.7.5)(1) continued.** Now we will give a proof of the statement (\*).

Recall that any Atkin–Lehner involution in  $W_e$  is of the form  $\begin{pmatrix} Ae & B \\ CN & De \end{pmatrix} \in \text{GL}_2(\mathbb{Q})$  of determinant  $e$  where  $N = ef$  (cf. (1.2)).

(a) Let  $\mathcal{A} = \begin{pmatrix} 1 & t \\ 0 & p \end{pmatrix}$  be a matrix representing the action of the prime ideal  $\mathfrak{p}$  where  $t = \frac{r m+b}{2} N k \ell$ . Suppose that  $\mathcal{A} \in W_e \cdot \text{GL}_2^+(\mathbb{Q})_\tau$ . Then we can write

$$\begin{pmatrix} 1 & t \\ 0 & p \end{pmatrix} = \gamma \begin{pmatrix} de - b\lambda & -c\lambda \\ \frac{a}{e}\lambda & d \end{pmatrix}$$

where  $\gamma$  is a matrix of the form  $\begin{pmatrix} A & B \\ Cf & De \end{pmatrix}$  with  $ef = N$  and  $\lambda, d \in \mathbb{Z}$ . This implies that  $e$  must divide  $a$ . But this cannot happen as  $(a, N) = 1$ .

(b) Now we have to show that if a matrix  $\mathcal{A}$  belongs to the trivial involutory subgroup  $W_1 = \Gamma_0(N)$ , then  $\mathfrak{p}$  is indeed a principal ideal in  $\mathcal{O}$ . Repeating the argument of (a) with  $e = 1, f = N$ , we see that  $a c \lambda^2 - b \lambda d + d^2 = p$  for some  $\lambda, d \in \mathbb{Z}$ . Hence,  $\mathfrak{p}$  is a principal ideal generated by  $\alpha' = (d - z_0 \lambda)$  where  $z_0$  is a root of  $z^2 - bz + ac = 0$  in  $\mathfrak{K}$ . Notice that  $\alpha'$  is relatively prime to  $N$ .

(c) Finally we show that a matrix  $\mathcal{A}$  representing the action of a principal ideal  $(\alpha)$  on  $T_g(\tau)$  does not lie in  $W_e \cdot \text{GL}_2(\mathbb{Q})^+$ , provided  $K \neq \mathbb{Q}(e^{2\pi i/r})$  with  $r \in \{4, 6\}$  and  $(a, N) = 1$ . Assume that  $\mathcal{A} \in W_e \cdot \text{GL}_2(\mathbb{Q})^+$  for some non-trivial Atkin–Lehner involution  $W_e$ . Applying the same arguments as in (a), we can write

$$\mathcal{A} = \gamma \begin{pmatrix} de - b\lambda & -c\lambda \\ \frac{a}{e}\lambda & d \end{pmatrix}$$

for some  $\gamma$  of the form described in (a). This again leads us to the fact that  $e$  must divide  $a$ , but this is not possible as  $(a, N) = 1$ .

**(3.7.8) Remark.** In Theorem (3.7.5)(2), the fact that the Shimura reciprocity law is totally disjoint from any non-trivial Atkin–Lehner involutions of  $\Gamma_0(N)$  when  $(a, N) = 1$  has the consequence:

*Let  $\mathcal{O}$  be an order in an imaginary quadratic field  $K$ . Then singular moduli of Thompson series for genus zero subgroups  $\Gamma_0(N) + e, f, \dots$  generate the same ring class field of  $\mathcal{O}$  as singular moduli of Thompson series for  $\Gamma_0(N)$ .*

For instance, let  $G = \Gamma_0(N) +$  with  $N - 1 | 24$ . As we noted in (1.5.1), a fundamental Thompson series for  $G$  is of the form  $T_g(z) + N^{12/m} / T_g(z)$  where  $T_g(z)$  is a Thompson

series for  $G = \Gamma_0(N)$ . Then the fact that the Atkin–Lehner involution  $W_N$  is totally disjoint from the Galois action on singular moduli guarantees that singular moduli  $T_g(\tau)$  and  $T_g(\tau) + N^{12/m}T_g(\tau)$  at  $\tau \in \mathcal{O} \cap \mathfrak{H}$  do generate the same ring class field of  $\mathcal{O}$ .

#### 4. Class polynomials

The purpose of this section is to prove explicit class field theory by constructing the minimal polynomials of singular moduli of fundamental Thompson series. In order to do this, we will rephrase the ideal formulation of the previous chapter in terms of equivalent objects which are suitable for computation. This will be accommodated by rephrasing everything in terms quadratic forms. In particular, we will describe the function  $\psi$  introduced in Lemma (3.5) as a map on quadratic forms. This will give an algorithm for constructing “class polynomials” of singular moduli of  $T_g$ .

Let  $K$  be an imaginary quadratic field with discriminant  $d_K$  and let  $\mathcal{O}$  be the order of discriminant  $N^2 d_K$ . Consider the map

$$\psi : I(\mathcal{O})/P(\mathcal{O}) \longrightarrow I_K(N)/P_{K,\mathbb{Z}}(N)$$

defined in Lemma (3.5). It is a well-known fact that the form class group  $\mathcal{Q}_{N^2 d_K}/\Gamma$  (i.e. the group of positive definite primitive quadratic forms of discriminant  $N^2 d_K$  modulo  $\Gamma$ ) and the ideal class group  $I(\mathcal{O})/P(\mathcal{O})$  are isomorphic through the map

$$[a, b, c] \mapsto \left[ a, \frac{-b + \sqrt{N^2 d_K}}{2} \right].$$

This correspondence between quadratic forms and ideals suggests there may also be a form class group (in some general sense) which corresponds to the generalized ideal class group  $I_K(N)/P_{K,\mathbb{Z}}(N)$ . This is indeed the case. We can describe an object corresponding to  $I_K(N)/P_{K,\mathbb{Z}}(N)$  as follows. Let  $\mathcal{Q}_{d_K}(N)$  denote the set of primitive quadratic forms  $[a, b, c]$  having discriminant  $d_K$  with the property that  $a > 0$  and  $(a, N) = 1$ . Transforming a quadratic form in  $\mathcal{Q}_{d_K}(N)$  by a matrix in  $\Gamma_0(N)$  yields another quadratic form in  $\mathcal{Q}_{d_K}(N)$ . Hence, the quotient  $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$  makes sense. We shall see in Proposition (4.1) that the usual correspondence between quadratic forms and ideals induces a bijection between this set and  $I_K(N)/P_{K,\mathbb{Z}}(N)$ . As it stands, there is no group structure on  $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$ . It may be possible to define a group structure on  $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$  by a composition law. (However, we shall not need an intrinsic group structure on  $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$  for our purposes and so we will not pursue this aspect any further.)

**(4.1) Proposition.** *The map*

$$\Theta : [a, b, c] \longrightarrow \left[ a, \frac{-b + \sqrt{d_K}}{2} \right]$$

*induces a bijection*

$$\mathcal{Q}_{d_K}(N)/\Gamma_0(N) \longleftrightarrow I_K(N)/P_{K,\mathbb{Z}}(N).$$

*Proof.* Let  $\langle T \rangle$  be the infinite cyclic group generated by  $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$ . It is well-known that  $\Theta$  gives a bijection between  $\mathcal{Q}_{d_K} / \langle T \rangle$  and  $I_K$ . On the other hand, observe that

$$\mathbf{N}([a, (-b + \sqrt{d_K})/2]) = \mathbf{N}([a, a\tau]) = [[1, a\tau] : [a, a\tau]] = a$$

where  $\tau \in \mathfrak{H}$  is a root of  $az^2 + bz + c = 0$ . Hence, if  $[a, b, c] \in \mathcal{Q}_{d_K}(N)$  then the corresponding ideal  $[a, (-b + \sqrt{d_K})/2]$  has norm  $a$  (which is prime to  $N$ ) and therefore lies in  $I_K(N)$ . Thus,  $\Theta$  actually gives a bijection between  $\mathcal{Q}_{d_K}(N)/T$  and  $I_K(N)$ .

We claim that  $\Theta$  extends to an injective map

$$\mathcal{Q}_{d_K}(N)/\Gamma_0(N) \rightarrow I_K(N)/P_{K,\mathbb{Z}}(N).$$

Let  $f = [a, b, c]$ ,  $f' = [a', b', c'] \in \mathcal{Q}_{d_K}(N)$  and let  $\tau, \tau'$  be their respective roots in  $\mathfrak{H}$ . Then

$$\begin{aligned} f \sim_{\Gamma_0(N)} f' &\iff \tau' = \begin{pmatrix} p & q \\ rN & s \end{pmatrix} (\tau) \quad \text{where } \begin{pmatrix} p & q \\ rN & s \end{pmatrix} \in \Gamma_0(N) \\ &\iff [1, \tau] = (rN\tau + s)[1, \tau'] \\ &\iff a[1, \tau] = \lambda a'[1, \tau'] \quad \text{where } \lambda = a(rN\tau + s)/a' \\ &\iff (a[1, \tau]) (a'[1, \tau'])^{-1} = \lambda \mathcal{O}_K. \end{aligned}$$

Since  $\lambda$  is congruent to an integer prime to  $N$  modulo  $N\mathcal{O}_K$ , we finally have

$$f \sim_{\Gamma_0(N)} f' \iff \Theta(f)\Theta(f')^{-1} \in P_{K,\mathbb{Z}}(N)$$

as desired.

The surjectivity of  $\Theta$  follows from the fact that it is surjective as a map from  $\mathcal{Q}_{d_K}(N)$  to  $I_K(N)$ .  $\square$

We now construct a map

$$\phi : \mathcal{Q}_{N^2 d_K} / \Gamma \longrightarrow \mathcal{Q}_{d_K}(N) / \Gamma_0(N)$$

which corresponds to the map  $\psi$ . This map will be described entirely in terms of quadratic forms. Before we do this, we require some preliminary Lemmas.

**(4.2.1) Lemma.** *Let  $Q = [a, b, c]$  be a primitive positive definite quadratic form and  $N$  an arbitrary integer. There exists a  $\gamma \in \Gamma$  such that*

$$[a', b', c'] = \gamma^t [a, b, c] \gamma \quad \text{satisfies } (a', N) = 1.$$

*Proof.* There exists  $x, y \in \mathbb{Z}$  such that  $Q(x, y) = ax^2 + bxy + cy^2$  is prime to  $N$  and  $(x, y) = 1$ . Let  $w, z$  be integers such that  $wx - zy = 1$ . Form the matrix  $\gamma = \begin{pmatrix} x & z \\ y & w \end{pmatrix}$ . Then  $\gamma$  transforms  $[a, b, c]$  into the desired form.  $\square$

**(4.2.2) Lemma.** *Let  $Q = [a, b, c]$  be a primitive quadratic form of discriminant  $N^2 d_K$ . Then there exists a  $\gamma \in \Gamma$  such that*

$$[a', b', c'] = \gamma^t [a, b, c] \gamma \quad \text{satisfies } b' \equiv 0 \pmod{N} \text{ and } c' \equiv 0 \pmod{N^2}.$$

*Proof.* By Lemma (4.2.1), we can assume that  $(a, 2N) = 1$ . Consider the following system of congruences in the variable  $k$ ,

$$(*) \quad \left\{ \begin{array}{l} b + 2ak \equiv 0 \pmod{N'} \\ b + 2ak \equiv \begin{cases} 0 \pmod{2^{\ell+2}} & \text{if } N^2 d_K \equiv 0 \pmod{4} \\ N \pmod{2^{\ell+2}} & \text{if } d_K \equiv 1 \pmod{4} \end{cases} \end{array} \right\}$$

where  $N = 2^\ell N'$  and  $(N', 2) = 1$ . It is easy to see that this system is always solvable in  $k$ .

Then by the Chinese Remainder Theorem, (\*) is solvable in  $k$ . Let  $k$  be a solution to (\*) and put  $\gamma = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ . Let

$$[a', b', c'] = \gamma^t [a, b, c] \gamma = [a, b + 2ak, ak^2 + bk + c].$$

Since  $k$  is a solution to (\*), we see that  $N|b'$ . Further, we claim that  $N^2|c'$ . For this, first note that  $(b'/N)^2 - d_K \equiv 0 \pmod{4}$ ,

and write  $(b'/N)^2 - d_K = 4t$  with some integer  $t$ . Then  $4tN^2 = 4a'c'$  so that  $tN^2 = a'c'$ . But  $(a', N) = 1$  so we must have  $N^2|c'$ .  $\square$

**(4.3) Definition.** We define a map

$$\phi : \mathcal{Q}_{N^2 d_K} / \Gamma \longrightarrow \mathcal{Q}_{d_K}(N) / \Gamma_0(N)$$

as follows. Let  $[a, b, c]$  be a quadratic form in  $\mathcal{Q}_{N^2 d_K}$ . By Lemma (4.2.2),  $[a, b, c]$  is  $\Gamma$ -equivalent to a quadratic form  $[a', b'N, c'N^2]$ . Put

$$\phi([a, b, c]) = [a', b', c'].$$

**(4.3.1) Lemma.** *The description of  $\phi$  above is a well-defined map.*

*Proof.* To show  $\phi$  is a well-defined map from  $\mathcal{Q}_{N^2 d_K}(N) / \Gamma$  to  $\mathcal{Q}_{d_K}(N) / \Gamma_0(N)$ , it suffices to show if

$$[a_1, b_1 N, c_1 N^2] \sim_\Gamma [a_2, b_2 N, c_2 N^2] \quad \text{then} \quad [a_1, b_1, c_1] \sim_{\Gamma_0(N)} [a_2, b_2, c_2].$$

Suppose that

$$[a_2, b_2 N, c_2 N^2] = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \circ [a_1, b_1 N, c_1 N^2] \quad \text{for some} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma.$$

By multiplying out the above matrices, we obtain the system of equations,

$$(4.3.1) \quad \left\{ \begin{array}{l} a_2 = a_1 \alpha + b_1 N \alpha \gamma + c_1 N^2 \gamma^2 \\ b_2 N = b_1 N (\alpha \delta + \beta \gamma) + 2(a_1 \alpha \beta + c_1 N^2 \gamma \delta) \\ c_2 N^2 = a_1 \beta^2 + b_1 N \beta \delta + c_1 N^2 \delta^2 \end{array} \right\}$$

The last equation in (4.3.1) gives  $\beta(a_1 \beta + b_1 N \delta) = c_2 N^2 - c_1 N^2 \delta$ . Consequently, we have  $N^2 | \beta(a_1 \beta + b_1 N \delta)$ .

