MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 155-170

HOW BRANCHING PROPERTIES DETERMINE MODULAR EQUATIONS

HARVEY COHN

Dedicated to D. H. Lehmer

Abstract. If a prime p is decomposed as x^2+4y^2, the power $2^m||y$ can be determined by an algorithm of polynomial efficiency based on use of singular moduli from the modular equation of order 2. The properties of the modular functions required in this algorithm are simple branching and parametrization properties, which in turn define the modular functions and equations (essentially uniquely). The well-known equations of "Klein's Icosahedron" and their Hecke analogues come into play here, and to some extent they can be uniquely characterized in this fashion. The extraneous cases which arise are in some sense interesting analogues of modular equations.

1. The power conductor algorithm

The motivating problem for this work comes out of a type of algorithm [2] of ring class field theory.

A prime $p \equiv 1 \bmod 4$ admits a (unique) representation in $\mathbf{Z}$ as a sum of squares. We shall consider only the additional power of 2 dividing the even square, namely the m for which

$$p = x^2 + 4y^2, \quad 2^m||y. \tag{1.1a}$$

The (polynomial-time) algorithm for m generates a sequence $\{a_0, a_1, \dots, a_{m-1}\}$ of length m as follows:

$$\begin{aligned} a_0 &= 9/8, \qquad r_k^2 \equiv a_k, \\ a_{k+1} &\equiv (r_k+3)^2/[8(r_k+1)] \mod p. \end{aligned} \tag{1.1b}$$

The last k for which $(a_k/p) = 1$ (or for which r_k is definable) defines the length of the sequence as $m = k+1$. (Incidentally, the method is independent of the choice of the sign of the square root in r_k.) This is illustrated below for $89 = 5^2 + 4 \cdot 4^2$ (where $m = 2$):

Received by the editor September 2, 1992.
1991 *Mathematics Subject Classification*. Primary 11F11, 11Y16.
Key words and phrases. Klein and Hecke modular functions, modular equations.
Research supported in part by NSF Grant CCR-8901064.

$$(1.1\text{c}) \qquad a_0 \equiv 79 \equiv \begin{cases} 41^2 \Rightarrow a_1 \equiv 10 \equiv \begin{cases} 30^2 \Rightarrow a_2 \equiv 27, \\ (-30)^2 \Rightarrow a_2 \equiv 31, \end{cases} \\ (-41)^2 \Rightarrow a_1 \equiv 50 \equiv \begin{cases} 36^2 \Rightarrow a_2 \equiv 77, \\ (-36)^2 \Rightarrow a_2 \equiv 60. \end{cases} \end{cases}$$

These are congruences modulo 89, and of course 27, 31, 77, and 60 are all nonresidues.

This algorithm is explainable in terms of modular functions if we write

$$(1.2\text{a}) \qquad p = X^2 + 4(2^m Y)^2$$

and note the condition for solvability is that p split completely when factored in the *ring class field*

$$(1.2\text{b}) \qquad K_m = \mathbf{Q}(i, j(2^{m+1}i)).$$

(The discriminant is $-16 \cdot 4^m$ and the "extra factor" 2^m is the conductor, hence the name of the algorithm.)

Here, $j(\tau)$ is the Klein (or Weber) modular function (see §3 below). We need the sequence (of *singular moduli*) $j(2i)$, $j(4i)$, $j(8i)$, ..., which we soon see involves a succession of quadratic field adjunctions. These fields are hopeless to write explicitly, but only the quadratic character modulo p is required in the algorithm.

The natural question arises on whether the use of transcendentals should be eliminated in the interests of number theoretic "purity". This action seems to be unfeasible at present, but the transcendental level might also be warranted by the fact that (as we show) the branching process of (1.1b) essentially determines both the modular equation (between $j(\tau)$ and $j(2\tau)$) and the modular function itself. The determination is almost unique, with the Hecke modular function appearing as an "extraneous" solution.

It is a classical exercise to interpret modular relations (including modular equations) as functional equations which generate coefficients of power series (and identities, congruence relations, etc., see Lehmer [7]). This idea was used again by Mahler [8] to generalize the relations and thereby extend the concept of modular functions. More recently, similar devices were used by Conway, McKay, Norton, and others (see [4, 1]) to study group representations. The present paper will be more restrictive, limited to properties deduced primarily from the theory of compact Riemann surfaces and not from local series (at $j = \infty$).

2. Role of the branching process

The relation between $j(\tau) = z$ and $j(2\tau) = w$ is the *symmetric* modular equation of order 2,

$$(2.1\text{a}) \qquad \begin{gathered} z^3 + w^3 - z^2w^2 + 2^4 3 \cdot 31(z^2w + w^2z) - 2^4 3^5 5^3(z^2 + w^2), \\ 3^4 5^3 4027 zw + 2^8 3^7 5^6(z + w) - 2^{12} 3^9 5^9 = 0. \end{gathered}$$

This seems paradoxical since the operation $\tau \rightarrow 2\tau$ is not symmetric, but the matter can be explained (see [3]) by the fact that there are three roots for w, given z, so

$$z = j(\tau) \Rightarrow w = \{j(2\tau),\ j(\tau/2),\ j((\tau+1)/2)\}. \tag{2.1b}$$

In the sense of analytic continuation, these roots are indistinguishable, so that the modular equation can be considered as a method of generating $j(\tau/2^m)$ as well as $j(2^m\tau)$ from $j(\tau)$.

The process of finding w from z can be designated as part of an iterated chain

$$j(2\tau) \to \begin{cases} j(\tau) \to \begin{cases} j(\tau/2), \\ j((\tau+1)/2), \end{cases} \\ *** \end{cases} \tag{2.1c}$$

(where the missing term "$***$" is $j((2\tau+1)/2)$).

We now see that the algorithm duplicates the pattern of the branching

$$j(\tau) \to \begin{cases} j(\tau/2) \to \begin{cases} j(\tau/4), \\ j((\tau+2)/4), \end{cases} \\ j((\tau+1)/2) \to \begin{cases} j((\tau+1)/4), \\ j((\tau+3)/4). \end{cases} \end{cases} \tag{2.1d}$$

We shall find it notationally more convenient to iterate the sequence

$$j(\tau) \to j(\tau/2) \to j(\tau/4) \to \cdots. \tag{2.1e}$$

To complete the connection with the algorithm, note that (2.1a) is parametrized [5] by

$$z = 64(t+4)^3/t^2, \tag{2.2a}$$

$$w = 64(u+4)^3/u^2, \tag{2.2b}$$

$$u = 1/t. \tag{2.2c}$$

Now to go from $z = j(\tau)$ to $w = j(\tau/2)$, we would clearly solve (2.2a) for three values of t and use (2.2c) to find three values of u, one of which makes (2.2b) produce $w = j(\tau/2)$ (compare (2.1b)).

