MATHEMATICS OF COMPUTATION
VOLUME 38, NUMBER 157
JANUARY 1982

An Explicit Modular Equation in Two Variables and Hilbert's Twelfth Problem*

By Harvey Cohn

Abstract. The Hilbert modular function field over $\mathbf{Q}(\sqrt{2})$ has generators satisfying modular equations when the arguments are multiplied by factors of norm two. These equations are found by machine use of Fourier series and are further used to show computationally that Weber's ring class field theory for rationals has an illustration of Hecke's type for $\mathbf{Q}(\sqrt{2})$. This has bearing on Hilbert's twelfth problem, the generation of algebraic fields by transcendental functions.

1. Introduction. The main result of the present computation is an explicit modular equation for a field of modular functions of two variables. In one variable, the corresponding field is generated by $j(z)$ (see (1.3)) and the classical modular equation expresses $j(bz)$ in terms of $j(z)$ by an algebraic equation with remarkably large coefficients. Even for $b = 2$, the result is a numerical curiosity,

$$\begin{aligned}&-(j^2(2z) - j(z))(j^2(z) - j(2z)) + 2^4 \cdot 3 \cdot 31 j(2z)j(z)(j(2z) + j(z))\\ &-2^4 \cdot 3^4 \cdot 5^3(j^2(z) + j^2(2z)) + 2^8 \cdot 7 \cdot 61 \cdot 373 j(z)j(2z)\\ &+2^8 \cdot 3^7 \cdot 5^6(j(z) + j(2z)) - 2^{12} \cdot 3^9 \cdot 5^9 = 0.\end{aligned} \tag{1.1}$$

Although such equations can be explained in simpler terms in individual cases (see [1], [4]), they are hard to find generally; see [8]. The new result here is for Hilbert modular functions over $\mathbf{Q}(\sqrt{2})$ which form a field with two generators $X(z, z')$, $Y(z, z')$ (replacing the classical $j(z)$, see (2.6)). We derive an explicit relation (see (4.4)) which determines algebraically $X((2 + \sqrt{2})z, (2 - \sqrt{2})z')$ and $Y((2 + \sqrt{2})z, (2 - \sqrt{2})z')$ from $X(z, z')$, $Y(z, z')$.

The modular equations are of some interest as a precise computation based on a rather long Fourier approximation (of 45 terms). The main purpose, however, is to illustrate the existence of what may be described as "Weber-Hecke ring class field" analogues. We cite Weber's classic result in computational, indeed rational, terms:

Let $f(x, y)$ be a binary quadratic form over $\mathbf{Z}$ of discriminant $d < 0$. We assume the coefficients are relatively prime but d need not be squarefree (or fundamental). Let $f(x, y)$ be principal (it represents 1), so $f(x, y) = x^2 - dy^2/4$ for d even and $f(x, y) = x^2 + xy - (d - 1)y^2/4$ for d odd. Then, for a prime $p \nmid 2d$,

$$\{p = f(x, y) \text{ solvable in } \mathbf{Z}\} \Leftrightarrow \{p \text{ splits in } \mathbf{Q}(\sqrt{d}, j((d + \sqrt{d})/2))\}. \tag{1.2}$$

Received September 22, 1980.
1980 *Mathematics Subject Classification.* Primary 12A65, 12A25; Secondary 32N10.
* Research partially supported by NSF Grant 7903060.

0025-5718/82/0000-0484/$03.50

The quantity $j_0 = j((d + \sqrt{d})/2)$ is called a "singular modulus" and is incidentally an algebraic integer in a field abelian over $\mathbf{Q}(\sqrt{d})$. The field $\mathbf{Q}(\sqrt{d}, j_0)$ is called a "ring class field" over $\mathbf{Q}(\sqrt{d})$ in reference to the splitting property and the ring $\mathbf{Z}[(d + \sqrt{d})/2]$.

To be more specific, $j(z)$ refers to the function

$$j(z) = \left(1 + 240\sum_1^\infty \sigma_3(m)q_1^m\right)^3 \Big/ q_1\prod_1^\infty (1 - q_1^m)^{24} \tag{1.3a}$$

for $\sigma_3(m)$ the sum of cubes of divisors of m and

$$q_1 = \exp 2\pi i z, \qquad \operatorname{Im} z > 0. \tag{1.3b}$$

The important properties are derived from the relations

$$j(z + 1) = j(z), \quad j(-1/z) = j(z) \tag{1.3c}$$

(invariance over the modular group $PSL_2(\mathbf{Z})$). The concept of "splitting" of p is rational; it means that the defining equation for any integral element of the field will completely factor modulo p. For a normal field of degree 2^t, in particular, this means that t quadratic residues exist modulo p, corresponding to the stages of solution by radicals.