Let  $p$  be a prime and let  $p^\nu$  be the highest power of  $p$  dividing  $N$ . Then either  $p^\nu | \beta$  or  $p^\nu | (a_1 \beta + b_1 N \delta)$ . In the latter case,  $p^\nu | N$  so that  $p^\nu | a_1 \beta$ . But  $(a_1, N) = 1$  implies

that  $p^\nu | \beta$ . Thus,  $N | \beta$ . We may rearrange (4.3.1) as follows,

$$\left\{ \begin{array}{l} a_2 = a_1 \alpha + b_1 \alpha (N\gamma) + c_1 (N\gamma)^2 \\ b_2 = b_1 (\alpha \delta + (\beta/N)(N\gamma)) + 2(a_1 \alpha (\beta/N) + c_1 (N\gamma)\delta) \\ c_2 = a_1 (\beta/N)^2 + b_1 (\beta/N)\delta + c_1 \delta^2 \end{array} \right\}.$$

From this set of equations, we see that

$$[a_2, b_2, c_2] = \begin{pmatrix} \alpha & \beta/N \\ N\gamma & \delta \end{pmatrix} \circ [a_1, b_1, c_1] \quad \text{with} \quad \begin{pmatrix} \alpha & \beta/N \\ N\gamma & \delta \end{pmatrix} \in \Gamma_0(N).$$

This proves the assertion. □

**(4.4) Theorem.** *The following diagram is commutative:*

$$\begin{array}{ccc} \mathcal{Q}_{N^2 d_K} / \Gamma & \xrightarrow{\Theta} & I(\mathcal{O}) / P(\mathcal{O}) \\ \phi \downarrow & & \downarrow \psi \\ \mathcal{Q}_{d_K}(N) / \Gamma_0(N) & \xrightarrow{\Theta} & I_K(N) / P_{K, \mathbb{Z}}(N) \end{array}$$

*Proof.* From the  $\Gamma$ -invariance of  $\Theta$  and  $\phi$ , we may assume that quadratic forms in  $\mathcal{Q}_{N^2 d_K} / \Gamma$  have the form  $[a, bN, cN^2]$  where  $(a, N) = 1$ . On the one hand, we have

$$(\Theta \circ \phi)([a, bN, cN^2]) = [a, (-b + \sqrt{d_K})/2].$$

On the other hand, by the description of the map  $\psi$  given in Lemma (3.5) we have

$$\psi \circ \Theta = \left\{ \begin{array}{ll} [a, N(b + \sqrt{d_K})/2][1, \sqrt{d_K}/2] & \text{if } d_K \equiv 0 \pmod{4} \\ [a, N(-b + \sqrt{d_K})/2][1, (-1 + \sqrt{d_K})/2] & \text{if } d_K \equiv 1 \pmod{4} \end{array} \right\}.$$

The proof can be completed by verifying the images of these two maps coincide in  $I_K(N) / P_{K, \mathbb{Z}}(N)$  (in fact, they coincide in  $I_K(N)$ ). □

The map  $\phi$ , when applied to our situation, gives us an explicit way of constructing class polynomials.

**(4.5) Theorem.** *Let  $T_g$  be a fundamental Thompson series of level  $N = o(g)$ . Let  $K$  be an imaginary quadratic field with discriminant  $d_K$  and let  $\mathcal{O}$  be the order of discriminant  $N^2 d_K$ . For  $i = 1, \dots, h(\mathcal{O})$ , let  $\{\mathcal{Q}_i\}$  form a complete set of representatives for  $\mathcal{Q}_{N^2 d_K} / \Gamma$ .*

*Define the polynomial*

$$M(X) =: \prod_{i=1}^{h(\mathcal{O})} (X - T_g(\tau_{\phi(\mathcal{Q}_i)}))$$

where the notation  $\tau_{\mathcal{Q}}$  stands for the root in  $\mathfrak{H}$  of the equation  $Q(z, 1) = 0$ . Then

- (1)  $M(X)$  is the minimal polynomial of  $T_g(\tau_0)$  over  $\mathbb{Q}$  where  $\tau_0 \in \mathcal{O} \cap \mathfrak{H}$  is a root of  $z^2 + z + (1 - d_K)/4 = 0$  if  $d_K \equiv 1 \pmod{4}$  or a root of  $z^2 - d_K/4 = 0$  if  $d_K \equiv 0 \pmod{4}$ .

- (2)  $M(X) \in \mathbb{Z}[X]$ , and is irreducible over  $\mathbb{Q}$ .  
 (3)  $M(X)$  generates the ring class field of  $\mathcal{O}$  over  $K$ .  
 (4)  $\text{Gal}(M/\mathbb{Q}) \cong \text{Pic}(\mathcal{O}) \rtimes C_2$ .

*Proof.* (1) First note that if  $Q$  is in the identity class of  $\mathcal{O}_{N^2 d_K}/\Gamma$  then  $T_g(\tau_{\phi(Q)}) = T_g(\tau_0)$  so  $M(X)$  certainly has  $T_g(\tau_0)$  as a root. By Theorem (3.6)(1),  $L = K(T_g(\tau_0))$  is the ring class field of the order  $\mathcal{O}$ . The conjugates in  $L$  of  $T_g(\tau_0)$  over  $K$  must have the form  $T_g(\tau')$  where  $\tau' \in \mathfrak{H}$  is a root of a quadratic form  $[a', b', c']$  of discriminant  $d_K$  satisfying  $(a', N) = 1$ . By Lemma (4.3.1) the conjugates of  $T_g(\tau_0)$  do arise from quadratic forms in  $\mathcal{O}_{d_K}/\Gamma_0(N)$ . As the cardinality of  $\mathcal{O}_{d_K}(N)/\Gamma_0(N)$  is  $h(\mathcal{O})$  and there are exactly  $h(\mathcal{O})$  conjugates of  $T_g(\tau_0)$ , we see that each class in  $\mathcal{O}_{d_K}(N)/\Gamma_0(N)$  gives rise to a conjugate of  $T_g(\tau_0)$ . Hence,  $M(X)$  is the minimal polynomial of  $T_g(\tau_0)$  over  $K$ . Note however that under complex conjugation, we have

$$\overline{T_g(\tau_{\phi(Q)})} = T_g(\tau_{\phi(\overline{Q})})$$

where  $\overline{Q} = [a, \bar{b}, c] = [a, -b, c]$ . Thus, complex conjugation stabilizes the roots of  $M(X)$  and hence  $M(X)$  is in fact the minimal polynomial of  $T_g(z)$  over  $\mathbb{Q}$ .

(2) This follows from  $T_g(\tau_0)$  being an algebraic integer. Since all conjugates of  $T_g(\tau_0)$  are distinct,  $M(X)$  is separable over  $\mathbb{Q}$  and hence irreducible over  $\mathbb{Q}$ .

(3) The splitting field of  $M(X)$  over  $\mathbb{Q}$  is nothing but the ring class field  $L$  over  $K$ .

(4) This follows as for the elliptic modular function  $j$ .  $\square$

Selected examples of class polynomials are tabulated in Appendix 3.

## 5. Gross–Zagier type formulae for resultants and discriminants of class polynomials for singular moduli of Thompson series

We observe based on extensive computational data that

(a) The discriminants of class polynomials for singular moduli of Thompson series are highly divisible numbers;

(b) The resultants of two class polynomials for singular moduli of Thompson series are also very highly divisible;

(c) The constant terms of class polynomials for singular moduli of Thompson series are also highly factorizable, and

(d) Almost all coefficients of class polynomials for singular modular of Thompson series of  $\Gamma_0(N)$  are divisible by  $N$ .

The observations (a),(b) and perhaps (c) suggest the existence of Gross–Zagier type formulae describing the primes and their exponents in discriminants and resultants of class polynomials. Here we shall discuss selected examples.

**(5.1) Discriminants.** (1) Let  $G = \Gamma_0(5)$ . Then  $T_g(z) = \eta(z)^6/\eta(5z)^6 + 6$  is a canonical Hauptmodul for  $G$ . Let  $d_K = -7$ , and take an order  $\mathcal{O} \subset \mathcal{O}_K$  of discriminant  $-7 \cdot 5^2$  and class number 6. Then the class polynomial of  $T_g$  is

$$M(X) = X^6 + 3 \cdot 5^3 \cdot 11X^5 + 3^2 \cdot 5^5 \cdot 7X^4 + 2^2 \cdot 5^8 \cdot 13X^3 + 3^2 \cdot 5^{10} \cdot 7X^2 \\ + 2 \cdot 3 \cdot 5^{13}X + 5^{15}.$$

remain = 62.0119pt  
 pagetotal=469.9881pt  
 pagegoal=540.0pt

The discriminant of  $M(X)$  is  $\text{disc}(M) = 3^{24}5^{77}7^2$ . Now let  $G = \Gamma_0(5)+$ . Then  $T_g(z) = \eta(q)^6/\eta(q^5)^6 + 125\eta(q^5)^6/\eta(q)^6 + 6$  is a canonical Hauptmodul for  $G$ . With  $\mathcal{O}$  as above, a class polynomial for  $T_g$  is:

$$M(X) = X^6 + 3 \cdot 5 \cdot 277X^5 + 2 \cdot 3 \cdot 5 \cdot 13 \cdot 821X^4 + 2 \cdot 5^2 \cdot 151 \cdot 3301X^3 \\ + 2^2 \cdot 3 \cdot 5^2 \cdot 509 \cdot 7411X^2 + 2^3 \cdot 3 \cdot 5^3 \cdot 7482317X + 5^3 \cdot 821 \cdot 1537681.$$

The discriminant of  $M(X)$  over  $\mathbb{Q}$  is computed to be

$$\text{disc}(M) = 3^{64} \cdot 5^{17} \cdot 7^8 \cdot 13^4 \cdot 17^2 \cdot 19^4 \cdot 31^2.$$

In both cases, the Galois group  $\text{Gal}(M/\mathbb{Q})$  is isomorphic to the generalized dihedral group  $D_6 \cong \text{Pic}(\mathcal{O}) \rtimes C_2$ .

(2) Let  $G = \Gamma_0(13)+$ . Then  $T_g(z) = \eta(z)^2/\eta(13z)^2 + 13\eta(13z)^2/\eta(z)^2 + 2$  is a canonical Hauptmodul for  $G$ . Let  $d_K = -19$ , and take an imaginary quadratic order  $\mathcal{O} \subset \mathcal{O}_K$  of discriminant  $-19 \cdot 13^3$  and class number 14. Then a class polynomial for  $T_g$  is

$$M(X) = X^{14} + 2 \cdot 3^3 \cdot 19 \cdot 863X^{13} - 3 \cdot 5 \cdot 13 \cdot 37 \cdot 4759X^{12} \\ + 2^2 \cdot 3^3 \cdot 13 \cdot 101 \cdot 3511X^{11} - 3 \cdot 13 \cdot 829 \cdot 72931X^{10} \\ + 2 \cdot 3^3 \cdot 13 \cdot 983 \cdot 2663X^9 + 13 \cdot 1019 \cdot 3370151X^8 \\ - 2^4 \cdot 3^5 \cdot 13 \cdot 307 \cdot 1117X^7 - 2^6 \cdot 3 \cdot 7 \cdot 13 \cdot 29 \cdot 397 \cdot 1013X^6 \\ + 2^{11} \cdot 3^3 \cdot 5 \cdot 11 \cdot 13 \cdot 857X^5 + 2^{12} \cdot 3 \cdot 13 \cdot 419 \cdot 7043X^4 \\ + 2^{16} \cdot 3^3 \cdot 5 \cdot 13 \cdot 17 \cdot 157X^3 - 2^{18} \cdot 13 \cdot 3719X^2 \\ - 2^{25} \cdot 3^3 \cdot 5 \cdot 7X + 2^{30} \cdot 3^6.$$

The discriminant of  $M$  is given by

$$\text{disc}(M) = 2^{370}3^{142}13^{13}19^829^631^437^241^253^459^467^271^2107^4167^2179^2227^2.$$

With  $\mathcal{O}$  as above, the discriminant of a class polynomial of  $T_g(z) = \eta(q)^2/\eta(q^{13})^2$  for  $G = \Gamma_0(13)$  is:  $\text{disc}(M) = 2^{156} \cdot 3^{60} \cdot 13^{169} \cdot 19^6$ .

(3) Let  $G = \Gamma_0(16)+$ . Then  $T_g(z) = \eta(2z)^6\eta(8z)^6/\eta(z)^4\eta(4z)^4\eta(16z)^4 - 4$  is a canonical Hauptmodul for  $G$ . Let  $d_K = -7$ , and take an imaginary quadratic order  $\mathcal{O} \subset \mathcal{O}_K$  of discriminant  $-7 \cdot 16^2$  and class number 8. Then a class polynomial of  $T_g$  is

$$M(X) = X^8 + 2^5 \cdot 127X^7 - 2^7 \cdot 5^3X^6 + 2^7 \cdot 3 \cdot 37X^5 + 2^4 \cdot 383X^4 \\ - 2^8 \cdot 3 \cdot 11X^3 + 2^{10} \cdot 5X^2 - 2^{10}X + 1.$$

The discriminant of  $M$  is given by

$$\text{disc}(M) = 2^{24}3^{20}5^87^613^241^259^283^289^2101^2.$$

Its Galois group  $\text{Gal}(M/\mathbb{Q})$  is  $D_8 \cong \text{Pic}(\mathcal{O}) \rtimes C_2$ .

(4) Let  $G = \Gamma_0(6) + 2$ ,  $\Gamma_0(6) + 3$  and  $\Gamma_0(6) + 6$ . Then the canonical Hauptmodul are expressed in terms of eta-functions, and they are denoted, respectively by  $T_{6+2}$ ,  $T_{6+3}$  and  $T_{6+6}$  (cf. Conway and Norton [8]). Now let  $d_K = -11$  and take an imaginary

quadratic order  $\mathcal{O} \subset \mathcal{O}_K$  of discriminant  $-11 \cdot 6^2$  and class number 6. We denote by  $M_{6+s}(X)$  the corresponding class polynomial of  $T_{6+s}$  evaluated at  $\mathcal{O}$ .

$$M_{6+2}(X) = X^6 + 2 \cdot 3^6 \cdot 23X^5 + 3^8 \cdot 127X^4 + 2^2 \cdot 3^{12} \cdot 13 \cdot 41X^3 \\ + 3^{16} \cdot 5 \cdot 83X^2 + 2 \cdot 3^{20} \cdot 23X + 3^{24};$$

$$M_{6+3}(X) = X^6 + 2^5 \cdot 1049X^5 + 2^8 \cdot 5 \cdot 7 \cdot 11 \cdot 19X^4 + 2^{15}787X^3 \\ + 2^{16} \cdot 7^2 \cdot 43X^2 + 2^{21} \cdot 3X + 2^{24};$$

and

$$M_{6+6}(X) = X^6 + 2 \cdot 3 \cdot 5581X^5 - 37 \cdot 73 \cdot 101X^4 + 2^2 \cdot 5 \cdot 11 \cdot 3347X^3 \\ + 23 \cdot 1433X - 2X + 1.$$

The discriminant of each class polynomial is computed as follows:

$$\text{disc}(M_{6+2}) = 2^{46}3^{123}7^4 11^3 13^2 19^2;$$

$$\text{disc}(M_{6+3}) = 2^{152}3^{376} 11^3 13^6 17^2 29^2;$$

$$\text{disc}(M_{6+6}) = 2^{46}3^{376} 11^7 13^2 19^2 29^2 41^2 43^2 61^2.$$

The Galois groups of  $M_{6+s}$  over  $\mathbb{Q}$  are all isomorphic to the generalized dihedral group  $D_6 \cong \text{Pic}(\mathcal{O}) \rtimes C_2$ .