If, however, we attempted to go to $j(\tau/4)$ by repeating the steps (mechanically), we would have difficulty since (2.2c) returns us to the original t and to $j(\tau)$, not $j(\tau/4)$. The method is to avoid *reversible* steps by taking s (instead of t), one of the two other conjugates of t in the solution of (2.2a), and by setting $u = 1/s$ in (2.2c) (rather than $u = 1/t$). Thus, the other root s ($\neq t$) is found from the quadratic

$$\frac{s^2t^2}{s-t}\left(\frac{(s+4)^3}{s^2} - \frac{(t+4)^3}{t^2}\right) = 0, \tag{2.3a}$$

$$s^2t^2 - 48st - 64(s+t) = 0, \tag{2.3b}$$

$$s = 8(3t+4 \pm (t+4)\sqrt{t+1})/t^2. \tag{2.3c}$$

We introduce ζ as a second *uniformizing parameter* and find

$$\zeta^2 = t+1, \tag{2.4a}$$

$$s = 8(1+\zeta)/(1-\zeta)^2, \tag{2.4b}$$

$$1/s \to t, \qquad t+1 \to (\zeta+3)^2/[8(1+\zeta)]. \tag{2.4c}$$

If we refer to (1.1b), a_k is $t+1$ in (2.4a) and a_{k+1} is $t+1$ in (2.4b). The initial value is set by the fact that $j(2i) = j(i/2) = 66^3$ (the value of z in (2.2a)). For this z, we have $t = 1/8$ and $a_0 = 9/8$. This verifies the algorithm.

Our ultimate goal is to use the properties of the algorithm to derive both the modular equation and $j(\tau)$.

3. Branching patterns of modular equations

We shall consider the usual modular function $j(\tau)$ (see [10]) as one of three related functions $j_M(\tau)$ (for which $M = 1$). The others are those of Hecke (see [9]).

For the index $M = 1, 2,$ or 3, we define the modular group

$$G_M = \langle \tau \to -1/\tau,\ \tau \to \tau + \sqrt{M} \rangle, \tag{3.1a}$$

which defines a discrete group on the upper half plane

$$H:\ \Im(\tau) > 0. \tag{3.1b}$$

Its fundamental domain is given (with boundary identifications under (3.1a)) by

$$|\Re(\tau)| \leq \sqrt{M}/2, \qquad |\tau| \geq 1, \tag{3.1c}$$

with fixed points of order 2 at $\tau = i$ and of order $B = \pi/\arccos(\sqrt{M}/2)$ at the $(2B)$th roots of unity:

$$\rho_M = \frac{\pm\sqrt{M} + i\sqrt{4-M}}{2}. \tag{3.1d}$$

The fundamental domain is uniformized by the holomorphic modular function

$$j_M(\tau) = 1/q + c_0 + c_1 q + c_2 q^2 + c_3 q^3 + \cdots, \tag{3.2a}$$

$$q = \exp 2\pi i\tau/\sqrt{M}, \tag{3.2b}$$

so $j_M = \infty$ (and $q = 0$) exactly when $\Im(q) = \infty$. The choice of j_M is fixed by conditions on two additional points

$$j_M(\rho_M) = 0, \qquad j_M(i) = H_M. \tag{3.2c}$$

Some values which will be useful for identification later on are in the table below (compare [9]):

(3.2d)

M	H_M	c_0	c_1	c_2	c_3
1	1728	744	196884	21493760	86429970
2	256	104	4372	96256	1240002
3	108	42	783	8672	65367

As a matter of convenience, we shall also refer to $j_1(\tau)$ by the more usual $j(\tau)$.

Our general objective shall be to examine branching properties of the modular equations

$$\Phi_{MN}(j_M(\tau), j_M(N\tau)) = 0 \tag{3.2e}$$

for $M = 1, 2, 3$ and $N = 2, 3, 4, 5$. Then we ask to what extent the modular equations and functions are unique consequences of the branching properties.

We now define the *branching patterns* of modular equations of order N for $j_M(\tau)$. The function $j_M(N\tau)$ satisfies a modular equation of degree k over $\mathbf{C}(j_M(\tau))$ as one of k conjugates

$$\text{(3.3a)}\qquad \left\{ j_M(N\tau),\ j_M\left(\frac{\tau}{N}\right),\ j_M\left(\frac{\tau+\sqrt{M}}{N}\right), \dots, \right. \\ \left. j_M\left(\frac{\tau+(N-1)\sqrt{M}}{N}\right), \dots \right\}.$$

(Possibly, $k > N+1$, see (3.4a) below.) If we denote

$$\text{(3.3b)}\qquad z = j_M(\tau), \qquad w = j_M(N\tau),$$

we find the various branches of w over z by analytic continuation are those given in the set (3.3a), so that at ∞ there is a pattern given by the types

$$\text{(3.3c)}\qquad w^t \approx z^u\omega$$

for ω a root of unity. For example, from just the $N+1$ items specified in (3.3a),

$$\text{(3.3d)}\qquad w \approx z^N, \qquad z \approx w^N$$

are always valid relations for the branches at ∞. If these are the only relations (i.e., $k = N+1$), call the branching pattern *simple.* (Note that the symbol $A \approx B$ is used in the *strict* meaning $A/B \to 1$.)

The branching patterns are shown in Tables I–V (at the end of the paper). To illustrate with a nonsimple pattern ($k > N+1$), for example, take Φ_{14} in Table III. Here we have the branches

$$\text{(3.4a)}\qquad \begin{aligned} &z = j(\tau), \\ &w = j(4\tau),\ j\left(\frac{\tau}{4}\right),\ j\left(\frac{\tau+1}{4}\right),\ j\left(\frac{\tau+2}{4}\right), \\ &\qquad j\left(\frac{\tau+3}{4}\right),\ j\left(\frac{2\tau+1}{2}\right). \end{aligned}$$

The first value of w leads to $w \approx z^4$, the next four values represent roots $w \approx z^{1/4}$, best written as $z \approx w^4$. The last value of w in (3.4a) comes out to be $w \approx -z$ (since for $\tau \to \tau + 1/2$, $q \to -q$). In summary, for Φ_{14}, the branching at ∞ has the pattern

$$\text{(3.4b)}\qquad w \approx z^4, \qquad z \approx w^4, \qquad z \approx -w.$$

4. Uniqueness results from parametrization restrictions

We start with modular equations of order N and degree k, but of genus zero,

$$\text{(4.1a)}\qquad z = j_M(\tau), \qquad w = j_M(N\tau), \qquad \Phi_{MN}(z, w) = 0.$$

This equation is parametrized by equations of degree k,

$$\text{(4.1b)}\qquad z = f(t), \qquad w = g(t).$$

Definition. Call an irreducible equation in z and w *strongly* uniformly parametrized when it has genus zero and, for the representation of either z or w (say w) the factors (in $\mathbf{C}$) of

$$g(s) - g(t) = 0 \tag{4.1c}$$

are curves of genus zero. (There is more than one factor, since $s-t$ is trivially a factor.) Call the equation *weakly* uniformly parametrized if there is at least one nontrivial factor (not $s-t$) in (4.1c) which is of genus zero. (Here "weak" includes "strong".)