To see how the modular equation is the key to Weber's theory, we consider *nonfundamental* discriminants of type $d = b^2 d_0$ for variable t in (1.2). This situation involves the modular equation relating $j(bz)$ and $j(z)$ algebraically. For instance (see [1]), for the form

$$(p =) f(x, y) = x^2 + 4 \cdot 4^t y^2, \tag{1.4}$$

we would need the modular equation for $b = 2$ to iteratively deduce $j(2^{t+1}i)$ from $j(2^t i)$ (two values of j_0).

What Hecke did, in effect, was to create an analogous theory for primes and quadratic forms in real quadratic integers rather than $\mathbf{Z}$, in which representation of primes was tantamount to splitting in fields of singular moduli created by Hilbert modular functions rather than by $j(z)$. We therefore call it an illustration of a "Weber-Hecke" theory to consider for $\mathbf{Z}[\sqrt{2}]$ the form

$$\pi = \xi^2 + (2 + \sqrt{2})2^t\eta^2 \tag{1.5}$$

representing a prime π in $\mathbf{Q}(\sqrt{2})$ of norm p. We shall then verify by computer that such a representation is governed by the splitting of p in a field K_t (see (6.2a)) involving new singular moduli, now special values of $X(z, z')$, $Y(z, z')$. Hecke's original theory [3] was limited to cases where $t = 0$ (fundamental discriminants), and, even so, was further limited in its scope. Indeed, the illustration (1.5) still is not quite a consequence of a comprehensive generalization of Weber's theorem.

Hilbert's twelfth problem is a generic classification for the study of objects like the singular moduli (more generally, algebraic values like j_0 taken by transcendental functions at algebraic arguments). These objects are within the limits of computation! For historical references, we cite [3], [4], [7], and, for a more modern viewpoint, [5], [6]. The construction of the Hilbert modular function field here follows [2]. The computations were performed with the cooperation of the CUNY Computation Center.

2. Hilbert Modular Functions. The modular group $PSL_2(\mathbf{Z})$ generated by (1.2) is generalized to $\Gamma = PSL_2(\mathbf{Z}[\sqrt{2}])$, the *Hilbert modular group*. It is generated on the half-planes Im $z > 0$, Im $z' > 0$, by

$$z \to z + 1, \qquad z' \to z' + 1, \tag{2.1a}$$

$$z \to z + \sqrt{2}, \qquad z' \to z' - \sqrt{2}, \tag{2.1b}$$

$$z \to -1/z, \qquad z' \to -1/z', \tag{2.1c}$$

$$z \to (1 + \sqrt{2})^2 z, \quad z' \to (1 - \sqrt{2})^2 z'. \tag{2.1d}$$

The last transformation is also unimodular ($z \to (1 + \sqrt{2})z/(-1 + \sqrt{2})$); it involves use of the unit $1 + \sqrt{2}$. We want to define Φ the *field of (rational) Hilbert modular functions* on Γ. (For analogies with the classical case governed by $j(z)$, see [5].)

For both theoretical and computational purposes it is easier to first define the *(rational) graded ring R of even modular forms* as those entire functions $F(z, z')$ for which

$$F\left(\frac{\alpha z + \beta}{\gamma z + \delta}, \frac{\alpha' z' + \beta'}{\gamma' z' + \delta'}\right) = F(z, z')((\gamma z + \delta)(\gamma' z' + \delta'))^m \tag{2.2}$$

for even (dimension) $m \geqslant 0$, with $z \to (\alpha z + \beta)/(\gamma z + \delta)$ in Γ. (Except for z, z' primes (′) denote conjugates over $\mathbf{Q}(\sqrt{2})$.) We restrict R further by the requirement of *rational coefficients* in the Fourier expansion (at the "cusp") in

$$q = \exp \pi i(z + z'), \tag{2.3a}$$

$$q_0 = \exp \pi i(z - z')/\sqrt{2}. \tag{2.3b}$$

(For elements of R with $m = 0$, we have just the constants $\mathbf{Q}$.) Then Φ is defined as the *quotient field* of R.