**(5.2) Resultants.** Let  $G = \Gamma_0(7) +$  (resp.  $\Gamma_0(7)$ ). Let  $d_1$  and  $d_2$  be two fundamental field discriminants. Let  $M_1(X)$  and  $M_2(X)$  denote the minimal polynomials of the singular values of the Thompson series  $T_g(z) = \eta(z)^4/\eta(7z)^4 + 49\eta(7z)^4/\eta(z)^4$  (resp.  $\eta(z)^4/\eta(7z)^4$ ) at imaginary quadratic orders of discriminants  $d_17^2$  and  $d_27^2$ , respectively. Then the resultants of  $M_1$  and  $M_2$  are computed for several values of  $d_1$  and  $d_2$ .

(a) Let  $d_1 = -3$  and  $d_2 = -7$ . Then

$$\text{resultant}(M_1, M_2) = 3^{10}5^{11} 17 \cdot 47 \cdot 101 \cdot 167 \cdot 227 \cdot 251 \cdot 257.$$

(resp.  $\text{resultant}(M_1, M_2) = 3^5 \cdot 5^5 \cdot 7^{26}$ .)

(b) Let  $d_1 = -7$  and  $d_2 = -11$ . Then

$$\text{resultant}(M_1, M_2) = -7^8 13^{14} 17^{13} 19^{11} 41^2 61^2 73 \cdot 83^2 \cdot 131 \cdot 241 \cdot 293 \cdot 523 \cdot 563 \\ \cdot 601 \cdot 733 \cdot 761 \cdot 787 \cdot 811 \cdot 853 \cdot 887 \cdot 937 \cdot 941.$$

(resp.  $\text{resultant}(M_1, M_2) = -7^{98} \cdot 13^7 \cdot 17^7 \cdot 19^7$ .)

(c) Let  $d_1 = -11$  and  $d_2 = -15$ . Then

$$\text{resultant}(M_1, M_2) = -7^{36} 11^{18} 13^{32} 29^{14} 41^{13} 43^6 73^2 101^4 127^2 131^4 193^2 277^2 373^2 457^2 \\ \cdot 461 \cdot 547^2 613^2 673^2 \cdot 761 \cdot 1091 \cdot 1151 \cdot 1319 \cdot 1559 \cdot 1601 \\ 1811 \cdot 1889 \cdot 1931 \cdot 1979.$$

(resp.  $\text{resultant}(M_1, M_2) = -7^{228} \cdot 11^8 \cdot 13^{16} \cdot 29^8 \cdot 41^8$ .)

**(5.3) Remarks.** (1) For class polynomials of Thompson series associated to  $G = \Gamma_0(N)$ , the largest prime factor for discriminant is bounded above by  $|d_K|$ . This is no longer the case for discriminants of class polynomials of Thompson series corresponding to  $G = \Gamma_0(N)_+$ .

(2) For each  $N$ , primes dividing discriminants (resp. resultants) of class polynomials of Thompson series associated to  $\Gamma_0(N)$  forms a subset of those corresponding to  $\Gamma_0(N)_+$ .

(3) The Galois group over  $\mathbb{Q}$  of class polynomials  $M(X)$  of degree up to 8 are computed using MAPLE. In all cases we obtain generalized dihedral group  $D_{h(\mathcal{O})} \cong \text{Pic}(\mathcal{O}) \rtimes C_2$ .

Further examples of discriminants, resultants and constant terms are computed and tabulated in Appendix A4 and Appendix A5.

## 6. Postscript

This section collects open problems for further discussions.

**(6.1) Singular moduli of “roots” of Thompson series.** Let  $T_g$  be a fundamental Thompson series of level  $N$ , which has shape

$$T_g(z) = \left\{ \frac{\eta(az)^\alpha \eta(bz)^\beta \cdots}{\eta(cz)^\gamma \eta(dz)^\delta \cdots} \right\}^r \quad \text{where } r \in \mathbb{Z}^+.$$

For instance, take Thompson series for  $\Gamma_0(N)$  with  $N-1|24$ , or for  $\Gamma_0(N) + e, f, \dots$  take, for example,  $T_{6+s}$  with  $s \in \{2, 3, 6\}$ , or  $T_{12+s}$  with  $s \in \{3, 4, 12\}$ .

We consider an  $r$ -th root of  $T_g(z)$ , denoted by  $t_g(z)$ , for instance, if  $N = 7$  and  $T_g(z) = \eta(z)^4/\eta(7z)^4$ , take  $t_g(z) = \{\eta(z)/\eta(7z)\}^r$  where  $r \in \{1, 2, 4\}$ .

Let  $K$  be an imaginary quadratic field and let  $\mathcal{O}$  be an order of discriminant  $N^2 d_K$ . We evaluate  $t_g(z)$  at the same imaginary quadratic arguments  $\tau \in \mathcal{O} \cap \mathfrak{H}$  as for  $T_g(z)$ .

With an appropriate choice of  $h(\mathcal{O})$  such roots representing  $\text{Pic}(\mathcal{O})$ , we form

$$m(X) := \prod_{i=1}^{h(\mathcal{O})} (X - t_g(\tau_{Q_i})).$$

### (6.1.1) Conjecture.

- (1)  $m(X)$  is a class polynomial;
- (2)  $m(X) \in \mathbb{Z}[X]$  and irreducible over  $\mathbb{Q}$ ;
- (3)  $t_g(\tau)$  generates over  $K$  the same ring class field as the original singular value  $T_g(\tau)$ ;
- (4) there are Gross–Zagier type formulae for the discriminant of  $m(X)$ , and for the resultants of two such polynomials.

**(6.2) Example.** Yui and Zagier [30] considered the group  $\Gamma_0(2)$  and the Weber functions, which are the 24-th roots of a Hauptmodul for  $\Gamma_0(2)$ . For  $z \in \mathfrak{H}$ , set  $q = e^{2\pi iz}$ .

The classical Weber functions are defined by

$$f(z) = q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1+q^{n-\frac{1}{2}}), f_1(z) = q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1-q^{n-\frac{1}{2}}), f_2(z) = \sqrt{2}q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1+q^n).$$

The 24–th powers of these functions are Hauptmoduln for  $\Gamma_0(2)$ , and should correspond to some translate of the Thompson series listed in the table 3 in [10].

The main observation in Yui–Zagier [30] was that singular values of Weber functions at imaginary quadratic arguments are algebraic integers, and that they generate the same ring class fields as the corresponding singular values of Thompson series for  $\Gamma_0(2)$ . Moreover, a construction of Weber class polynomials was discussed and a conjectural description of Gross–Zagier type formulae for the resultants and discriminants of Weber class polynomials was given.

**(6.3) A generic construction of class fields.** Norton [21], and Norton, et al. ([1], [10]) introduced and studied *replicable* and *completely replicable* functions. Conway raised a question of a “generic” construction of the ring class field of  $\mathcal{O}$ :

*Do the singular moduli of a Thompson series  $T_g$  and those of the replicates of  $T_g$  generate the same ring class field of  $\mathcal{O}$ ?*

For example, for the group  $\Gamma_0(2)$ , Norton explained to us the following procedure of getting replicable functions:

Step 1: Take a Thompson series  $\eta(q)^{24}/\eta(q^2)^{24}$  (2B)

Step 2: Apply a dash operator, that is, change variables from  $z \rightarrow z + 1/2$ . Then one gets

$$\eta(q^2)^{48}/\eta(q)^{24}\eta(q^4)^{24} \quad (4A = 2A').$$

Step 3: Now take the 24–th root of the function in (2). Then one gets

$$\eta(q^{48})^2/\eta(q^{24})\eta(q^{96}) \quad (96a),$$

which is a non-monstrous Hauptmodul.

What Yui–Zagier [30] implicitly proved for Weber functions is that singular moduli of the replicates of a Hauptmodul for  $\Gamma_0(2)$  generate the same ring class field as the original Hauptmodul for  $\Gamma_0(2)$ .

**Appendix 1: Modular relations for  $\Gamma_0(N)+$** **Modular Relations for  $\Gamma_0(N)+$** 

$G$	Modular Relation	Class
$\Gamma_0(2)+$	$j^2 + (-t^2 - 49t + 6656)j + t^3 + 816t^2 + 221952t + 20123648$	2A
$\Gamma_0(3)+$	$j^2 + (-t^3 - 36t^2 + 1916t + 50976)j + t^4 + 792t^3 + 221400t^2 + 24690528t + 803894544$	3A
$\Gamma_0(4)+$	$(t + 32)j^2 + (-t^5 - 64t^4 - 304t^3 + 46847t^2 + 784880t + 737792)j + t^6 + 816t^5 + 245040t^4 + 32683520t^3 + 1885827840t^2 + 48330387456t + 455821889536$	4A
$\Gamma_0(5)+$	$j^2 + (-t^5 - 30t^4 + 310t^3 + 13700t^2 + 38424t - 614000)j + t^6 + 780t^5 + 218940t^4 + 25968800t^3 + 1177897200t^2 + 22576632000t + 155720872000$	5A
$\Gamma_0(7)+$	$j^2 + (-t^7 - 28t^6 + 21t^5 + 6328t^4 + 39361t^3 - 240492t^2 - 2176581t - 1711008)j + t^8 + 776t^7 + 217756t^6 + 26195512t^5 + 1276406726t^4 + 31050881848t^3 + 404938789276t^2 + 2721214073864t + 7427483226241$	7A
$\Gamma_0(13)+$	$j^2 + (-t^{13} - 26t^{12} - 156t^{11} + 1508t^{10} + 21658t^9 + 39624t^8 - 612742t^7 - 3355976t^6 + 454779t^5 + 43741490t^4 + 95939974t^3 - 41335164t^2 - 291162600t - 174668400)j + t^{14} + 772t^{13} + 216424t^{12} + 26333528t^{11} + 1359640022t^{10} + 39120460496t^9 + 716780223796t^8 + 8956723925032t^7 + 79070093432161t^6 + 500196729175884t^5 + 2260671730897788t^4 + 7142292018579744t^3 + 15009662255513328t^2 + 18874201488396480t + 10755802087387200$	13A

Modular Relations for  $\Gamma_0(N)+$  continued

$\Gamma_0(25)+$	$ \begin{aligned} & (t^4 + 10t^3 + 35t^2 + 50t + 25)j^2 + (-t^{29} \\ & - 35t^{28} - 485t^{27} - 2800t^{26} + 4225t^{25} + 161845t^{24} \\ & + 864725t^{23} - 22850t^{22} - 20887250t^{21} - 90547750t^{20} \\ & - 11474690t^{19} + 1222969000t^{18} + 4238808800t^{17} \\ & + 1045637500t^{16} - 32518637000t^{15} - 95458801300t^{14} \\ & - 48963635375t^{13} + 356022802375t^{12} \\ & + 986319593125t^{11} + 832448067500t^{10} \\ & - 1088678257825t^9 - 3689606848625t^8 \\ & - 4032794243125t^7 - 1080734391250t^6 \\ & + 2331719776874t^5 + 3136801920370t^4 \\ & + 1758792060010t^3 + 429820525700t^2 \\ & - 1059621800t - 14445350000)j + t^{30} + 780t^{29} \\ & + 223440t^{28} + 28551800t^{27} + 1665256050t^{26} \\ & + 57545141280t^{25} + 1350792437500t^{24} \\ & + 23276229621000t^{23} + 309068256159375t^{22} \\ & + 3266996305387500t^{21} + 28127903370740940t^{20} \\ & + 200553915290998800t^{19} + 1198800119579065900t^{18} \\ & + 6061981238068524000t^{17} \\ & + 26103417401070507000t^{16} \\ & + 96159940538465958800t^{15} \\ & + 303926662237029171375t^{14} \\ & + 825324094220824558500t^{13} \\ & + 1925470951829505205000t^{12} \\ & + 3853445000148849135000t^{11} \\ & + 6595196414635487298450t^{10} \\ & + 9606667551869790072000t^9 \\ & + 11826745812811382023500t^8 \\ & + 12187709498718981825000t^7 \\ & + 10375322758438101630625t^6 \\ & + 7163889745680371494500t^5 \\ & + 3908812977514032097500t^4 \\ & + 1621074253736945180000t^3 \\ & + 479923748121571350000t^2 \\ & + 90307158983082600000t + 8113088731693672000 \end{aligned} $	25A
-----------------	--	-----

## Appendix 2: Modular equations

This appendix contains a sample of modular equations for a fundamental Thompson series  $T_g$  for  $G = \Gamma_0(N)$  or  $\Gamma_0(N)^+$  of order 2 and 3. They were computed using Mahler's explicit description of modular equations for "basic"  $S_p$ -series (Mahler [20], p.90/93). (By a "basic"  $S_p$ -series we mean one which has constant term 0.)

(We note that Mahler's description of an order 3 modular equation is slightly in error: one should exclude  $b_1$  from the constant term (Mahler [20], p.93).)

### Modular Equations of Order 2

$G$	$\Phi_2^T(X, Y)$
$\Gamma_0(3)$	$X^3 + (-Y^2 + 108)X^2 + (-153Y + 2268)X + (Y^3 + 108Y^2 + 2268Y - 46224)$
$\Gamma_0(3)^+$	$X^3 + (-Y^2 + 1566)X^2 + (17343Y + 741474)X + (Y^3 + 1566Y^2 + 741474Y + 28166076)$
$\Gamma_0(5)$	$X^3 + (-Y^2 + 18)X^2 + (19Y - 6)X + (Y^3 + 18Y^2 - 6Y - 1044)$
$\Gamma_0(5)^+$	$X^3 + (-Y^2 + 268)X^2 + (1519Y + 24244)X + (Y^3 + 268Y^2 + 24244Y + 323456)$
$\Gamma_0(7)$	$X^3 + (-Y^2 + 4)X^2 + (15Y - 12)X + (Y^3 + 4Y^2 - 12Y - 144)$
$\Gamma_0(7)^+$	$X^3 + (-Y^2 + 102)X^2 + (407Y + 3810)X + (Y^3 + 102Y^2 + 3810Y + 27100)$

### Modular Equations of Order 3

$G$	$\Phi_3^T(X, Y)$
$\Gamma_5$	$X^4 + (-Y^3 + 27Y + 30)X^3 + (-90Y^2 + 288Y + 1728)X^2 + (27Y^3 + 288Y^2 - 3745Y + 5406)X + (Y^4 + 30Y^3 + 1728Y^2 + 5406Y - 101124)$
$\Gamma_0(5)^+$	$X^4 + (-Y^3 + 402Y + 2280)X^3 + (10035Y^2 + 342288Y + 2911728)X^2 + (402Y^3 + 342288Y^2 + 10954880Y + 89206656)X + (Y^4 + 2280Y^3 + 2911728Y^2 + 89206656Y + 693893376)$
$\Gamma_0(7)$	$X^4 + (-Y^3 + 6Y + 24)X^3 + (-15Y^2 + 36Y + 192)X^2 + (6Y^3 + 36Y^2 - 289Y - 60)X + (Y^4 + 24Y^3 + 192Y^2 - 60Y - 4368)$
$\Gamma_0(7)^+$	$X^4 + (-Y^3 + 153Y + 612)X^3 + (2043Y^2 + 37080Y + 168507)X^2 + (153Y^3 + 37080Y^2 + 652391Y + 2982276)X + (Y^4 + 612Y^3 + 168507Y^2 + 2982276Y + 13600629)$

### Appendix 3: Class polynomials

We have constructed class polynomials for most of the fundamental Thompson series listed in Conway and Norton [8], p. 331. These computations were performed for several field discriminants  $d_K$  up to  $-95$ . Here is an algorithm for the construction of class polynomials.

