Fricke's Two-Valued Modular Equations

By Harvey Cohn*

Abstract. The modular equation of order b is a polynomial relation between j(z) and j(z/b), which has astronomically large coefficients even for small values of b. Fricke showed that a two-valued relation exists for 37 small values of b. This relation would have much smaller coefficients and would also be convenient for finding singular moduli. Although Fricke produced no two-valued relations explicitly (no doubt because of the tedious amount of algebraic manipulation), they are now found by use of MACSYMA. For 31 cases ranging from b=2 to 49, Fricke provided the equations necessary to generate the relations (with two corrections required). The remaining six cases (of order 39, 41, 47, 50, 59, 71) require an extension of Fricke's methods, using the discriminant function, theta functions, and power series approximations.

1. Introduction. The modular equation of order b is a well-known polynomial relation between j(z) and j(z/b) for $1 < b \in \mathbb{Z}$. Here we use the usual definitions

(1.1a)
$$j(z) = \left[1 + 240 \sum_{1}^{\infty} n^3 q^n / (1 - q^n)\right]^3 / \Delta(z),$$

(1.1b)
$$\Delta(z) = q \prod_{1}^{\infty} (1 - q^n)^{24},$$

$$(1.1c) q = \exp 2\pi i z.$$

The (Weber) modular invariant j(z) is defined for $z \in H$, the upper half plane, and its important properties are its invariance under the modular group $\Gamma = \mathrm{PSL}(2, \mathbf{Z})$ and its behavior at ∞ :

$$(1.2a) j(z+1) = j(-1/z) = j(z),$$

$$(1.2b) j(z) = 1/q + 744 + O(q)$$

as $z \to i\infty$ $(q \to 0)$, see [7], [8], [5]. The function j(z/b) is invariant under a subgroup of the modular group, namely $\Gamma^0(b)$, which is of index

$$(1.3) m = b \prod (1 + 1/p)$$

Received December 19, 1987; revised February 22, 1988.

1980 Mathematics Subject Classification (1985 Revision). Primary 11F11; Secondary 11F27, 11R37.

Key words and phrases. Modular equation, singular moduli, theta-functions.

^{*}Research supported by NSF Grant DMS 8700878.

(over primes $p \mid b$). This is the degree of the modular equation. The compactified quotient space $H/\Gamma^0(b)$ is a Riemann surface S_b over H/Γ for which the genus is shown (see [7]) to equal

$$(1.4) g = 1 + (m - 4a_0 - 3a_1 - 6c)/12,$$

where

(1.5a)
$$a_0 = \operatorname{card}\{x \mod b : x^2 + x + 1 \equiv 0\},\$$

(1.5b)
$$a_1 = \operatorname{card}\{x \mod b : x^2 + 1 \equiv 0\},\$$

and (the number of cusps) c is given by

(1.5c)
$$c = \sum_{d|b} \phi(d/(d, b/d)).$$

Now Fricke [7] considered the extension of the group $\Gamma^0(b)$ via the involution $z \leftrightarrow W(z) = -b/z$ to form $\Gamma^0(b)^* = \Gamma^0(b) + W\Gamma^0(b)$, an extension with index 2. (This involution was generalized by Atkin and Lehner [1].) Thus the compactified quotient space $H/\Gamma^0(b)^* = S_b^*$ is a Riemann surface over which S_b is a double covering. The genus of S_b^* was shown [7] to be

(1.6a)
$$g^* = (1+g)/2 - e_b h(-4b)/12 \qquad (b > 4),$$

where h(d) is the class number for primitive quadratic forms of discriminant d and

(1.6b)
$$e_b = \begin{cases} 4, & b \equiv 3 \mod 8, \\ 6, & b \equiv 7 \mod 8, \\ 3, & \text{otherwise.} \end{cases}$$

(For $b \le 4$, special calculations show $g^* = 0$.)

Fricke restricts attention to the 37 cases where $g^* = 0$ (see Table I). For such cases a single-valued function t exists on S_b^* which becomes double-valued on S_b . So a general point on S_b is determined by the pair (t,s) where

$$(1.7) s^2 = P_{2q+2}(t)$$

for $P_{2g+2}(t)$ a polynomial of degree 2g+2 (with simple roots). Because j(z/b)=j(-b/z)=j(W(z)), it follows that a rational function $F_b(t,s)$ exists on S_b such that

$$(1.8a) j(z) = F_b(t, s),$$

(1.8b)
$$j(z/b) = F_b(t, -s).$$

From (1.6a), the 37 cases where $g^* = 0$ necessarily include all cases of genus g = 0 or 1. Conversely, the cases with g > 1 are hyperelliptic. (Some hyperelliptic cases do not occur, however, such as b = 37, and this is a matter of continuing study; see [14], [17], [19].) For the 14 cases of genus g = 0, Fricke [7] gives only a rational parametrization of the relation between j(z) and j(z/b), and it is necessary for us to derive the relation (1.8a,b) from it (see Section 2). For 17 of his cases

where g > 0 (listed in Table I), Fricke [7], [8] gives the function $F_b(t, s)$ explicitly in a remarkably simple form each time (see Section 3).

TABLE I

Fricke's 37 Cases for Two-valued Modular Equations

10 11 12 13 14 remarks

b = order- 1 g = genus24 48 30 42 36 m = degree7c8n 8n 8n remarks c

The cases were run from data common to [7] and [8] (see Tables II and III), but we note these exceptions as remarks:

- 7 =data offered only in [7]
- 8 =data offered only in [8]
- c = corrections required (see Section 3)
- n = not enough data offered by Fricke for computation
- o = omitted by Fricke (no data offered)

In all 37 cases where $g^* = 0$, we then have the two-valued modular equation

$$(1.9a) j(z)j(z/b) = N_b(t),$$

(1.9b)
$$j(z) - j(z/b) = D_b(t,s) \quad [= sR_b(t)],$$

where $N_b(t)$ is the norm and $D_b(t, s)$ is the different, if we think of j(z) and j(z/b) as roots of the equation

(1.10a)
$$X^2 - S_b(t)X + N_b(t) = 0.$$

Here, $S_b(t)$ is the trace function defined by

(1.10b)
$$j(z) + j(z/b) = S_b(t) = (D_b^2(t,s) + 4N_b(t))^{1/2}$$

(with positive branch at ∞). It is easily seen that $N_b(t)$ and $S_b(t)$ as symmetric functions are rational in t, and so is $R_b(t)$. The functions $N_b(t)$ and $D_b(t,s)$ are shown in Tables II and III of the Appendix.

