MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 211
JULY 1995, PAGES 1267-1285

HALF-STEP MODULAR EQUATIONS

HARVEY COHN

ABSTRACT. The classical modular equations relating Klein-Weber's $j(\tau)$ to $j(b\tau)$ can be computed as the composition of two "half-step" equations relating $j_m(\tau)$ and $j_m(\tau\sqrt{b})$, where j_m is an extended modular function (corresponding to $\tau \to \tau + \sqrt{m}$, $\tau \to -1/\tau$, et al.). The half-step equations are easily constructed and manipulated in computer algebra. The cases computed here are b prime, $m = a$ (or ab), $\gcd(a, b) = 1$, $ab|30$. This includes many cases where the property of "normal parametrization" occurs, which is of interest in class field theory. Extended modular functions have found recent application in group character theory but they arose in the present context as traces at ∞ of Hilbert modular equations.

1. INTRODUCTION

In view of the readily available computer algebra systems, the explicit computation of modular equations can be regarded as achieved *implicitly* by the potential use of resultants of explicit equations. A reasonable objective is to use the simplest structured equations for this purpose.

For instance, a classical method of Klein and Fricke [10, Ch.5, §2] represents the modular equation (of order N) between $j(\tau)$ and $j(N\tau)$ when the equation yields a curve of genus zero (for 14 values of N between 2 and 25), by eliminating t between equations of the form

$$j(N\tau) = F_N(t), \quad j(\tau) = F_N(1/t) \tag{1.1}$$

for $F_N(t)$ an appropriate rational function. For instance [5, Ch.11, §3],

$$F_2(t) = 64(4t+1)^3/t, \tag{1.2a}$$

so the modular equation of order 2 can be found by eliminating t between the equations

$$j(2\tau) = \frac{64(4t+1)^3}{t}, \quad j(\tau) = \frac{64(t+4)^3}{t^2}. \tag{1.2b}$$

Anticipating later terminology (of §4), we would write this equation (in terms of $z = j(\tau)$ and $Z = j(2\tau)$) as

$$\begin{aligned}\Phi_{1\vee 2}(Z, z) = z^3 + Z^3 - z^2Z^2 + 2^4 3 \cdot 31(z^2Z + Z^2z) - 2^4 3^5 5^3(z^2 + Z^2)\\ + 3^4 5^3 4027 zZ + 2^8 3^7 5^6(z + Z) - 2^{12} 3^9 5^9 = 0.\end{aligned} \tag{1.2c}$$

Received by the editor June 8, 1993 and, in revised form, June 23, 1994.

1991 *Mathematics Subject Classification.* Primary 11F11, 30F35.

Key words and phrases. Klein and Hecke modular functions, Atkin–Lehner involutions, modular equations.

Research supported in part by NSF Grant CCR-8901064.

The parametrization (1.2b) is surely easier to grasp than the expanded result (1.2c).

We propose to extend this process of definition of modular equations through (implicit) elimination of parameters. We shall introduce "half-step" modular transformations (denoted in §3 by $f(u, z) = 0$). They involve auxiliary functions where symbolically the transition $\tau \to N\tau$ seems to be broken into two steps, each resembling "$\tau \to \sqrt{N}\tau$." The required auxiliary functions are extended modular functions defined as $j_N(\tau)$ in §3 below. They are the global uniformizing parameters (Hauptmoduln) of certain extended modular groups. The exact result is given in the Main Theorem of §4 below.

The parametrization of cases of genus zero is explored further for evidence of "normal parametrization" (used in class field theory [8]).

2. Extended modular functions and groups

The parametrization process requires equations of genus zero, but there is a reduction process for handling higher genus (see [10, Ch.5, §3], [6]). To this end, we define "extended modular functions."

The traditional Klein modular group Γ operates on H^+, the upper-half w-plane so as to preserve $j(w)$. For a given $N \in \mathbf{Z}^+$, we next define $\Gamma^0(N)$, the subgroup of Γ which keeps $j(w/N)$ as well as $j(w)$ invariant. Then $\Gamma^0(N)$ has an extension $\Gamma^c(N)$, which was discovered by Fricke and Bessel-Hagen [11] in 1929 and proved by Atkin and Lehner [1] in 1970 to be (within equivalence) the maximal discrete normal extension group of $\Gamma^0(N)$ in $SL_2(\mathbf{R})$. In particular, $\Gamma^c(N)$ is a collection of sets of matrices S_T (over $\mathbf{Z}$) indexed by T, a divisor of N restricted to primary factors, i.e.,

$$T|N, \ \gcd(T, N/T) = 1. \tag{2.1}$$

The matrices in S_T are represented for convenience by the linear fractional formulation $w' = S_T(w)$ with coefficients in $\mathbf{Z}$. Thus,

(2.2)
$$\Gamma^c(N) = \{S_T\}, \ S_T : \left\{ w' = \frac{Aw + B}{Cw + D}, \ AD - BC = T, \ T|\gcd(A, D), \ N|B \right\}.$$

Of course, $S_1 = \Gamma^0(N)$. Thus, as special cases,

$$\{w' = w + N\} \in S_1, \ \{w' = -N/w\} \in S_N. \tag{2.3}$$

To see the transformations in terms of isometric circles when $C \neq 0$, we could write the transformation of S_T in (2.2) in terms of only A, C, and D as

$$\left(w' - \frac{A}{C}\right)\left(w + \frac{D}{C}\right) = -\frac{T}{C^2}, \ \frac{AD - T}{C} \equiv 0 \bmod N, \ T|\gcd(A, D). \tag{2.4}$$

It can be verified (see [6]) that if $M_T \in S_T$ and $M_U \in S_U$, then $M_T M_U \in S_V$, where $V =_2 TU$ (equivalent modulo square factors). Thus, each $M_T^2 \in S_1$, so that if there are ν (≥ 1) distinct prime factors in N, it follows that

$$|\Gamma^c(N)/\Gamma^0(N)| = 2^\nu. \tag{2.5}$$

In order to standardize these groups for differing values of N, it is useful to make the change of notation

$$w = \sqrt{N}\tau \ (\tau \in H^+), \tag{2.6}$$

so from now on in (2.2) the transformation of S_T is modified to read

$$\tau' = \frac{A\tau + B/\sqrt{N}}{C\tau\sqrt{N} + D}. \tag{2.7}$$

The special transformations of (2.3) are now

$$\{\tau' = \tau + \sqrt{N}\} \in S_1, \ \{\tau' = -1/\tau\} \in S_N, \tag{2.8}$$

and the isometric form of (2.7) is

$$\begin{gathered}\left(\tau' - \frac{A}{C\sqrt{N}}\right)\left(\tau + \frac{D}{C\sqrt{N}}\right) = -\frac{T}{NC^2}, \\ \frac{AD-T}{C} \equiv 0 \bmod N, \quad T|\gcd(A, D).\end{gathered} \tag{2.9}$$

The use of τ calls for the local uniformizing parameter at ∞:

$$r = \exp 2\pi i\tau/\sqrt{N}. \tag{2.10}$$

The notation adopted here permits a certain uniformity in the ubiquitous role of $\tau' = -1/\tau$, useful in the interaction of different orders N.

We finally introduce the notation

$$\Gamma_N = \Gamma^c(N), \tag{2.11}$$

now viewed as a group acting on the upper-half τ-plane. We shall consider only cases where Γ_N is of genus zero. There are 64 such N (> 1). The last is 119, and first exception is $N = 37$ (see [6]).

2.12. **Lemma.** *If the definition of Γ_N is modified to the subgroup Γ_{N*Q} by the requirement that B is divisible by a fixed Q relatively prime to N, i.e.,*

$$\Gamma_{N*Q} = \Gamma_N \cap \{Q|B\} \quad (\gcd(Q, N) = 1), \tag{2.12a}$$

then the index is

$$|\Gamma_N/\Gamma_{N*Q}| = Q\prod(1 + 1/p), \quad \text{prime } p|Q. \tag{2.12b}$$

2.13. **Lemma.** *If the definition of Γ_N is modified to the subgroup $\Gamma_{N:Q}$ by the requirement that $AD - BC = T$ is relatively prime to Q, a primary divisor of N, i.e.,*

$$\Gamma_{N:Q} = \Gamma_N \cap \{\gcd(T, Q) = 1\} \quad (\gcd(Q, N/Q) = 1), \tag{2.13a}$$

then the index is

$$|\Gamma_N/\Gamma_{N:Q}| = 2^\kappa, \tag{2.13b}$$

where Q has κ distinct prime divisors.