**Input:** The discriminant  $d_K$  of an imaginary quadratic field  $K$  and a fundamental Thompson series  $T_g$  of level  $N$ .

**Output:** A class polynomial for  $T_g$  and an imaginary quadratic order  $\mathfrak{O} \subset \mathfrak{O}_K$  of discriminant  $N^2 d_K$ .

**Process:**

(1) Find the primitive positive definite reduced quadratic forms  $Q = [a, b, c] \in \mathcal{Q}(N^2 d_K)$  of discriminant  $d_K N^2$ .

(2) Transform each  $Q_i$  by  $\phi$  and let  $Q' = [a', b', c'] = \phi(Q) \in \mathcal{Q}_{d_K}(N)/\Gamma_0(N)$  with  $(a', N) = 1$ .

(3) For each  $Q'$ , let  $\tau_{Q'}$  be the root of the quadratic equation  $a'z^2 + b'z + c' = 0$  in  $\mathfrak{h} \cap \mathfrak{O}$ .

(4) Construct the class polynomial:

$$M(X) = \prod (X - T_g(\tau_{Q'}))$$

where the product runs over  $h(\mathfrak{O})$  quadratic forms in  $\mathcal{Q}_{d_K}(N)/\Gamma_0(N)$ .

(Alternatively, one can directly find the representatives  $Q' = [a', b', c'] \in \mathcal{Q}_{d_K}(N)/\Gamma_0(N)$  with  $(a', N) = 1$  using an explicit description of the  $\Gamma_0(N)$  cosets of  $\Gamma$ . This would in principle yield another algorithm for the construction of monstrous class equations, although we have not yet implemented this on computer.)

The construction was done with a program written in C using the PARI library package. The floating point precision used was adjusted so that the resulting polynomials had coefficients whose roundoff errors were less than  $10^{-10}$ .

We observe that the constant terms of class polynomials are very highly factorizable. Indeed, for  $\Gamma_0(N)$ , the constant terms are divisible by high powers of  $N$ .

This appendix contains examples of class polynomials for Thompson series

$$T_3, T_5, T_6, T_{6+2}, T_{6+6}, T_{7+}, T_{13}, T_{13+}.$$

Class polynomials for  $T_3$ 

$d_K$	$M(X)$
-3	$X + 3^5$
-4	$X^2 - 486X - 3^9$
-7	$X^4 + 4131X^3 + 196830X^2 + 19131876X + 3^{18}$
-8	$X^2 - 7290X + 3^{12}$
-11	$X^2 + 33534X + 3^{12}$
-15	$X^6 + 192456X^5 + 8503056X^4 + 37106273502X^3 + 711304017804X^2 - 2541865828329X + 3^{30}$
-19	$X^4 + 885492X^3 + 196830X^2 + 19131876X + 3^{18}$
-20	$X^4 - 1262628X^3 - 1459336986X^2 - 26344593252X + 3^{24}$
-23	$X^6 + 3494097X^5 + 406552365X^4 + 12226990632840X^3 + 111559666909950X^2 + 38501641701699363X + 3^{36}$
-24	$X^6 - 4833270X^5 + 10232896455X^4 + 709926522732X^3 + 15115210378335X^2 + 66088511536554X + 3^{30}$
-31	$X^{12} + 39493575X^{11} + 1030523148X^{10} + 1559782510359975X^9 + 1714011392875707X^8 + 1580390392427658738X^7 + 297852253732774276110X^6 + 20481291317845045833084X^5 + 585720749388797440840503X^4 + 5943530070634619839873671X^3 + 514050410939845063563882X^2 + 8614775852302231065242988X + 3^{54}$
-35	$X^4 + 117966780X^3 + 10172843622X^2 + 209207064060X + 3^{24}$

Class polynomials for  $T_3$  continued

-39	$X^{12} + 331533891X^{11} + 80350690554X^{10} + 109923131349948861X^9 + 2389123443244098318X^8 +$ $2241494575392888371574X^7 - 7141631017606513143507X^6 - 395209231077563584534107X^5 +$ $133289835800443095494035440X^4 + 4147535974225063022855318556X^3 + 33270264341591216373968419656X^2 -$ $34017596146778434918878248865X + 3^{60}$
-40	$X^8 - 425691288X^7 + 8781322680396X^6 - 8378877953288X^5 - 8144233419406410X^4 - 164913995505693672X^3 +$ $518540628979116X^2 + 14824161510814728X + 3^{36}$
-43	$X^4 + 884736756X^3 + 196830X^2 + 19131876X + 3^{18}$
-47	$X^{10} + 2257839117X^9 - 423767333313X^8 + 5097884050024492689X^7 - 1084237219618314903324X^6 +$ $130211867647133030958075X^5 + 13311934630610194013247396X^4 + 412119948005504278706786751X^3 +$ $7411259759158378636424597232X^2 + 80944433908231763089023115248X + 3^{60}$
-51	$X^6 + 5541101298X^5 + 576893554407X^4 + 58591580700636X^3 + 1180984336971903X^2 - 482954507382510X + 3^{30}$
-52	$X^8 - 6896878488X^7 - 572877592314804X^6 - 1357512554529288X^5 - 131950184502593610X^4 -$ $2671984504940234472X^3 + 518540628979116X^2 + 14824161510814728X + 3^{36}$
-55	$X^{16} + 13136687649X^{15} + 8845606472661X^{14} + 172575343729572360003X^{13} + 1118879631633140415144409X^{12} +$ $33968358640649945562195645X^{11} + 3302188035293621384522265978X^{10} + 67043449899394255772375608701X^9 +$ $34382086534446404677712279658X^8 + 3567883207494628675248159884679X^7 +$ $208313820881941262996807375519493X^6 + 6752928678182826932022500705572890X^5 +$ $113170123579762509401159069945440104X^4 + 763912566602277117527633243577534297X^3 +$ $375416097685314698322591500428056X^2 + 4450054231099096180116572419708176X + 3^{72}$

Class polynomials for  $T_5$ 

$d_K$	$M(X)$
-3	$X^2 + 250X + 5^5$
-4	$X^2 - 500X - 5^6$
-7	$X^6 + 4125X^5 + 196875X^4 + 20312500X^3 + 615234375X^2 + 7324218750X + 5^{15}$
-8	$X^6 - 7250X^5 + 196875X^4 + 20312500X^3 + 615234375X^2 + 7324218750X + 5^{15}$
-11	$X^4 + 33500X^3 - 406250X^2 + 23437500X + 5^{12}$
-15	$X^{10} + 192500X^9 + 18125000X^8 + 37466796875X^7 + 3011718750000X^6 + 46484375000000X^5 + 526428222656250X^4 + 14781951904296875X^3 + 252723693847656250X^2 + 2086162567138671875X + 5^{27}$
-19	$X^4 + 885500X^3 + 12593750X^2 + 85937500X + 5^{12}$
-20	$X^{10} - 1262500X^9 - 1628515625X^8 - 248671875000X^7 - 25808105468750X^6 - 799804687500000X^5 - 11817932128906250X^4 - 110626220703125000X^3 - 789165496826171875X^2 - 3576278686523437500X - 5^{27}$
-23	$X^{18} + 3494000X^{17} + 88606250X^{16} + 12248762890625X^{15} + 159389951171875X^{14} + 141537712402343750X^{13} + 28060103118896484375X^{12} + 2291336051940917968750X^{11} + 97725039577484130859375X^{10} + 2428162932395935058593750X^9 + 36985136866569519042968750X^8 + 356823652982711791992187500X^7 + 2435635775327682495117187500X^6 + 17392216250300407409667968750X^5 + 161456409841775894165039062500X^4 + 127474774004936218261718750000X^3 + 6630216375924646854400634765625X^2 + 20463630789890885353088378906250X + 5^{45}$
-24	$X^8 - 4833500X^7 + 11315562500X^6 - 1579695312500X^5 - 22564941406250X^4 + 2282714843750X^3 + 625610351562500X^2 + 1907348632812500X + 5^{24}$

Class polynomials for  $T_5$  continued

-31	$ \begin{aligned} & X^{12} + 39493500X^{11} - 1694531250X^{10} + 1559789386718750X^9 - 87191675537109375X^8 + 3065164764404296875X^7 + \\ & 278784549713134765625X^6 + 5955729961395263671875X^5 + 44779300689697265625000X^4 + \\ & 23864209651947021484375X^3 - 444240868091583251953125X^2 + 3841705620288848876953125X + 5^{36} \end{aligned} $
-35	$ \begin{aligned} & X^{10} + 117966250X^9 - 51641484375X^8 + 25791984375000X^7 + 1113086425781250X^6 + 13706616210937500X^5 + \\ & 40199279785156250X^4 - 95367431640625000X^3 + 431537628173828125X^2 + 596046447753906250X + 5^{27} \end{aligned} $
-39	$ \begin{aligned} & X^{16} + 331534625X^{15} + 325685796875X^{14} + 109993475173828125X^{13} + 106556809354003906250X^{12} + \\ & 24778235467773437500000X^{11} + 2984769744258880615234375X^{10} + 159370722042560577392578125X^9 + \\ & 5711490522325038909912109375X^8 + 142711162470281124114990234375X^7 + \\ & 2458093085326254367828369140625X^6 + 28445509844459593296051025390625X^5 + \\ & 212340528378263115882873535156250X^4 + 966298102866858243942260742187500X^3 + \\ & 2541355570429004728794097900390625X^2 + 4234834705130197107791900634765625X + 5^{48} \end{aligned} $
-40	$ \begin{aligned} & X^{10} - 425691250X^9 + 8762592265625X^8 + 354374890625000X^7 + 7976605957031250X^6 + 92641528320312500X^5 + \\ & 517799377441406250X^4 + 1346588134765625000X^3 + 3292560577392578125X^2 + 6556510925292968750X + 5^{27} \end{aligned} $
-43	$ X^6 + 884736750X^5 + 196875X^4 + 2031250X^3 + 615234375X^2 + 7324218750X + 5^{15} $

Class polynomials for  $T_6$ 

$d_K$	$M(X)$
-3	$X^3 + 228X^2 + 48X + 2^6$
-4	$X^4 - 536X^3 - 1344X^2 - 2048X - 2^9$
-7	$X^4 + 4072X^3 + 12480X^2 + 11776X + 2^{12}$
-8	$X^4 - 7232X^3 + 4704X^2 + 4864X - 2^9$
-11	$X^6 + 33504X^5 + 28752X^4 + 1608320X^3 + 2146560X^2 + 6144X + 2^{12}$
-15	$X^6 + 192408X^5 + 1960512X^4 + 2229248X^3 + 61440X^2 - 196608X + 2^{18}$
-19	$X^{12} + 885432X^{11} - 39648768X^{10} + 738423040X^9 - 6480039168X^8 + 30369263616X^7 - 35931537408X^6 - 134799556608X^5 + 229292310528X^4 + 522278404096X^3 + 232167309312X^2 + 50331648X + 2^4$
-20	$X^8 - 1263808X^7 + 12949120X^6 + 199838720X^5 + 885474304X^4 + 702119936X^3 + 82542592X^2 + 37486592X + 2^{18}$
-23	$X^6 + 3493968X^5 + 4739136X^4 + 9196544X^3 + 10678272X^2 + 2457600X + 2^{18}$
-24	$X^{12} - 4831152X^{11} - 71803680X^{10} - 70359296X^9 + 15284252160X^8 - 173564706816X^7 - 613845958656X^6 - 1835272765440X^5 - 2624478511104X^4 - 1144210325504X^3 + 110050148352X^2 + 36440113152X - 2^{27}$
-31	$X^{12} + 39493560X^{11} + 991029504X^{10} + 51236386816X^9 + 496554246144X^8 + 4629459566592X^7 + 2293095727104X^6 - 9017644548096X^5 - 1920051707904X^4 + 10929081155584X^3 + 4854386786304X^2 - 798863917056X + 2^{36}$
-35	$X^{12} + 117966720X^{11} + 4864340064X^{10} + 636526336X^9 - 475298189568X^8 + 653188792320X^7 + 12335358492672X^6 + 44382256496640X^5 + 72109045776384X^4 + 69579632017408X^3 + 30924324470784X^2 + 50331648X + 2^{24}$

Class polynomials for  $T_6$  continued

-39	$X^{12} + 331533552X^{11} - 27397767552X^{10} + 786719704576X^9 + 4188943429632X^8 + 25725229498368X^7 +$ $109728704495616X^6 + 205900329517056X^5 + 193985469480960X^4 + 101533295312896X^3 + 279892228126208X^2 +$ $1984274890752X + 2^{36}$
-40	$X^{16} - 425670752X^{15} + 33364781184X^{14} - 710449045504X^{13} + 13058452158464X^{12} - 183370244702208X^{11} +$ $1362090882236416X^{10} - 4435222197174272X^9 + 6551861293744128X^8 - 2907498604396544X^7 -$ $59842620645441536X^6 + 4254644532412416X^5 + 105782310216925184X^4 + 56833184809091072X^3 -$ $482513805901824X^2 - 177021372071936X + 2^{36}$
-43	$X^{12} + 884736696X^{11} - 39812955648X^{10} + 724612608256X^9 - 6638016072960X^8 + 29685346873344X^7 -$ $37200109486080X^6 - 135894353707008X^5 + 228305343283200X^4 + 521838966341632X^3 + 231928473059328X^2 +$ $50331648X + 2^{24}$
-47	$X^{10} + 2257839280X^9 - 24129796032X^8 + 966541559808X^7 + 5355890688000X^6 + 11265528102912X^5 +$ $10579452100608X^4 + 4255484215296X^3 + 547054682112X^2 - 33957085184X + 2^{30}$
-51	$X^{18} + 5541101208X^{17} + 161310960720X^{16} + 37775309579520X^{15} - 831097807331328X^{14} + 2668467332837376X^{13} +$ $27061599816056832X^{12} + 21705912637784064X^{11} - 1394608726314713088X^{10} - 363842686884511744X^9 +$ $14619796718022033408X^8 + 29213175104063668224X^7 + 29494976415359041536X^6 + 33684215870320017408X^5 +$ $36173479840655081472X^4 + 22311421028937498624X^3 + 5949712697867108352X^2 + 309237645312X + 2^{36}$
-52	$X^{16} - 6896961632X^{15} + 459924207744X^{14} - 15143074975744X^{13} + 260417146087424X^{12} -$ $2649971962134528X^{11} + 17854207215271936X^{10} - 77976404552056832X^9 + 157211162832273408X^8 +$ $128620413935681536X^7 - 743085830523846656X^6 + 199823199364448256X^5 + 1741332098783903744X^4 +$ $92703280152379392X^3 + 1966648344969216X^2 + 713583046426624X + 2^{36}$