The choice of t and s for g > 0 was made by Fricke, and is motivated by the condition that z = 0 (and ∞) correspond to ∞ with the following orders of magnitude:

(1.11a)
$$j(z) = t^b + bC_b t^{b-1} + O(t^{b-2}),$$

(1.11b)
$$j(z/b) = t + C_b + 744 + O(1/t)$$

(see (1.2b)). For g = 0, we shall construct the functions $F_b(t, s)$ (in Section 2) to satisfy the same asymptotic conditions. Of course there is still an arbitrary translation in t, as well as an arbitrary rational transformation in the choice of s.

The modular equations have astronomically large coefficients and are known in relatively few cases (although the computation is rather straightforward [20]). We shall note that Fricke's two-valued form (1.9a,b) keeps coefficients small, at

least in the factored form of the norm and the different (although not the trace). We observe that the norm is either a cube or it has a major cubic factor whose coefficients are "one-third" as long as otherwise. The different also must have factors of "low degree" to correspond with the small class numbers connected with singular moduli, defined as values of $j(z_0)$ for which $j(z_0) = j(z_0/b)$. These values are necessarily associated with roots t_0 of $D_b(t,s)$ (see [3], [6], and [9]). These roots satisfy

$$(1.12) j(z_0) = j(z_0/b) [= N(t_0)^{1/2}].$$

Such values arise from equations for z_0 of the type

$$(1.13) z_0/b = M(z_0)$$

for M(z) an element of Γ . This will be illustrated in Section 2 for b=2. We should also cite another approach [2] to modular equations (currently associated with Ramanujan). In this approach the coefficients are kept small by using invariants other than j(z), which determine special subgroups of the modular group.

To complete the introduction, we make clear that the present computation serves to create the equations (1.9a,b) from formulas given in Fricke [7], [8] (and reformulated somewhat when g=0). We do this by means of MACSYMA, a symbolic language system which handles polynomials and substitutions in (almost) natural language. First, the polynomial $s^2 - P_{2g+2}(t)$ is read explicitly into the system so that a rational substitution for s^2 is performed every time s^2 is encountered. Then the rational simplification operation is performed on the explicit formulas for the product $F_b(t,s)F_b(t,-s)$ to produce $N_b(t)$. Likewise, $(F_b(t,s)-F_b(t,-s))/s$ reduces to the rational function $D_b(t,s)/s$. Finally, the factorization operation renders the formulas in Tables II and III.

2. Genus Zero. For the cases with g = 0, Fricke [7], [8] gave implicit modular equations by a rational function $F_b(x)$. We shall change variables (see (2.3a,b,c) below) to produce $F_b(t,s)$. Thus

$$(2.1a) j(z) = F_b(x),$$

$$xy=1.$$

$$(2.1b) j(z/b) = F_b(y),$$

Here, x is uniquely defined by the values x=0 at $z=\infty$, x=1 at $z=\sqrt{-b}$, and $x=\infty$ at z=0. Then it follows that as $z\to\infty$,

$$(2.2a) j(z) \approx (B/x)^b,$$

(2.2b)
$$j(z/b) \approx B/x$$
,

for some positive B. Thus the involution $z \leftrightarrow W(z)$ is expressed by $x \leftrightarrow y$ or $j(z) \leftrightarrow j(z/b)$. We now change variables so as to turn the symmetry of x and y into that of (t, s) and (t, -s):

(2.3a)
$$x = (1-w)/(1+w), \quad y = (1+w)/(1-w),$$

(2.3b)
$$w^2 = (t - 2B)/(t + 2B).$$

Of course, with s = (t + 2B)w, we can write (1.7) as

$$(2.3c) s^2 = t^2 - 4B^2.$$

Actually, Fricke's data are not always consistent. Sometimes the roles of x and y are interchanged and sometimes x and y are scaled to avoid radicals (say \sqrt{a}) so "xy = 1" becomes "xy = a". We do not dwell on this matter, particularly since algebraic systems like MACSYMA can treat the radical as a symbol.

For the special cases where (b-1)|24, we can take

(2.4)
$$x = (\Delta(z)b^6/\Delta(z/b))^{1/(b-1)},$$

since $\Delta(z)$ is a modular form for Γ of weight 12, i.e.,

(2.5)
$$\Delta(z) = \Delta(z+1) = \Delta(-1/z)z^{-12}.$$

Thus from the various expansions into q, we evaluate

$$(2.6a) B = b^{6/(b-1)},$$

(2.6b)
$$C_b = 24/(b-1)$$
.

As an illustration for b=2,

(2.7a)
$$F_2(x) = 64(x+4)^3/x^2,$$

and so from (2.2a) or (2.6a), B = 64, and the result in Tables II and III follows. Explicit use of formulas (1.10a,b) would yield

$$(2.8a) j(z) = [t^2 + 49t - 6656 + (t+47)(t^2 - 128^2)^{1/2}]/2,$$

(2.8b)
$$j(z/2) = [t^2 + 49t - 6656 - (t+47)(t^2 - 128^2)^{1/2}]/2.$$

To find singular moduli, we take the roots of $D_2(t,s)=0$, i.e., $t_0=128, -47, -128$, and substitute them to find $j(z_0)=j(z_0/2)=20^3$ [= $j(\sqrt{-2})$], -15^3 [= $j((1+\sqrt{-7})/2)$], 12^3 [= j(i)]. The values of z_0 that enter here (see (1.13)) come from

(2.9a)
$$z_0/2 = -1/z_0$$
 $(z_0 = \sqrt{-2}),$

(2.9b)
$$z_0/2 = -1/(z_0 - 1) \qquad (z_0 = (1 + \sqrt{-7})/2),$$

(2.9c)
$$z_0/2 = (z_0 - 1)/z_0$$
 $(z_0 = 1 + i)$.