The proofs are classical. Lemma 2.12 is proved analogously to the case $N = 1$, where Γ_{N*Q} reduces to $\Gamma^0(Q)$ in the usual terminology (see [5, Ch.10, §2]). Lemma 2.13 follows from the removal of κ generators $\{S_T, T|Q\}$ in Γ_N.

3. Modular equations and their Riemann surfaces

The global uniformizing parameter $j_N(\tau)$ for Γ_N can be constructed by classical methods based on the Dedekind eta function

$$\eta(\tau) = q^{1/24}\prod_{h=1}^{\infty}(1 - q^h), \qquad q = \exp 2\pi i\tau \tag{3.1a}$$

(see [6, 9]), for (at least) those small N (factors of 30) which figure into the current computation. In practice, we simplify the computation by use of the function

$$\Pi_m(r) = \prod_{h=1}^{\infty}(1 - r^{hm}), \qquad r = \exp 2\pi i\tau/\sqrt{N}. \tag{3.1b}$$

The relevant formulas are summarized in Table I, as well as the elliptic generators and fixed points of the fundamental domains. Also the values of j_N are given at these points (noted later in Table II).

We note that $j_N(\tau)$ is the familiar Klein-Weber modular function for $N = 1$ and the Hecke modular function (see [8]) for $N = 2$ and 3. (For these cases alone, the relations (2.8) suffice to define $\Gamma^c(N)$.) There is a "free" parameter in the choice of $j_N(\tau)$, namely an additive constant, but (compare [12]), there seems to be no convenient universal criterion of choice (short of just omitting the constant)! In general the constant is chosen (ad lib) so as to make the values at the elliptic points small or to make coefficients of later modular equations small (see Table II).

We now consider the Riemann surface generated by any function element $u(z)$ defined implicitly (by elimination of τ) from the relation between $u = j_{ab}(\tau)$ and $z = j_a(\tau\sqrt{b})$, with (say) $a, b \in \mathbf{Z}^+$. Clearly, the relation is multivalued. For instance, from $\tau \to -1/\tau$ it is seen that $(j_a(-\sqrt{b}/\tau) =)\ j_a(\tau/\sqrt{b})$ is another value of z for the same u. There are only a finite number of branches since the invariance groups $\Gamma^c(N)$ are of finite extensions of Γ. We specialize the choice of a, b for simplicity and find the equation of this Riemann surface:

3.2. **Theorem** (Case $a \vee b$). *For b prime and* $\gcd(a, b) = 1$, *there is an irreducible algebraic (compact) Riemann surface determined by the "half-step" polynomial*

$$\begin{aligned} f(u, z) := u^{b+1} + z^2 - zu^b + (c_0 + d_0 z) + (c_1 + d_1 z)u \\ + \cdots + (c_{b-1} + d_{b-1} z)u^{b-1} + c_b u^b = 0, \end{aligned} \tag{3.2a}$$

which has branches denoted collectively by "u" and "z" as follows:
(3.2b)

$$(z =) j_a(\tau) \to (u =) \begin{cases} j_{ab}(\tau\sqrt{b}), \\ j_{ab}(\dfrac{\tau + k\sqrt{a}}{\sqrt{b}}), \\ \quad (k = 0, \cdots, b-1); \end{cases} \qquad (u =) j_{ab}(\tau) \to (z =) \begin{cases} j_a(\tau\sqrt{b}), \\ j_a(\dfrac{\tau}{\sqrt{b}}). \end{cases}$$

Proof of left-hand branching: Here $j_a(\tau)$ is invariant under Γ_a, so we just prove that under Γ_a the branch $j_0 = j_{ab}(\tau/\sqrt{b})$ has the $b + 1$ conjugates shown by the arrow. The conjugates are achieved by the repeated application of $\tau' = -1/\tau$ and $\tau' = \tau + \sqrt{a}$ (in Γ_a). Now consider a general element of Γ_a,

$$\tau \to \tau' = \frac{A\tau + B/\sqrt{a}}{C\sqrt{a}\tau + D}, \quad AD - BC = T \,|\, \gcd(A, D),\ T|a|B. \tag{3.3a}$$

TABLE I. The modular invariants

The modular invariants $j_N(\tau)$ are described here for all $N|30$. Explicit formulas are given for $N > 1$ in terms of

$$\Pi_m(r) = \prod_{h=1}^{\infty}(1 - r^{hm})$$

(abbreviated Π_m). Here the local parameter for the Laurent series of $j_N(\tau)$ at $\tau = \infty$ is

$$r = \exp 2\pi i\tau/\sqrt{N}.$$

Here, $e_1 r + e_2 r^2 + \cdots + e_m r^m$ is written $r[e_1, e_2, \ldots, e_m]$ (with $m = 10$, see §5.1).

The group Γ_N has the translation $\tau' = \tau + \sqrt{N}$. This places the fundamental domain of H^+/Γ_N between the boundaries

$$-\sqrt{N} \le \Re(\tau) \le \sqrt{N}.$$

A full set of elliptic generators is listed in a form which displays the isometric circles bounding the floor of the fundamental domain of H^+/Γ_N.

The elliptic points τ where these circles intersect are next listed in the form of values of $j_N(\tau)$.

$$\begin{aligned} j_1(\tau) = 1/r + 744 + r[&196884, 21493760, 864299970, 20245856256,\\ &333202640600, 4252023300096, 44656994071935,\\ &401490886656000, 3176440229784420,\\ &22567393309593600, \cdots];\end{aligned}$$

$$\tau\tau' = -1; \quad j_1(i) = 1728, \ j\left(\frac{\pm 1 + \sqrt{-3}}{2}\right) = 0.$$

$$\begin{aligned} j_2(\tau) &= \frac{1}{w} + 128 + 4096w, \quad w = r\left(\frac{\Pi_2}{\Pi_1}\right)^{24}\\ &= 1/r + 104 + r[4372, 96256, 1240002, 10698752, 74428120,\\ &\qquad 431529984, 2206741887, 10117578752,\\ &\qquad 42616961892, 166564106240, \cdots];\end{aligned}$$

$$\tau\tau' = -1; \quad j_2(i) = 256, \ j\left(\frac{\pm 1 + i}{\sqrt{2}}\right) = 0.$$

$$\begin{aligned} j_3(\tau) &= \frac{1}{w} + 54 + 729w, \quad w = r\left(\frac{\Pi_3}{\Pi_1}\right)^{12}\\ &= 1/r + 42 + r[783, 8672, 65367, 371520, 1741655, 7161696,\\ &\qquad 26567946, 90521472, 288078201, 864924480 \cdots];\end{aligned}$$

$$\tau\tau' = -1; \quad j_3(i) = 108, \ j\left(\frac{\pm\sqrt{3} + i}{2}\right) = 0.$$

$$\begin{aligned} j_5(\tau) &= \frac{1}{w} + 22 + 125w, \quad w = r\left(\frac{\Pi_5}{\Pi_1}\right)^{6}\\ &= 1/r + 16 + r[134, 760, 3345, 12256, 39350, 114096, 307060,\\ &\qquad 776000, 1867170, 4298600, \cdots];\end{aligned}$$

$$\tau\tau' = -1, \ \left(\tau \pm \frac{\sqrt{5}}{2}\right)\left(\tau' \pm \frac{\sqrt{5}}{2}\right) = -\frac{1}{4};$$

$$j_5(i) = 22 + 10\sqrt{5}, \ j_5\left(\frac{\pm 2 + i}{\sqrt{5}}\right) = 0, \ j_5\left(\frac{\pm\sqrt{5} + i}{2}\right) = 22 - 10\sqrt{5}.$$