The main requirement [2] is that $R = \mathbf{Q}[G_2, G_4, G_6]$, where G_m are the so-called "Eisenstein series", with expansion

$$G_m = A_m + B_m \sum q^b q_0^a s_{m-1}(a + b\sqrt{2}), \qquad m \geqslant 2, \tag{2.4a}$$

summed over the range of integers

$$b > 0, \quad |a| < b\sqrt{2}, \tag{2.4b}$$

with ideal divisor function (summed to ignore associates)

$$s_u(\alpha) = \sum |\mu\mu'|^u, \quad (\mu) \mid (\alpha), \tag{2.4c}$$

and with A_m and B_m chosen for the convenience of integral values,

$$A_2 = 1, \quad B_2 = 48; \qquad A_4 = 11, \quad B_4 = 480; \qquad A_6 = 361, \quad B_6 = 1008. \tag{2.4d}$$

The function $s_u(\alpha)$ can easily be evaluated in terms of principal ideal factors of $(\alpha) = (a + b\sqrt{2}) = (\sqrt{2})^{e_2} \prod \mathfrak{p}^{e_p}\mathfrak{p}'^{e_p + g_p} \prod r^{f_r}$, with product extended over prime factors $(p) = \mathfrak{p}\mathfrak{p}'$ for $p \equiv \pm 1 \pmod 8$ and (r) for $r \equiv \pm 3 \pmod 8$ with indicated nonnegative exponents. Therefore everything comes from the rational formulas

$$\gcd(a, b) = 2^{[e_2/2]} \prod p^{e_p} \prod r^{f_r}, \qquad |a^2 - 2b^2| = 2^{e_2} \prod p^{e_p + g_p} \prod r^{2f_r}. \tag{2.4e}$$

These lead to

$$\begin{aligned} s_u(\alpha) = {} & (1 + 2^u + \cdots + 2^{e_2 u}) \prod (1 + p^u + \cdots + p^{e_p u}) \\ & \times (1 + p^u + \cdots + p^{(e_p + g_p)u}) \prod (1 + r^{2u} + \cdots + r^{2f_r u}). \end{aligned} \tag{2.4f}$$

It is more convenient to write $R = \mathbf{Q}[G_2, H_4, H_6]$ with generators which have simpler starting terms (subscripts always denote dimension of forms),

$$G_2 = 1 + q\{48, 144, 48\} + q^2\{336, 384, 720, 384, 336\} + \dots, \tag{2.5a}$$

$$H_4 = (11G_2^2 - G_4)/576 = q\{1, -2, 1\} + q^2\{-4, -8, 24, -8, -4\} + \dots, \tag{2.5b}$$

$$\begin{aligned} H_6 &= (361G_2^3 - G_6 - 50976G_2H_4)/224640 \\ &= q + 2q^2\{-1, -8, 6, -8, -1\} + \dots. \end{aligned} \tag{2.5c}$$

The symbol $\{\ \}$ denotes a finite series in q_0,

$$\{a_u, \dots, a_1, a_0, a_{-1}, \dots, a_{-u}\} = \sum_{-u}^{u} a_m q_0^m. \tag{2.5d}$$

Here the symmetry $a_u = a_{-u}$ (or $q_0 \to q_0^{-1}$, or $z \to z' \to z$), is an incidental property of R.

Therefore the (rational) Hilbert modular function field is

$$\Phi = \mathbf{Q}(X, Y), \tag{2.6a}$$

with two generators given by

$$X = X(z, z') = G_2^2/H_4, \quad Y = Y(z, z') = G_2H_4/H_6. \tag{2.6b}$$

Our problem relates to the functions

$$X_0 = X((2 + \sqrt{2})z, (2 - \sqrt{2})z'), \quad Y_0 = Y((2 + \sqrt{2})z, (2 - \sqrt{2})z'). \tag{2.7}$$

We shall find the equations which X_0 and Y_0 satisfy over Φ; these are the "modular equations with factor $2 + \sqrt{2}$ (of norm 2)".