To find singular moduli for all b was indeed a principal goal of Fricke's Algebra [8] (also see [10]). Fricke could not carry it out completely, however, since he had only the radical factor s in $D_b(t,s)$, rather than the whole expansion into factors.

3. Higher Genus. For g > 0 but $g^* = 0$, Fricke presented expressions of the form

$$(3.1a) j(z) = F_b(t, s),$$

(3.1b)
$$j(z/b) = F_b(t, -s),$$

$$(3.1c) s^2 = P_{2a+2}(t),$$

with rational $F_b(t, s)$ and polynomial $P_{2g+2}(t)$ (of degree 2g + 2). The derivations of these functions are an ingenious patchwork of methods; the most interesting is

perhaps the use of theta series of quadratic forms to define t and s. Fricke does such a derivation for b = 11 (the first case of genus 1):

(3.2a)
$$F_{11}(t,s) = \frac{4t(61t^2 - 368t + 352 + 60s)^3}{(t(t^2 - 21t + 88) - s(t - 11))^2},$$

(3.2b)
$$s^2 = t(t^3 - 20t^2 + 56t - 44).$$

Here, as elsewhere, the equations (1.9a,b) are derived by using MACSYMA (see Section 1). Fricke's formulas for $F_b(t,s)$ have only two errors, which we proceed to correct (see Table I).

For b = 27, Fricke [8, p. 464] used as his starting point the formula for b = 9 (genus g = 0):

(3.3a)
$$F_9(X) = 27(X+1)^3(9X^3 + 27X^2 + 27X + 1)/X(X^2 + 3X + 3),$$

so that for (2.1a,b),

$$(3.3b) j(z) = F_9(X),$$

(3.3c)
$$j(z/9) = F_9(Y),$$

but here XY = 3 (to avoid using $\sqrt{3}$). To proceed to b = 27, Fricke needed new variables x and y in $F_9(x)$ and $F_9(y)$ to write

$$(3.4a) j(z) = F_9(x),$$

(3.4b)
$$j(z/27) = F_9(y).$$

The correct values are given by

$$(3.5a) x3y3 = 81(x2 + 3x + 3)(y2 + 3y + 3),$$

$$(3.5b) t = 3(x+3)(y+3)/(xy-9),$$

$$(3.5c) s = 27(x-y)(2xy+3x+3y)/(xy-9),$$

(3.5d)
$$s^2 = (t+3)(t^3 - 3t^2 - 9t - 9).$$

Thus we substitute into (3.4a,b) x = G(t, s), y = G(t, -s), where

(3.6)
$$G(t,s) = 3((t+3)^2 + s)/(t^2 - 9 - s).$$

There is another error in Fricke [7, p. 418] for b = 23. It is necessary to replace "-288" by "-24" in the formula (47).

4. Introduction to Remaining Cases. For six cases (of order b = 39, 41, 47, 50, 59, 71), Fricke did not provide the formulas to deduce the modular equations by direct substitution. We must therefore examine Fricke's methods in enough detail to extend the computations. We use the discriminant function for b = 39 and 50 and theta functions for b = 41, 47, 59, and 71.

We need to express j(z) in terms of these modular forms:

(4.1)
$$j(z) = E_2^3(z)/\Delta(z) = 12^3 + E_3^2(z)/\Delta(z),$$

where

(4.2a)
$$E_2(z) = 1 + 240 \sum_{1}^{\infty} n^3 q^n / (1 - q^n),$$

(4.2b)
$$E_3(z) = 1 - 504 \sum_{1}^{\infty} n^5 q^n / (1 - q^n).$$

When $z \to z/b$, the parameter $q = \exp 2\pi i z$ is replaced by

(4.3)
$$r = q^{1/b} = \exp 2\pi i z/b.$$

Following Fricke [7], we express the action of the involution $W:(z \to -b/z)$ by the use of "primed" symbols:

$$(4.4a) F = F(z/b), F' = F(z)b^k$$

for F(z) a modular form of weight 2k, and likewise

(4.4b)
$$j = j(z/b), \quad j' = j(z).$$

We also need the result from class field theory [7, p. 366] that for prime $b \equiv 3 \pmod{4}$, the polynomial $P_{2g+2}(t)$ lies in $\mathbf{Z}[t]$ and has factors of degree h(-b) and h(-4b), where h(d) is the class number for primitive quadratic forms of discriminant d. Thus in Fricke's cases (compare (1.6a,b) above),

$$(4.5) 2g + 2 = h(-b) + h(-4b) (b > 3).$$

Also, h(-4b) = h(-b) or 3h(-b) for $b \equiv 7$ or 3 (mod 8), respectively.