Class polynomials for  $T_{6+2}$ 

$d_K$	$M(X)$
-3	$X^3 + 243X^2 + 2187X + 3^{10}$
-4	$X^4 - 540X^3 + 4374X^2 + 78732X + 3^{12}$
-7	$X^4 + 4077X^3 + 4374X^2 + 78732X + 3^{12}$
-8	$X^4 - 7128X^3 - 695466X^2 - 4251528X + 3^{16}$
-11	$X^6 + 33534X^5 + 833247X^4 + 1133032212X^3 + 17864389215X^2 + 160392082446X + 3^{24}$
-15	$X^6 + 192456X^5 + 9850248X^4 + 206081010X^3 + 1396626948X^2 - 1678822119X + 3^{20}$
-19	$X^{12} + 885492X^{11} + 8166258X^{10} + 784118363220X^9 + 175153919103X^8 + 18526275597096X^7 + 614329570043388X^6 + 9610386743137032X^5 + 74213162012502927X^4 + 251675219394510948X^3 + 13588814718246834X^2 + 66708726798666276X + 3^{36}$
-20	$X^8 - 1264896X^7 + 1396784412X^6 + 19812120480X^5 + 1487952958086X^4 + 7810397058240X^3 - 245148837665508X^2 - 2196172075676256X + 3^{32}$
-23	$X^6 + 3493935X^5 - 135018819X^4 + 3409725456X^3 + 63967427406X^2 + 575319426165X + 3^{24}$
-24	$X^{12} - 4828896X^{11} - 10936946430X^{10} - 655510034880X^9 + 6417936076239X^8 + 1039576245907392X^7 + 25823725000722972X^6 + 250309390156088832X^5 + 1848421953568393839X^4 + 10917171388186668576X^3 + 59537538667809651330X^2 + 28818169977023831232X + 3^{40}$
-31	$X^{12} + 39493737X^{11} + 7704949716X^{10} + 758338809849X^9 + 39920293455075X^8 + 1404193595392062X^7 + 31296049480780686X^6 + 428423891148427572X^5 + 3305060195996172807X^4 + 11155783959089396793X^3 + 13588814718246834X^2 + 66708726798666276X + 3^{36}$

Class polynomials for  $T_{6+2}$  continued

-35	$ \begin{aligned} & X^{12} + 117966780X^{11} + 11234544642X^{10} + 13916533156130412X^9 + 1200063732930284463X^8 + \\ & 35480056376660825592X^7 + 531676059562449884700X^6 + 4926884930984187483192X^5 + \\ & 29223727534616511708783X^4 + 114025693678047856230732X^3 + 291808286348284405081602X^2 + \\ & 531776287179150065755740X + 3^{48} \end{aligned} $
-39	$ \begin{aligned} & X^{12} + 331533405X^{11} - 78453922950X^{10} + 9401606227323X^9 - 366783403089762X^8 + 4644090759945690X^7 + \\ & 129329620788072573X^6 + 2313281765407639131X^5 + 26221928554895217264X^4 + 226934029359250506396X^3 + \\ & 856139799734082986184X^2 - 99512743201910417223X + 3^{40} \end{aligned} $
-40	$ \begin{aligned} & X^{16} - 425650032X^{15} - 8783551784520X^{14} + 19507574711376X^{13} + 190520782969773276X^{12} - \\ & 1298445690046066992X^{11} - 176285580391085425272X^{10} - 60857858808228366015216X^9 - \\ & 97312298397204958217082X^8 - 782998641464026128173136X^7 - 3155867369504079541948152X^6 - \\ & 5784061008055239444106512X^5 - 28394327342465294422151844X^4 - 63885581727192763034532624X^3 + \\ & 13130278695781483105080X^2 + 47269003304813339178288X + 3^{48} \end{aligned} $
-43	$ \begin{aligned} & X^{12} + 884736756X^{11} + 7962827634X^{10} + 782759127439684692X^9 + 174143598212223X^8 + \\ & 18493975059526440X^7 + 613592143036851708X^6 + 9597428876003283720X^5 + 74037384364876491663X^4 + \\ & 249877378029060472932X^3 + 13588814718246834X^2 + 66708726798666276X + 3^{36} \end{aligned} $
-47	$ \begin{aligned} & X^{10} + 2257839603X^9 + 689347467279X^8 + 103266260132967X^7 - 904126294543212X^6 + 45128993733386469X^5 - \\ & 406137062614115772X^4 - 100161460405557463X^3 + 29470433083499679264X^2 + 199325675674414832688X + 3^{40} \end{aligned} $

Class polynomials for  $T_{6+6}$ 

$d_K$	$M(X)$
-3	$X^3 + 219X^2 - 21X + 1$
-4	$X^4 - 548X^3 + 198X^2 - 44X + 1$
-7	$X^4 + 4060X^3 + 198X^2 - 35X + 1$
-8	$X^4 - 7240X^3 - 2602X^2 + 40X + 1$
-11	$X^6 + 33486X^5 - 272801X^4 + 736340X^3 + 32959X^2 - 2X + 1$
-15	$X^6 + 192393X^5 + 806004X^4 + 28514X^3 + 3384X^2 - 72X + 1$
-19	$X^{12} + 885396X^{11} - 63555198X^{10} + 15078882612X^9 - 12605189265X^8 + 28226562408X^7 - 4264398948X^6 + 784051216200X^5 + 154272879X^4 - 30996860X^3 + 886530X^2 - 60X + 1$
-20	$X^8 - 1263840X^7 + 42016796X^6 + 72894400X^5 + 150566406X^4 - 4525280X^3 + 167196X^2 - 1280X + 1$
-23	$X^6 + 3493957X^5 - 2248866X^4 + 441696X^3 - 9811X^2 + 47X + 1$
-24	$X^{12} - 4831200X^{11} + 116611938X^{10} + 98144896X^9 + 4467756591X^8 - 389202825024X^7 + 407125079772X^6 - 121436864640X^5 - 2320325073X^4 + 43725856X^3 + 278370X^2 + 2304X + 1$
-31	$X^{12} + 39493524X^{11} - 75296382X^{10} + 35885949673X^9 - 11235792249X^8 + 1449730170036X^7 + 727164962286X^6 + 213029874270X^5 + 3673335699X^4 + 39336169X^3 + 2244X^2 + 57X + 1$
-35	$X^{12} + 117966684X^{11} + 1679239362X^{10} - 20034471092X^9 + 1587640249583X^8 + 10397429028408X^7 - 3604923210852X^6 + 2053506955768X^5 - 594053249297X^4 + 55208538988X^3 + 117950402X^2 + 444X + 1$

Class polynomials for  $T_{6+6}$  continued

-39	$X^{12} + 331533513X^{11} - 37343773800X^{10} + 1399867647340X^9 - 5390301072384X^8 + 5162293391355X^7 +$ $2191648182621X^6 - 339786317862X^5 + 13943818206X^4 - 140724149X^3 + 691722X^2 - 963X + 1$
-40	$X^{16} - 425670800X^{15} + 49965941112X^{14} - 1848032773840X^{13} + 23618989732508X^{12} + 352945014869040X^{11} -$ $8883048242697656X^{10} + 139245187265282800X^9 - 278616280004972730X^8 + 43806873084101200X^7 +$ $18126252062110344X^6 + 217535583987600X^5 - 8751987701092X^4 - 829016560X^3 - 1252488X^2 + 20560X + 1$
-43	$X^{12} + 884736660X^{11} - 63700846206X^{10} + 1496984221300X^9 - 12634001239185X^8 + 28203637156200X^7 -$ $4267079045220X^6 + 782759084947677000X^5 + 153944392815X^4 - 30965791100X^3 + 884737794X^2 - 60X + 1$
-47	$X^{10} + 2257839248X^9 - 76060099328X^8 + 1324679257433X^7 + 42083241652X^6 + 52565849413X^5 -$ $3147543948X^4 + 33027383X^3 + 317247X^2 + 1523X + 1$
-51	$X^{18} + 5541101154X^{17} - 88038594567X^{16} + 24986327520336X^{15} - 1898445886850988X^{14} - 25467728192165160X^{13} +$ $221971926087756260X^{12} + 128857387556345913072X^{11} + 135454643722637821134X^{10} +$ $587462237704994149100X^9 - 19895137599681284850X^8 + 10461033327450765744X^7 + 5358981223195665828X^6 -$ $638850941969150952X^5 + 17832547913573268X^4 - 10140407672304X^3 + 5544363321X^2 - 1854X + 1$
-52	$X^{16} - 6896961680X^{15} + 728905711992X^{14} - 31154725977040X^{13} + 1212950886928028X^{12} -$ $46015905689046480X^{11} + 1063046328840239944X^{10} - 7957674420585693200X^9 + 8306214282327520070X^8 -$ $2881343942098362800X^7 + 7569165131953039944X^6 - 14352373718436720X^5 + 573276281488028X^4 -$ $13885438960X^3 + 5071992X^2 - 83120X + 1$
-55	$X^{16} + 13136686960X^{15} + 96572727672X^{14} - 77781993539905X^{13} + 2656034361944648X^{12} - 15797539034298930X^{11} +$ $23715491975774869X^{10} + 24963754278522025X^9 - 110652143924999430X^8 + 321289886589298075X^7 -$ $10670474836538006X^6 + 1624678711085715X^5 - 6686495476327X^4 + 13131321605X^3 + 142197X^2 - 545X + 1$

Class polynomials for  $T_7^+$ 

$d_K$	$M(X)$
-3	$X^2 + 224X + 2^6 7$
-4	$X^4 - 528X^3 - 9024X^2 - 5120X - 2^6 3^3$
-7	$X^7 + 4046X^6 - 64799X^5 + 16442335X^4 + 14883071X^3 + 199370017X^2 - 45950625X + 3^6 5^6$
-8	$X^8 - 7328X^7 + 655872X^6 + 1089536X^5 + 155062656X^4 - 53286912X^3 - 60612608X^2 + 81920000X + 2^{12} 5^6$
-11	$X^8 + 33440X^7 - 1912512X^6 + 55881728X^5 - 288411648X^4 + 905576448X^3 + 706478080X^2 - 335544320X + 2^{30}$
-15	$X^{16} + 192369X^{15} - 4197822X^{14} + 36690860290X^{13} - 163529712045X^{12} - 65044892382876X^{11} +$ $1704591507792516X^{10} - 2505702562602048X^9 - 67969082190335805X^8 + 167035279593002305X^7 +$ $663879166228328673X^6 + 1049388677706960192X^5 + 2834231398559323714X^4 + 4280232188870316000X^3 +$ $2854209050476272000X^2 + 237249749088000000X + 3^{12} 5^6 11^6$
-19	$X^6 + 885424X^5 - 41419776X^4 + 481543168X^3 + 799436800X^2 + 2916089856X + 2^2 4_3 6^6$
-20	$X^{12} - 1262664X^{11} - 1440391392X^{10} - 42495512640X^9 - 8112990421824X^8 + 808445735009280X^7 -$ $21041946583953408X^6 + 219888953506455552X^5 - 893322424093364224X^4 + 1140179566145536000X^3 +$ $264014113311232000X^2 - 145077211136000000X + 2^{18} 5^6 11^6$

Class polynomials for  $T_7^+$  continued

<p>-23</p>	$  \begin{aligned}  & X^{24} + 3493766X^{23} - 676554757X^{22} + 12306680102585X^{21} - 2158492576201234X^{20} + 309126414910160449X^{19} - \\  & 2000226508654704099X^{18} + 30065120873346028564X^{17} - 13996148587444115625944X^{16} + \\  & 287664810475508599808229X^{15} - 635171143388389029445537X^{14} - 9236955195828154190126444X^{13} - \\  & 116498956029172724347403308X^{12} + 309453050295745494762312584X^{11} + \\  & 3068105138424147011053040488X^{10} + 21675608104870118264521261440X^9 + \\  & 111528516232026898865027867821X^8 + 222014002984361521245720506171X^7 + \\  & 315669218290467854756212075163X^6 + 273009826706388968115485720000X^5 + \\  & 83841175737062197175618093750X^4 - 10600495534355481045937500000X^3 - \\  & 219547559093271046875000000X^2 + 6737075195778125000000000X + 5^{18}11^617^6  \end{aligned}  $
<p>-24</p>	$  \begin{aligned}  & X^{12} - 4833568X^{11} + 11571739408X^{10} - 2012852637952X^9 + 15204068799424X^8 + 493204380225536X^7 + \\  & 11141216141178880X^6 - 31850426719240192X^5 + 184900908191444992X^4 + 1598968808958984192X^3 + \\  & 7770514603029626880X^2 - 2102123472092135424X + 2^{18}3^{12}17^6  \end{aligned}  $
<p>-31</p>	$  \begin{aligned}  & X^{18} + 39493319X^{17} - 8250436889X^{16} + 1560555239669203X^{15} - 299366679263556508X^{14} + \\  & 27174822822968821420X^{13} - 1221404151387353265615X^{12} + 38541440958671434700136X^{11} - \\  & 983734726309308798928392X^{10} + 15352937085011540598251104X^9 - 871633553614969809126185535X^8 - \\  & 485304462788606182653667268X^7 + 6797762798684684689979504236X^6 + 5198996470274846151658855934X^5 + \\  & 15552216996770866329027732871X^4 + 44481688662919854197910480894X^3 + \\  & 39328394250111260745114374031X^2 + 14996548962329654972629035450X + 3^{12}11^617^623^6  \end{aligned}  $
<p>-35</p>	$  \begin{aligned}  & X^{14} + 117966128X^{13} - 64263867584X^{12} + 31012270600192X^{11} - 1012068160495616X^{10} - \\  & 16897601508343808X^9 + 1097232374489939968X^8 - 17132395598314471424X^7 + 146468146059675697152X^6 - \\  & 1135700799373354991616X^5 + 12288138394985274802176X^4 + 19899478484833009664000X^3 + \\  & 14275688439625023488000X^2 + 2462906046218240000000X + 2^{54}5^6  \end{aligned}  $

