On the singular values of Weber modular functions

Noriko Yui
Don Zagier

Noriko Yui
Department of Mathematics
Queen's University
Kingston
Canada K7L 3N6

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
53225 Bonn
Germany

MPI / 94-35

On the singular values of Weber modular functions

Noriko Yui
Don Zagier

Noriko Yui
Department of Mathematics
Queen's University
Kingston
Canada K7L 3N6

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
53225 Bonn
Germany

MPI / 94-35

On the singular values of Weber modular functions

Noriko Yui and Don Zagier

Introduction. Singular moduli, the values of the elliptic modular function of level one $j(\tau)$ at imaginary quadratic arguments τ in the upper half complex plane $\mathfrak{H}$, were studied extensively by many mathematicians in the early part of this century [11, 10, 2]. Their most important application is to explicit class field theory: if $K = \mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field of discriminant d, then the numbers $j(\tau)$, where τ ranges over the $SL_2(\mathbb{Z})$-inequivalent points in $\mathfrak{H}$ satisfying a quadratic equation of discriminant d, are the roots of a computable polynomial $H_d(X) \in \mathbb{Z}[X]$, the *class polynomial.* Since each root generates the class field of K when adjoined to K, this gives an explicit way to construct the class fields of K. There are other applications, e.g. to the problems of primality testing/proving [1] and to the study of representability of primes by quadratic forms $x^2 + ny^2$ [5].

A drawback of the polynomials $H_d(X)$, however, is that they have coefficients of astronomical size, even for quite modest discriminants d, e.g., $H_{-55}(X)$ is

$$X^4 + 3^7 5^3 29\cdot 134219 X^3 - 3^7 5^3 23\cdot 101\cdot 32987 X^2 + 3^9 5^7 11^2 101\cdot 110641 X - 3^{12} 5^6 11^3 29^3 41^3 .$$

In this paper we shall look at the class equations obtained by using the Weber function $f(\tau)$ of level 48 and index 72 instead of the modular invariant $j(\tau)$ of level 1. We will concentrate on the case of discriminants d congruent to 1 modulo 8 and not divisible by 3 (although other discriminants will also be considered), since the results are optimal here: the values of f at suitable points $\tau \in \mathfrak{H}$ of discriminant d generate the same fields as before but are the roots of a polynomial $W_d(X)$ having far smaller coefficients than $H_d(X)$, e.g. for $d = -55$ we have simply $W_{-55}(X) = X^4 + X^3 - 2X - 1$.

The paper has two aims. The first is to give an efficient procedure for calculating the roots of the Weber class polynomials $W_d(X)$. To do this, we have to discover the rule for picking out of each $SL_2(\mathbb{Z})$-equivalence class of points $\tau \in \mathfrak{H}$ of discriminant d one Γ-equivalence class (where $\Gamma \subset SL_2(\mathbb{Z})$ is the subgroup of index 72 under which $f(\tau)$ is invariant) in such a way that the corresponding values of $f(\tau)$ are the roots of $W_d(X)$. The second, and more important, is to give analogues for the Weber function of the results of Gross-Zagier [7] on the norms of the differences of singular moduli $j(\tau)$, i.e., on the disciminants and resultants of the class polynomials $H_d(X)$. The result of [7], following earlier work of Deuring [6], was that the norms in question are highly factorizable and that there is a closed formula for their decomposition into prime powers. The corresponding numbers for the Weber polynomials are far smaller—for instance, the discriminant of the polynomial H_{-55} given above is

$$-3^{78}5^{20}11^{5}19^{6}23^{6}29^{2}37^{2}41^{2}47^{4}53^{2} \approx -4.7 \times 10^{91},$$

while that of $W_{-55}(X)$ is only $-5^2 11 = -275$ —but the rule for finding their prime factors and the exponents to which they occur turns out to be considerably more complicated. More precisely, the formula given in [7] for the prime factorization of norms of differences $j(\tau_1) - j(\tau_2)$ involved a certain arithmetic function $\mathfrak{F}(m)$ which takes on prime power values; we will find that $\mathfrak{F}(m)$ decomposes naturally into the product of 8 more complicated functions $\mathfrak{F}_r(m)$, indexed by the divisors r of 24, which can be used in a similar way to describe the norms of differences of singular values of $f(\tau)^r$. The formulas we give are empirical observations, based on (extensive) numerical computations. Detailed proofs are being worked out by Alan Laing at the University of Maryland as part of his doctoral thesis.