5. The Cases b = 26, 39, and 50. We follow the pattern set by Fricke for b = 26. We must calculate not only $P_{2g+2}(t)$ but also $F_b(t,s)$ for (1.8a,b). These cases have the common property that b = kg, where the (integral) factors k and g are such that the following groups determine function fields of indicated genus (compare Newman [15], [16]):

(5.1a)
$$\Gamma^0(k)$$
 of genus 0,

(5.1b)
$$\Gamma^0(b)$$
 of genus g ,

where

(5.1c)
$$(k-1)(g-1) = 24/h$$
 $(h \in \mathbf{Z}).$

The functions $F_k(x)$ used in (2.1a,b) (above) are renormalized as

(5.2a)
$$G_k(x) = F_k(K^{1/2}/x), \qquad K = k^{12/(k-1)},$$

so that instead of (2.1a,b), we have

(5.2b)
$$j(z) = G_k(x) \approx x^k \quad (\text{as } x \to \infty),$$

(5.2c)
$$j(z/b) = G_k(K/x) \approx K/x \quad (\text{as } x \to 0).$$

The following cases fall under (5.1a,b,c):

Fricke [7] provides us with the formulas:

(5.2d)
$$G_{13}(x) = (x^2 + 5x + 13)(x^4 + 7x^3 + 20x^2 + 19x + 1)^3/x,$$

$$(5.2e) \quad G_{25}(x) = \frac{(x^{10} + 10x^9 + 55x^8 + 200x^7 + 525x^6 + 1010x^5 + 1425x^4 + 1400x^3 + 875x^2 + 250x + 5)}{x(x^4 + 5x^3 + 15x^2 + 25x + 25)}$$

We now define parameters invariant under $\Gamma^0(b)$ (and indicate the leading term in the Laurent series in r),

(5.3a)
$$t = \left[\frac{\Delta(z/k)\Delta(z/g)}{\Delta(z)\Delta(z/kg)} \right]^{h/24} \approx \frac{1}{r},$$

(5.3b)
$$u = \left[\frac{\Delta(z/k)^g \Delta(z/g)}{\Delta(z)^g \Delta(z/kg)}\right]^{h/24} \approx \frac{1}{r^{g+1}}.$$

Then Wt = t and $Wu = Kt^{g+1}/u$, so we have a (monic) polynomial

$$(5.3c) P(t) = u + Kt^{g+1}/u$$

invariant under W, while 2u - P(t) (= s) changes sign. Thus,

(5.3d)
$$s^2 = P(t)^2 - 4Kt^{g+1} \qquad (= P_{2g+2}(t)).$$

Finally, we have the function required for (1.8a,b):

(5.4)
$$F_b(t,s) = G_k[(P(t) + s)/2t].$$

For our specific cases we verify that (5.3d) becomes

$$(5.5a) b = 26: s2 = (t3 - 4t2 - 4t + 1)2 - 52t3,$$

(5.5b)
$$b = 39: \quad s^2 = (t^3 - 3t^2 - 3t + 1)^2 - 52t^4,$$

(5.5c)
$$b = 50: s^2 = (t^3 - 2t^2 - 2t + 1)^2 - 20t^3.$$

The equations (5.5a,b,c), or more precisely, the polynomials P(t), are found by expanding t and u into Laurent series truncated to width g+1 in r with pole at 0. (Here "width" refers to the difference between the highest and lowest exponent.) Then in (5.3c), the series for P(t) has a pole of order g+1, which can be reverted into an expansion in t (actually a polynomial). This is even easily done by hand. The polynomial P(t) was found for b=26 by Fricke [7] and for b=50 by Birch [4]. (Compare Kenku [11] for b=39.)

6. Some Special Theta Functions. For the remaining four values of b, the relation between s and t is found by using three closely related theta functions. We start with the form

(6.1)
$$F(m,n) = Rm^2 + Smn + Tn^2 \qquad (R > 0, S^2 - 4RT < 0).$$

For $-b = S^2 - 4RT$, $b \equiv 3 \mod 4$, we define the series

(6.2a)
$$\theta(R, S, T) = \sum r^{F(m,n)} \qquad (n, m \in \mathbf{Z}).$$

For $-b = S^2 - 4RT$, $b \equiv 3 \mod 8$, we define the series

(6.2b)
$$\phi(R, S, T) = \sum_{n} r^{F(m,n)/2} (-1)^n \qquad (n, m \in \mathbf{Z}, m \text{ odd}).$$

For $-b = (S^2 - 4RT)/4$, $b \equiv 1 \mod 4$, we define the series

(6.2c)
$$\sigma(R, S, T) = \sum_{n} r^{F(m,n)/4} (-1)^n \quad (n, m \in \mathbf{Z}, m \text{ odd}).$$

These functions are interrelated for $b \equiv 3 \mod 8$, e.g.,

(6.3)
$$\phi(R, S, T) = -\theta(R/2, S/2, T/2) + \theta(R/2, S, 2T) + \theta(2R, S, T/2) - \theta(2R, 2S, 2T).$$

If we use the symbol γ to denote θ , ϕ , or σ , then by Poisson's summation method, for each case (see [7] or [18])

(6.4)
$$\gamma(z) = i\sqrt{b}\gamma(-b/z)/z.$$

This shows the action of Wz = -b/z. A more difficult analysis is required for $U(z) = (Az + B)/(Cz + D) \in \Gamma^0(b)$ ($B \equiv 0 \mod b$). We summarize a result in Fricke [7] (compare [18]): Set

(6.5)
$$\mu(z) = \gamma(z)\Delta(z)^e,$$

where $e=0,\ 1/2,\ {\rm or}\ k/4$ according to $\gamma=\theta,\phi,\ {\rm or}\ \sigma,$ respectively, with $R\equiv k$ mod 4 and k=1 or 3. Then

(6.6)
$$\mu(z) = \mu(U(z))(D/b)/(Cz+D)^{1+12e},$$

with (D/b) the Legendre symbol. Thus each of the theta functions is a form of weight 1 with multiplier dependent on U(z).

Fricke's method [7] is to express t in terms of the theta functions by taking a ratio of linear or quadratic forms in theta functions (see Sections 8 and 9 below). One such ratio can be chosen as t. Now for any such quadratic form T, the function

$$(6.7) S = (dt/dz)/T$$

is invariant in $\Gamma^0(b)$, while WS = -S. For a well-chosen T, we can choose s as S. (This is done in Sections 8 and 9 below.)