TABLE I (continued)

$$j_6(\tau) = \frac{1}{w} - 2 + w, \quad w = r\left(\frac{\Pi_1\Pi_6}{\Pi_2\Pi_3}\right)^{12}$$

$$= 1/r + 10 + r[79, 352, 1431, 4160, 13015, 31968, 81162, 183680, 412857, 864320, \cdots];$$

$$\tau\tau' = -1, \quad \left(\tau \pm \frac{\sqrt{6}}{2}\right)\left(\tau' \pm \frac{\sqrt{6}}{2}\right) = -\frac{1}{2};$$

$$j_6(i) = 32, \quad j_6\left(\frac{\pm\sqrt{2}+i}{\sqrt{3}}\right) = 0, \quad j_6\left(\frac{\pm\sqrt{3}+i}{\sqrt{2}}\right) = -4.$$

$$j_{10}(\tau) = \frac{1}{w} + 2 + w, \quad w = r\left(\frac{\Pi_1\Pi_{10}}{\Pi_2\Pi_5}\right)^{6}$$

$$= 1/r + 8 + r[22, 56, 177, 352, 870, 1584, 3412, 5952, 11442, 19240, \cdots];$$

$$\tau\tau' = -1, \quad \left(\tau \pm \frac{\sqrt{10}}{2}\right)\left(\tau' \pm \frac{\sqrt{10}}{2}\right) = -\frac{1}{2};$$

$$j_{10}(i) = 20, \quad j_{10}\left(\frac{\pm 3+i}{\sqrt{10}}\right) = 4, \quad j_{10}\left(\frac{\pm\sqrt{5}+i}{\sqrt{2}}\right) = 0.$$

$$j_{15}(\tau) = \frac{1}{w} - w, \qquad w = r\left(\frac{\Pi_1\Pi_{15}}{\Pi_3\Pi_5}\right)^{3}$$

$$= 1/r + 3 + r[8, 22, 42, 70, 155, 246, 421, 722, 1101, 1730, \cdots];$$

$$\tau\tau' = -1, \quad \left(\tau \pm \frac{\sqrt{15}}{3}\right)\left(\tau' \pm \frac{\sqrt{15}}{3}\right) = -\frac{1}{3},$$

$$\left(\tau \pm \frac{\sqrt{15}}{2}\right)\left(\tau' \pm \frac{\sqrt{15}}{2}\right) = -\frac{1}{4};$$

$$j_{15}(i) = 11, \quad j_{15}\left(\frac{\pm 7+\sqrt{11}}{2\sqrt{15}}\right) = j_{15}\left(\frac{\pm 13+\sqrt{-11}}{2\sqrt{15}}\right) = 0,$$

$$j_{15}\left(\frac{\pm\sqrt{15}+i}{2}\right) = -1.$$

$$j_{30}(\tau) = \frac{1}{w} + w, \qquad w = r\left(\frac{\Pi_2\Pi_3\Pi_5\Pi_{30}}{\Pi_1\Pi_6\Pi_{10}\Pi_{15}}\right)^{3}$$

$$= 1/r - 3 + r[4, 2, 6, 10, 15, 18, 37, 30, 57, 70\cdots];$$

$$\tau\tau' = -1, \quad \left(\tau \pm \sqrt{\frac{6}{5}}\right)\left(\tau' \mp \sqrt{\frac{6}{5}}\right) = -\frac{1}{5}, \quad \left(\tau \pm \sqrt{\frac{10}{3}}\right)\left(\tau' \mp \sqrt{\frac{10}{3}}\right) = -\frac{1}{3},$$

$$\left(\tau \pm \sqrt{\frac{15}{2}}\right)\left(\tau' \pm \sqrt{\frac{15}{2}}\right) = -\frac{1}{2};$$

$$j_{30}(i) = 2, \quad j_{30}\left(\frac{\pm\sqrt{5}+i}{\sqrt{6}}\right) = -2, \quad j_{30}\left(\frac{\pm\sqrt{15}+i}{2\sqrt{2}}\right) = -3,$$

$$j_{30}\left(\frac{\pm 2\sqrt{6}+i}{\sqrt{5}}\right) = -6, \quad j_{30}\left(\frac{\pm\sqrt{15}+i}{\sqrt{2}}\right) = -7.$$

In terms of the argument of j_0, namely $\sigma = \tau/\sqrt{b}$ (and $\sigma' = \tau'/\sqrt{b}$), the transformation (3.3a) is now

$$\sigma \to \sigma' = \frac{A\sigma + B/\sqrt{ab}}{C\sqrt{ab}\sigma + D}. \tag{3.3b}$$

This transformation preserves the branch j_0 if it is in Γ_{ab} or $b|B$ (whence $ab|B$). The subgroup Γ_{a*b}, however, is of index $b+1$ by Lemma 2.12. This accounts for the $b+1$ branches.

Proof of right-hand branching: Here $j_{ab}(\tau)$ is invariant under Γ_{ab}, so we just prove that under Γ_{ab} the branch $j_0 = j_a(\tau\sqrt{b})$ has the two conjugates shown by the arrow. The conjugates are achieved by $\tau' = -1/\tau$ (in Γ_{ab}). Now consider a general element of Γ_{ab},

$$\tau \to \tau' = \frac{A\tau + B/\sqrt{ab}}{C\tau\sqrt{ab} + D}, \quad AD - BC = T|\gcd(A, D),\ T|ab|B. \tag{3.4a}$$

In terms of the argument of j_0, namely $\sigma = \tau\sqrt{b}$ (and $\sigma' = \tau'\sqrt{b}$), the transformation (3.4a) is now

$$\sigma \to \sigma' = \frac{A\sigma + B/\sqrt{a}}{C\sigma\sqrt{a} + D}. \tag{3.4b}$$

This transformation preserves the branch j_0 if it is in Γ_a or $T|a$ whence $\gcd(T, b) = 1$. The subgroup $\Gamma_{ab:b}$, however, is of index 2 ($\mu = 1$) by Lemma 2.13. This accounts for the two branchings.

The polynomial $f(u, z) = 0$ which determines the Riemann surface is clearly of degree $b+1$ in u and 2 in z. The behavior at $\Im\tau = \infty$ is given by

$$j_a(\tau) \approx 1/\exp 2\pi i\tau/\sqrt{a}, \quad j_{ab}(\tau) \approx 1/\exp 2\pi i\tau/\sqrt{ab}. \tag{3.5a}$$

So the left-hand branching produces the $b+1$ relations

$$u \approx z, \quad u \approx z^{1/b}\exp 2\pi ik/b\ (k = 0, \dots, b-1). \tag{3.5b}$$

Likewise, the right-hand branching produces the two relations

$$z \approx u, \quad z \approx u^b. \tag{3.5c}$$

Of course the relations (3.5c) include (3.5b) and lead to a Newton polygon dominating $f(u, z)$ and given by the terms:

$$\text{Case } a \vee b: \quad f(u, z) \approx u^{b+1} + z^2 - zu^b. \tag{3.5d}$$

4. Classical modular equations as resultants of half-step modular equations

We now can exhibit the polynomial relation for the Case $a \vee b$ (in Theorem 3.2) as a *half-step* modular equation

$$\begin{aligned} f(u, z) := u^{b+1} + z^2 - zu^b + (c_0 + d_0 z) + (c_1 + d_1 z)u \\ + \cdots + (c_{b-1} + d_{b-1}z)u^{b-1} + c_b u^b = 0, \end{aligned} \tag{4.1}$$

which connects the function elements of (3.2b). For example,

$$(z =)\ j_a(\tau) \to (u =) j_{ab}(\tau\sqrt{b})), \quad (u =)\ j_{ab}(\tau) \to (z =) j_a(\tau\sqrt{b}), \tag{4.2}$$

so by iteratively transforming from z to u and u to $z\ (= Z)$ again, we have a relation between $j_a(\tau)$ and $j_a(b\tau)$, i.e., a *modular equation*:

$$\Phi_{a\vee b}(z\,,\,Z) = 0\,, \quad z = j_a(\tau)\,, \ \ Z = j_a(b\tau). \tag{4.3a}$$

Likewise, starting the cycle with u, we again have a *modular equation*,

$$\Psi_{a\vee b}(u\,,\,U) = 0\,, \quad u = j_{ab}(\tau)\,, \ \ U = j_{ab}(b\tau). \tag{4.3b}$$

The application of the factor $\sqrt{b}$ twice in (4.2) leads to the designation "half-step" for each application.

The correspondences in (4.2) are multivalued, so it is necessary to count conjugates. To begin with, as an iteration (4.2) provides z (or u) with $2(b+1)$ conjugate values of Z (or U resp.), which we can now enumerate.