We used strong uniformity in the algorithm of §1 to represent the branching (see (2.4a, b)) where s is a two-valued function of t. For purposes of the algorithm, it would have been sufficient to have weak uniformity (see §9 below).

Main Problem. Given a branching pattern generated by a weakly uniform modular equation, does this pattern determine the modular equation uniquely (to within an additive constant on the modular functions)?

Uniqueness results. For the simple branching pattern $w \approx z^2$, $z \approx w^2$ corresponding to the modular equations

$$\Phi_{12}(j(2\tau), j(\tau)) = 0 \quad \text{and} \quad \Phi_{32}(j_3(2\tau), j_3(\tau)) = 0, \tag{4.2a}$$

there is essentially a *unique* common strongly uniform equation with a parameter yielding these two cases (see Table I). For the simple branching pattern $w \approx w^3$, $z \approx w^3$ corresponding to the modular equations

$$\Phi_{13}(j(3\tau), j(\tau)) = 0 \quad \text{and} \quad \Phi_{23}(j_2(3\tau), j_2(\tau)) = 0, \tag{4.2b}$$

there are essentially *two* strongly uniform equations, one for each equation (see Table II). In all these cases, the result would be the same if we replaced "strongly uniform" by "weakly uniform".

Other results on modular equations of genus zero. These equations are strongly uniform (see Tables III and V):

$$\begin{gathered} \Phi_{22}(j_2(2\tau), j_2(\tau)) = 0, \qquad \Phi_{14}(j(4\tau), j(\tau)) = 0, \\ \Phi_{15}(j(5\tau), j(\tau)) = 0. \end{gathered} \tag{4.3a}$$

These equations are (only) weakly uniform (see Table IV):

$$\begin{gathered} \Phi_{33}(j_3(3\tau), j_3(\tau)) = 0, \quad \Phi_{34}(j_3(4\tau), j_3(\tau)) = 0, \\ \Phi_{24}(j_2(4\tau), j_2(\tau)) = 0. \end{gathered} \tag{4.3b}$$

Finally, the character of this case is unknown at present (see Table V):

$$\Phi_{25}(j_2(5\tau), j_2(\tau)) = 0. \tag{4.3c}$$

(Indeed no claim of uniqueness for a given branching pattern is made in any of the cases (4.3a–c).)

For the simple branching cases Φ_{15} and Φ_{25} the modular equations of Table V are shown embedded in a one-parametric family of equations with the same branching, but (again) it is not known whether or not the families are unique. (The "missing" case Φ_{35} is of genus one.)

5. Preliminary considerations

We know two facts ahead of time concerning the modular relations of (3.2e)

$$(5.1) \qquad \Phi_{MN}(z, w) = 0 \quad \text{for } z = j_M(\tau), \ w = j_M(N\tau).$$

First of all, the relation must be symmetric, since for given z, the k ($\geq N+1$) conjugates w include not only $j_M(N\tau)$ but also $j_M(\tau/N)$ (as seen in the listings of Tables I–V). Furthermore, the poles of z must occur only where there are poles of w.

Simplifying Lemma. *In the cases where $\Phi_{MN}(z, w)$ is of genus zero, on the basis of branching patterns alone, we can restrict the parametrization of the relation* (5.1) *to*

$$(5.2) \qquad z = R(t) \quad (= A(t)/B(t)), \qquad w = R(u), \qquad tu = 1,$$

(*with polynomials $A(t)$ and $B(t)$*) *as follows*:

1. *The degree of $A(t)$ is k $(\geq N+1)$, while the degree of $B(t)$ is $k-1$, so the poles of z consist at least of $t = \infty$* (*simple pole*) *and $t = 0$* (*zero of order N for $B(t)$ with $A(0) \neq 0$*).

2. *Furthermore, when $k > N+1$, there is another set of $k - N - 1$ poles t* (*namely the roots of $B(t)/t^N$*) *invariant under $t \to 1/t$.*

For a proof, start with a parametrization $z = R(t)$ and $w = S(t)$, for which (by linear change of parameter) $t = \infty$ produces $w \approx z^N$ and $t = 0$ produces $z \approx w^N$. Then the symmetry validates $z = S(u)$ and $w = R(u)$. Thus, we have a one-to-one mapping of the t-sphere onto the u-sphere which is linear and indeed involutory in such a manner as to interchange 0 and ∞. The involution must be $tu = \text{constant}$, reducible to $tu = 1$ by a scaling of t and u. The rest follows from the branching pattern.

6. The true modular equations and "pseudomodular equations"

In each one of the cases of (3.2e) except $M = 3$, $N = 5$ the modular equation is of genus zero. This equation can be derived from the branching information, augmented by the knowledge of the fixed points of (3.2c). The classic cases were worked out for $j(\tau)$ by Klein and Fricke (see [5] and [3]) and the analogues for Hecke's $j_M(\tau)$ are routinely similar. (The single most powerful tool is the fact that $j_M(\tau)$ and $j_M(\tau) - H_M$ have known multiple roots corresponding to the fixed points.)

In those cases of simple branching (poles only at $t = 0$ and $t = \infty$) any parametrization retains its branching pattern (adjusting for constant factors on z and w) under

$$(6.1) \qquad t \to t/g, \qquad u \to ug.$$

Essentially, $R(t)$ has just acquired an *essential* parameter g. Now the transformation (6.1), of course, cannot affect the parametrizability restrictions of §4 (above). Therefore there is an infinite set of of solutions to the *parametrization as a functional equation* formed by eliminating t in the following:

$$(6.2a) \qquad z = R(t) = 1/q + c_0 + c_1 q + c_2 q^2 + c_3 q^3 + \cdots,$$

(6.2b) $$w = R(1/t) = 1/q^N + c_0 + c_1 q^N + c_2 q^{2N} + c_3 q^{3N} + \cdots,$$

with $q = 0$ (i.e., $\Im(\tau) = \infty$) at $t = \infty$. (A suitable change of variables from $t = \infty$ to $T = 0$ simplifies the manipulation of the power series, see Tables I, II, and V.) The coefficients c_0, c_1, c_2, and c_3 are listed to help identify the functions.