1. The Weber functions and Weber class equations. For $\tau \in \mathfrak{H}$ (upper half-plane) we set $q = e^{2\pi i\tau}$ and more generally $q^a = e^{2\pi i a\tau}$ ($a \in \mathbb{Q}$). The classical Weber functions are defined by

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

The 8th powers of these functions are cubic over $j^{1/3}$ (f^8, $-f_1^8$ and $-f_2^8$ are the roots of $X^3 - j^{1/3}X - 16 = 0$) and their 24th powers are cubic over j (f^{24}, $-f_1^{24}$ and $-f_2^{24}$ are the roots of the equation $(x-16)^3 - xj = 0$), where $j = j(\tau)$ is the elliptic modular function and $j^{1/3}$ the cube root of j which is asymptotic to $q^{1/3}$ at infinity. In particular, $SL_2(\mathbb{Z})$ preserves the set of functions $\{f, f_1, f_2\}$ up to permutation and multiplication by 48th roots of unity. The action of the generators of $SL_2(\mathbb{Z})$ on these functions is given by

$$\begin{pmatrix} f(\tau+1) \\ f_1(\tau+1) \\ f_2(\tau+1) \end{pmatrix} = \begin{pmatrix} 0 & \zeta^{-1} & 0 \\ \zeta^{-1} & 0 & 0 \\ 0 & 0 & \zeta^2 \end{pmatrix} \begin{pmatrix} f(\tau) \\ f_1(\tau) \\ f_2(\tau) \end{pmatrix}, \quad \begin{pmatrix} f(-1/\tau) \\ f_1(-1/\tau) \\ f_2(-1/\tau) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} f(\tau) \\ f_1(\tau) \\ f_2(\tau) \end{pmatrix},$$

where $\zeta = \zeta_{48} = e^{2\pi i/48}$. We will continue to use the classical notations f, f_1, f_2, but mention that a more uniform and less arbitrary notation for the Weber functions would be

$$f_{\binom{0}{1}}(\tau) = f_1(\tau), \qquad f_{\binom{1}{0}}(\tau) = f_2(\tau), \qquad f_{\binom{1}{1}}(\tau) = \zeta\, f(\tau),$$

since: (i) the functions f_ξ^8 are conjugate over $\mathbb{C}(j^{1/3})$ and the functions f_ξ^{24} over $\mathbb{C}(j)$; (ii) $f_\xi(\tau)^{24} = \dfrac{2^{12}}{(c\tau+d)^{12}} \dfrac{\Delta(M\tau)}{\Delta(\tau)}$ where $\Delta(\tau) = q\prod(1-q^n)^{24}$ is the classical discriminant function and $M = \binom{a \;\; b}{c \;\; d}$ any 2×2 integral matrix of determinant 2 with $M\xi \equiv 0 \pmod 2$; and (iii) the transformation law becomes $f_\xi(\gamma\tau) = \lambda f_{\xi'}(\tau)$ for any $\gamma \in SL_2(\mathbb{Z})$, where $\gamma\xi' \equiv \xi \pmod 2$ and λ is a 24th root of unity.

We now define the Weber class invariants which we want to study. Consider d such that

$$d < 0, \qquad d \equiv 1 \pmod 8, \qquad d \not\equiv 0 \pmod 3). \tag{1}$$

i.e., d is the discriminant of an order $\mathcal{O}$ in an imaginary quadratic field in which 2 splits and 3 is unramified. Let $\mathrm{Pic}(\mathcal{O})$ denote the group of ideal classes of $\mathcal{O}$. We will represent its elements by $SL_2(\mathbb{Z})$-equivalence classes $[Q]$ of primitive positive definite quadratic forms $Q = [a,b,c]$ of discriminant $b^2 - 4ac = d$. To each Q is associated the number $\tau_Q = (-b+\sqrt{d})/2a$ which is the unique root in $\mathfrak{H}$ of $Q(\tau,1) = 0$. From the transformation formulas just given it is clear that the number $f_\xi(\tau_Q)^{24}$, where ξ is the unique vector in $\mathbb{F}_2^2$ with $Q(\xi) \not\equiv 0 \pmod 2$, depends only on the class $[Q]$. We now define a certain 24th root of (the negative of) this number with the same invariance property.