4.4. **Lemma.** *Under the iteration* (4.2) *where* $(j_a(\tau) =)z \to u \to Z$, Z *is one of the following sets of* $2b+2$ *conjugates*:

$$Z \;=\; j_a(b\tau)\,,\, j_a\left(\frac{\tau + k\sqrt{a}}{b}\right)(k = 0\,,\,\cdots\,,\,b-1)\,;\ \ j_a(\tau)\ \ (b+1\ \ \textit{times}). \tag{4.4a}$$

The orders of magnitude represented here may be listed as

$$Z \approx z^b\,, \ \ z \approx Z^b\,; \quad z = Z\ \ (b+1\ \ \textit{times}). \tag{4.4b}$$

Likewise, under the iteration (4.2) *where* $(j_{ab}(\tau) =)u \to z \to U$, U *is one of the following sets of* $2b+2$ *conjugates*:

$$U \;=\; j_{ab}(b\tau)\,,\, j_{ab}\left(\frac{\tau + k\sqrt{ab}}{b}\right)(k = 0\,,\,\cdots\,,\,b-1)\,,$$

$$j_{ab}\left(\tau + k\sqrt{\frac{a}{b}}\right)(k = 1\,,\,\cdots\,,\,b-1)\,;\ \ j_{ab}(\tau)\ (\textit{twice}). \tag{4.4c}$$

The orders of magnitude represented here may be listed as

(4.4d)

$$U \approx u^b\,, \ \ u \approx U^b\,, \ \ u \approx U \exp 2\pi i k/b \quad (k = 1\,,\,\cdots\,,\,b-1)\,; \quad u = U\ (\textit{twice}).$$

The proof consists of a trace of branches of the trees in (3.2b). To illustrate, look at the special branches of $u \to z$, $z \to U$ given by

$$j_{ab}(\tau) \;\to\; j_a(\tau\sqrt{b})\,, \quad j_a(\tau) \;\to\; j_{ab}\left(\frac{\tau + k\sqrt{a}}{\sqrt{b}}\right)(k = 0\,,\,\cdots\,,\,b-1). \tag{4.5a}$$

These branches on composition become part of (4.4c), namely

$$(u =)j_{ab}(\tau) \;\to\; (U =)j_{ab}\left(\tau + k\sqrt{\frac{a}{b}}\right)(k = 0\,,\,\cdots\,,\,b-1). \tag{4.5b}$$

The case $k = 0$ of course is one of the two components of $u = U$ in (4.4c).

4.6. **Main theorem.** *The resultants* (*or eliminants*) *of* $f(u\,,\,z)$ *in* (4.1) *yield* (*for* $\gcd(a\,,\,b) = 1$) *the modular polynomials* $\Phi_{a\vee b}(z\,,\,Z)$ *of* (4.3a) *and* $\Psi_{a\vee b}(z\,,\,Z)$ *of* (4.3b) *as follows*:

$$u\textit{-resultant}(f(u\,,\,z)\,,\,f(u\,,\,Z)) \;=\; (z - Z)^{b+1}\Phi_{a\vee b}(z\,,\,Z)\,, \tag{4.6a}$$

$$z\textit{-resultant}(f(u\,,\,z)\,,\,f(U\,,\,z)) \;=\; (u - U)^2\Psi_{a\vee b}(u\,,\,U). \tag{4.6b}$$

The Newton polygon terms are deduced from (4.4b) *and* (4.4d) *as follows*:

$$\Phi_{a\vee b}(z, Z) = z^{b+1} + Z^{b+1} - z^b Z^b + \cdots , \tag{4.7a}$$

$$\Psi_{a\vee b}(u, U) = u^{2b} + U^{2b} - u^b U^b (u^{b-1} + u^{b-1}U + \cdots + U^{b-1}) + \cdots . \tag{4.7b}$$

4.8. **Corollary.** *The Newton polygons of* $f(u, z)$ *in* (4.1) *and* $\Phi_{a\vee b}(z, Z)$ *and* $\Psi_{a\vee b}(u, U)$ *in* (4.7a,b) *are valid only if* $\gcd(a, b) = 1$.

For *proof*, note that if $\gcd(a, b) > 1$, then in (3.2b) j_{ab} would have more than the $b+1$ branches shown. For instance, under $\tau \to -1/\tau$ the branch $j_{ab}((\tau + \sqrt{a})/\sqrt{b})$ could become $j_{ab}((\tau + k\sqrt{a})/\sqrt{b})$ under Γ_a (as in the proof of Theorem 3.2) only if $1 + ka \equiv 0 \bmod b$.

5. The computation of half-step modular equations

This section is largely an explanation of Table II (next page) which covers all cases $a \vee b$ where b is prime and $ab|30$ (so $\gcd(a, b) = 1$).

5.1. **Half-step polynomials.** First we calculate the polynomial $f(u, z)$ of (4.1) for Table II. We need to know the Laurent expansions up to $O(r^{2b+1})$ (in the parameter $r = \exp 2\pi i\tau/\sqrt{a}$), namely

$$\begin{aligned}(j_a(\tau) =) z &\approx 1/r + k_0 + \cdots + k_{2b} r^{2b}, \\ (j_{ab}(\tau\sqrt{b}) =) u &\approx 1/r + K_0 + \cdots + K_{2b} r^{2b}.\end{aligned} \tag{5.1a}$$

The k_i and K_i of course come from Table I, which is valid up to r^{10} (for $b = 5$).

Then we can view (4.1) as a quadratic equation in z with the roots $z_1 = z(r)$ (as in (5.1a)) and $z_2 = z(r^b)$ (derived by $r \to r^b$). Next we consider the symmetric root functions (using the unknowns c_i, d_i),

$$z_1 + z_2 = u^b - d_0 - d_1 u - \cdots - d_{b-1} u^{b-1}, \tag{5.1b}$$

$$z_1 z_2 = u^{b+1} + c_0 + c_1 u + \cdots + c_{b-1} u^{b-1} + c_b u^b. \tag{5.1c}$$

These equations are now known from (5.1a) to $O(r^{b+1})$ (after the cancellation of $1/r^{b+1}$ on both sides in (5.1c)). In each of (5.1bc) we expand both sides as Laurent series in r and compare coefficients of r^{-i} to obtain equations for the c_i and d_i (in descending order of the subscripts).

5.2. **Discriminants and parametrizations.** The genus of the curve $f(u, z) = 0$ is determined by the z-discriminant of the quadratic equation $z = z(u)$ which it implies. In those cases where the genus is zero, a parametrization $z(t)$, $u(t)$ is given in Table II. The parametrization is standardized by the symmetry $t \to 1/t$ in the rational (quadratic) function $u(t)$. The case $1 \vee 5$ is the only one where a radical ($\sqrt{5}$) occurs.

Also the roots of the z-discriminant are values of $(u =) j_{ab}$ at special points, which include the elliptic points of its fundamental domain (and likewise for the roots of the u-discriminant and j_a). In fact, in Table I the values of j_N at the elliptic points had been determined experimentally by selecting from among these roots. (Details of this hand calculation are omitted.)

TABLE II. The half-step modular equations

Listings include $f(u, z)$ with discriminants, parametrizations, and equations for singular moduli.

Case $1 \vee 2$:

$$(z =)j_1(\tau) \rightarrow (u =)j_2(\sqrt{2}\tau),$$
$$(u =)j_2(\tau) \rightarrow (z =)j_1(\sqrt{2}\tau).$$
$$f(u, z) = -62208u + 3456z - 207uz - 432u^2 - u^3 + u^2z - z^2 - 2985984,$$
$$z\text{-disc} = u(u - 256)(-81 + u)^2,$$
$$u\text{-disc} = z^2(z - 1728)(z + 3375)^2,$$
$$z(t) = 64(4t + 1)^3/t, \quad u(t) = 64(t + 1)^2/t.$$
$$j_1(\tau) = j_1(2\tau) \;\Rightarrow\; (z - 1728)(z - 8000)(z + 3375)^2 = 0,$$
$$j_2(\tau) = j_2(2\tau) \;\Rightarrow\; (-648 + u)(u + 144)^2(-81 + u)^2 = 0.$$

Case $1 \vee 3$:

$$(z =)j_1(\tau) \rightarrow (u =)j_3(\sqrt{3}\tau),$$
$$(u =)j_3(\tau) \rightarrow (z =)j_1(\sqrt{3}\tau).$$
$$f(u, z) = 7077888u - 2944uz + 126u^2z + 110592u^2 + 576u^3$$
$$- u^3z + u^4 + z^2,$$
$$z\text{-disc} = u(u - 108)(u - 8)^2(u - 64)^2,$$
$$u\text{-disc} = z^2(z - 8000)^2(z + 32768)^2(z - 1728)^2,$$
$$z(t) = 27(9t + 1)^3(t + 1)/t, \quad u(t) = 27(t + 1)^2/t.$$
$$j_1(\tau) = j_1(3\tau) \;\Rightarrow\; z(-54000 + z)(z + 32768)^2(z - 8000)^2 = 0,$$
$$j_3(\tau) = j_3(3\tau) \;\Rightarrow\; (u^2 - 576u - 1728)(u + 192)^2(u - 8)^2(u - 64)^2 = 0.$$