7. Power Series Approximations. Assume that by methods of Section 6 or 7 we have the Laurent series

$$(7.1) t = 1/r - C_b + O(r),$$

(7.2)
$$s = 1/r^{g+1} + O(1/r^g).$$

For the computation of the polynomial $P_{2g+2}(t)$, we truncate both of the above series to width 2g + 2. Then we can express

(7.3)
$$s^2 = 1/r^{2g+2} + \dots = P_{2g+2}(t).$$

Only the terms of nonpositive degree in the expansion of s^2 are required, as we can then use (7.1) to revert the series to t. The constant C_b is important for the equations

$$(7.4a) j(z/b) = 1/r + 744 + O(r) = t + C_b + 744 + O(1/t),$$

(7.4b)
$$j(z) = 1/r^b + 744 + O(r^b) = t^b + bC_b t^{b-1} + O(t^{b-2}).$$

Although it is a higher state of the art to use modular forms to calculate $F_b(s,t)$, it is possible to find the equations (1.8a,b) directly, by a crude approximation, when b is prime. Note

(7.5)
$$R_b(t) = [j(z) - j(z/b)]/s,$$

a polynomial in t of degree b-g-1 (< b-1 when g > 0). Therefore, if s and t are known in r by series truncated to width b-g-1 (see (7.1) and (7.2)), we can then effectively approximate both j(z) and j(z)-j(z/b) by the same approximation $1/r^b$

(see (7.4a,b)) and $R_b(t)$ comprises the terms of nonpositive degree of the expansion in t,

(7.6)
$$1/(r^b s) = R_b(t) + O(1/t).$$

Finally, to find $N_b(t)$, we need to find s as a power series in t truncated to width b (e.g., from (7.3)). Then we approximate

(7.7)
$$D_b(t,s) = R_b(t)s = L_b(t) + O(1/t)$$

thus obtaining a polynomial $L_b(t)$ of degree b. From (7.4a,b),

(7.8)
$$S_b(t) = j(z) + j(z/b) = L_b(t) + 2(t + 744 + C_b).$$

Finally, $N_b(t)$ is found from $D_b(t,s)$ and $S_b(t)$ by

$$(7.9) N_b(t) = (S_b(t)^2 - D_b(t,s)^2)/4.$$

8. A Short Arithmetic Progression. The primes b = 23, 47, 71 satisfy

$$(8.1) b = 24k - 1, g = 2k (k = 1, 2, 3)$$

and can be treated by the method which Fricke [7] developed for b=23 (see correction in Section 3 above). We set

$$(8.2) t = T_1/T_0,$$

where the following cases arise (according to Section 6):

$$b = 23: \quad T_1 = \theta(1, 1, 6) \approx 1,$$

$$T_0 = [\theta(1, 1, 6) - \theta(2, 1, 3)]/2 \approx r;$$

$$b = 47: \quad T_1 = [\theta(1, 1, 12) - \theta(3, 1, 4)]/2 \approx r,$$

$$T_0 = [\theta(1, 1, 12) - \theta(3, 1, 4)]/2 \approx r^2;$$

$$b = 71: \quad T_1 = [\theta(2, 1, 9) - \theta(3, 1, 6)]/2 \approx r^2,$$

$$T_0 = [\theta(3, 1, 6) - \theta(4, 3, 5)]/2 \approx r^3.$$

Thus, $T_1 \approx r^{k-1}$, $T_0 \approx r^k$, and $t \approx 1/r$. Actually, in each case,

(8.3)
$$T_0 = [\Delta(z)\Delta(z/b)]^{1/24}.$$

We define (as in (6.7))

(8.4)
$$s = -r(dt/dr)/T_0^2 \approx 1/r^{g+1}.$$

Then we compute (and factor as in (4.5))

(8.5)
$$s^2 = P_{2g+2}(t) = p_1(t)p_2(t),$$

obtaining factors each of degree g + 1. (The factors are seen in the radicands in Table III.) Actually, Fricke found the polynomial $P_{2g+2}(t)$ for these three cases, but failed to factor it for b = 71 (see [12]).

By generalizing Fricke's method for b = 23, we write

(8.6)
$$F_b(t,s) = \frac{(q_1(t) + sq_2(t))^3}{2(r_1(t)p_1(t)^{1/2} - r_2(t)p_2(t)^{1/2})^2}.$$

Here, $q_i(t)$ and $r_i(t)$ (i=1,2) are defined as in (4.4a,b) by

(8.7a)
$$(E_2' + E_2)/T_0^4 = q_1(t), \qquad (E_2' - E_2)/T_0^4 = q_2(t)s,$$

(8.7b)
$$(\sqrt{\Delta'} + \sqrt{\Delta})/T_0^6 = r_1(t)\sqrt{p_1(t)}, \qquad (-\sqrt{\Delta'} + \sqrt{\Delta})/T_0^6 = r_2(t)\sqrt{p_2(t)},$$

(8.8)
$$\deg q_1 = 2g$$
, $\deg q_2 = g - 1$, $\deg r_1 = \deg r_2 = 5g/2 - 1$.

To see the capacity for approximation inherent in (8.7a,b), note that with power series truncated to width deg q_i or deg r_i , $E'_2 \approx b^2$ and $\sqrt{\Delta'} \approx 0$, so we effectively define $q_i(t)$ and $r_i(t)$ by

$$(8.9a) (b2 + E2)/T04 = q1(t) + O(1/t), (b2 - E2)/(T04s) = q2(t) + O(1/t),$$

(8.9b)
$$\sqrt{\Delta}/(T_0^6\sqrt{p_1(t)}) = r_1(t) + O(1/t), \qquad \sqrt{\Delta}/(T_0^6\sqrt{p_2(t)}) = r_2(t) + O(1/t).$$

The data for (8.6) are given in Table IV of the appendix, and the computation of $D_b(t, s)$ and $N_b(t)$ proceeds as in Section 7.