PROPOSITION. *Let d be a discriminant satisfying (1). For $Q = [a,b,c]$ a quadratic form of discriminant d, define*

$$f(Q) = \begin{cases} \zeta^{b(a-c-ac^2)} f(\tau_Q) & \text{if } 2|a,\ 2|c, \\ \varepsilon_d\, \zeta^{b(a-c-ac^2)} f_1(\tau_Q) & \text{if } 2|a,\ 2\nmid c, \\ \varepsilon_d\, \zeta^{b(a-c+a^2c)} f_2(\tau_Q) & \text{if } 2\nmid a,\ 2|c, \end{cases}$$

where $\varepsilon_d = (-1)^{(d-1)/8}$ and $\zeta = e^{2\pi i/48}$. Then:

(i) *$f(Q)$ depends only on the $SL_2(\mathbb{Z})$-equivalence class $[Q]$ of Q.*

(ii) *$f(Q) \in \mathbb{Q}(j(\tau_Q))$.*

By (i), we can write $f([Q])$ for $f(Q)$. We call the $h(d)$ numbers $f(\mathcal{A})$, $\mathcal{A} \in \mathrm{Pic}(\mathcal{O})$, the ***Weber singular moduli*** or ***Weber class invariants*** for the discriminant d. The minimal polynomial of $f(\mathcal{A}_0)$, where $\mathcal{A}_0 \in \mathrm{Pic}(\mathcal{O})$ is the principal class (corresponding to the form $Q_0 = [1,1,(1-d)/4]$), will be denoted $W_d(X)$ and called the ***Weber polynomial*** for the discriminant d. It follows from (ii) of the proposition that the roots of $W_d(X)$, i.e. the conjugates of $f(\mathcal{A}_0)$, are up to sign the numbers $f(\mathcal{A})$. Indeed, we know that each $j(\tau_Q)$ is a conjugate of $j(\tau_{Q_0})$, so the corresponding conjugate of $f(Q)$ is a real root of the equation $(X^{24}-1)^3 = j(\tau_{Q_0})X^{24}$. But this equation has only two real roots $\pm f(Q_0)$ (since as a cubic in X^{24} it has negative discriminant and hence only one real root, and a real number has only two real 24th roots). Based on the study of a large number of examples, we conjecture that the $f(\mathcal{A})$ themselves, and not merely their squares, are conjugates of one another (the choice of sign in the definition of $f(Q)$ was based on these examples). The truth of this conjecture could be verified by carefully working out the statement of the Shimura reciprocity law in this situation, but we have not done this. If it is true, then we have

$$W_d(X) = \prod_{\mathcal{A} \in \mathrm{Pic}(\mathcal{O})} (X - f(\mathcal{A}))\,. \tag{2?}$$

PROOF OF THE PROPOSITION: To prove (i), we must check the invariance under the generators of $SL_2(\mathbb{Z})$. Let $Q = [a,b,c]$, $Q^* = [c,-b,a]$, so that $\tau_{Q^*} = -1/\tau_Q$. Then, using the transformation formulas for the Weber functions under $\tau \mapsto -1/\tau$, we find

$$f(Q^*) = \begin{cases} \zeta^{-b(c-a-a^2c)} f(\tau_Q) & \text{if } 2|a,\ 2|c, \\ \varepsilon_d\, \zeta^{-b(c-a+ac^2)} f_1(\tau_Q) & \text{if } 2|a,\ 2\nmid c, \\ \varepsilon_d\, \zeta^{-b(c-a-a^2c)} f_2(\tau_Q) & \text{if } 2\nmid a,\ 2|c, \end{cases}$$