Class polynomials for  $T_{13}$ 

$d_K$	$M(X)$
-3	$X^4 + 247X^3 + 3380X^2 + 15379X + 13^4$
-4	$X^6 - 494X^5 - 20618X^4 - 237276X^3 - 1313806X^2 - 3712930X - 13^6$
-7	$X^{14} + 4121X^{13} + 196885X^{12} + 21099988X^{11} + 778915592X^{10} + 15274994020X^9 + 189124030238X^8 + 1610126946220X^7 + 9858921494006X^6 + 44326807379140X^5 + 146681435327336X^4 + 351263437231252X^3 + 582452128062025X^2 + 605750213184506X + 13^{13}$
-8	$X^{14} - 7254X^{13} + 196885X^{12} + 21099988X^{11} + 778915592X^{10} + 15274994020X^9 + 189124030238X^8 + 1610126946220X^7 + 9858921494006X^6 + 44326807379140X^5 + 146681435327336X^4 + 351263437231252X^3 + 582452128062025X^2 + 605750213184506X + 13^{13}$
-11	$X^{14} + 33514X^{13} + 196885X^{12} + 21099988X^{11} + 778915592X^{10} + 15274994020X^9 + 189124030238X^8 + 1610126946220X^7 + 9858921494006X^6 + 44326807379140X^5 + 146681435327336X^4 + 351263437231252X^3 + 582452128062025X^2 + 605750213184506X + 13^{13}$
-19	$X^{14} + 885482X^{13} + 196885X^{12} + 21099988X^{11} + 778915592X^{10} + 15274994020X^9 + 189124030238X^8 + 1610126946220X^7 + 9858921494006X^6 + 44326807379140X^5 + 146681435327336X^4 + 351263437231252X^3 + 582452128062025X^2 + 605750213184506X + 13^{13}$

Class polynomials for  $T_{13}$  continued

-15	$ \begin{aligned} & X^{28} + 192517X^{27} + 22167561X^{26} + 37945909521X^{25} + 4102427924205X^{24} + 158293585287864X^{23} + \\ & 3692997358070800X^{22} + 75297864866902678X^{21} + 1635781777040094996X^{20} + 34309009887325754750X^{19} + \\ & 608312177602763685584X^{18} + 8747783018654113786872X^{17} + 102311767411731958491242X^{16} + \\ & 985711414281403819070633X^{15} + 7919484344402419724886990X^{14} + 53567960766537878544818909X^{13} + \\ & 307088013249663196351250918X^{12} + 1497995548412338418226807504X^{11} + \\ & 6227553692297321607854120204X^{10} + 22044017169162111048563523080X^9 + \\ & 66206147925305350064193694824X^8 + 167603559212992177879621935736X^7 + \\ & 353929820478880625564779799020X^6 + 613743867510637352334311327472X^5 + \\ & 853658596177231164124251319665X^4 + 918418903473434907609539350812X^3 + \\ & 719753821516415299935135448686X^2 + 366933320773074466633598464036X + 13^{26} \end{aligned} $
-20	$ \begin{aligned} & X^{28} - 1262508X^{27} - 1623465714X^{26} - 248526687604X^{25} - 26598582115495X^{24} - 975048073961936X^{23} - \\ & 18532500815879700X^{22} - 199882327230143272X^{21} - 706993182883660504X^{20} + 19964032640509674600X^{19} + \\ & 543815564695930507084X^{18} + 8534357863216956723472X^{17} + 101800670328974556049942X^{16} + \\ & 984863931873770371145008X^{15} + 7918602962698480939044340X^{14} + 53567520075685909151897584X^{13} + \\ & 307088013249663196351250918X^{12} + 1497995548412338418226807504X^{11} + \\ & 6227553692297321607854120204X^{10} + 22044017169162111048563523080X^9 + \\ & 66206147925305350064193694824X^8 + 167603559212992177879621935736X^7 + \\ & 353929820478880625564779799020X^6 + 613743867510637352334311327472X^5 + \\ & 853658596177231164124251319665X^4 + 918418903473434907609539350812X^3 + \\ & 719753821516415299935135448686X^2 + 366933320773074466633598464036X + 13^{26} \end{aligned} $

Class polynomials for  $T_{13+}$ 

$d_K$	$M(X)$
-3	$X^4 + 234X^3 + 1417X^2 + 1872X + 2^6 13$
-4	$X^6 - 514X^5 - 13115X^4 - 46312X^3 - 65024X^2 - 16192X - 2^6 3^3$
-7	$X^{14} + 4077X^{13} + 36894X^{12} + 16650738X^{11} + 231506457X^{10} + 1734526521X^9 + 6868376476X^8 + 15276096342X^7 + 21236022366X^6 + 20339907354X^5 + 13443270438X^4 + 5043723984X^3 + 525386368X^2 - 120960000X + 3^6 5^6$
-8	$X^{14} - 7298X^{13} + 480519X^{12} + 10439988X^{11} + 264926207X^{10} + 1733195646X^9 + 6380832601X^8 + 15696948592X^7 + 24139991616X^6 + 20165119104X^5 + 7532706688X^4 + 1146921984X^3 + 695738368X^2 + 286720000X + 2^{12} 5^6$
-11	$X^{14} + 33470X^{13} - 1109433X^{12} + 32699316X^{11} + 145149823X^{10} + 1737965502X^9 + 8128189849X^8 + 14188614128X^7 + 13732165824X^6 + 20791560192X^5 + 28716167168X^4 + 15113060352X^3 + 85196800X^2 - 1174405120X + 2^{30}$
-15	$X^{28} + 192429X^{27} + 6192042X^{26} + 36792391077X^{25} + 1378638695577X^{24} - 35807601674286X^{23} + 221699117481296X^{22} + 13367940522206868X^{21} + 111214235171865033X^{20} + 778713781852397313X^{19} + 6324876077566066722X^{18} + 36856476087905463093X^{17} + 130549875041979162159X^{16} + 280718446506202235664X^{15} + 381777576859782135639X^{14} + 458312947019935381917X^{13} + 970716406662384319548X^{12} + 2300289267475985828094X^{11} + 3736872997334170473299X^{10} + 395749017001342255279X^9 + 2833177764973331986392X^8 + 1578702135495296077578X^7 + 973223023710110798274X^6 + 70166416471777237574X^5 + 392376105594559300474X^4 + 130790797741716606000X^3 + 21346905860658288000X^2 + 830374121808000000X + 3^{12} 5^6 11^6$
-19	$X^{14} + 885438X^{13} - 34336185X^{12} + 497873844X^{11} - 2357932161X^{10} + 1837645758X^9 + 44644390297X^8 - 17332497936X^7 - 203770152768X^6 + 33882900480X^5 + 471407259648X^4 + 306976849920X^3 - 12673875968X^2 - 31708938240X + 2^{30} 3^6$

Class polynomials for  $\mathcal{T}_{13}$  continued

-20	$ \begin{aligned} & X^{28} - 1262596X^{27} - 1518674158X^{26} - 125671335348X^{25} - 12621766087073X^{24} + 349481490549464X^{23} + \\ & 58829316859196X^{22} - 24822546373511432X^{21} + 108741652903973583X^{20} + 2709648928656192588X^{19} + \\ & 9718145855562736722X^{18} - 4497689319272299332X^{17} - 31663009157284742991X^{16} + \\ & 385153033765967684064X^{15} + 2158129423803672462464X^{14} + 4525986636520440769792X^{13} + \\ & 3197249194146559189248X^{12} - 5182792338835679533056X^{11} - 15809757760938441138176X^{10} - \\ & 17696459717086501584896X^9 - 4326086449924039876608X^8 + 18213531702465075478528X^7 + \\ & 34154218472751247130624X^6 + 32845632768175818932224X^5 + 19343847219000507367424X^4 + \\ & 6536837027112943616000X^3 + 907171215485960192000X^2 - 30871880990720000000X + 2^{24}5^611^6 \end{aligned} $
-23	$ \begin{aligned} & X^{36} + 3493852X^{35} - 397049574X^{34} + 12268438079537X^{33} - 1323247760219236X^{32} + 205454392609790679X^{31} + \\ & 11673551341333953692X^{30} + 358164948135481296876X^{29} - 6056214696145988471003X^{28} - \\ & 103700203525413810593791X^{27} + 630141600752857119174783X^{26} + 19650644581914166253734390X^{25} + \\ & 599064396493383390421890X^{24} - 470616727738362758582835470X^{23} - 1330026650511059984642852855X^{22} + \\ & 25882710655668652913990164381X^{21} + 204305682853607984738736861362X^{20} + \\ & 540804515830335387836252444806X^{19} - 257180798543191449054013827983X^{18} - \\ & 5229057845556860101236765189491X^{17} - 12575834674341414613901683966541X^{16} - \\ & 5865090897840193682181517892573X^{15} + 31787257436160887962427793459121X^{14} + \\ & 8488390225952529226776866417352X^{13} + 130221835587672689303390407190739X^{12} + \\ & 201536417255270151950095674813967X^{11} + 331706294505343423636109426336093X^{10} + \\ & 434857664539251196342169025975379X^9 + 396149630719126371950771858115233X^8 + \\ & 246118198833341355538720891209206X^7 + 10476614004493362154202595837782X^6 + \\ & 29391252199506549987973488632500X^5 + 4310272582108450347361161765625X^4 + \\ & 62295901027525052850527343750X^3 + 11787487168184566517333984375X^2 + \\ & 1379250674405926818847656250X + 5^{18}11^617^6 \end{aligned} $

## Appendix 4: Discriminants of class polynomials

This appendix contains the discriminants of selected class polynomials with degree 30 or less. The discriminants were factored into primes less than 2,000,000.

We can make several observations.

- (1) For Thompson series for  $\Gamma_0(N)$ , the absolute values of the discriminants of class polynomials are bounded by  $|d_K|$ .
- (2) For Thompson series for  $\Gamma_0(N)_+$ , the absolute values of the discriminants of class polynomials are bounded by  $|N d_K|$ .
- (3) For Thompson series for  $\Gamma_0(N) + e, f, g, \dots$ , the absolute values of the discriminants of class polynomials are bounded by  $|d_K \cdot e \cdot f \cdot g \dots|$ .

Discriminants of class polynomials for  $T_3$ 

$d_K$	Degree	Discriminant
-4	2	$2^4 3^9$
-7	4	$-3^{57} 5^6 7^2$
-8	2	$2^5 3^{13}$
-11	2	$2^6 3^{13} 11$
-15	6	$3^{15} 5^9 7^{12} 11^4 13^4$
-19	4	$-2^{42} 3^{57} 19^2$
-20	4	$2^{26} 3^{74} 5^6 11^2 17^2$
-23	6	$3^{18} 5^{20} 7^{12} 11^4 17^2 23^3$
-24	6	$2^{69} 3^{156} 13^4 17^2 19^4 23^2$
-31	12	$-3^{65} 11^{30} 13^{24} 17^{14} 23^{14} 29^8 31^6$
-35	4	$2^{50} 3^{74} 5^4 7^2 23^2$
-39	12	$-3^{69} 7^{60} 13^{14} 17^{14} 19^{16} 23^8 29^6 31^8 37^4$
-40	8	$2^{132} 3^{278} 5^{18} 17^8 29^6 31^4$
-43	4	$-2^{48} 3^{61} 5^6 7^4 43^2$
-47	10	$3^{54} 5^{60} 11^{26} 13^{16} 19^8 23^6 29^6 41^4 47^5$
-51	6	$2^{110} 3^{156} 7^{12} 17^3 31^4 47^2$
-52	8	$2^{128} 3^{274} 5^{36} 13^4 23^6 41^8 43^4$
-55	16	$3^{119} 5^{92} 11^{30} 19^{28} 23^{32} 29^{14} 37^8 41^{14} 47^{16} 53^8$
-56	8	$2^{130} 3^{340} 7^{12} 11^{16} 17^6 29^6 41^2 47^4 53^2$
-59	6	$2^{114} 3^{183} 11^4 13^4 23^4 47^2 59^3$
-67	4	$-2^{42} 3^{57} 5^6 7^4 11^6 31^4 67^2$
-68	8	$2^{132} 3^{340} 5^{36} 17^8 19^4 29^4 41^6 47^2 59^4$
-71	14	$3^{109} 7^{84} 11^{44} 13^{36} 17^{30} 23^{12} 31^8 41^6 47^6 53^6 59^6 71^7$
-79	20	$-3^{189} 7^{180} 17^{54} 29^{22} 37^{16} 41^{16} 43^{12} 47^{22} 53^{14} 59^{22} 61^8 71^{16}$ $79^{10}$
-83	6	$2^{116} 3^{183} 5^{20} 13^4 47^4 71^2 83^3$

Discriminants of class polynomials for  $T_5$ 

$d_K$	Degree	Discriminant
-3	2	$2^4 5^5$
-4	2	$2^2 5^7$
-7	6	$3^{24} 5^{77} 7^2$
-8	6	$2^{38} 5^{77} 7^4$
-11	4	$-2^{28} 5^{39} 11$
-15	10	$3^{48} 5^{247} 7^{20} 11^{10} 13^8$
-19	4	$-2^{28} 3^8 5^{39} 19$
-20	10	$2^{126} 5^{247} 11^{10} 13^8 17^8 19^2$
-23	18	$5^{789} 7^{84} 11^{44} 17^{24} 19^{16} 23^8$
-24	8	$2^{80} 3^{30} 5^{174} 13^4 17^4 19^6$
-31	12	$-3^{124} 5^{405} 11^{18} 13^{16} 17^8 23^8 29^4 31^5$
-35	10	$2^{228} 5^{247} 7^{12} 19^2 23^8 31^2$
-39	16	$3^{142} 5^{732} 7^{64} 13^{16} 17^{20} 19^{18} 23^8 29^{12} 31^8 37^4$
-40	10	$2^{136} 3^{88} 5^{247} 17^8 29^8 31^2$
-43	6	$2^{84} 3^{28} 5^{77} 7^4 43^2$
-51	8	$2^{140} 3^{30} 5^{174} 7^{12} 17^4 31^6$
-52	12	$2^{188} 3^{124} 5^{340} 13^6 23^{12} 41^{12} 43^4$
-55	20	$-3^{388} 5^{1044} 11^{33} 19^{26} 23^{28} 29^{16} 37^8 41^{16} 47^{16} 53^8$
-56	16	$2^{364} 5^{732} 7^{38} 11^{38} 17^{20} 29^8 31^8 37^4 41^{12} 43^4 47^4 53^4$
-59	12	$-2^{332} 5^{405} 11^{20} 13^{16} 23^4 31^4 47^4 59^5$
-67	6	$2^{72} 3^{24} 5^{77} 7^4 11^{12} 31^4 67^2$
-68	24	$2^{856} 5^{1424} 17^{36} 19^{40} 29^{24} 37^{12} 41^{24} 43^4 47^{24} 59^{16} 61^{12} 67^4$
-71	28	$-5^{2289} 7^{228} 11^{128} 13^{104} 17^{72} 23^{44} 31^{32} 41^{24} 47^{16} 53^{12} 59^{12} 61^{12} 67^4 71^{13}$
-79	20	$-3^{388} 5^{1155} 7^{108} 17^{32} 29^{20} 37^{12} 41^8 43^4 47^{12} 53^8 59^{18} 61^4 71^8 79^9$