3. The Modular Equation. We are concerned with three conjugate operations under Γ,

$$T_1(z, z') = ((2 + \sqrt{2})z, (2 - \sqrt{2})z'), \tag{3.1a}$$

$$T_2(z, z') = ((2 + \sqrt{2})z/2, (2 - \sqrt{2})z'/2), \tag{3.1b}$$

$$T_3(z, z') = ((2 + \sqrt{2})(z + 1)/2, (2 - \sqrt{2})(z' + 1)/2). \tag{3.1c}$$

Then it can be verified from (2.1) and (2.2) that, for the form $F(z, z')$, the triple

$$F^{(1)} = 2^m F(T_1(z, z')), \quad F^{(2)} = F(T_2(z, z')), \quad F^{(3)} = F(T_3(z, z')) \tag{3.2}$$

is an invariant set under Γ, so its symmetric functions are again modular forms of dimension m times the degree of the symmetric function. Likewise the modular function

$$W(z, z') = F(z, z')/E(z, z') \tag{3.3a}$$

(a ratio of two forms of dimension m) has three conjugates

$$W^{(j)} = W(T_j(z, z')) = F^{(j)}/E^{(j)}, \quad j = 1, 2, 3, \tag{3.3b}$$

satisfying a modular equation

$$W^3 - \frac{3\ \mathrm{sym}(F, E)}{\mathrm{sym}(E, E)} W^2 + \frac{3\ \mathrm{sym}(E, F)}{\mathrm{sym}(E, E)} W - \frac{\mathrm{sym}(F, F)}{\mathrm{sym}(E, E)} = 0, \tag{3.4a}$$

where we now define "sym" a modular form of dimension $3m$, namely,

$$\mathrm{sym}(E, F) = (F^{(1)}E^{(2)}E^{(3)} + F^{(2)}E^{(3)}E^{(1)} + F^{(3)}E^{(1)}E^{(2)})/2^m. \tag{3.4b}$$

The (multiplicative) norm is recognized as a special case,

$$\text{norm}(E) = \text{sym}(E, E)/3 = E^{(1)}E^{(2)}E^{(3)}/2^m. \tag{3.4c}$$

We avail ourselves of integral powers (as well as integral coefficients) by writing F_1, F_2, F_3 (subscripts not dimensions!), defined by

$$F^{(1)} = F_1/2^m, \tag{3.5a}$$

$$F^{(2)} = F_2 + F_3/\sqrt{q}, \tag{3.5b}$$

$$F^{(3)} = F_2 - F_3/\sqrt{q}. \tag{3.5c}$$

Now F_1, F_2, F_3 are integral-powered (and F_3, for instance, has no constant term). If we write

$$F = \sum q_0^a q^b f(a + b\sqrt{2}), \tag{3.6}$$

then, with the change in variables (3.1),

$$F_1 = \sum q_0^{2a} q^b f((2a - b) + (b - a)\sqrt{2}), \tag{3.7a}$$

$$F_2 = \sum q_0^a q^b f((2a - 2b) + (2b - 2a)\sqrt{2}), \tag{3.7b}$$

$$F_3 = \sum q_0^a q^b f((2a - 2b + 1) + (2b - 2a - 1)\sqrt{2}). \tag{3.7c}$$

Here, each sum is, of course, restricted to those a and b which produce arguments of f already present in the sum (3.6). Then,

$$\text{sym}(E, F) = F_1(E_2^2 - E_3^2/q) + 2E_1(E_2F_2 - E_3F_3/q), \tag{3.8a}$$

$$\text{norm}(E) = E_1(E_2^2 - E_3^2/q). \tag{3.8b}$$

There is no loss of accuracy in polynomial operations with Fourier coefficients, but the transformations (3.1) lead to half-exponents. So it is not trivial to decide how many terms are to be used. It turns out in Section 4 that for $X = G_2^2/H_4$ (and $Y = G_2H_4H_6$) modular forms of dimension $3 \cdot 4 = 12$ (and $3 \cdot 6 = 18$) are required, and these are determined by the Fourier series up to q^3 (and q^4 respectively). If we examine the sym( ), we see that in both cases it suffices for the modular forms of transformed type F_2 and F_3 to be known up to q^3 in (3.7). This degree of accuracy requires 45 coefficients in G_2, H_4, H_6, namely

$$\begin{cases} a = 0, b = 0 & \text{(one coeff.)}, \\ 1 \leqslant b \leqslant 5, |a| < b\sqrt{2} & \text{(43 coeff.)}, \\ a = 6, b = 6 & \text{(one coeff.)}. \end{cases} \tag{3.9}$$

We are omitting a rather tedious hand analysis, one point at a time, to establish that the range (3.9) is sufficient. We might just illustrate the fact that the last point, $a = 6$, $b = 6$, of (3.9) is required in (3.7b) to cover the term $q_0^0 q^3 f(-6 + 6\sqrt{2})$, which is only of order 3 in q. The process uses the unit condition (2.1d), e.g., $f(-6 + 6\sqrt{2}) = f((6 + 6\sqrt{2})(1 - \sqrt{2})^2)$. The problem was set up for 40-digit multiple precision arithmetic, but the largest coefficient which appeared was of order 10^{15}.