Case $1 \vee 5$:

$$(z =)j_1(\tau) \rightarrow (u =)j_5(\sqrt{5}\tau),$$
$$(u =)j_5(\tau) \rightarrow (z =)j_1(\sqrt{5}\tau).$$
$$f(u, z) = -u^5z - 7776zu + 12600zu^2 - 1890zu^3 + 80zu^4 + 2985984$$
$$+ 13436928u + 20217600u^2 + 10264320u^3 + 140400u^4$$
$$+ 648u^5 + u^6 + z^2 - 3456z,$$
$$z\text{-disc} = u^2(u^2 - 44u - 16)(u - 36)^2(u - 18)^2(u - 4)^2,$$
$$u\text{-disc} = z^4(z - 287496)^2(z + 32768)^2(z + 884736)^2(z - 1728)^4,$$
$$z(t) = 5\sqrt{5}(25t^2 + 10t\sqrt{5} + 1)^3/t, \quad u(t) = 5\sqrt{5}(t + 1/t) + 22.$$
$$j_1(\tau) = j_1(5\tau) \;\Rightarrow$$
$$(-681472000 - 1264000z + z^2)(z - 287496)^2(z + 32768)^2$$
$$\times (z - 1728)^2(z + 884736)^2 = 0,$$
$$j_5(\tau) = j_5(5\tau) \;\Rightarrow$$
$$u^2(u^2 - 540u - 6480)(u - 18)^2(u - 36)^2(u - 4)^2(u^2 + 216u + 144)^2 = 0.$$

TABLE II (continued)

Case $2 \vee 3$:

$$(z =)j_2(\tau) \to (u =)j_6(\sqrt{3}\tau),$$
$$(u =)j_6(\tau) \to (z =)j_2(\sqrt{3}\tau).$$

$$f(u, z) = 1536u^2 + 64u^3 + u^4 + 30u^2z - u^3z - 64uz + 16384u - 512z + z^2 + 65536,$$

$$z\text{-disc} = u^2(u+4)(u-32)(u-16)^2,$$

$$u\text{-disc} = z^3(z+1024)^2(z-256)^3,$$

$$z(t) = 9(3t+1)^4/t, \quad u(t) = (9t^2+14t+9)/t.$$

$$j_2(\tau) = j_2(3\tau) \;\;=>\; (z+144)(z-2304)(z+1024)^2(z-256)^2 = 0,$$

$$j_6(\tau) = j_6(3\tau) \;\;=>\; u^2(u-96)(u-16)^2(u+16)^3 = 0.$$

Case $2 \vee 5$:

$$(z =)j_2(\tau) \to (u =)j_{10}(\sqrt{5}\tau),$$
$$(u =)j_{10}(\tau) \to (z =)j_2(\sqrt{5}\tau).$$

$$f(u, z) = z^2 + 2048z - 40960u^2 + 5120u^3 + 1040u^4 - 262144u + 56u^5 + u^6 + 1048576 - zu^5 + 40zu^4 - 530zu^3 + 2760zu^2 - 5376zu,$$

$$z\text{-disc} = u(u-20)(u-16)^2(u-2)^2(u-8)^2(u-4)^2,$$

$$u\text{-disc} = z^5(z+12288)^2(z-648)^2(z-2304)^2(z-256)^3,$$

$$z(t) = (5t^2+6t+5)(5t+1)^4/t, \quad u(t) = 5(t+1)^2/t.$$

$$j_2(\tau) = j_2(5\tau) \;\;=>$$
$$z^2(z+1024)(z-20736)(z+12288)^2(z-648)^2(z-2304)^2 = 0,$$

$$j_{10}(\tau) = j_{10}(5\tau) \;\;=>$$
$$(u^3 - 100u^2 + 640u - 1280)(u-16)^2(u-2)^2(u-8)^2 \times (u-4)^2(u+16)^3 = 0.$$

Case $3 \vee 2$:

$$(z =)j_3(\tau) \to (u =)j_6(\sqrt{2}\tau),$$
$$(u =)j_6(\tau) \to (z =)j_3(\sqrt{2}\tau).$$

$$f(u, z) = -64 - 19uz + u^2z - 48u + 16z - 12u^2 - u^3 - z^2,$$

$$z\text{-disc} = u(-u+32)(5-u)^2,$$

$$u\text{-disc} = z^2(-4z+432)(27+z)^2,$$

$$z(t) = 8(2t+1)^3/t, \quad u(t) = 8(t+1)^2/t.$$

$$j_3(\tau) = j_3(2\tau) \;\;=>\; (100-2u)(u+4)^2(5-u)^2 = 0,$$

$$j_6(\tau) = j_6(2\tau) \;\;=>\; (-z+8)(-z+216)(27+z)^2 = 0.$$

TABLE II (continued)

Case $3 \vee 5$:

$(z =)j_3(\tau) \to (u =)j_{15}(\sqrt{5}\tau)$,

$(u =)j_{15}(\tau) \to (z =)j_3(\sqrt{5}\tau)$.

$$f(u, z) = 4096 + 6144u + 3840u^2 + 1280u^3 + 240u^4 + 24u^5 + u^6 - zu^5 + z^2 - 128z - 96zu + 20zu^2 - 50zu^3 + 15zu^4,$$

z-disc $= u^2(u - 11)(u + 1)(u^2 + 4)(u - 2)^2(u - 8)^2$, (genus 1),

u-disc $= z^5(z - 216)^2(z + 1728)^2(z - 64)^2(z - 108)^3$.

$$j_3(\tau) = j_3(5\tau) \Rightarrow (z + 27)(z - 3375)(z^2 + 32z + 8000)(z - 216)^2 \times (z + 1728)^2(z - 64)^2 = 0,$$

$$j_{15}(\tau) = j_{15}(5\tau) \Rightarrow u^2(u^3 - 42u^2 + 48u - 44)(u - 2)^2(u - 8)^2(u + 4)^5 = 0.$$

Case $5 \vee 2$:

$(z =)j_5(\tau) \to (u =)j_{10}(\sqrt{2}\tau)$,

$(u =)j_{10}(\tau) \to (z =)j_5(\sqrt{2}\tau)$.

$$f(u, z) = u^3 - u^2z + z^2 - 16 - 44z + 20u - 8u^2 + 15uz,$$

z-disc $= (u - 4)(u - 20)(u - 5)^2$,

u-disc $= z(z^2 - 44z - 16)(z + 3)^2$,

$z(t) = 4(t + 1)(1 + 2t)^2/t, \quad u(t) = 4(3t + t^2 + 1)/t$.

$$j_5(\tau) = j_5(2\tau) \Rightarrow z(z - 72)(z + 3)^2 = 0,$$

$$j_{10}(\tau) = j_{10}(2\tau) \Rightarrow (u - 2)(u^2 - 30u + 100)(u - 5)^2 = 0.$$

Case $5 \vee 3$:

$(z =)j_5(\tau) \to (u =)j_{15}(\sqrt{3}\tau)$,

$(u =)j_{15}(\tau) \to (z =)j_5(\sqrt{3}\tau)$.

$$f(u, z) = u^4 - u^3z + z^2 + 16 - 8z + 16u + 12u^2 + 4u^3 - 4uz + 9u^2z,$$

z-disc $= u^2(u + 1)(u - 11)(u - 4)^2$,

u-disc $= z^2(z^2 - 44z - 16)(z + 28)^2(z - 4)^2$,

$z(t) = 3(1 + 3t + 3t^2)^2/t, \quad u(t) = (3t^2 + 3 + 5t)/t$.

$$j_5(\tau) = j_5(3\tau) \Rightarrow (z + 3)(z - 147)(z + 28)^2(z - 4)^2 = 0,$$

$$j_{15}(\tau) = j_{15}(3\tau) \Rightarrow u^2(u^2 - 18u - 44)(u^2 + 2u + 4)(u - 4)^2 = 0$$

Case $6 \vee 5$:

$(z =)j_6(\tau) \to (u =)j_{30}(\sqrt{5}\tau)$,

$(u =)j_{30}(\tau) \to (z =)j_6(\sqrt{5}\tau)$.

$$f(u, z) = u^6 - u^5z + z^2 + 12544 + 16128u + 8320u^2 + 2240u^3 + 340u^4 + 28u^5 + 224z + 144zu - 80zu^2 - 70zu^3 - 15zu^4,$$

z-disc $= u^2(u - 2)(u + 7)(u + 3)(u + 2)(u + 6)^2(u + 4)^2$, (genus 1),

u-disc $= z^3(z + 112)^2(z + 16)^2(z + 4)^3(z - 32)^4$.