Discriminants of class polynomials for  $T_6$ 

$d_K$	Degree	Discriminant
-3	3	$-2^{14}3^{11}$
-4	4	$-2^{30}3^{19}$
-7	4	$-2^{36}3^{19}7^2$
-8	4	$2^{32}3^{26}5^2$
-11	6	$2^{76}3^{63}11^3$
-15	6	$2^{90}3^{52}5^37^411^2$
-19	12	$-2^{332}3^{213}19^6$
-20	8	$2^{144}3^{116}5^811^417^2$
-23	6	$2^{90}3^{63}5^611^223^3$
-24	12	$2^{348}3^{230}13^417^419^423^2$
-31	12	$-2^{396}3^{217}11^823^831^6$
-35	12	$2^{350}3^{270}5^{18}7^623^6$
-39	12	$-2^{396}3^{233}7^{16}13^619^423^631^4$
-40	16	$2^{640}3^{396}5^{24}17^829^831^4$
-43	12	$-2^{356}3^{225}5^{24}7^{12}43^6$
-47	10	$2^{270}3^{185}5^{18}11^613^423^447^5$
-51	18	$2^{792}3^{534}7^{36}17^931^{12}47^6$
-52	16	$2^{632}3^{392}5^{48}13^823^841^843^4$
-55	16	$2^{720}3^{396}5^{24}11^{16}19^423^{16}47^8$
-56	16	$2^{636}3^{488}7^{16}11^{20}17^829^641^447^453^2$
-59	18	$2^{798}3^{621}11^{18}13^{12}23^{12}47^659^9$
-67	12	$-2^{332}3^{213}5^{24}7^{12}11^{24}31^{12}67^6$
-68	16	$2^{640}3^{488}5^{48}17^{12}19^429^441^647^459^4$
-71	14	$2^{546}3^{371}7^{24}11^{10}13^817^623^647^459^271^7$
-79	20	$-2^{1140}3^{623}7^{52}17^843^447^{16}59^871^879^{10}$
-83	18	$2^{816}3^{621}5^{66}13^{12}47^{12}71^683^9$

Discriminants of class polynomials for  $T_{6+2}$ 

$d_K$	Degree	Discriminant
-3	3	$-2^8 3^{21}$
-4	4	$-2^{12} 3^{39} 7^2$
-7	4	$-3^{39} 5^2 7^6 13^2$
-8	4	$2^{14} 3^{50} 5^2 7^2 13^2$
-11	6	$2^{46} 3^{123} 7^4 11^3 13^2 19^2$
-15	6	$3^{108} 5^7 7^{12} 11^6 13^4$
-19	12	$-2^{200} 3^{437} 13^{10} 19^{10} 29^2 31^8 37^2$
-20	8	$2^{60} 3^{228} 5^{12} 11^8 13^6 17^2 19^4 31^2 37^2$
-23	6	$3^{123} 5^{12} 7^4 11^6 19^6 23^3 37^2 43^2$
-24	12	$2^{150} 3^{468} 13^{16} 17^8 19^8 23^6 37^4 41^4 43^4$
-31	12	$-3^{449} 11^{24} 13^{10} 17^8 23^8 31^{10} 37^{10} 43^8 53^2 61^2$
-35	12	$2^{218} 3^{534} 5^{36} 7^{18} 19^8 23^6 31^4 37^4 43^6 61^2 67^2$
-39	12	$-3^{465} 7^{40} 13^{14} 17^{10} 19^8 23^{18} 31^8 37^4 53^4 67^4 73^4$
-40	16	$2^{280} 3^{796} 5^{60} 17^{16} 29^8 31^{14} 43^8 61^8 67^8 71^2 73^8 79^2$
-43	12	$-2^{224} 3^{449} 5^{54} 7^{32} 19^8 37^2 43^{10} 61^2 73^8$
-47	10	$3^{365} 5^{36} 11^{10} 13^{14} 19^6 23^4 29^4 31^8 43^4 47^5 67^6 73^4$
-51	18	$2^{486} 3^{1080} 7^{84} 17^{17} 31^{20} 37^8 47^{14} 59^4 61^4 73^4 79^4 83^4 89^4 97^4$
-52	16	$2^{272} 3^{800} 5^{104} 13^{24} 23^{10} 37^8 41^{16} 43^{12} 73^8 79^2 97^8 103^2$
-55	16	$3^{796} 5^{60} 11^{32} 19^{20} 23^{16} 29^2 37^8 47^{16} 61^{10} 67^8 79^8 97^8 101^2 103^8$ $109^2$
-56	16	$2^{276} 3^{968} 7^{42} 11^{40} 17^{24} 29^{10} 31^{10} 37^6 41^4 43^4 47^4 53^2 67^8 73^4 97^4$ $103^2 109^2$
-59	18	$2^{492} 3^{1233} 11^{50} 13^{38} 23^{20} 31^8 37^{10} 43^6 47^6 59^9 61^4 67^4 73^8 97^4$ $103^4 109^2$
-67	12	$-2^{200} 3^{437} 5^{56} 7^{32} 11^{24} 13^{10} 31^{20} 53^2 61^8 67^{10} 97^8 109^2$
-68	16	$2^{280} 3^{968} 5^{104} 17^{12} 19^{20} 29^8 37^8 41^{10} 43^8 47^4 59^4 61^2 67^4 73^8 97^4$ $103^4 109^6 127^2$

Discriminants of class polynomials for  $T_{6+6}$ 

$d_K$	Degree	Discriminant
-3	3	$-2^8 3^3 5^2 11^2$
-4	4	$-2^{12} 3^7 7^2 11^2 19^2$
-7	4	$-3^7 5^4 7^2 13^2 19^2 31^2$
-8	4	$2^{14} 3^2 5^4 7^2 29^2 31^2 37^2$
-11	6	$2^{46} 3^3 7^6 11^7 13^2 19^2 29^2 41^2 43^2 61^2$
-15	6	$3^{12} 5^7 7^6 11^4 29^2 37^2 43^2 59^2 67^2 71^2 73^2$
-19	12	$-2^{200} 3^{81} 13^{10} 19^{10} 29^4 31^2 37^4 41^2 53^2 59^4 67^2 71^2 79^4 89^2 97^2$ $103^2 107^2 109^2$
-20	8	$2^{60} 3^4 5^{12} 11^{10} 13^6 17^8 19^2 31^2 37^2 53^2 59^2 71^2 73^2 79^2 97^2 113^2$
-23	6	$3^3 5^{16} 7^6 11^4 23^3 37^2 67^2 79^2 97^2 107^2 109^2$
-24	12	$2^{150} 3^{54} 13^{14} 17^{14} 19^{16} 23^8 37^2 41^2 43^2 47^2 61^2 67^4 71^2 89^4 109^4$ $113^2 137^2 139^2$
-31	12	$-3^{85} 11^{22} 13^{10} 17^8 23^{18} 29^6 31^{10} 37^2 53^4 61^4 73^2 79^2 83^2 89^2$ $127^2 137^2 139^2 151^4 167^2 179^2 181^2$
-35	12	$2^{218} 3^{65} 5^{40} 7^{18} 19^6 23^{10} 31^6 37^2 41^4 43^2 53^2 59^2 61^2 67^4 89^2 101^2$ $107^2 113^2 127^2 131^2 137^2 139^2 163^2 181^2 193^2 197^2 199^2$
-39	12	$-3^{57} 7^{36} 13^{10} 17^{10} 19^{16} 23^8 29^8 31^8 37^2 53^2 67^2 97^2 107^2 109^4$ $113^2 131^2 151^2 163^2 173^2 179^4 191^2 193^2 223^2 229^2$
-40	16	$2^{280} 3^{156} 5^{64} 7^{22} 29^{18} 31^{12} 43^2 61^2 67^2 71^2 73^2 79^4 83^2 97^4 101^2$ $107^4 109^2 113^2 137^2 149^4 151^2 163^4 181^2 191^2 193^2 199^2 227^2$ $229^2 233^2$
-43	12	$-2^{224} 3^{93} 5^{60} 7^{36} 19^6 29^2 37^4 43^6 61^2 71^4 89^2 131^2 137^2 149^2$ $151^2 157^2 179^2 191^2 199^2 211^2 227^2 241^2$
-47	10	$3^5 5^{44} 11^{10} 13^{14} 19^6 23^8 29^4 31^2 41^2 43^2 47^5 107^2 109^2 151^2 163^4$ $179^2 181^2 193^2 199^2 211^2 223^2 229^2 233^2$
-51	18	$2^{486} 3^{126} 7^{90} 17^{19} 31^{22} 37^6 47^{10} 53^8 59^8 61^2 73^2 79^2 83^2 97^4 101^4$ $109^2 137^2 139^2 149^2 163^4 179^2 181^4 191^4 193^2 199^2 211^4 239^2$ $241^4 251^4 263^2 277^2 281^2 283^2 293^2$

Discriminants of class polynomials for  $T_{7+}$ 

$d_K$	Degree	Discriminant
-3	2	$2^8 3^3 7$
-4	4	$-2^{26} 3^{12} 7^3 11^2 23^2$
-7	7	$-3^{56} 5^{22} 7^9 13^6 17^6 19^4 31^2 41^4 47^2$
-8	8	$-2^{130} 5^{30} 7^{15} 13^6 23^4 29^4 37^2 47^2 53^2$
-11	8	$-2^{210} 7^{15} 11^8 13^6 17^6 19^4 29^2 41^2$
-15	16	$3^{216} 5^{86} 7^{66} 11^{58} 13^{44} 29^{14} 37^{10} 41^{10} 43^8 59^4 67^4 71^4 73^6 89^4 97^4$ $101^2 103^2$
-19	6	$2^{114} 3^{38} 7^5 13^4 19^3 29^2 41^2 53^2 89^2 113^2$
-20	12	$2^{318} 5^{50} 7^{10} 11^{30} 13^{30} 17^{22} 19^{14} 31^6 37^6 53^4 59^4 71^4 73^2 79^2 97^2$ $113^4 131^2 137^2$
-23	24	$-5^{386} 7^{153} 11^{146} 17^{78} 19^{68} 23^{32} 37^{24} 43^{20} 53^{16} 61^{10} 67^{12} 79^8$ $83^8 89^{12} 97^6 103^4 107^8 109^6 113^{10} 137^8 149^6 157^2$
-24	12	$2^{322} 3^{118} 7^{10} 13^{24} 17^{22} 19^{14} 23^{16} 37^6 41^6 43^4 47^4 61^2 67^2 71^2 89^2$ $109^2 113^4 137^2 139^2 157^2 163^2$
-31	18	$3^{474} 7^{15} 11^{76} 13^{60} 17^{48} 23^{36} 29^{28} 31^{17} 37^{18} 43^{14} 53^{12} 61^8 73^8 79^4$ $83^4 89^8 127^4 137^{10} 167^6 179^4 181^2 197^6 199^2$
-35	14	$2^{708} 5^{67} 7^{32} 19^{20} 23^{22} 31^8 37^8 41^8 43^6 53^6 59^6 67^4 89^4 101^2 113^4$ $137^4 193^2 197^2 233^2$
-40	12	$2^{322} 3^{208} 5^{56} 7^{10} 17^{22} 29^{12} 31^8 43^4 71^4 73^2 83^2 101^2 107^2 109^2$ $113^2 137^4 149^2 163^2 181^2 191^2 227^2 233^2 239^2 257^2 269^2$
-43	8	$-2^{224} 3^{82} 5^{32} 7^{15} 19^4 29^2 37^2 43^4 71^2 89^2 113^2 137^2 233^2 257^2$
-51	16	$2^{926} 3^{216} 7^{66} 17^{22} 31^{18} 37^{10} 47^{10} 53^{10} 59^6 61^6 73^6 79^2 83^4 89^2$ $97^4 137^4 149^2 181^2 193^2 241^2 257^2 277^2 281^2 313^2 337^2$
-52	12	$2^{318} 3^{200} 5^{92} 7^{10} 13^{18} 23^{14} 37^6 41^{14} 43^4 73^2 89^4 103^2 107^2 131^2$ $137^2 191^2 193^2 197^2 211^2 251^2 263^2 281^2 293^2 311^2 317^2 347^2$ $353^2$

Discriminants of class polynomials for  $T_{13}$ 

$d_K$	Degree	Discriminant
-3	4	$-2^4 3^1 13^{15}$
-4	6	$2^{10} 3^6 13^{35}$
-7	14	$3^{60} 5^{24} 7^6 13^{169}$
-8	14	$2^{90} 5^{24} 7^{12} 13^{169}$
-11	14	$2^{156} 7^{12} 11^6 13^{169}$
-15	28	$3^{168} 5^{66} 7^{80} 11^{36} 13^{704}$
-19	14	$2^{156} 3^{60} 13^{169} 19^6$
-20	28	$2^{444} 5^{66} 11^{36} 13^{704} 17^{28} 19^{12}$
-24	28	$2^{446} 3^{168} 13^{704} 17^{24} 19^{28} 23^{12}$
-35	24	$2^{544} 5^{48} 7^{30} 13^{574} 19^8 23^{20} 31^8$
-40	24	$2^{338} 3^{228} 5^{48} 13^{574} 17^{20} 29^{16} 31^8$
-43	12	$-2^{128} 3^{52} 5^{16} 7^8 13^{143} 43^5$
-51	24	$2^{540} 3^{122} 7^{56} 13^{574} 17^{12} 31^{20} 47^8$
-52	26	$2^{382} 3^{258} 5^{112} 13^{637} 23^{20} 41^{24} 43^{10}$
-67	14	$2^{156} 3^{60} 5^{24} 7^{12} 11^{24} 13^{169} 31^{12} 67^6$
-88	24	$2^{336} 3^{226} 5^{100} 7^{56} 11^{30} 13^{574} 17^{16} 41^{16} 59^{20} 79^8$
-91	26	$2^{652} 3^{256} 7^{36} 11^{68} 13^{637} 17^{20} 71^{24}$