4. Evaluation of Modular Forms. First the bases of the modular forms of dimensions 12 and 18 are listed manually by partitioning 12 and 18 into 2, 4, and 6.

Then the machine calculates and prints the 45 coefficients in the range (3.9). We abbreviate the list to show only the leading terms.

dimension 12

$$G_2^6 = 1 + 288q\{1, 3, 1\} + \ldots, \quad G_2^4H_4 = q\{1, -2, 1\} + \ldots,$$
$$G_2^3H_6 = q + \ldots, \quad G_2^2H_4^2 = q^2\{1, -4, 6, -4, 1\} + \ldots,$$
$$G_2H_4H_6 = q^2\{1, -2, 1\} + \ldots, \quad H_6^2 = q^2 + \ldots,$$
$$H_4^3 = q^3\{1, -6, 15, -20, 15, -6, 1\} + \ldots.$$

dimension 18

$$G_2^9 = 1 + 432q\{1, 3, 1\} \ldots, \quad G_2^6H_6 = q + \ldots, \quad G_2^7H_4 = q\{1, -2, 1\} + \ldots,$$
$$G_2^3H_6^2 = q^2 + \ldots, \quad G_2^4H_4H_6 = q^2\{1, -2, 1\} + \ldots,$$
$$G_2^5H_4^2 = q^2\{1, -4, 6, -4, 1\} + \ldots, \quad H_6^3 = q^3 + \ldots,$$
$$G_2H_4H_6^2 = q^3\{1, -2, 1\} + \ldots, \quad G_2^2H_4^2H_6 = q^3\{1, -4, 6, -4, 1\} + \ldots,$$
$$G_2^3H_4^3 = q^3\{1, -6, 15, -20, 15, -6, 1\} + \ldots,$$
$$H_4^3H_6 = q^4\{1, -6, 15, -20, 15, -6, 1\} + \ldots,$$
$$G_2H_4^4 = q^4\{1, -8, 28, -56, 70, -56, 28, -8, 1\} + \ldots.$$

The machine computes the Fourier series of sym( ) and norm( ) for the numerators and denominators of X and Y in (2.6b). The output is accurate to q^3 for X and q^4 for Y, which is sufficient to verify the following expansions:

$$\text{(4.1)} \qquad \begin{cases} \text{norm}(G_2) = G_2^3 + 144G_2H_4 - 1728H_6, \\ \text{norm}(H_4) = -H_6^2, \\ \text{norm}(H_6) = H_4^3(G_2H_4 + 4H_6), \end{cases}$$

(note, the multiplicativity, e.g., $\text{norm}(G_2H_4) = \text{norm}(G_2)\text{norm}(H_4)$),

$$\text{(4.2)} \qquad \begin{cases} \text{sym}(G_2^2, H_4) = -4G_2^4H_4 - 207G_2^3H_6 - 1152G_2^2H_4^2 - 19008G_2H_4H_6 \\ \qquad\qquad -62208H_6^2 - 82944H_4^3, \\ \text{sym}(H_4, G_2^2) = 432H_6^2 + 156G_2H_4H_6 - G_2^3H_6, \end{cases}$$

$$\text{(4.3)} \qquad \begin{cases} \text{sym}(H_6, G_2H_4) = G_2^2H_4^2H_6 - 4G_2H_4^4 + 48H_4^3H_6, \\ \text{sym}(G_2H_4, H_6) = -5G_2^2H_4^2H_6 + 108G_2H_4H_6^2. \end{cases}$$

We finally obtain modular equations of type (3.4a) by division. Thus, in (2.6b) and (2.7), X_0 and Y_0 are determined from X and Y by

$$\text{(4.4a)} \qquad \Phi_1(X_0, X, Y) = 0,$$

$$\text{(4.4b)} \qquad \Phi_2(Y_0, X, Y) = 0,$$

where

$$\text{(4.4c)} \qquad \begin{aligned} \Phi_1(X_0, X, Y) &= X_0^3 + (432 + 156Y - XY)X_0^2 \\ &+ (4XY^2 + 207XY + 1152Y^2 + 19008Y + 62208 + 82944Y^2/X)X_0 \\ &+ (XY + 144Y - 1728)^2, \end{aligned}$$