so $f(Q^*)$ and $f(Q)$ are the same if a or c is odd and differ by a factor $\zeta^{abc(a+c)}$ if both are even. But in the latter case $abc(a+c)$ is always divisible by 48 ($a/2$, $c/2$ and $(a+c)/2$ cannot all be odd, and $b^2-4ac \not\equiv 0 \pmod 3$ implies that at least one of $a, b, c, a+c$ is divisible by 3). Similarly, if we take $Q^* = [a, b-2a, c-b+a]$, with $\tau_{Q^*} = \tau_Q + 1$, then using the transformation formulas for the Weber functions under $\tau \mapsto \tau + 1$ we find that the desired equality $f(Q^*) = f(Q)$ is equivalent to the congruences

$$(b-2a)(b-c-a(c-b+a)^2) - 1 + 3(d-1) \equiv b(a-c-ac^2) \pmod{48} \quad \text{if } 2|a\,,$$
$$(b-2a)(b-c+a^2(c-b+a)) + 2 \equiv b(a-c+a^2c) \pmod{48} \quad \text{if } 2\nmid a\,,$$

and these can be checked by case-by-case analysis. This proves (i).

Now the $SL_2(\mathbb{Z})$-invariance lets us give an alternate definition of $f(\mathcal{A})$: choose a representative $Q = [a, b, c]$ for $\mathcal{A}$ with $(a, 6) = 1$ (this is possible because a primitive form represents numbers prime to any fixed modulus) and with $b \equiv -a \pmod{24}$ (this can be done by changing b by a suitable multiple of $2a$, since b is odd). Then since $a^2 \equiv 1 \pmod{24}$ we find

$$f(\mathcal{A}) = \varepsilon_d\, \zeta^{-1} f_2(\tau_Q) = \varepsilon_d \sqrt{2}/f(2\tau_Q - 1)\,,$$

where we have used the identity $f_2(\tau) = \zeta\sqrt{2}/f(2\tau - 1)$. But $\varpi = 2\tau_Q - 1$ is a root of the quadratic equation $A\varpi^2 + 2B\varpi + C = 0$ with A $(= a)$ and C $(= a+b+c)$ both odd, B $(= a+b)$ divisible by 24, and $AC - B^2$ $(= |d|)$ congruent to 7 modulo 8 and to ± 1 modulo 3, and for such a number Weber showed that $\sqrt{2}\, f(\varpi)$ is in the same field as the j-invariant ([11], §127; see also [3], [9] for more modern discussions). This proves (ii).

2. Examples of Weber class equations, their discriminants and resultants. As we just saw, we could have defined the Weber invariants $f(\mathcal{A})$ as $\varepsilon_d \sqrt{2}/f(2\tau_Q - 1)$, where $Q = [a, b, c]$ is any form in $\mathcal{A}$ with $(a, 6) = 1$ and $24|a + b$, rather than by the more complicated formulas in the proposition. The advantage of the definition we gave is that $f(\mathcal{A})$ can be computed using the root of *any* representative Q, so we can assume Q is reduced ($|b| \le a \le c$). Then τ_Q lies in the standard fundamental domain of $SL_2(\mathbb{Z})$ and the Weber functions converge at worst like power series in $e^{-\pi\sqrt{3}} \approx 0.004$, so that a few terms of the product expansion give $f(Q)$ as a complex number to high accuracy. Then $W_d(X)$ can be computed using (2?), where the roots $f(\mathcal{A})$ have been computed to sufficient accuracy to recognize each coefficient of W_d as a rational integer. This is much faster than the method used in [8] of computing only one real root to high accuracy and then finding its minimal polynomial by the "LLL" algorithm. Similarly, to compute the discriminant of a Weber class polynomial W_d, or the resultant of two such polynomials W_{d_1} and W_{d_2}, we compute the product of the differences of the roots as complex numbers to sufficient precision and then round to the nearest integer. The fact that we do in fact get integers to high accuracy provides at the same time a verification of the validity of formula (2?).