9. Cases b = 41 and b = 59. In these cases we do not find $F_b(t, s)$ directly, but use the cruder approximation methods of Eqs. (7.5)–(7.9).

The case b=41 is handled similarly to b=17 and 29 (see [7]), but there does not seem to be a way of parametrizing all three cases, as in Section 8. We set

$$(9.1a) T_1 = \sigma(3, 2, 14)/2 = r^{3/4}(1 - r^3 - r^4 + \cdots),$$

(9.1b)
$$T_0 = \sigma(7, 2, 6)/2 = r^{7/4}(1 - r - r^2 + \cdots).$$

The genus q = 3. We define (see Section 6 above)

(9.2a)
$$t = T_1/T_0 \approx 1/r$$
,

(9.2b)
$$s = -r(dt/dr)/[T_0^3(T_1 - T_0)]^{1/2} \approx 1/r^4,$$

so we can obtain the equation (7.3) relating s and t. Incidentally,

(9.3)
$$T_0 = [\Delta(z)\Delta(z/41)]^{1/24}.$$

We finally obtain $D_b(t, s)$ by the approximation process of (9.6) and $N_b(t)$ by (7.9). For the case b = 59, we define

(9.4a)
$$\theta_0 = \theta(1, 1, 15) \approx 1, \quad \theta_1 = \theta(3, 1, 5) \approx 1,$$

$$(9.4b) \hspace{1cm} \phi_3 = \phi(1,1,15) \approx 2r^{1/2}, \hspace{1cm} \phi_4 = \phi(3,1,5) \approx 2r^{3/2},$$

(9.5a)
$$\theta_{12} = (\theta_1^2 - \theta_0^2)/4, \quad \theta_{22} = (\theta_1 - \theta_0)^2/4,$$

(9.5b)
$$\theta_{33} = \phi_3^2/4, \quad \theta_{34} = \phi_3\phi_4/4, \quad \theta_{44} = \phi_4^2/4.$$

A search for higher-order terms produces the combinations

(9.6a)
$$T_1 = (\theta_{34} - 2\theta_{22} + \theta_{12} - \theta_{33} + \theta_{44})/4 \approx r^4,$$

(9.6b)
$$T_0 = (-3\theta_{34} + 2\theta_{22} + \theta_{12} - \theta_{33} + \theta_{44})/4 \approx r^5.$$

Analogously to (8.3) and (9.3),

(9.7)
$$T_0 = [\Delta(z)\Delta(z/59)]^{1/12}.$$

The genus g = 5. We have expansions

$$(9.8) t = T_1/T_0 \approx 1/r,$$

(9.9)
$$s = -r(dt/dr)/T_0 \approx 1/r^6,$$

and the relation between s and t comes out as

$$(9.10) s^2 = P_{12}(t) = p_3(t)p_9(t)$$

(with factors of degree 3 and 9, see (4.5)). We could proceed with the same crude technique of the last case, but here we can use a power series truncated to smaller width by following Fricke's method [7] for the cases b = 11 and 19. In the notation of (4.4a,b),

(9.11a)
$$(E_3'/\sqrt{\Delta'} + E_3/\sqrt{\Delta})/\sqrt{p_3(t)} = p_{28}(t),$$

(9.11b)
$$(E_3'/\sqrt{\Delta'} - E_3/\sqrt{\Delta})/\sqrt{p_9(t)} = p_{23}(t),$$

for polynomials of degrees 28 and 23 as shown. In practical terms, we can calculate these polynomials as

$$(9.12a) p_{28}(t) + O(1/t) = 1/(r^{59/2}p_3(t)),$$

(9.12b)
$$p_{23}(t) + O(1/t) = 1/(r^{59/2}p_9(t)).$$

We then have $D_{59}(t,s) = p_{23}(t)p_{28}(t)s$ by (4.1), and we proceed as in Section 7 to compute $N_{59}(t)$.

Curiously, the hardest numerical case was b=41, which was dismissed by Fricke as not worth mentioning ("dürften kaum besondere Schwierigkeiten darbieten" [8, p. 493]). The hardest theta function computation was for b=59, which Fricke failed to include in his list.

10. Concluding Remarks. The cases were run on VAX MACSYMA with individual times ranging from one minute for b=2 to two hours for b=49. Generally, the time increased with the degree, but the cases of genus zero took much longer to run, given the same degree. Otherwise, the genus is scarcely a major factor in the running time. Most time-consuming was the factorization of the rational function $D_b(t,s)/s$, made generally slow by the presence of very many nonlinear factors (often of the same degree). The rest of the calculation took at most a half-hour in each case.

The author is indebted to the Science Computation Laboratory at City College (CUNY) and the Mathematics Department of the University of Arizona for making MACSYMA available, to Jesse Deutsch for help in running the problem, to Martin Hassner and Victor Miller of IBM and John McKay for challenging discussions, and to the referees for their tireless labor.

Appendix. The norms $N_b(t)$ and differents $D_b(t,s)$, and data for b=23,47,71.

TABLE II. Norms

```
(t + 272)
                    (t + 54) (t + 246)<sup>3</sup>
                  2
(t + 272 t + 7696) / (t + 32)
             3 3 2 3 5
(t + 18) (t + 270 t + 8292 t + 67848) / (t + 17)
                    2 2 3
(t + 13) (t + 250 t + 3529)
N = \frac{4}{8} + \frac{3}{2} + \frac{2}{109184} + \frac{3}{439312} / (t + 12)
N_{9} = (t + 12)^{3} (t^{3} + 252 t^{2} + 4320 t + 19200)^{3} / (t + 9)^{2}
N = (t + 224 t - 192 t - 832 t + 1024)
      = (t + 5) (t + 254 t + 5077 t + 34092 t + 75492)
N = (t - t + 1) (t + 229 t + 494 t - 743 t + 254 t - 11 t + 1) /t
N_{17} = (t + 236 t + 1662 t + 3092 t + 3001 t + 1080 t + 144)
 N_{18} = (t^{3} + 18 t^{2} + 102 t + 186)^{3} (t^{9} + 270 t^{8} + 9270 t^{7} + 147222 t^{6} 
 + 1359612 t^{7} + 7920936 t^{7} + 29726220 t^{7} + 70093152 t^{7} + 94886136 t^{7} 
 + 56441256)^{3} / ((t + 5)^{3} (t^{7} + 9 t^{7} + 21)^{3} ) 
N_{19} = (t - 1)^{2} (t^{6} + 222 t^{5} - 1087 t^{4} - 96 t^{3} + 8128 t^{2} - 15168 t + 9216)^{3}
N = (t-1)^{2} (t + t + 1) (t + 5 t + 1)
(t + 228 t - 180 t - 34 t + 60 t - 12 t + 1) / t
 N_{23} = (t + 224 t - 864 t - 544 t + 9664 t - 26112 t + 36288 t - 27648 t + 9216)
```