$$\Phi_2(Y_0, X, Y) = Y_0^3 - (X - 4Y + 48)Y_0^2/(Y + 4) + (-5Y + 108)XY_0/Y(Y + 4) + X(XY + 144Y - 1728)/Y^2(Y + 4), \tag{4.4d}$$

and, in addition,

$$\Phi_2(Y, X_0, Y_0) = 0. \tag{4.4e}$$

The last equation is valid by the symmetry of (3.1a) and (3.1b). (To see this symmetry, note the unit in (2.1d) enables us to rewrite (3.1b) as $z(2 + \sqrt{2})/2 \to z(2 + \sqrt{2})(1 - \sqrt{2})^2/2 = z/(2 + \sqrt{2})$, so T_1 and T_2 effectively cancel.) We need (4.4e) because our correspondence (3.1) involves three values of (X_0, Y_0) for each (X, Y) and not nine! Thus, if we are given (X, Y), we find three values of Y_0 from (4.4b), and then we find one value of X_0 for each Y_0 from simultaneously solving the cubic (4.4a) and the quadratic (4.4e) for X_0. (The equation $\Phi_1(X, X_0, Y_0) = 0$ is also valid, but unnecessary.)

5. Iterated Singular Moduli. Given $X(z_0, z_0')$ and $Y(z_0, z_0')$, we want to use the modular equations to find, iteratively,

$$\begin{cases} X_t = X\big((2 + \sqrt{2})^t z_0, (2 - \sqrt{2})^t z_0'\big), \\ Y_t = Y\big((2 + \sqrt{2})^t z_0, (2 - \sqrt{2})^t z_0'\big). \end{cases} \tag{5.1}$$

In principle, these equations

$$\Phi_2(Y_{t+1}, X_t, Y_t) = 0, \tag{5.2a}$$

$$\Phi_1(X_{t+1}, X_t, Y_t) = 0, \quad \Phi_2(Y_t, X_{t+1}, Y_{t+1}) = 0, \tag{5.2b}$$

determine three values of (X_{t+1}, Y_{t+1}) for each (X_t, Y_t). By using the symmetry of (3.1a) and (3.1b) again, we see that one value of (X_{t+1}, Y_{t+1}) must be a repetition of (X_{t-1}, Y_{t-1}); so iteration leads to only two new (X_{t+1}, Y_{t+1}) each time. Thus a quadratic relation can be found by removing Y_{t-1} as a possible root of (5.2a). The equation now becomes

$$Y_{t+1}^2 - Y_{t+1}((X_t - 4Y_t + 48)/(Y_t + 4) - Y_{t-1}) - X_t(X_tY_t + 144Y_t - 1728)/Y_t^2(Y_t + 4)Y_{t-1} = 0. \tag{5.3a}$$

With Y_{t+1} known, a rational expression for X_{t+1} can be found by combining the quadratics $\Phi_1(X_{t+1}, X_t, Y_t)/(X_{t+1} - X_{t-1})$ and $\Phi_2(Y_t, X_{t+1}, Y_{t+1})$ to cancel the X_{t+1}^2 term. This produces a linear relation

$$X_{t+1} = P/Q, \tag{5.3b}$$

$$P = (X_tY_t + 144Y_t - 1728)^2/X_{t-1} + Y_t^2Y_{t+1}(Y_tY_{t+1} + 4Y_t + 4Y_{t+1} - 48), \tag{5.3c}$$

$$Q = 288 + 48Y_t - X_tY_t + X_{t-1} + Y_t^2Y_{t+1} + 5Y_tY_{t+1} + 1728/Y_{t+1}. \tag{5.3d}$$

A convenient way to initiate the procedure is to note that for $z = -(2 + \sqrt{2})/z$, $z' = -(2 - \sqrt{2})/z'$, one root of (4.4a, b) must satisfy $X = X_0$, $Y = Y_0$. Moreover, it is not surprising that we obtain the *rational* integers

$$X(i\sqrt{(2 + \sqrt{2})}, i\sqrt{(2 - \sqrt{2})}) = 576, \quad Y(i\sqrt{(2 + \sqrt{2})}, i\sqrt{(2 - \sqrt{2})}) = 12 \tag{5.4}$$

(because of a class number argument [4], which we do not give here). The values in (5.4) are discovered by a decimal computation using the 45-term expansion of G_2, H_4, and H_6, (with an accuracy to 10^{-7}). Of course, we easily verify that $\Phi_1(576, 576, 12) = \Phi_2(12, 576, 12) = 0$.