Thus, with the usual notation $q = \exp 2\pi i\tau/\sqrt{M}$, we then obtain a solution of the parametrization equation, say $z = j^*(\tau)$, with the property that $w = j^*(N\tau)$ is one branch of w. Of course, the other branches will be somewhat amorphous in general, although for certain values of g which belong to a *modular equation,* other branches will be identifiable in familiar fashion as $j^*(\tau/N)$, etc. These are in a sense "pseudomodular" functions parametrized by g.

The most remarkable case is for $N = 2$ (Table I), where two values $g = 4$ and 2 link $j(\tau)$ and $j_3(\tau)$ to the same parametrization.

Naturally, in the cases of nonsimple branching ($k > N + 1$), the scaling (6.1) will be invalid except for trivial cases (like $g = -1$), since it violates condition 2 of the lemma in §5. In these cases, the functional equations (like (6.2a, b)) would lead only to the true modular functions, so no further attention was given to the power series (see Tables III and IV).

7. Uniqueness proofs

We have only to verify that the cases in Tables I and II are unique for the (simple) branching patterns under the additional requirement of weakly uniform parametrization. In other words, for $w \approx z^N$ and $z \approx w^N$, Table I (for $N = 2$) and Table II (for $N = 3$) show the only parametric equations for which $w(t) - w(s)$ has at least one nontrivial factor which is a curve of genus zero. (It will happen that *all* factors are of genus zero, leading to strongly uniform parametrization.) It is understood, as before, that "uniqueness" holds only to within a common additive constant for both z and w. So we can make an a priori assumption that z and w have at least one multiple factor by choice of this constant. Also, we can ignore any multiplicative constant on z or w since they are not essential to the parametrization. Finally, we shall work with w since the lower power of t in the denominator is advantageous. The details are plethoric, so "obvious" trivial cases shall be ignored, as many other details.

Uniqueness for $N = 2$. We start with

(7.1a) $$w(t) = (t+1)^2(t+a)/t.$$

This is, by linear transformations,

(7.1b) $$t \to \lambda t + \mu, \qquad w \to \rho w + \sigma,$$

the most general form of w for the simple branching pattern. The only values of a for which $w(s) - w(t)$ has a nontrivial factor of genus zero are $a = 1$ and $a = -8$. These are recognized as belonging to the parametric relation in Table I.

We verify that

(7.1c) $$(w(s) - w(t))st/(s-t) = ts(s+t) + (a+2)ts - a.$$

Solving this quadratic for s, we obtain the fourth-degree discriminant

$$D(t) = (t^2 + (a+2)t)^2 + 4at, \tag{7.1d}$$

which now must have a double root. The condition on its *cubic* factor is

$$(a+2)^3 = 27a, \tag{7.1e}$$

which produces the roots $a = 1, -8$. We can easily recognize the polynomials in (7.1a),

$$w(t) = (t+1)^3/t, \quad (t+1)^2(t-8)/t \tag{7.1f}$$

in the *common* parametric forms for Φ_{12} and Φ_{32} in Table I.

Uniqueness for $N = 3$. We start with

$$w(t) = (t+1)^2(t+b)(t+c)/t. \tag{7.2a}$$

This is again, by linear transformations,

$$t \to \lambda t + \mu, \qquad w \to \rho w + \sigma, \tag{7.2b}$$

the most general form of w for the simple branching pattern. The only values of (b, c) for which $w(s) - w(t)$ has a nontrivial factor of genus zero are four root pairs

$$(b, c) = (1, 9), (\alpha, \alpha), \quad \text{where } \alpha = (3 - 2\sqrt{3})/(3 + 2\sqrt{3}), \tag{7.2c}$$

$$(b, c) = (1, 1), (-7 + 2\sqrt{-8}, -7 - 2\sqrt{-8}). \tag{7.2d}$$

These are seen as producing (respectively) the polynomials

$$w(t) = (t+1)^3(t+9)/t, \quad (t^2 + 6t - 3)^2/t \tag{7.3a}$$

seen to be present in Φ_{13} (in Table II) and the polynomials

$$w(t) = (t+1)^4/t, \quad (t+1)^2(t^2 - 14t + 81)/t \tag{7.3b}$$

seen to be present in Φ_{23} (in Table II).

The verification is lengthier, since with the two unknowns b and c in (7.2a) we must invoke the method of "multiple roots" twice. To start,

$$(w(s) - w(t))st/(s-t) = st(s^2 + st + t^2) + st(s+t)C + stB - A, \tag{7.4a}$$

where A, B, C are the coefficients of $(t+1)^2(t+b)(t+c)$, namely

$$A = bc, \qquad B = 1 + bc + 2b + 2c, \qquad C = 2 + b + c. \tag{7.4b}$$

If we let $S = s + t$, $P = st$, then (7.4a) becomes

$$PS^2 - P^2 + PSC + PB - A = 0. \tag{7.4c}$$

This determines a subfield $\mathbf{C}(P, S)$, which has to be of genus zero since the same is expected of $\mathbf{C}(s, t)$. We rewrite (7.4c) as

$$P(S + C/2)^2 = P^2 - PE + A \qquad (E = B - C^2/4). \tag{7.4d}$$

Then the genus zero requirement becomes $E^2 = 4A$, or, from (7.4b),

$$(b + c - (b-c)^2/4)^2 = bc. \tag{7.4e}$$

If we substitute $b = \beta^2$ and $c = \gamma^2$, this leads to

$$(7.4f) \qquad \pm\beta \pm \gamma = 0 \text{ or } 2.$$

By symmetry, we reduce to two cases,

$$(7.4g) \qquad \beta = \gamma \quad \text{or} \quad \beta = \gamma + 2.$$

We now look for the second condition on b and c. We go from $\mathbf{C}(S, P)$ to $\mathbf{C}(s, t)$ by using the pefect square in (7.4d). We see

$$(7.5a) \qquad \left(\frac{st - E/2}{s + t + C/2}\right)^2 = st.$$

Now $\mathbf{C}(s, t) = \mathbf{C}(s, x)$ if $x^2 s = t$ with

$$(7.5b) \qquad x = \frac{st - E/2}{st + s^2 + Cs/2}.$$

Then the new equation in s,

$$(7.5c) \qquad s^2(x^2 - x - x^3) - xCs/2 - E/2 = 0,$$

leads to a discriminant

$$(7.5d) \qquad D = (Cx/2)^2 + 2E(x^2 - x - x^3)$$

with a double root when

$$(7.5e) \qquad C^2/4 + 2E = \pm 4E.$$

The plus sign leads us to Φ_{13}. If it is combined with $\beta = \gamma$, we obtain the first root pair of (7.2c), and with $\beta = \gamma + 2$ the second root pair. Likewise, the minus sign leads us to Φ_{23}. If it is combined with $\beta = \gamma$, we obtain the first root pair of (7.2d), and with $\beta = \gamma + 2$ the second root pair. This accounts for all weakly (and strongly) uniform parametrizations.