In this section we tabulate some of our numerical data which provides the basis for the conjectural formulas given in §§3–5. We calculated the polynomial W_d and their discriminants for all d satisfying (1) with $|d| < 2000$. Table 1 gives the results for a few values of d in the range $-500 < d < 0$. Instead of writing out all the powers in $W_d(X)$, we give just

$\lvert d\rvert$	$h(d)$	$W_d(x)$	$\mathrm{Disc}(W_d)$
7	1	$1,1$	1
23	3	$1,-1,0,1$	-23
31	3	$1,0,1,-1$	-31
47	5	$1,2,2,1,0,-1$	47^2
55	4	$1,1,0,-2,-1$	$-5^2 11$
71	7	$1,-1,-1,1,-1,-1,2,1$	-71^3
79	5	$1,-1,1,-2,3,-1$	79^2
95	8	$1,-1,0,1,-2,-1,2,2,-1$	$-5^4 17^2 19^3$
103	5	$1,-2,3,-3,1,1$	103^2
119	10	$1,1,2,4,5,7,9,8,5,4,1$	$7^4 17^5 19^2$
127	5	$1,-1,-2,1,3,-1$	127^2
143	10	$1,-3,6,-6,3,3,-9,13,-12,6,-1$	$5^2 11^4 13^5$
167	11	$1,-1,5,-4,10,-6,11,-7,9,-4,2,1$	$-17^2 167^5$
175	6	$1,1,0,0,0,-4,1$	$3^4 5^5 7^2$
191	13	$1,-2,0,4,-5,1,5,-11,19,-22,16,-10,6,-1$	$7^4 41^2 191^6$
215	14	$1,2,0,-6,-3,8,13,-4,-16,-7,13,11,-4,-6,-1$	$5^{11} 13^2 19^2 43^6$
239	15	$1,-4,4,4,-5,-13,20,4,-15,-13,27,-4,-8,-2,6,-1$	$-13^2 19^2 139^2 239^7$
247	6	$1,-3,6,-7,7,-4,-1$	$3^2 13^3 19^2$
311	19	$1,-1,2,-5,8,-14,13,-10,-1,9,-18,25,-10,-4,38,$ $-42,37,-16,4,1$	$-17^4 19^2 23^4 103^2\cdot$ $\cdot 211^2 311^9$
319	10	$1,5,11,14,10,2,1,5,9,6,-1$	$3^8 11^4 29^5$
335	18	$1,5,14,25,33,42,64,102,144,171,179,174,163,144,106,$ $55,20,4,-1$	$5^9 11^2 17^2 41^2 67^8 73^2\cdot$ $\cdot 127^2 139^2$
367	9	$1,-2,-1,6,-2,0,2,-3,9,-1$	$3^6 19^2 367^4$
383	17	$1,-1,-1,-1,0,1,13,7,11,4,1,7,23,31,42,24,6,-1$	$5^6 11^4 13^6 59^2 89^2 383^8$
407	16	$1,-1,2,-1,9,2,15,0,12,0,4,-19,-17,-33,-4,-10,-1$	$-5^4 11^7 37^8 41^4 83^2 97^2 199^2$
431	21	$1,3,6,9,9,-4,-10,-36,-30,-14,-2,66,41,83,44,$ $10,21,-40,16,-15,12,-1$	$13^{10} 31^2 43^2 73^2 107^2\cdot$ $\cdot 331^2 431^{10}$
455	20	$1,-6,15,-23,26,-16,-15,57,-73,30,76,-194,246,$ $-191,38,129,-200,142,-50,6,1$	$5^{14} 7^{14} 11^2 13^{14} 43^2 73^2\cdot$ $\cdot 97^2 131^2$
479	25	$1,3,9,22,41,60,66,47,6,-48,-82,-76,11,138,280,$ $336,317,205,144,109,126,104,76,23,10,-1$	$13^6 17^6 31^6 41^4 79^2 113^2\cdot$ $\cdot 283^2 379^2 479^{12}$

Table 1: Some Weber class polynomials and their discriminants

$h(d)$ and the coefficients of X^i in $W_d(X)$ ($h(d) \geq i \geq 0$); thus the fifth entry of the table means that $W_{-55}(X)$ is $X^4 + X^3 - 2X - 1$, with discriminant $-275 = -5^2 11$.

The discussion of these numbers will be postponed to §5; here we make only the observations that in Table 1 the sign of the discriminant of $W_d(x)$ is given by

$$\begin{cases} + & \text{if } \quad h \equiv 1 \text{ or } 2 \pmod 4 \\ - & \text{if } \quad h \equiv 0 \text{ or } 3 \pmod 4. \end{cases}$$

and that the primes dividing the discriminant of W_d are bounded above by $|d|$, with the power of $|d|$ (if $|d|$ is prime) being $(h(d) - 1)/2$.