$$N_{24} = (t^{4} - 10 t^{2} + 12 t - 2) (t^{2} + 216 t^{2} - 2622 t^{2} + 13860 t^{2} + 2160 t^{2} + 2160 t^{2} + 2160 t^{2} + 21860 t^{2} +$$

$$\begin{array}{c} N \\ 26 \end{array} = \begin{array}{c} 2 \\ (t - t + 1) \\ 6 \\ + 6566 \end{array} \begin{array}{c} 12 \\ (t + 231 \ t + 503 \ t - 1236 \ t + 3149 \ t - 5859 \ t \\ 3 \\ 4 \\ 3 \\ 2 \\ 3 \\ 15 \end{array}$$

$$N_{39} = (t + 1) \quad (t - t + 1) \quad (t + 4 t - 7 t + 4 t + 1)$$

$$(t + 231 t + 282 t + 25 t - 504 t - 165 t + 560 t + 75 t$$

$$- 264 t + 25 t + 42 t - 9 t + 1) \quad /t$$

$$\begin{array}{c} N \\ 49 \\ -5383 \text{ t} \\ +57708 \text{ t} \\ -3283 \text{ t} \\ +57708 \text{ t} \\ -324114 \text{ t} \\ +895426 \text{ t} \\ +99029 \text{ t} \\ -3383 \text{ t} \\ +57708 \text{ t} \\ -324114 \text{ t} \\ +895426 \text{ t} \\ +99029 \text{ t} \\ -324114 \text{ t} \\ -324114 \text{ t} \\ +895426 \text{ t} \\ +99029 \text{ t} \\ -324114 \text$$

TABLE III. Differents

$$D_{2} = (t + 47)(t^{2} - 128^{2})^{1/2}$$

$$D_{3} = (t - 10)(t + 46)(t^{2} - 54^{2})^{1/2}$$

$$D_{4} = (t + 16)(t + 31)(t^{2} + 17 t - 479)((t - 32)/(t + 32))^{1/2}$$

$$D_{5} = (t - 14)(t + 4)(t + 18)(t + 22)(t^{2} - 500)^{1/2}$$

$$D_{6} = (t + 16)(t^{2} - 128)^{1/2}(t^{2} + 16 t - 16)(t^{2} + 27 t + 171)(t^{3} + 22 t^{2} - 125 t - 3571)/(t + 17)^{3}$$

$$D_{7} = (t - 11)(t + 5)(t + 11)(t + 13)(t^{2} - 196)^{1/2}(t^{2} + 16 t + 160)(t^{2} + 17 t +$$

$$D = (t-1) (t+1) (t^2 - 5t + 1) (t^2 - 3t + 1) (t-t-1) (t+t-1)$$

$$(t-t+1) (t-4t + 2t - 1) (t-2t - 3t - 1)$$

$$(t-4t - 5t - 2t - 1) (t-2t - 7t - 2t + 1)$$

$$(t-2t - t+2t - 1) (t-5t + 3t + t - t - 1)$$

$$(t-5t + 2t + t - 4t + t - 1) (t-4t - 6t + 6t - 1)$$

$$(t-7t + 11t - 7t + 1) (t+t-t+t+1) / t$$

$$D_{49} = (t - 4) (t - 3) (t - 2) (t - 1) (t - 9 t + 16) (t - 7 t + 7)
(t - 7 t + 11) (t - 6 t + 4) (t - 5 t + 3) (t - 5 t + 5) (t - 4 t + 1) (t - 4 t + 2) (t - 3 t + 1) (t - 14 t + 66 t - 119 t + 58)
(t - 14 t + 67 t - 126 t + 71) (t - 13 t + 53 t - 78 t + 36)
(t - 12 t + 44 t - 60 t + 25) (t - 12 t + 47 t - 66 t + 22)
(t - 12 t + 50 t - 84 t + 46) (t - 10 t + 26 t - 20 t + 4)
(t - 14 t + 63 t - 98 t + 21) /(t - 7 t + 14 t - 7)$$

TABLE IV. Data for b = 23, 47, 71

$$r_{1} = t^{4} - 21t^{3} + 148t^{2} - 380t + 212$$

$$r_{2} = t^{4} - 17t^{3} + 90t^{2} - 142t - 14$$

$$q_{1} = 530t^{4} - 4000t^{3} + 5440t^{2} - 9120t + 2880$$

$$q_{2} = 528t - 768$$

$$s^{2} = t^{6} - 14t^{5} + 57t^{4} - 106t^{3} + 90t^{2} - 16t - 19$$

$$p_{1} = t^{3} - 3t^{2} + 2t + 1$$

$$p_{2} = t^{3} - 11t^{2} + 22t - 19$$

$$b = 47$$

$$r = t^{9} - 17 t^{8} + 112 t^{7} - 355 t^{6} + 546 t^{5} - 388 t^{4} + 149 t^{3} + 292 t^{7} - 740 t + 36$$