8. The parameters

Finally, let us examine the parameters. The parameters have a historical significance since they played a role in Klein's "Icosahedron" as the sphere undergoing the finite rotation groups [6]. Indeed, there it is shown in effect (see also [3]) that for the case Φ_{1N}, the sphere is actually the ζ-sphere, where

$$(8.1a) \qquad t = t(\zeta^N), \quad s = s(\zeta) \quad \text{for } N = 2, 3, 4,$$

$$(8.1b) \qquad t = t(\zeta^5 - \zeta^{-5}), \quad s = s(\zeta) \quad \text{for } N = 5.$$

Contrary to appearances, the relation in (8.1b) yields five values of s (not ten) for each t since $s(\zeta) = s(-1/\zeta)$ (see [2]).

Table I: The case Φ_{12} was handled in (2.4a, b) (and Φ_{32} is similar since it is connected by the parameter g).

Table II: The case Φ_{13} follows by setting $(b, c) = (1, 9)$ and uniformizing the discriminant in (7.5d) by $x = \xi^3/3$. Then (7.5c) yields s while (7.5a) yields t for Φ_{13} as follows:

$$(8.2a) \qquad 1 + 9/s = (1 - \xi)^3, \qquad 1 + 9/t = (1 - 3/\xi)^3.$$

So ζ is in effect $(1-3/\xi)$. More important, $s \to t$ under the linear fractional transformation

$$1 - 3/\xi \to 1 - 1/\xi. \tag{8.2b}$$

The case Φ_{23} is novel since it involves a nonabelian parameter. As before, we set $(b, c) = (1, 1)$ and uniformize the discriminant in (7.5d) by $x = -\xi^2$. Then (7.5c) yields s while (7.5a) yields t as follows:

$$1/s = \xi + \xi^2 + \xi^3, \qquad 1/t = 1/\xi + 1/\xi^2 + 1/\xi^3, \tag{8.3a}$$

$$[s \to t] \Leftarrow [\xi \to 1/\xi]. \tag{8.3b}$$

Table III: With the parameters shown in each case,

$$\Phi_{22}: \ [s \to t] \Leftarrow [\zeta \to -1-\zeta], \tag{8.4a}$$

$$\Phi_{14}: \ [s \to t] \Leftarrow [\zeta \to (\zeta-1)/(\zeta+1)]. \tag{8.4b}$$

Finally, we can see that in the Hecke cases Φ_{32}, Φ_{23}, and Φ_{22} an iterative algorithm exists which is algebraically analogous to that which was used in the Klein cases ($N = 1$) as an illustration of class field theory.

9. The modular equation of Klein and Hecke

The modular equation of Table I with parameter g is remarkable since it embraces both Klein's $j(\tau)$ and Hecke's $j_3(\tau)$. We start with the simultaneous equations of Table I (in the variable T), namely

$$zT = (1+g^4T)^3 \quad \text{and} \quad wT^2 = (1+g^2T)^3. \tag{9.1}$$

If we eliminate T, we obtain (ignoring a constant factor)

$$\begin{aligned} 0 = {} & -9g^8 + 36g^{10} - 84g^{12} + g^6 + 84g^{18} - g^{24} \\ & + 9g^{22} + 126g^{14} - 126g^{16} - 36g^{20} \\ & + (3g^{16} + 45g^8 + 3g^4 + 45g^{12} - 60g^{10} - 18g^6 - 18g^{14})z \\ & + (3g^{16} + 45g^8 + 3g^4 + 45g^{12} - 60g^{10} - 18g^6 - 18g^{14})w \\ & + (-9g^4 + 3g^2 + 9g^6 - 3g^8)z^2 \\ & + (-36g^8 - 1 + 35g^6 - 9g^4 + 9g^{10} + 2g^{12})wz \\ & - w^2z^2 + z^3 + w^3 + (-9g^4 + 3g^2 + 9g^6 - 3g^8)w^2 \\ & + (-3g^2 + 6g^4)wz^2 + (-3g^2 + 6g^4)w^2z. \end{aligned} \tag{9.2}$$

If we substitute $g = 4$ (for Klein), we get the familiar equation (2.1a) for $z = j(\tau)$ and $w = j(2\tau)$:

$$\begin{aligned} 0 = {} & 8748000000z + 8748000000w - 162000z^2 \\ & + 40773375wz - w^2z^2 + z^3 + w^3 - 162000w^2 \\ & + 1488wz^2 + 1488w^2z - 157464000000000; \end{aligned} \tag{9.3a}$$

and if we substitute $g = 2$ (for Hecke), we get the less familiar equation for $z = j_3(\tau)$ and $w = j_3(2\tau)$:

$$\begin{aligned} 0 = {} & 34992z + 34992w - 324z^2 + 10287wz - w^2z^2 \\ & + z^3 + w^3 - 324w^2 - 1259712 + 84wz^2 + 84w^2z. \end{aligned} \tag{9.3b}$$

TABLE I. Derivation of the modular functions $j(\tau)$ and $j_3(\tau)$ from the unique strongly uniform modular equation expressing the branching pattern $w \approx z^2$, $z \approx w^2$

$$\Phi_{12}: z = j(\tau),\ w = j(2\tau),\ j\left(\frac{\tau}{2}\right),\ j\left(\frac{\tau+1}{2}\right),$$

$$\Phi_{32}: z = j_3(\tau),\ w = j_3(2\tau),\ j_3\left(\frac{\tau}{2}\right),\ j_3\left(\frac{\tau+\sqrt{3}}{2}\right).$$

The modular equations belong to the unique family

$$z(t) = \frac{g^3(g+t)^3}{t^2} = \frac{27g^4}{4} + \frac{g^3(t-2g)^2(4t+g)}{4t^2},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{g^3(1+tg)^3}{t} = \frac{27g^4}{4} + \frac{g^3(2gt-1)^2(tg+4)}{4t}.$$

For the power series expansion set $t = 1/(Tg^3)$ ($T \to 0$),

$$\begin{aligned} z &= (1+g^4T)^3/T = 1/T + 3g^4 + 3g^8T + g^{12}T^2 \\ &= 1/q + c_0 + c_1q + c_2q^2 + c_3q^3 + \cdots, \\ w &= (1+g^2T)^3/T^2 = 1/T^2 + 3g^2/T + 3g^4 + g^6T \\ &= 1/q^2 + c_0 + c_1q^2 + c_2q^4 + c_3q^6 + \cdots. \end{aligned}$$

Comparing the power series, we find

$$c_0 = 3g^4 - \tfrac{3}{2}g^2,\quad c_1 = 3g^8 + \tfrac{9}{8}g^4 - \tfrac{3}{4}g^2,\quad c_2 = g^{12} + \tfrac{9}{2}g^{10} - \tfrac{1}{2}g^6,$$
$$c_3 = 3g^{14} + \tfrac{27}{8}g^{12} + \tfrac{9}{4}g^{10} + \tfrac{15}{128}g^8 + \tfrac{27}{32}g^6 + \tfrac{9}{32}g^4 - \tfrac{3}{8}g^2.$$

For $g = 4$ we have $j(\tau)$ and for $g = 2$ we have $j_3(\tau)$.