In Table 2 we give the resultant of W_{d_1} and W_{d_2} for various pairs of discriminants d_1, d_2. The last five entries, marked off by a line, give some examples where $(d_1, d_2) \neq 1$, while the discriminants marked with an asterisk are not fundamental. We give only the absolute values since the sign of the resultant is easily computable and not very interesting (for instance, if d_1 and d_2 are prime then the sign depends only on d_1 and d_2 modulo 16 if $d_1 \equiv d_2 + 8 \pmod{16}$ and on $sgn(d_1 - d_2)$ if $d_1 \equiv d_2 \pmod{16}$).

$\|d_1\|$	$\|d_2\|$	$h(d_1)$	$h(d_2)$	—Resultant(W_{d_1}, W_{d_2})|
71	119	7	10	$23^{2}523$
151	295	7	8	$3^{8}179\cdot 211$
119	215	10	14	$19^{5}23^{4}1531$
143	239	7	15	$13\cdot 43^{2}107\cdot 139^{2}2131$
167	335	11	18	$5^{4}17^{6}79\cdot 331\cdot 379\cdot 499\cdot 739$
*175	239	6	15	$19^{2}41\cdot 59^{2}2411$
191	407	13	16	$7^{4}11\cdot 31^{2}41^{4}73\cdot 83\cdot 4003\cdot 4507$
215	479	14	25	$13^{6}17^{2}19^{4}29^{4}47^{2}691\cdot 877^{2}1051\cdot 2179$
247	431	6	21	$7^{4}599\cdot 1427\cdot 2963\cdot 6491$
287	367	14	9	$5^{7}29^{2}263^{2}5003$
311	191	19	13	$11^{4}19^{3}29^{2}31^{5}71^{2}2011$
319	383	10	17	$11^{4}13^{6}163^{2}1847\cdot 6947$
*343	431	7	21	$13^{2}131\cdot 181^{2}251\cdot 3947\cdot 8627\cdot 8699$
407	287	16	14	$5^{6}7^{4}139\cdot 149^{2}179^{2}787\cdot 811\cdot 1231$
431	263	21	13	$7^{12}167\cdot 257^{2}409\cdot 617^{2}787\cdot 883$
455	431	20	21	$7^{4}47^{2}71^{2}113^{2}131\cdot 181\cdot 199\cdot 239^{2}251\cdot 359^{2}1291\cdot 1699\cdot 2111^{2}12211$
479	359	25	19	$13^{6}19^{2}31\cdot 43^{3}67^{3}113^{2}157\cdot 227\cdot 239^{2}761^{2}977^{2}1163$
55	95	4	8	23^{2}
*175	287	6	14	$5\cdot 59^{2}419\cdot 2099$
247	455	6	20	$5^{2}11^{2}47^{2}4931\cdot 7019$
287	*343	14	7	$5^{5}31^{2}59\cdot 61^{2}4451$
319	407	10	16	$7^{8}89^{2}113^{2}1151\cdot 3659$

Table 2: Resultants of Weber class polynomials

This time we make the following observations: First, the primes dividing the resultant of W_{d_1} and W_{d_2} are bounded by $d_1 d_2/16$. Looking more carefully, we find that if p is such a prime, then p divides some positive integer m of the form $(d_1 d_2 - x^2)/16$ satisfying $m \not\equiv 1 \pmod 3$ and either $m \equiv 7 \pmod 8$ or $m \equiv 4 \pmod{16}$ or $m \equiv 0 \pmod{32}$. Refinements of these observations will lead in §3 to a complete conjectural formula for the resultants.

3. The prime factorization of the resultants. Let Q_1 and Q_2 be quadratic forms of (the same or different) discriminants d_1 and d_2 satisfying (1). Because of the relation $j(Q) = (f(Q)^{24} - 16)^3/f(Q)^{24}$, we see that any prime dividing $f(Q_1) - f(Q_2)$ also divides $j(Q_1) - j(Q_2)$. Hence to find the formula for the factorization of the norm of $f(Q_1) - f(Q_2)$, we start with the result of [7] on the factorization of $\mathcal{N}(j(Q_1) - j(Q_2))$. This involves an arithmetic function $\mathfrak{F}$ (depending on d_1 and d_2) whose definition we first recall.