TABLE II (continued)

$$j_6(\tau) = j_6(5\tau) \Rightarrow (z+49)(z-5)(z-320)(z-16)(z-32)^2 \times (z+112)^2(z+16)^2 = 0,$$

$$j_{30}(\tau) = j_{30}(5\tau) \Rightarrow u^2(u^3+16u^2+72u+108)(u^3+14u^2+72u+112)(u^2-8u-24) \times (u+6)^2(u+4)^2 = 0.$$

Case $10 \vee 3$:

$(z =) j_{10}(\tau) \to (u =) j_{30}(\sqrt{3}\tau)$,

$(u =) j_{30}(\tau) \to (z =) j_{10}(\sqrt{3}\tau)$.

$$f(u, z) = u^4 - u^3 z + z^2 + 256 - 4z + 320u + 132u^2 + 20u^3 - 16uz - 9u^2 z,$$

z-disc $= (u-2)(u+7)(u+6)(u+3)(u+2)^2$, (genus 1),

u-disc $= -27z^3(z-20)^2(z-4)^3$.

$$j_{10}(\tau) = j_{10}(3\tau) \Rightarrow z^2(z-5)(z+5)(z-40)(z-8) = 0,$$

$$j_{30}(\tau) = j_{30}(3\tau) \Rightarrow (u+8)(u^2-24)(u+2)^2(u+4)^3 = 0.$$

Case $15 \vee 2$:

$(z =) j_{15}(\tau) \to (u =) j_{30}(\sqrt{2}\tau)$,

$(u =) j_{30}(\tau) \to (z =) j_{15}(\sqrt{2}\tau)$.

$$f(u, z) = u^3 - u^2 z + z^2 + 52 - 10z + 44u + 12u^2 - 7uz,$$

z-disc $= (u+6)(u-2)(u+3)^2$,

u-disc $= (z-11)(z^2+4)(z+1)^2$,

$z(t) = 2(2t^3+2t^2+2t+1)/t, \quad u(t) = (2t^2-2t+2)/t$.

$$j_{15}(\tau) = j_{15}(2\tau) \Rightarrow (z-2)(z-14)(z+1)^2 = 0,$$

$$j_{30}(\tau) = j_{30}(2\tau) \Rightarrow (u-3)(u^2+10u+26)(u+3)^2 = 0.$$

5.3. **Modular equations and singular moduli.** The modular equations are determined as described in §4, by elimination. They are not listed, in the interests of brevity and, in principle, it should not be necessary to do so. Nevertheless, we might remark that for a large index N the modular equation for j_N does have *small* coefficients. For instance, with $z = j_{15}(\tau)$ and $Z = j_{15}(2\tau)$ (Case $15 \vee 2$),

$$\Phi_{15\vee 2}(z, Z) := Z^3 + z^3 - z^2Z^2 + 6z^2Z + 6Z^2z - 2z^2 - 2Z^2 + 7zZ - 20Z - 20z - 28 = 0. \tag{5.3a}$$

(Compare this for coefficient size with the modular equation (1.2c) for $j(\tau)$ and $j(2\tau)$!)

The singular moduli, or the roots $Z = z$ and $U = u$ are also listed in Table II. Historically, these values were the objective in computing modular equations (see [5, Ch.11]).

6. Normal parametrization

It is natural to ask which properties of the polynomial $f(u, z)$ in (4.1) characterize a half-step modular equation. A partial answer is a normalization property first used in [8] for traditional modular equations related to class field theory.

When $f(u, z)$ is of genus zero, it can be parametrized as $u = u(t)$, $z = z(t)$. The modular equation in (4.3b) is not just a transition from (u, z) to (U, z), because if we write $U = u(t^*)$, $z = z(t^*)$, it is a transition from t to t^* (but note $z(t) = z(t^*)$). Under certain conditions we can choose t^* so that (as before) $u(t^*) = U$, but $z(t^*) = Z \neq z(t)$. Hence, (u, z) with parameter t shall be transformed (below) into a completely different (U, Z) with parameter t^*, satisfying $f(U, Z) = 0$. *The transition* $t \to t^*$ *is a simplification of the modular relations* (4.3ab) *between* u *and* U (*or* z *and* Z).

We shall use notation like "$f(\overset{n}{u})$" to denote the degree n (maximum exponent of u) in a rational function $f(u)$.

6.1. **Definition of normal parametrization.** *An irreducible* (*polynomial*) *equation of genus zero,*

$$f(\overset{n}{u}, \overset{m}{z}) = 0, \tag{6.1a}$$

with $n > 2$ *is said to be normally parametrized in* (*say*) u *if, first of all, the usual birational parametrization holds*:

$$u = u(\overset{n}{t}), \quad z = z(\overset{m}{t}). \tag{6.1b}$$

Suppose further that for any given t *and* $z(t)$ *we can regard* (6.1a) *as an equation in* u, *with one root assuredly* $u(t)$ *but with other roots* $\{U_i, 1 \leq i \leq n-1\}$ $(U_i \neq u(t))$ *satisfying*

$$R(\overset{n-1}{U}, \overset{m(n-1)}{t}) := \frac{f(U, z(t)) - f(u(t), z(t))}{U - u(t)} = 0. \tag{6.1c}$$

Normal parametrization will (*by definition*) *require that the roots* $\{U_i\}$ *can be parametrizable further in* (*say*) s *as*

$$t = t(\overset{n-1}{s}), \quad U = U(\overset{(n-1)m}{s}). \tag{6.1d}$$

The $n-1$ *roots* s_i *of* $t = t(s)$ *are then parameters in* $U_i = U(s_i)$.

We use the new variable s for the transition from the old parameter t for the point $(u(t), z(t))$ to the new parameter t^* for one of the conjugate points $(U(s), z(t))$. In fact, from (6.1b) and (6.1d), the transition $t \to t^*$ comes from the determination of t^* in

$$u(t^*) - U(s) = 0, \tag{6.2a}$$

which must factor into n rational factors linear in t^*. Hence (6.2a) must produce n (rational) determinations of $t^*(s)$. *Only one of these functions preserves* $z(t^*) = z(t)$, *so we take any one of the other* $n-1$. Thus, we are defining (U, Z) $(Z \neq z(t))$ at the parameter

$$t^* = t^*(\overset{n-1}{s}). \tag{6.2b}$$

6.3. **Definition of iterated (pure) parametrization.** *The equation*

$$t(s^*) - t^*(s) = 0 \tag{6.3a}$$

defines an $(n-1)$*-valued transformation* $s \rightarrow s^*$, *which in turn describes* $(u, z) \rightarrow (U, Z)$. *This transformation may be iterated indefinitely often. In the event that it takes the form*

$$s^* = \sqrt[n-1]{w(s)}, \tag{6.3b}$$

for $w(s)$ *a rational function of* s, *then the iteration is called pure.*

The iteration is most useful when the equations (6.3ab) are used to find singular moduli fields of the form $K(j_N(b^k\tau))$ for $k = 0, 1, 2, \dots$. Then each factor of b in b^k is an iteration step and the values $s \rightarrow s^* \rightarrow \cdots$ generate successive class fields $K(s) \rightarrow K(s^*) \rightarrow \cdots$. (See [2], [5, Ch.11, §3]).