TABLE II. Derivation of the modular functions $j(\tau)$ and $j_2(\tau)$ from two uniquely determined strongly uniform modular equations expressing the branching pattern $w \approx z^3$, $z \approx w^3$

$$\Phi_{13}: z = j(\tau),\ w = j(3\tau),\ j\left(\frac{\tau}{3}\right),\ j\left(\frac{\tau+1}{3}\right),\ j\left(\frac{\tau+2}{3}\right).$$

The modular equation belongs to the unique family

$$z(t) = \frac{g^2(3t+g)(t+3g)^3}{t^3} = 64g^3 + \frac{3g^2(t^2-6gt-3g^2)^2}{t^3},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{g^2(gt+3)(3gt+1)^3}{t} = 64g^3 + \frac{3g^2(3g^2t^2+6gt-1)^2}{t}.$$

For the power series expansion, set $t = 1/(3g^2T)$ ($T \to 0$),

$$\begin{aligned} z &= (1+g^3T)(1+9g^3T)^3/T \\ &= 1/T + 28g^3 + 270g^6T + 972g^9T^2 + 729g^{12}T^3 \\ &= 1/q + c_0 + c_1q + c_2q^2 + c_3q^3 + \cdots, \\ w &= (1+9gT)(1+gT)^3/T^3 = 1/T^3 + 12g/T^2 + 30g^2/T + 28g^3 + 9g^4T \\ &= 1/q^3 + c_0 + c_1q^3 + c_2q^6 + c_3q^9 + \cdots. \end{aligned}$$

Comparing the power series, we find

$$\begin{aligned} c_0 &= -4g + 28g^3, \qquad c_1 = 6g^2 + 270g^6, \\ c_2 &= 972g^9 + 1080g^7 - \tfrac{8}{3}g^3 - \tfrac{4}{3}g, \\ c_3 &= 729g^{12} + 7776g^{10} + 2700g^8 - 3g^4. \end{aligned}$$

For $g = 3$ we have $j(\tau)$.

$$\Phi_{23}: \; z = j_2(\tau), \; w = j_2(3\tau), \; j_2\left(\frac{\tau}{3}\right), \; j_2\left(\frac{\tau+\sqrt{2}}{3}\right), \; j_2\left(\frac{\tau+2\sqrt{2}}{3}\right).$$

The modular equation belongs to the unique family

$$z(t) = \frac{g^2(t+g)^4}{t^3} = \frac{256g^3}{27} + \frac{g^2(t-3g)^2(27t^2+14gt+3g^2)}{27t^3},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{g^2(gt+1)^4}{t} = \frac{256g^3}{27} + \frac{g^2(3gt-1)^2(3g^2t^2+14gt+27)}{27t}.$$

For the power series expansion, set $t = 1/(g^2T)$ ($T \to 0$),

$$\begin{aligned} z &= (1+g^3T)^4/T = 1/T + 4g^3 + 6g^6T + 4g^9T^2 + g^{12}T^3 \\ &= 1/q + c_0 + c_1q + c_2q^2 + c_3q^3 + \cdots, \\ w &= (1+gT)^4/T^3 = 1/T^3 + 4g/T^2 + 6g^2/T + 4g^3 + g^4T \\ &= 1/q^3 + c_0 + c_1q^3 + c_2q^6 + c_3q^9 + \cdots. \end{aligned}$$

Comparing the power series, we find

$$\begin{aligned} c_0 &= 4g^3 - \tfrac{4}{3}g, \qquad c_1 = 6g^6 - \tfrac{2}{9}g^2, \\ c_2 &= 4g^9 + 8g^7 + \tfrac{88}{81}g^3 - \tfrac{4}{9}g, \\ c_3 &= g^{12} + \tfrac{32}{3}g^{10} + 12g^8 - \tfrac{1}{3}g^4. \end{aligned}$$

For $g = 3$ we have $j_2(\tau)$.

Table III. Other cases where the modular equation is strongly uniform

Branching pattern: $w \approx z^2, \; z \approx w^2, \; z \approx -w.$

$$\Phi_{22}: \; z = j_2(\tau), \; w = j_2(2\tau), \; j_2\left(\frac{\tau}{2}\right), \; j_2\left(\frac{\tau+\sqrt{2}}{2}\right), \; j_2\left(\tau+\frac{\sqrt{2}}{2}\right).$$

The corresponding modular equation is

$$z(t) = \frac{16(t+2)^4}{t^2(t+1)} = 256 + \frac{16(t^2-4t-4)^2}{t^2(t+1)},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{16(2t+1)^4}{t(t+1)} = 256 + \frac{16(4t^2+4t-1)^2}{t(t+1)}.$$

To prove strong uniformity, factor

$$w(t) - w(s) = 16\frac{(t+1+s)(t-s)(16t^2s^2+16t^2s+16ts^2+16ts-1)}{t(t+1)s(s+1)}.$$

The quadratic root shows genus zero: With $t = \zeta^2/(1-\zeta^2)$,

$$s = \frac{-2t^2-2t+(2t+1)\sqrt{t^2+t}}{4t^2+4t} = -\frac{(1+\zeta)^2}{4\zeta}.$$

Branching pattern: $w \approx z^4, \; z \approx w^4, \; w \approx -z.$

$$\Phi_{14}: \; z = j(\tau), \; w = j(4\tau), \; j\left(\frac{\tau}{4}\right), \; j\left(\frac{\tau \pm 1}{4}\right), \; j\left(\frac{\tau+2}{4}\right), \; j\left(\frac{2\tau+1}{2}\right).$$