Suppose that d_1 and d_2 are fixed negative discriminants. For convenience we exclude the values -3 and -4 (later d_1 and d_2 will be assumed to satisfy (1)). We also assume that d_1 and d_2 are coprime. Then for a prime p such that $(\frac{d_1 d_2}{p}) \neq -1$ we define

$$\varepsilon(p) = \begin{cases} (\frac{d_1}{p}) & \text{if } p \nmid d_1 \\ (\frac{d_2}{p}) & \text{if } p \nmid d_2 \end{cases}$$

(note that this is well-defined and always equal to ±1). For a positive integer n all of whose prime factors satisfy $(\frac{d_1 d_2}{p}) \neq -1$ we extend ε multiplicatively, i.e., we define $\varepsilon(n) = \prod_{p|n} \varepsilon(p)^{\mathrm{ord}_p(n)}$, where $\mathrm{ord}_p(n)$ denotes the power of p dividing n. Finally, if m is such that $\varepsilon(m)$ is defined and equal to -1, we set

$$\mathfrak{F}(m) = \prod_{\substack{nn'=m \\ n,n'>0}} n^{\varepsilon(n')}.$$

An easy proposition, proved in [7], is that $\mathfrak{F}(m)$ is always a prime power:

$$\mathfrak{F}(m) = \ell^{(a+1)(b_1+1)\cdots(b_s+1)} \tag{3}$$

if m has the form

$$m = \ell^{2a+1} p_1^{2a_1} \cdots p_r^{2a_r} q_1^{b_1} \cdots q_s^{b_s} \qquad (\varepsilon(\ell) = \varepsilon(p_i) = -1, \quad \varepsilon(q_i) = 1 \text{ for all } i)$$

(i.e., if there is a unique prime ℓ with $\varepsilon(\ell) = -1$ and $\mathrm{ord}_\ell(m)$ odd) and $\mathfrak{F}(m) = 1$ otherwise (i.e., if there are three or more such primes; note that there are always an odd number of them since $\varepsilon(m) = -1$). The main result of [7] is the formula

$$\mathcal{N}(j(Q_1) - j(Q_2))^2 = \prod \mathfrak{F}\left(\frac{d_1 d_2 - x^2}{4}\right), \tag{4a}$$

where the product is taken over all x such that $x^2 < d_1 d_2$ and that $x^2 \equiv d_1 d_2 \pmod 4$. Note that each of the integers $m = (d_1 d_2 - x^2)/4$ satisfies $\varepsilon(m) = -1$, so that $\mathfrak{F}(m)$ is defined. If d_1 and d_2 are both odd, the formula can be simplified to

$$\mathcal{N}(j(Q_1) - j(Q_2)) = \pm \prod_{\substack{0 < x < \sqrt{d_1 d_2} \\ x \text{ odd}}} \mathfrak{F}\left(\frac{d_1 d_2 - x^2}{4}\right). \tag{4b}$$

The formula implies that any prime p dividing the norm has the following properties:
(i) $(\frac{d_1}{p}) \neq 1$ and $(\frac{d_2}{p}) \neq 1$;
(ii) p divides a positive integer of the form $\frac{d_1 d_2 - x^2}{4}$, and in particular $p < d_1 d_2/4$;
(iii) $p < d_1 d_2/8$ if d_1 and d_2 are both congruent to 1 modulo 8.

We now want to find a similar type of formula for the norm of $f(Q_1) - f(Q_2)$, i.e., for the resultant of the Weber polynomials W_{d_1} and W_{d_2}. Since this norm divides that of $j(Q_1) - j(Q_2)$, as already mentioned, we know that only primes satisfying (i)–(iii) can occur. Looking at Table 2 in the previous section, we find that this is true and that in fact (iii) can be strengthened to $p < d_1 d_2/16$. However, even after studying this table (and a much larger collection of numerical results of which it is only an excerpt) in detail it was not obvious what the exact rule was for deciding which primes occurred and to which powers. To find this rule, we first split the problem into a series of simpler ones by passing, not from j directly to f, which satisfies an algebraic equation of degree 72 over j, but first to the cubic extension $\mathbb{C}(f^{24})$ of $\mathbb{C}(j)$ and then step by step to the $(24/r)$th degree extension $\mathbb{C}(f^r)$ of this, where r ranges over the divisors of 24.