Discriminants of class polynomials for  $T_{13+}$ 

$d_K$	Degree	Discriminant
-3	4	$-2^{20}3^75^211^213^3$
-4	6	$2^{34}3^{18}7^611^413^523^247^2$
-7	14	$3^{142}5^{60}7^{20}13^{13}17^{10}19^831^441^247^659^673^283^489^2$
-8	14	$2^{214}5^{60}7^{40}13^{13}23^829^631^637^247^453^461^271^4101^2$
-11	14	$2^{370}7^{40}11^{16}13^{13}17^{10}19^829^441^443^283^4107^2131^2$
-15	28	$3^{384}5^{158}7^{192}11^{104}13^{56}29^{24}37^{14}41^{18}43^{18}59^{12}67^{12}71^{10}73^4$ $89^897^2101^4103^6127^6131^6149^4157^4163^6179^4191^2193^2$
-19	14	$2^{370}3^{142}13^{13}19^829^631^437^241^253^459^467^271^2107^4167^2179^2$ $227^2$
-20	28	$2^{956}5^{162}11^{104}13^{56}17^{68}19^{48}31^{22}37^{14}53^{14}59^{12}71^{12}73^479^6$ $97^2113^6131^4137^4151^2157^2173^4179^4191^4193^2197^6199^2$ $211^2233^4239^4251^2257^2$
-24	28	$2^{972}3^{384}13^{56}17^{64}19^{60}23^{44}37^{14}41^{14}43^{18}47^{16}61^667^{10}71^{10}$ $89^6109^4113^2137^6139^2157^4163^2167^4181^2191^2211^2229^2$ $233^2239^2257^4263^2277^4281^2283^2307^2$
-35	24	$2^{1186}5^{122}7^{80}13^{22}19^{36}23^{42}31^{24}37^{10}41^843^{14}53^{10}59^{10}61^8$ $67^689^{10}101^4107^8113^6131^4137^4139^2163^2251^4263^2311^2$ $347^4419^2443^2$
-40	24	$2^{740}3^{490}5^{120}13^{22}17^{48}29^{32}31^{18}43^{14}61^267^871^{10}79^483^897^6$ $101^2107^8113^4137^2149^4151^2191^4227^2233^4239^2257^2269^2$ $311^4313^2347^2349^2353^2359^4389^2421^2431^2443^4457^2461^2$ $467^2479^2509^2$
-43	12	$-2^{294}3^{114}5^{44}7^{30}13^{11}19^629^243^771^2113^2131^2137^2163^2$ $191^2227^2347^2383^2467^2491^2$
-51	24	$2^{1186}3^{286}7^{142}13^{22}17^{28}31^{32}37^{10}47^{26}53^{10}59^{10}61^279^683^6$ $89^697^6109^2137^4139^4149^2163^6179^2199^2211^2251^2263^2$ $283^4359^2379^2443^4487^2491^2499^2547^2563^2571^2587^2619^2$ $643^2$

### Appendix 5: Resultants of class polynomials

This appendix contains some resultants of the class polynomials for  $T_2$ ,  $T_7$ ,  $T_{7+}$ . We note that the resultants are highly factorizable numbers.

Resultants of class polynomials for  $T_2$

$d_1$	$d_2$	Resultant of $M_1(X)$ and $M_2(X)$
-3	-4	$-2^8 \cdot 3$
	-7	$2^8 \cdot 3 \cdot 5$
	-8	$2^{16} \cdot 5^2$
	-11	$-2^{31}$
	-15	$-2^{16} \cdot 3^2 \cdot 5 \cdot 11$
-4	-7	$2^9 \cdot 3^2$
	-8	$-2^{19} \cdot 7$
	-11	$-2^{24} \cdot 7^2 \cdot 11$
	-15	$2^{18} \cdot 3^2 \cdot 7^2$
-7	-8	$2^{18} \cdot 5^2 \cdot 7$
	-11	$-2^{24} \cdot 7 \cdot 14 \cdot 17 \cdot 19$
	-15	$-2^{24} \cdot 3^2 \cdot 5$
-8	-11	$2^{48} \cdot 7^4 \cdot 13^2$
	-15	$2^{36} \cdot 5^2 \cdot 7^2 \cdot 13^2$
-11	-15	$-2^{48} \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 29 \cdot 41$

Resultants of class polynomials for  $T_7$ 

$d_1$	$d_2$	Resultant of $M_1(X)$ and $M_2(X)$
-3	-4	$-2^6 \cdot 3^3 \cdot 7^{14}$
	-7	$3^5 \cdot 5^5 \cdot 7^{26}$
	-8	$2^{12} \cdot 5^6 \cdot 7^{28}$
	-11	$2^{30} \cdot 7^{28}$
	-15	$3^{12} \cdot 5^6 \cdot 7^{56} \cdot 11^6$
-4	-7	$3^{21} \cdot 7^{49}$
	-8	$-2^{28} \cdot 7^{57}$
	-11	$-2^{24} \cdot 7^{57} \cdot 11^4$
	-15	$3^{24} \cdot 7^{114} \cdot 11^8$
-7	-8	$5^{21} \cdot 7^{98} \cdot 13^7$
	-11	$-7^{98} \cdot 13^7 \cdot 17^7 \cdot 19^7$
	-15	$-3^{42} \cdot 5^{21} \cdot 7^{196} \cdot 13^{14}$
-8	-11	$2^{48} \cdot 7^{114} \cdot 13^8$
	-15	$5^{24} \cdot 7^{228} \cdot 13^{16} \cdot 29^8$
-11	-15	$7^{228} \cdot 11^8 \cdot 13^{16} \cdot 29^8 \cdot 41^8$

Resultants of class polynomials  $T_{7+}$ 

$d_1$	$d_2$	Resultant of $M_1(X)$ and $M_2(X)$
-3	-4	$-2^{12} \cdot 3^6 \cdot 11^2 \cdot 47 \cdot 83 \cdot 131$
	-7	$3^{10} \cdot 5^{11} \cdot 17 \cdot 47 \cdot 101 \cdot 167 \cdot 227 \cdot 251 \cdot 257$
	-8	$2^{24} \cdot 5^{13} \cdot 23^2 \cdot 71^2 \cdot 173 \cdot 269 \cdot 293$
	-11	$2^{64} \cdot 11^2 \cdot 17 \cdot 29^2 \cdot 41 \cdot 83 \cdot 101$
	-15	$3^{24} \cdot 5^{12} \cdot 11^{10} \cdot 29^2 \cdot 41^2 \cdot 59^2 \cdot 89 \cdot 131 \cdot 311 \cdot 419 \cdot 461 \cdot 479 \cdot 509 \cdot 521$
-4	-7	$3^{46} \cdot 7^4 \cdot 19^3 \cdot 31 \cdot 59^2 \cdot 131^2 \cdot 167^2 \cdot 199 \cdot 307$
	-8	$-2^{56} \cdot 7^9 \cdot 23^2 \cdot 31^3 \cdot 47^2 \cdot 103 \cdot 167 \cdot 223 \cdot 271 \cdot 311 \cdot 367 \cdot 383$
	-11	$-2^{48} \cdot 7^9 \cdot 11^6 \cdot 19^3 \cdot 43^2 \cdot 79^2 \cdot 107^2 \cdot 139 \cdot 283 \cdot 439 \cdot 503 \cdot 523$
	-15	$3^{48} \cdot 7^{18} \cdot 11^{18} \cdot 43^2 \cdot 59 \cdot 67^2 \cdot 71^4 \cdot 103^2 \cdot 127^2 \cdot 223^2 \cdot 251 \cdot 283^2 \cdot 307^2 \cdot 367^2 \cdot 479 \cdot 719$
-7	-8	$5^{42} \cdot 7^8 \cdot 13^4 \cdot 31^4 \cdot 47^2 \cdot 61 \cdot 101^2 \cdot 157 \cdot 181^2 \cdot 271^2 \cdot 293^2 \cdot 311^2 \cdot 397 \cdot 461 \cdot 661 \cdot 677$
	-11	$-7^8 \cdot 13^{14} \cdot 17^{13} \cdot 19^{11} \cdot 41^2 \cdot 61^2 \cdot 73 \cdot 83^2 \cdot 131 \cdot 241 \cdot 293 \cdot 523 \cdot 563 \cdot 601 \cdot 733 \cdot 761 \cdot 787 \cdot 811 \cdot 853 \cdot 887 \cdot 937 \cdot 941$
	-15	$-3^{84} \cdot 5^{42} \cdot 7^{16} \cdot 13^{28} \cdot 41^3 \cdot 59^5 \cdot 73^4 \cdot 89^3 \cdot 103^4 \cdot 157^4 \cdot 269^3 \cdot 311^3 \cdot 367^2 \cdot 433^2 \cdot 523^2 \cdot 577^2 \cdot 607^2 \cdot 643^2$
-8	-11	$2^{96} \cdot 7^{18} \cdot 13^{16} \cdot 29^4 \cdot 61^3 \cdot 79^2 \cdot 101^3 \cdot 151^2 \cdot 239^2 \cdot 263^2 \cdot 349 \cdot 359^2 \cdot 853 \cdot 997 \cdot 1069$
	-15	$5^{48} \cdot 7^{36} \cdot 13^{32} \cdot 29^{16} \cdot 37^6 \cdot 71^2 \cdot 101 \cdot 127^2 \cdot 149^4 \cdot 157^2 \cdot 191^4 \cdot 223^2 \cdot 239^4 \cdot 397^2 \cdot 463^2 \cdot 487^2 \cdot 509 \cdot 607^2 \cdot 727^2 \cdot 733^2 \cdot 941 \cdot 1109 \cdot 1181 \cdot 1301$
-11	-15	$-7^{36} \cdot 11^{18} \cdot 13^{32} \cdot 29^{14} \cdot 41^{13} \cdot 43^6 \cdot 73^2 \cdot 101^4 \cdot 127^2 \cdot 131^4 \cdot 193^2 \cdot 277^2 \cdot 373^2 \cdot 457^2 \cdot 461 \cdot 547^2 \cdot 613^2 \cdot 673^2 \cdot 761 \cdot 1091 \cdot 1151 \cdot 1319 \cdot 1559 \cdot 1601 \cdot 1811 \cdot 1889 \cdot 1931 \cdot 1949 \cdot 1979$

## References

- [1] Alexander D., Cummins, C, McKay, J., and Simons, C., *Completely replicable functions*, in “Groups, Combinatorics and Geometry (LMS Lecture Note Series **165**)”, ed. M. W. Liebeck and J. Saxl, Cambridge University Press, 1992, pp. 87–95.
- [2] Birch, B., *Weber’s class invariants*, *Mathematik* **16** (1969), pp. 283–294.
- [3] Birch, B., *Some calculations of modular relations*, in *Modular Functions of One Variable I*, *Lecture Notes in Mathematics* **320**, Springer-Verlag, 1973, pp. 177–186.
- [4] Borel, A., Chowla, S., Herz, C., Iwasawa, K., and Serre, J.-P., (eds.), *Seminar on Complex Multiplication*, *Lecture Notes in Mathematics* **21**, Springer-Verlag, 1966.
- [5] Borcherds, R., *Monstrous moonshine and monstrous Lie superalgebras*, *Inventiones Math.* **109** (1992), pp. 405–444.
- [7] Cohn, H., *Introduction to the construction of class fields*, *Cambridge studies in advanced mathematics* **6**, Cambridge University Press, 1985.
- [8] Conway, J. and Norton, S., *Monstrous moonshine*, *Bull. London Math. Soc.* **11** (1979), pp. 308–339.
- [9] Cox, D., *Primes of the form  $x^2 + ny^2$* , John Wiley & Sons, 1989.
- [10] Ferenbaugh, C., *On the modular functions involved in “Monstrous moonshine”*, Ph.D. Thesis, Princeton University, 1992.
- [11] Ford, D., McKay, J., and Norton, S., *More on replicable functions*, *Communications in Algebra* **22** (13) (1994), pp. 5175–5193.
- [12] Frenkel, I., Leopowsky, J. and Meurman, A., *Vertex Operator Algebras and the Monster*, Academic Press, New York, 1988.
- [13] Fricke, R., *Die Elliptische Funktionen und Ihre Anwendungen*, 2-ter Teil, Teubner, Leipzig, 1922.
- [14] Fricke, R., *Lehrbuch der Algebra III (Algebraische Zahlen)*, Vieweg, Braunschweig, 1928.
- [15] Gross, B., *Heegner points and the modular curve of prime level*, *J. Math. Soc. Japan*, **39**, No. 2 (1987), pp. 345–362.
- [16] Gross, B. and Zagier, D., *On singular moduli*, *J. Reine Angew Math.* **355** (1985), pp. 191–220.
- [17] Koike, M., *On replication formula and Hecke operators*, Preprint.
- [18] Laing, A., *Shimura reciprocity for modular functions with rational Fourier coefficients*, in “Advances in Number Theory”, *Proc. of CNTA ’91*, Oxford University Press, 1993, pp. 271–280.
- [19] Lang, S., *Elliptic Functions*, Addison–Wesley, 1973.
- [20] Mahler, K., *On a class of non-linear functional equations*, *J. Austral. Math. Soc.* **22A** (1976), pp. 65–118.
- [21] Norton, S., *More on Moonshine*, in “Computational Group Theory”, ed. M.D. Atkinson, Academic Press, 1984, pp. 185–193.
- [22] Norton, S., *Generalized Moonshine*, in “Proc. Symp. Pure Math.” **47** (1987), pp. 208–209.
- [23] Ogg, A., *Automorphismes de courbes modulaires*, *Séminaire Delange–Pisot–Poitou (Théorie des nombres)* **16** année (1974/75), No. 7, pp. 7-01–7-08.
- [24] Schertz, R., *Die singulären Werte der Weberschen Funktionen  $f, f_1, f_2, \gamma_2, \gamma_3$* , *J. Reine Angew Math.* **286/287** (1976), pp. 46–74.
- [25] Shimura, G., *Introduction to the Theory of Automorphic Functions*, Iwanami Publishing Company and Princeton University Press, 1974.

- [26] Siegel, C., *Transcendental numbers*, Annals of Math. Studies **16**, Princeton University Press, 1949.
- [27] Söhngen, H., *Zur komplexen Multiplikation*, Math. Annalen **111** (1935), pp. 302–328.
- [28] Thompson, J.G., *A finiteness theorem for subgroups of  $PSL_2(\mathbb{R})$  which are commensurable with  $PSL_2(\mathbb{Z})$* , Symposia in Pure Math. **37** (1980), pp. 533–555.
- [29] Weber, H., *Lehrbuch der Algebra*, Bd. III, Braunschweig, 1908.
- [30] Yui, N., and Zagier, D., *On the singular values of Weber modular functions*, Preprint MPIM Bonn, 1994.
- [31] Yui, N., *Explicit form of the modular equation*, J. Reine Angew. Math. **299/300** (1978), pp. 185–200.

Imin Chen  
Mathematical Institute  
University of Oxford  
24–29 St. Giles, Oxford  
England OX1 3LB  
email: chen@maths.oxford.ac.uk

Noriko Yui  
Department of Mathematics and Statistics  
Queen’s University  
Kingston, Ontario  
Canada K7L 3N6  
email: yui@ny.mast.queensu.ca