The corresponding modular equation is

$$z(t) = \frac{16(t^2+16t+16)^3}{t^4(t+1)} = 1728 + \frac{16(t+2)^2(t^2-32t-32)^2)^2}{t^4(t+1)},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{16(16t^2+16t+1)^3}{t(t+1)} = 1728 + \frac{16(2t+1)^2(32t^2+32t-1)^2}{t(t+1)}.$$

To prove strong uniformity, factor

$$w(t) - w(s) = 16\frac{(t-s)(t+1+s)f}{(t(t+1)s(s+1)},$$

where, in the new variables $u = t(t+1)$ and $v = s(s+1)$, $f = 4096vu^2 + 768uv + 4096uv^2 - 1$,

$$f = 0 \quad \text{for } v = \frac{-4096u^2 - 768u + 128(16u+1)\sqrt{4u^2+u}}{8192u},$$

$$t = \frac{k^2}{1-k^2}, \quad u = \frac{k^2}{(1-k^2)^2}, \quad 4v+1 = (2s+1)^2 = \frac{(k^2+6k+1)^2}{16k(1+k)^2}.$$

With $k = \zeta^2$, $t = \zeta^4/(1-\zeta^4)$ and $s = (\zeta-1)^4/(8\zeta(1+\zeta^2))$ (showing genus zero).

TABLE IV. Cases where the modular equation is only weakly uniform

Branching pattern: $w \approx z^3$, $z \approx w^3$, $z \approx \omega w$, $w \approx \omega z$ $(\omega^2 + \omega + 1 = 0)$.

$$\Phi_{33}: \ z = j_3(\tau), \ w = j_3(3\tau), \ j_3\left(\frac{\tau}{3}\right), \ j_3\left(\frac{\tau+\sqrt{3}}{3}\right),$$

$$j_3\left(\frac{\tau+2\sqrt{3}}{3}\right), \ j_3\left(\tau + \frac{1}{\sqrt{3}}\right), \ j_3\left(\tau + \frac{2}{\sqrt{3}}\right).$$

The corresponding modular equation is

$$z(t) = \frac{3\sqrt{3}(t+\sqrt{3})^6}{t^3(t^2+t\sqrt{3}t+1)} = 108 + \frac{3\sqrt{3}(t^3 - 3\sqrt{3}t^2 - 9t - 9\sqrt{3})^2}{t^3(t^2+\sqrt{3}t+1)},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{3\sqrt{3}(\sqrt{3}t+1)^6}{t(t^2+\sqrt{3}t+1)} = 108 + \frac{3\sqrt{3}(9\sqrt{3}t^3 + 9t^2 + 3\sqrt{3} - 1)^2}{t(t^2+\sqrt{3}t+1)}.$$

To check for weak uniformity of the equation, factor

$$w\left(\frac{t}{\sqrt{3}}\right) - w\left(\frac{s}{\sqrt{3}}\right) = \frac{27(t-s)(t^2+3t+3+st+3s+s^2)f}{s(s^2+3s+3)t(t^2+3t+3)},$$

$$f = [(s+1)^3 - 1][(t+1)^3 - 1] - 1 \quad \text{(genus one)}.$$

Branching pattern: $w \approx z^4$, $z \approx w^4$, $w \approx -z$.

$$\Phi_{34}: \ z = j_3(\tau), \ w = j_3(4\tau), \ j_3\left(\frac{\tau}{4}\right), \ j_3\left(\frac{\tau \pm \sqrt{3}}{4}\right), \ j_3\left(\frac{\tau+2\sqrt{3}}{4}\right), \ j_3\left(\tau + \frac{\sqrt{3}}{2}\right).$$

The corresponding modular equation is

$$z(t) = \frac{4(t+2)^6}{t^4(t+1)} = 108 + \frac{4(t^2+t+1)(t^2-8t-8)^2}{t^4(t+1)},$$

$$z\left(\frac{1}{t}\right) = w(t) = \frac{4(2t+1)^6}{t(t+1)} = 108 + \frac{4(t^2+t+1)(8t^2+8t-1)^2}{t(t+1)}.$$

To check for weak uniformity of the equation, factor

$$w(t) - w(s) = \frac{(t-s)(1+s+t)f}{t(t+1)s(s+1)},$$

$$f = 64vu^2 + 48uv + 64uv^2 - 1 \quad \text{with } u = t(t+1), \ v = s(s+1);$$

$$f = 0 \quad \text{for } v = \frac{-64u^2 - 48u + 16(4u+1)\sqrt{u^2+u}}{128u}.$$

This displays a subfield of genus one ($u^2 + u = t(t+1)(t^2+t+1)$).

Branching pattern: $w \approx z^4$, $z \approx w^4$, $w \approx -z^2$, $z \approx -w^2$.

$$\Phi_{24}: \ z = j_2(\tau), \ w = j_2(4\tau), \ j_2\left(\frac{\tau}{4}\right), \ j_2\left(\frac{\tau \pm \sqrt{2}}{4}\right), \ j_2\left(\frac{\tau+2\sqrt{2}}{4}\right),$$

$$j_2\left(\frac{\sqrt{2}\tau \pm 1}{2\sqrt{2}}\right), \ j_2\left(\frac{2\sqrt{2}\tau+1}{\sqrt{2}}\right).$$

The corresponding modular equation is

$$\begin{aligned} z(t) &= \frac{8(t^2+4\sqrt{2}t+4)^4}{t^4(1+t\sqrt{2})(t+\sqrt{2})^2} \\ &= 256 + \frac{8(t^4-8\sqrt{2}t^3-36t^2-32\sqrt{2}t-16)^2}{t^4(1+t\sqrt{2})(t+\sqrt{2})^2}, \\ z\left(\frac{1}{t}\right) = w(t) &= \frac{8(4t^2+4\sqrt{2}t+1)^4}{t(t+\sqrt{2})(1+t\sqrt{2})^2} \\ &= 256 + \frac{8(16t^4+32\sqrt{2}t^3+36t^2+8\sqrt{2}t-1)^2}{t(t+\sqrt{2})(1+t\sqrt{2})^2}. \end{aligned}$$

To check for weak uniformity of the equation, factor

$$w\left(\frac{t}{\sqrt{2}}\right) - w\left(\frac{s}{\sqrt{2}}\right) = 16\frac{(t-s)(t+s+1)(t^2+2t+s^2+2s+1)f}{t(t+2)(t+1)^2s(s+2)(s+1)^2},$$

$$\begin{aligned} f &= 16u^2v^2 - 16u^2v - 16v^2u + 16uv - 1, \\ &\text{with } u = t(t+1), \quad v = s(s+1); \\ f &= 0 \quad \text{for } v = \frac{2(u^2-u)+(2u-1)\sqrt{u^2-u}}{4(u^2-u)}. \end{aligned}$$

This displays a subfield of genus one ($u^2 - u = t(t+1)(t^2+t-1)$).