Thus, in Table III (next page), we see some pure iterated forms simplifying the modular equations for type $\Phi(z, Z)$ or $\Psi(u, U)$:

$$\begin{aligned} &\text{Case } 1 \vee 2: \ s^* = \frac{s+3}{\sqrt{8(s+1)}}, \\ &\text{Case } 3 \vee 2: \ s^* = \sqrt{\frac{s^2+3}{2(s+1)}} \\ &\text{Case } 1 \vee 3: \ s^* = \frac{s+2}{\sqrt[3]{9(s^2+s+1)}}. \end{aligned} \tag{6.3c}$$

6.4. **Theorem on normal parametrization from Table III.** Where $f(u, z)$ has the pattern of singularities of $a \vee 2$, i.e., with dominant terms

$$f(u, z) = u^3 - u^2 z + z^2 + \cdots, \tag{6.4a}$$

the only cases of normal parametrization are given (esssentially) in terms of one parameter α.

Where $f(u, z)$ has the pattern of singularities of $a \vee 3$, i.e., with dominant terms

$$f(u, z) = u^4 + z^2 - u^3 z + \cdots, \tag{6.4b}$$

the only cases of normal parametrization over $\mathbf{R}$ are given (essentially) in terms of one parameter α.

Both of the above cases lead to pure iteration.

Finally, the case $1 \vee 5$ is authenticated as normally parametrized (but not with pure iteration).

TABLE III. Normal parametrizations

Special cases $a \vee b$ of order $b = 2, 3$, and 5.

$$Case\ a \vee 2:\ f(u, z) = u^3 - u^2 z + z^2 + \cdots,$$

$$z(t) = \frac{\alpha^3(\alpha t + 1)^3}{t}, \quad u(t) = \frac{\alpha^3(t+1)^2}{t};$$

$$\begin{aligned} f(u, z) = {} & u^3 - u^2 z + z^2 + (\alpha - 1)(4\alpha^2 + \alpha + 1)uz + 3\alpha^2(\alpha - 1)^2 u^2 \\ & - 2\alpha^3(\alpha - 1)^3 z + 3\alpha^4(\alpha - 1)^4 u + \alpha^6(\alpha - 1)^6. \end{aligned}$$

$$t(s) = \frac{4}{(s^2 - 1)\alpha}, \quad U(s) = \frac{(s^2 + 2\alpha s - 2s + 1 + 2\alpha)^2 \alpha^2}{2(s+1)(s-1)^2};$$

$$u(t^*) - U(s) = 0 \Rightarrow t^*(s) = \frac{2(s+1)\alpha}{(s-1)^2}.$$

$$t(s^*) - t^*(s) = 0 \Rightarrow s^* = \sqrt{\frac{(2s^2 + s\alpha^2 - 4s + 2 + \alpha^2)}{(s+1)\alpha^2}}.$$

$$Case\ 1 \vee 2\ (\alpha = 4):\ t^*(s) = \frac{8(s+1)}{(s-1)^2}, \quad t(s^*) = \frac{1}{s^{*2} - 1}, \quad s^* = \frac{s+3}{\sqrt{8(s+1)}},$$

$$Case\ 3 \vee 2\ (\alpha = 2):\ t^*(s) = \frac{4(s+1)}{(s-1)^2}, \quad t(s^*) = \frac{1}{2(s^{*2} - 1)}, \quad s^* = \sqrt{\frac{s^2 + 3}{2(s+1)}}.$$

Parametrization Remark. The cubic $f(u, z) = 0$ has a double point at (u_0, z_0) where

$$u_0 = 1 - 3\alpha^2 + 2\alpha^3, \quad z_0 = 1 - 3\alpha^2 + 3\alpha^4 - \alpha^6.$$

If $u' = u - u_0$ and $z' = z - z_0$, then $f(u, z)$ simplifies to

$$F(u', z') = u'^3 - u'^2 z' + z'^2 + 3(\alpha^2 - 1)u'z' + (\alpha^6 - 3\alpha^2 + 2)u'^2.$$

The parameter t is defined uniquely from (u, z) (or (u', z')) by

$$\alpha^3 t + 1 = z'/u'.$$

$$Case\ a \vee 3:\ f(u, z) = u^4 + z^2 - u^3 z + \cdots,$$

$$z(t) = \frac{\alpha^2(\alpha t + 1)^3(\alpha t + 9)}{27t}, \quad u(t) = \frac{\alpha^2(t+1)^2}{3t},$$

$$\begin{aligned} f = {} & \alpha^4(\alpha - 9)^2(\alpha - 1)^6 + 36\alpha^3(\alpha^2 - 6\alpha + 21)(\alpha - 1)^4 u + 54\alpha^2(\alpha - 9)(\alpha - 1)^3 z \\ & + 54\alpha^2(5\alpha^2 - 18\alpha + 45)(\alpha - 1)^2 u^2 - 243(\alpha - 1)(3\alpha^3 - 13\alpha^2 - 3\alpha - 3)uz \\ & + 729z^2 + 1458\alpha(\alpha - 2)u^2 z + 108\alpha(7\alpha^2 - 18\alpha + 27)u^3 + 729u^4 - 729zu^3. \end{aligned}$$

$$t(s) = \frac{9}{\alpha(s^3 - 1)}, \quad U(s) = \frac{\alpha(s^3 - 3s^2 + \alpha s^2 + \alpha s + 3s + \alpha - 1)^2}{3(s^2 + s + 1)(s-1)^3};$$

$$u(t^*) - U(s) = 0 \Rightarrow t^*(s) = \frac{\alpha(s^2 + s + 1)}{(s-1)^3}.$$

$$t(s^*) - t^*(s) = 0 \Rightarrow s^* = \sqrt[3]{\frac{9s^3 - 27s^2 + 27s - 9 + \alpha^2 s^2 + \alpha^2 s + \alpha^2}{\alpha^2(s^2 + s + 1)}}.$$

$$Case\ 1 \vee 3\ (\alpha = 9):\ t^*(s) = \frac{9(s^2 + s + 1)}{(s-1)^3}, \quad t(s^*) = \frac{1}{s^{*3} - 1},$$

$$s^* = \frac{s+2}{\sqrt[3]{9(s^2 + s + 1)}}.$$

TABLE III (continued)

Case $1 \vee 5$:

$$f = u^6 + z^2 - u^5 z - 3456z + 13436928u + 20217600u^2 + 10264320u^3 \\ +140400u^4 + 648u^5 - 7776uz - 1890zu^3 + 80zu^4 + 12600zu^2 + 2985984$$

$$z(t) = -\frac{(3125 - 250t + t^2)^3}{t^5}, \quad u(t) = -\frac{125 - 22t + t^2}{t};$$

$$t(s) = s^5 - 5s^4 + 15s^3 - 25s^2 + 25s,$$
$$U(s) = -\frac{(s^2 - 2s + 5)(s^4 - 10s^3 + 45s^2 - 100s + 125)^2}{s^5(s^4 - 5s^3 + 15s^2 - 25s + 25)};$$

$$u(t^*) - U(s) = 0 \Rightarrow t^*(s) = t\left(\frac{5}{s}\right),$$

$$t(s^*) - t^*(s) = 0 \Rightarrow 125 = t(s)t\left(\frac{5}{s^*}\right)$$

For *proof*, we first note that the "essential" uniqueness asserted here is of course valid only to within translations of u and z and fractional linear transformations of t. The two singularities are taken to be $t = 0$ and ∞ and the translations are so chosen that both $u = 0$ and $z = 0$ have multiple roots in t.

Case $a \vee 2$: In view of the behavior at ∞ inferred from (6.4a) we must start with two parameters α and β. They are used in such a fashion that as $t \to \infty$, $z \approx u^2$, and as $t \to 0$, $z \approx u$:

$$z = \frac{\alpha^2\beta(\alpha t + 1)^2(\beta t + 1)}{t}, \quad u = \frac{\alpha^2\beta(t + 1)^2}{t}. \tag{6.5a}$$

Proceeding, as in the definition (and omitting routine steps in computer algebra), we obtain $f(u, z)$ as the t-resultant of (6.5a) with parameters α and β. Likewise, we compute $R(U, t)$ from (6.1c), and we next calculate the discriminant

$$U\text{-disc}(R) = t(\beta t + 1)(\alpha^2\beta t^2 + \alpha^2 t + 4\alpha\beta t + 4b) \cdot F^2, \tag{6.5b}$$

where F is some rational function of t (with parameters α, β). This will lead to a nonuniformizable (elliptic) curve unless $(\beta t + 1)$ divides the last factor, possible only if $\alpha = \beta$. Thus, now,

$$U\text{-disc}(R) = t\alpha^3(\alpha t + 4) \cdot F^2, \tag{6.5c}$$

which leads to the uniformization $t(s)$.