For reasons which will become clear in the next section (see (6.2)), we adjust our notation to define

$$X_t = X\big(i(2+\sqrt{2})^{t+1}\sqrt{(2+\sqrt{2})}, i(2-\sqrt{2})^{t+1}\sqrt{(2-\sqrt{2})}\big), \tag{5.5a}$$

$$Y_t = Y\big(i(2+\sqrt{2})^{t+1}\sqrt{(2+\sqrt{2})}, i(2-\sqrt{2})^{t+1}\sqrt{(2-\sqrt{2})}\big). \tag{5.5b}$$

Then the values (5.4) enable us to start the iteration (5.3), with the values

$$(X_{-2}, Y_{-2}) = (X_{-1}, Y_{-1}) = (576, 12), \tag{5.5c}$$

and to proceed to solve quadratic equations to iterate (X_t, Y_t), $t = 0, 1, 2, \ldots$. It turns out that a consistent choice of radical would be the sign which maximizes X_t and Y_t each time. The first few are

$$X_0 = 288(7+5\sqrt{2}), \quad Y_0 = 12(1+\sqrt{2}), \tag{5.6a}$$

$$X_1 = 72\big(388 + 275\sqrt{2} + 30(1+\sqrt{2})^3\sqrt{(2+\sqrt{2})}\big), \tag{5.6b}$$

$$Y_1 = 6(2 + 5\sqrt{2} + 6\sqrt{(2+\sqrt{2})}),$$

$$X_2 \text{ and } Y_2 \text{ involve the radical } \sqrt[4]{2} \text{ in addition.} \tag{5.6c}$$

The exact values are increasingly cumbersome. In fact, (5.6c) comes out of a calculation of the discriminant of (5.3a) only. It will prove very fortunate that we need only program the iteration (5.3) for arithmetic modulo p.

6. A Weber-Hecke Type Illustration. We consider the form representing a prime π (of norm p) in $\mathbf{Z}[\sqrt{2}]$

$$\pi = \xi^2 + (2+\sqrt{2})2'\eta^2 \qquad (p = \pi\pi'). \tag{6.1}$$

Thus our considerations are limited to primes p which split in $\mathbf{Q}(\sqrt{2})$, $p \equiv \pm 1 \pmod 8$. Also, for $t \geqslant 0$, p must also split in $K_0 = \mathbf{Q}(\sqrt{2}, i\sqrt{(2+\sqrt{2})})$. We assert that if we define X_t, Y_t as in (5.5), and

$$K_t = \mathbf{Q}(\sqrt{2}, i\sqrt{(2+\sqrt{2})}, X_t, Y_t) = K_0(X_t, Y_t), \tag{6.2a}$$

then we obtain, analogously with (1.2),

$$\{\text{repres. by (6.1)}\} \Leftrightarrow \{p \text{ splits in } K_t\}. \tag{6.2b}$$

This would illustrate the desired Weber-Hecke theory.

Summarizing (5.6), we find rational conditions on p

$$t = 0, \quad K_0 = \mathbf{Q}(\sqrt{2}, i\sqrt{(2+\sqrt{2})}), \qquad p \equiv 1, 7 \pmod{16}, \tag{6.3a}$$

$$t = 1, \quad K_1 = K_0(i), \qquad p \equiv 1 \pmod{16}, \tag{6.3b}$$

$$t = 2, \quad K_2 = K_1(\sqrt[4]{2}), \qquad \text{(ditto) and } p = r^2 + 32s^2. \tag{6.3c}$$

We now go back to the computer with primes $p \equiv 1 \pmod{16}$ and check the highest power of t for which (6.1) is possible and compare this value of t with the length of the longest chain

$$(X_1, Y_1), \ldots, (X_t, Y_t) \pmod p. \tag{6.4}$$

The chain starts with (5.5), and (X_0, Y_0) exists to begin with. The chain keeps going as long as the discriminant of (5.3a) comes out to be a perfect square modulo p. We therefore have two determinations of t and we find they agree for all p up to 10000, (144 values of p with values of t ranging up to 6). The process takes less than a minute of Amdahl Computer time.