Table V. Derivation of the modular functions $j(\tau)$ and $j_2(\tau)$ from two strongly uniform modular equations expressing the branching pattern $w \approx z^5$, $z \approx w^5$

$$\Phi_{15}: \; z = j(\tau), \; w = j(5\tau), \; j\left(\frac{\tau}{5}\right), \; j\left(\frac{\tau \pm 1}{5}\right), \; j\left(\frac{\tau \pm 2}{5}\right).$$

The modular equation (with $z(1/t) = w(t)$ as usual) belongs to the family

$$\begin{aligned} z &= \frac{5\sqrt{5}(t^2+10\sqrt{5}g^2t+25g^4)^3g^3}{t^5} \\ &= 1728g^5 + \frac{(5\sqrt{5}t^2+22tg^2+5\sqrt{5}g^4)(t^2+20\sqrt{5}tg^2-125g^4)^2g^3}{t^5}, \\ w &= \frac{5\sqrt{5}(1+10\sqrt{5}g^2t+25g^4t^2)^3g^3}{t} \\ &= 1728g^5 + \frac{(5\sqrt{5}+22tg^2+5\sqrt{5}t^2g^4)(125g^4t^2-20\sqrt{5}g^2t-1)^2g^3}{t}. \end{aligned}$$

For the power series expansion, set $t = 1/(5\sqrt{5}Tg^3)$ $(T \to 0)$,

$$\begin{aligned} z &= (1+250g^5T+3125g^{10}T^2)^3/T \\ &= 1/T + 750g^5 + 196875g^{10}T + 20312500g^{15}T^2 \\ &\quad + 615234375g^{20}T^3 + 7324218750g^{25}T^4 + 30517578125g^{30}T^5 \\ &= 1/q + c_0 + c_1q + c_2q^2 + c_3q^3 + \cdots, \\ w &= (1+10gT+5g^2T^2)^3/T^5 \\ &= 1/T^5 + 30g/T^4 + 315g^2/T^3 + 1300g^3/T^2 + 1575g^4/T \\ &\quad + 750g^5 + 125g^6T \\ &= 1/q^5 + c_0 + c_1q^5 + c_2q^{10} + c_3q^{15} + \cdots. \end{aligned}$$

Comparing power series, we find

$$\begin{aligned} c_0 &= 750g^5 - 6g, \qquad c_1 = 196875g^{10} + 9g^2, \\ c_2 &= 20312500g^{15} + 1181250g^{11} + 10g^3, \\ c_3 &= 615234375g^{20} + 243750000g^{16} + 5315625g^{12} - 30g^4. \end{aligned}$$

For $g = 1$ we have $j(\tau)$.

$$\Phi_{25}: \; z = j_2(\tau), \; w = j_2(5\tau), \; j_2\left(\frac{\tau}{5}\right), \; j_2\left(\frac{\tau \pm \sqrt{2}}{5}\right), \; j_2\left(\frac{\tau \pm 2\sqrt{2}}{5}\right).$$

$$\begin{aligned} z &= \frac{(t + 5g^2)^4(5t^2 + 6g^2t + 5g^4)g^3}{t^5} \\ &= 256g^5 + \frac{5g^3(t^3 - 15g^2t^2 - 25g^4t - 25g^6)^2}{t^5}, \\ w &= \frac{(1 + 5g^2t)^4(5g^4t^2 + 6g^2t + 5)g^3}{t} \\ &= 256g^5 + \frac{5g^3(25g^6t^3 + 25g^4t^2 + 15g^2t - 1)^2}{t}. \end{aligned}$$

For the power series expansion, set $t = 1/(5g^3T)$ $(T \to 0)$,

$$\begin{aligned} z &= (1 + 25g^5T)^4(1 + 6g^5T + 25g^{10}t^2)/T \\ &= 1/T + 106g^5 + 4375g^{10}T + 87500g^{15}T^2 \\ &\quad + 859375g^{20}T^3 + 3906250g^{25}T^4 + 9765625g^{30}T^5 \\ &= 1/q + c_0 + c_1q + c_2q^2 + c_3q^3 + \cdots, \\ w &= (1 + gT)^4(1 + 6gT + 25g^2T^2)/T^5 \\ &= 1/T^5 + 10g/T^4 + 55g^2/T^3 + 140g^3/T^2 \\ &\quad + 175g^4/T + 106g^5 + 25g^6T \\ &= 1/q^5 + c_0 + c_1q^5 + c_2q^{10} + c_3q^{15} + \cdots. \end{aligned}$$

Comparing the power series, we find

$$\begin{aligned} c_0 &= 106g^5 - 2g, \qquad c_1 = 4375g^{10} - 3g^2, \\ c_2 &= 87500g^{15} + 8750g^{11} + 6g^3, \\ c_3 &= 859375g^{20} + 350000g^{16} + 30625g^{12} + 2g^4. \end{aligned}$$

For $g = 1$ we have $j_2(\tau)$.

Bibliography

1. D. Alexander, C. Cummins, J. McKay, and C. Simons, *Completely replicable functions* (to appear).
2. H. Cohn, *Iterated ring class fields and the icosahedron*, Math. Ann. **255** (1981), 107–122.
3. ——, *Introduction to the construction of class fields*, Cambridge Univ. Press, London and New York, 1985.

→ J. H. Conway and S. P. Norton, *Monstrous moonshine*, Bull. London Math. Soc. **11** (1979), 308–339.

5. R. Fricke, *Lehrbuch der Algebra* III (*Algebraische Zahlen*), Vieweg, Braunschweig, 1928.
6. F. Klein, *Vorlesungen über das Ikosaeder*, Teubner, Leipzig, 1884.

→ D. H. Lehmer, *Properties of coefficients of the modular invariant* $J(\tau)$, Amer. J. Math. **64** (1942), 488–502.

8. K. Mahler, *On a class of non-linear functional equations connected with modular equations*, J. Austral. Math. Soc. Ser. A **22** (1976), 65–118.
9. C. Pohl, G. Rosenberger, and A. Schoofs, *Arithmetische Eigenschaften von Eisenstein-Reihen zu den Hecke-Gruppen* $G(\sqrt{2})$ *und* $G(\sqrt{3})$, Abh. Math. Sem. Univ. Hamburg **54** (1984), 49–68.
10. H. Weber, *Elliptische Funktionen und algebraische Zahlen*, Vieweg, Braunschweig, 1891.

DEPARTMENT OF MATHEMATICS, CITY COLLEGE (CUNY), NEW YORK, NEW YORK 10031
E-mail address: hihcc@cunyvm.bitnet