The parameters are in Table III, and the familiar cases "$1 \vee 2$" ($\alpha = 4$) and "$3 \vee 2$" ($\alpha = 2$) are also shown.

Case $a \vee 3$: Similarly, we must start with three parameters used in such a fashion that as $t \to \infty$, $z \approx u^3$, and as $t \to 0$, $z \approx u$:

$$z = \frac{\alpha\beta(\alpha t + 1)^2(\beta^2 t^2 + \gamma t + 1)}{t}, \quad u = \frac{\alpha\beta(t + 1)^2}{t}. \tag{6.6a}$$

Once again, we define $f(u, z)$ and $R(U, t)$, this time with α, β, and γ as parameters. We know again that for further parametrization there must be a square discriminant, which we calculate as before:

$$\begin{aligned}
U\text{-disc}(R) &= \alpha d_1 d_2 \cdot F^2, \\
d_1 &= \beta^2 t^2 + \gamma t + 1, \\
d_2 &= 36\alpha^2\beta^4 t + 26\alpha^3\beta^4 t^2 + 7\alpha^5\beta^4 t^4 + 27\beta^4\alpha + 4\alpha^5\beta^2 t^2 + 18\alpha^3\beta^2\gamma t \\
&\quad + 16\alpha^4\beta^6 t^5 + 34\alpha^3\beta^6 t^4 + 20t^3\alpha^4\beta^4 + \alpha^5\beta^2\gamma^2 t^4 + 48\alpha^2\beta^4\gamma t^2 \\
&\quad + 5\alpha^5\beta^4 t^5\gamma + 28\alpha^4\beta^4 t^4\gamma + 20\alpha^4\beta^2\gamma t^2 + 18\alpha^3\beta^2\gamma^2 t^2 + 56\alpha^3\beta^4\gamma t^3 \\
&\quad + 6\alpha^5\beta^2\gamma t^3 + 8\alpha^4\beta^2\gamma^2 t^3 + 36\beta^6\alpha^2 t^3 - \gamma^3\alpha^5 t^3 - \alpha^5\gamma^2 t^2 \\
&\quad + 12\alpha^2\beta^2\gamma^2 t + 4\beta^6 t + 15\alpha\beta^4\gamma t - 4\gamma^3\alpha^3 t - 4\alpha^4\gamma^3 t^2 \\
&\quad + 3\alpha^5\beta^6 t^6 + 19\beta^6\alpha t^2.
\end{aligned} \tag{6.6b}$$

To have a perfect square, $d_1 | d_2$, thus

$$t\text{-resultant}(d_1, d_2) := 16\beta^{14}(-\alpha\gamma + \alpha^2 + \beta^2)^4 = 0. \tag{6.6c}$$

So we substitute $\beta^2 = \alpha\gamma - \alpha^2$ and ask when the polynomial $d_{12} = d_2/d_1$ is a perfect square. Thus,

$$\begin{aligned}
d_{12} = {} & 3\alpha^6 t^4 - 6\alpha^5 t^4\gamma + 16\alpha^5 t^3 + 3\alpha^4 t^4\gamma^2 - 34\alpha^4 t^3\gamma + 30\alpha^4 t^2 \\
& + 18\alpha^3 t^3\gamma^2 - 76\alpha^3 t^2\gamma + 32\alpha^3 t + 45\alpha^2\gamma^2 t^2 - 90\gamma\alpha^2 t \\
& + 27\alpha^2 + 54\alpha\gamma^2 t - 54\alpha\gamma + 27\gamma^2,
\end{aligned} \tag{6.6d}$$

which is a perfect square only when

$$t\text{-disc}(d_{12}) := 256(-9\gamma + 10\alpha)^2(-\gamma + \alpha)^2(-\gamma + 2\alpha)^2(2\alpha - 3\gamma)^4\alpha^{14} = 0. \tag{6.6e}$$

There are four possible relations in α and γ as seen by the factors. The second is degenerate ($\gamma = \alpha$, $\beta = 0$) and the last two lead to β imaginary, so we are left with

$$\gamma = 10\alpha/9, \quad \beta = \alpha/3. \tag{6.6f}$$

The parameters again are in Table III, and the only familiar case is "$1 \vee 3$" ($\alpha = 9$).

Case $1 \vee 5$: Here "icosahedral" techniques enter which are computationally much more difficult, and no requirement for parametrization can be established at this point. We content ourselves with a reference to [2], where the iterative parameters have been already calculated and are summarized in Table III. (Note the variable t of Table II is changed to $-\sqrt{125}/t$ in Table III mostly for the convenience of removing $\sqrt{5}$).

7. Concluding remarks

This work would not have been possible without the intensive use of Taylor series, discriminants, resultants, and polynomial factorization all in multivariate mode. The system used was MAPLE for the Sun Workstation.

The immediate context in which the half-step modular equation arose was that of the Hilbert modular equations for $\mathbf{Q}(\sqrt{2})$ and for $\mathbf{Q}(\sqrt{3})$. Without burdensome details (see [3, 7]) we can make the analogy that the transformation "$\tau \to 2\tau$" becomes

$$\mathbf{Q}(\sqrt{2}): \ (\tau, \tau') \to ((2 + \sqrt{2})\tau, (2 - \sqrt{2})\tau'), \ (2 \pm \sqrt{2})^2 = 2 \cdot (\text{unit}); \tag{7.1a}$$

$$\mathbf{Q}(\sqrt{3}): \ (\tau, \tau') \to ((1 + \sqrt{3})\tau, (1 - \sqrt{3})\tau'), \ (1 \pm \sqrt{3})^2 = 2 \cdot (\text{unit}). \tag{7.1b}$$

Thus, the transformation for Hilbert modular equations is intrinsically "half-step." This is seen explicitly. While the modular equations in one variable τ are curves, the modular equations in two variables (τ, τ') are two-dimensional varieties in four-space. As such they have trace curves at ∞ which are half-step curves. For instance, $\mathbf{Q}(\sqrt{2})$ leads to Case $1 \vee 2$ (see [4]), while $\mathbf{Q}(\sqrt{3})$ is more complicated. The latter has a curve at ∞ with two branches denoted (see [7]) by "D^*", which is Case $1 \vee 2$ again, and "D", which is Case $3 \vee 2$.

If the modular equations in two variables can also be built out of infinite behavior (like singularities) then these modular equations would also be easier to compute.

As often before, we must acknowledge our debt to John McKay for his advice on many details and for his unrelenting advocacy (see [12]) of extended modular functions as a tool for group characters. We also thank the referees for valuable suggestions.

Bibliography

1. A.O.L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.
2. H. Cohn, *Iterated ring class fields and the icosahedron*, Math. Ann. **255** (1981), 107–122.
3. ——, *An explicit modular equation in two variables and Hilbert's twelfth problem*, Math. Comp. **38** (1982), 227–236.
4. ——, *Some examples of Weber-Hecke ring class field theory*, Math. Ann. **265** (1983), 83–100.
5. ——, *Introduction to the construction of class fields*, Cambridge Univ. Press, 1985.
6. ——, *A numerical survey of the reduction of modular curve genus by Fricke's involutions*, Number Theory (New York Seminar (1989-1990)), Springer-Verlag, New York, 1991, pp. 85–104.
7. H. Cohn and J. Deutsch, *Some singular moduli for* $\mathbf{Q}(\sqrt{3})$, Math. Comp. **59** (1992), 231–247.
8. H. Cohn, *How branching properties determine modular equations*, Math. Comp. **61** (1993), 155–170.
9. H. Cohn and M.I. Knopp, *Application of Dedekind eta-multipliers to modular equations*, in *The Rademacher Legacy to Mathematics* (G. E. Andrews, D. M. Bressoud and L. A. Parson, eds.), Contemp. Math., vol. 166, Amer. Math. Soc., Providence, RI, 1994, pp. 9–34.
10. R. Fricke, *Lehrbuch der Algebra* III (*Algebraische Zahlen*), Vieweg, Braunschweig, 1928.
11. R. Fricke, *Über die Berechnung der Klasseninvarianten*, Acta Math. **52** (1929), 257–279.
12. J. McKay and H. Strauss, *The q-decompositions of monstrous moonshine and the decomposition of the head characters*, Comm. Algebra **18** (1990), 253–278.

Department of Mathematics, City College (CUNY), New York, New York 10031
E-mail address: hihcc@cunyvm.edu