The decomposition of $p = \pi\pi' = g_1^2 - 2g_2^2$ was done by trying successive g_2 (knowing they are even). Then $\pi = \xi^2 + (2 + \sqrt{2})\eta_0^2$ was accomplished by recognizing an "ellipsoid". We write

$$\pi = g_1 + g_2\sqrt{2}, \quad \xi = x_1 + x_2\sqrt{2}, \quad \eta_0 = y_1 + y_2\sqrt{2}, \tag{6.6a}$$

$$g_1 = x_1^2 + 2x_2^2 + 4(y_1 + y_2)^2 + 4y_2^2, \tag{6.6b}$$

$$g_2/2 = x_1x_2 + 2(y_1 + y_2)^2 - y_1^2. \tag{6.6c}$$

Thus a short search limited by (6.6b) determines ξ and η_0 and provides the value of t for (6.1) from $2^t \| \eta_0\eta_0'$ $(= y_1^2 - 2y_2^2)$.

We conclude with a list of the first cases occurring for each $t = 1, \ldots, 6$.

$t = 1, p = 17, \pi = 5 + 2\sqrt{2} = 1^2 + 2(2 + \sqrt{2})1^2;$

$$(X_0, Y_0) \equiv (6, 8), (X_1, Y_1) \equiv (4, 1) \pmod{17};$$

$t = 2, p = 113, \pi = 11 + 2\sqrt{2} = (1 - \sqrt{2})^2 + 2^2(2 + \sqrt{2})1^2;$ for $i = 0, 1, 2$

$$(X_i, Y_i) \equiv (85, 59), (46, 20), (9, 1) \pmod{113};$$

$t = 3, p = 337, \pi = 25 + 12\sqrt{2} = (1 + 2\sqrt{2})^2 + 2^3(2 + \sqrt{2})1^2;$ for $i = 0, \ldots, 3$

$$(X_i, Y_i) \equiv (298, 37), (208, 38), (138, 157), (79, 272) \pmod{337};$$

$t = 4, p = 577, \pi = 36 + 16\sqrt{2} = 1^2 + 2^4(2 + \sqrt{2})1^2;$ for $i = 0, \ldots, 4$

$$(X_i, Y_i) \equiv (200, 420), (313, 239), (472, 358), (47, 407),$$
$$(170, 511) \pmod{577};$$

$t = 5, p = 2689, \pi = 67 + 30\sqrt{2} = (1 - \sqrt{2})^2 + 2^5(2 + \sqrt{2})1^2;$ for $i = 0, \ldots, 5$

$$(X_i, Y_i) \equiv (1489, 523), (1467, 2122), (1844, 2539), (2484, 1415),$$
$$(2402, 864), (1468, 2606) \pmod{2689};$$

$t = 6, p = 9473, \pi = 131 + 62\sqrt{2} = (1 - \sqrt{2})^2 + 2^6(2 + \sqrt{2})1^2;$ for $i = 0, \ldots, 6$

$$(X_i, Y_i) \equiv (8752, 7015), (4323, 1866), (5976, 4135), (4105, 4527),$$
$$(1206, 8477), (3180, 2809), (8767, 6548) \pmod{9473}.$$

(It is a strange coincidence that for these first occurrences $\eta = 1$.)

Mathematics Department
City College of New York
New York, New York 10031

1. H. COHN, "Iterated ring class fields and the icosahedron," *Math. Ann.*, v. 225, 1981, pp. 107–122.

2. K. B. GUNDLACH, "Die Bestimmung der Funktionen zu einigen Hilbertschen Modulgruppen," *J. Reine Angew. Math.*, v. 220, 1965, pp. 109–153. MR 33 #1290.

3. E. HECKE, "Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie," *Math. Ann.*, v. 71, 1912, pp. 1–37.

4. F. KLEIN, "Über die Transformationen der elliptischen Funktionen und die Auflösung der Gleichung fünften Grades," *Math. Ann.*, v. 14, 1878, pp. 111–172.

5. A. OGG, "Survey of modular functions of one variable," *Modular Functions of One Variable*. I, Lecture Notes in Math., Vol. 320, Springer-Verlag, Berlin and New York, 1973, pp. 1–36. MR **49** #2554

→ G. SHIMURA, "Construction of class fields and zeta functions of algebraic curves," *Ann. of Math.*, v. 85, 1967, pp. 58–159. MR **34** #4268

7. H. WEBER, *Elliptische Funktionen und algebraische Zahlen*, Braunschweig, 1891.

8. N. YUI, "Explicit form of the modular equation," *J. Reine Angew. Math.*, v. 299/300, 1978, pp. 185–200. MR **57** #16201