$$r = t^{9} - 15 t^{8} + 84 t^{7} - 207 t^{6} + 172 t^{5} + 120 t^{4} - 283 t^{3} + 266 t^{7} - 66 t - 194$$

$$q = 2210 t^{8} - 8600 t^{7} + 14700 t^{6} - 23160 t^{5} + 17570 t^{4} - 12000 t^{7} + 960 t^{7} + 2720 t^{7} - 1600$$

$$q = 2208 t^{3} - 2448 t^{2} + 2256 t^{7} - 768$$

$$s^{2} = t^{10} - 6 t^{9} + 11 t^{8} - 24 t^{7} + 19 t^{6} - 16 t^{5} - 13 t^{4} + 30 t^{7} - 38 t^{7} + 28 t^{7} + 11 t^{7$$

b = 71

$$r_{1} = t^{14} - 6 t^{13} - 5 t^{12} + 76 t^{11} - 8 t^{10} - 408 t^{9} + 2 t^{8} + 1231 t^{7} + 484 t^{6} - 2049 t^{5} - 1575 t^{4} + 1185 t^{3} + 1570 t^{2} + 500 t - 310$$

$$r_{2} = t^{14} - 8 t^{13} + 7 t^{12} + 82 t^{11} - 132 t^{10} - 414 t^{9} + 610 t^{8} + 1533 t^{7} - 1366 t^{6} - 3829 t^{5} + 1313 t^{4} + 5207 t^{3} + 338 t^{2} - 3100 t - 612$$

$$q_{1} = 5042 t^{12} + 20408 t^{11} + 13204 t^{10} - 64592 t^{9} - 136154 t^{8} - 47104 t^{7} + 123316 t^{6} + 130168 t^{5} - 4814 t^{4} - 60784 t^{3} - 20240 t^{2} + 8224 t + 4256$$

$$q_{2} = 5040 t^{5} + 9840 t^{4} + 2400 t^{3} - 6480 t^{2} - 3120 t + 480$$

$$r_{3} = t^{14} + 4 t^{13} - 2 t^{12} - 38 t^{11} - 77 t^{10} - 26 t^{9} + 111 t^{8} + 148 t^{7} + t^{6} - 122 t^{5} - 70 t^{4} + 30 t^{3} + 40 t^{2} + 4 t - 11$$

$$r_{3} = t^{7} - 7 t^{5} - 11 t^{4} + 5 t^{3} + 18 t^{2} + 4 t - 11$$

$$r_{3} = t^{7} + 4 t^{6} + 5 t^{5} + t^{4} - 3 t^{3} - 2 t^{2} + 1$$

Department of Mathematics City College (CUNY) New York, New York 10031

- 1. A. O. L. ATKIN & J. LEHNER, "Hecke operators on $\Gamma_0(m)$," Math. Ann., v. 185, 1970, pp. 134–160.
- 2. B. C. BERNDT, A. J. BIAGIOLI & J. M. PURTILO, "Ramanujan's modular equation of large prime degree." (Manuscript.)
- 3. W. E. H. BERWICK, "Modular invariants expressible in terms of quadratic and cubic irrationalities," *Proc. London Math. Soc.*, v. 28, 1927, pp. 53-69.
- 4. B. BIRCH, "Some calculations of modular relations," *Modular Functions of One Variable* I, Lecture Notes in Math., vol. 320, Springer-Verlag, Berlin and New York, 1973, pp. 175-176.
- 5. H. COHN, Introduction to the Construction of Class Fields, Cambridge Univ. Press, New York, 1985.
- 6. H. COHN, "Singular moduli and modular equations for Fricke's cases," *Proc. Bowdoin AMS Summer Institute* 1987. (Manuscript.)
 - 7. R. FRICKE, Die elliptischen Funktionen und ihre Anwendungen II, Leipzig, 1922.
 - 8. R. FRICKE, Lehrbuch der Algebra III (Algebraische Zahlen), Braunschweig, 1928.
- 9. B. GROSS & D. ZAGIER, "On singular moduli," J. Reine Angew. Math., v. 355, 1985, pp. 191-220.
- 10. E. KALTOFEN & N. Yui, "Explicit construction of the Hilbert class fields of imaginary quadratic fields with class numbers 7 and 11," (Eurosam 84), Lecture Notes in Comput. Sci., vol. 174, Springer-Verlag, Berlin and New York, 1984, pp. 310–320.
- 11. M. A. KENKU, "The modular curve $X_0(39)$ and rational isogeny," Math. Proc. Cambridge Philos. Soc., v. 85, 1979, pp. 21–23.
- 12. F. KLEIN & R. FRICKE, Vorlesungen über die Theorie der elliptischen Modulfunctionen, Vol. II, Leipzig, 1892, pp. 445-474.
- 13. G. LIGOZAT, "Courbes modulaires de genre 1," Bull. Soc. Math. France, Mém. 43, Paris, 1975.
- 14. B. MAZUR & P. SWINNERTON-DYER, "Arithmetic of Weil curves," *Invent. Math.*, v. 25, 1974, pp. 1-61.
- 15. M. NEWMAN, "Construction and application of a class of modular functions," *Proc. London Math. Soc.*, v. 7, 1957, pp. 334-350.
 - 16. M. NEWMAN, "Conjugacy, genus, and class numbers," Math. Ann., v. 196, 1972, pp. 198-217.
- 17. A. P. OGG, "Hyperelliptic modular curves," Bull. Soc. Math. France, v. 102, 1974, pp. 107–148.
- 18. B. SCHOENEBERG, Elliptic Modular Functions, Springer-Verlag, New York, 1984.
- 19. J. VÉLU, "Les points rationnels de $X_0(37)$," Bull. Soc. Math. France, Mém. 37, Paris, 1974, pp. 169–179.
- 20. N. Yui, "Explicit form of the modular equation," J. Reine Angew. Math., v. 299/300, 1978, pp. 185-200.