The first step is easy. Looking at a number of examples of factorizations of the norm of $f(Q_1)^{24} - f(Q_2)^{24}$, we find that, just as for f, the prime divisors are always bounded by $d_1 d_2/16$ and that the only numbers $m = (d_1 d_2 - x^2)/4$ which contribute prime factors are those divisible by 4 (note that m is always even since d_1 and d_2 are 1 modulo 8 and x is even). This suggests the formula

$$\mathcal{N}(f(Q_1)^{24} - f(Q_2)^{24}) = \pm \prod_{x>0} \mathfrak{F}\left(\frac{d_1 d_2 - x^2}{16}\right), \tag{$5_?$}$$

where the product extends over all x between 0 and $\sqrt{d_1 d_2}$ for which $d_1 d_2 - x^2$ is divisible by 16, and this formula indeed turns out to be correct experimentally in all cases. To prove it, one would have to repeat the analysis in [7] with $SL_2(\mathbb{Z})$ replaced by the group $\Gamma_0(2)$.

To go further, we observe that the polynomial $X^{24} - 1$ factorizes as $\prod_{r|24} \varphi_r(X)$, where $\varphi_r(X)$ denotes the rth cyclotomic polynomial. We can write this in the homogeneous form $X^{24} - Y^{24} = \prod_{r|24} \Phi_r(X, Y)$ with the $\Phi_r(X, Y)$ $(r = 2^\alpha 3^\beta | 24)$ given by the table

	$\alpha = 0$	$\alpha = 1$	$\alpha = 2$	$\alpha = 3$
$\beta = 0$	$X - Y$	$X + Y$	$X^2 + Y^2$	$X^4 + Y^4$
$\beta = 1$	$X^2 + XY + Y^2$	$X^2 - XY + Y^2$	$X^4 - X^2Y^2 + Y^4$	$X^8 - X^4Y^4 + Y^8$

This factorization suggests that the function $\mathfrak{F}$ should have a corresponding decomposition as $\prod_{r|24} \mathfrak{F}_r$ in such a way that the norm of each $\Phi_r(f(Q_1), f(Q_2))$ is given a formula like $(5_?)$ but with $\mathfrak{F}$ replaced by $\mathfrak{F}_r$.

We have to give a formula for the arithmetic functions $\mathfrak{F}_r$. By looking at a large number of numerical examples, we found the following description. If $\mathfrak{F}(m) = 1$, then we set $\mathfrak{F}_r(m) = 1$ for each r. Otherwise by equation (3) we have $\mathfrak{F}(m) = \ell^{\gamma(m)}$ for some prime ℓ, where $\gamma(m) = \prod_{p|m} \gamma(p, m)$ with

$$\gamma(p, m) = \begin{cases} \operatorname{ord}_p(m) + 1 & \text{if } \varepsilon(p) = +1, \\ 1 & \text{if } \varepsilon(p) = -1,\ \operatorname{ord}_p(m) \text{ even}, \\ \frac{1}{2}(\operatorname{ord}_p(m) + 1) & \text{if } \varepsilon(p) = -1,\ \operatorname{ord}_p(m) \text{ odd (i.e. } p = \ell). \end{cases}$$

In this case we define $\mathfrak{F}_r(m)$ by

$$\mathfrak{F}_r(m) = \ell^{\gamma_r(m)}, \qquad \gamma_r(m) = \gamma_\alpha(2,m)\,\gamma_\beta(3,m) \prod_{p>3} \gamma(p,m)$$

where r has again been written as $2^\alpha 3^\beta$ with $0 \le \alpha \le 3$, $0 \le \beta \le 1$ and the numbers $\gamma_\alpha(2,m)$ and $\gamma_\beta(3,m)$ are given by the following two tables:

	$\alpha = 0$	$\alpha = 1$	$\alpha = 2$	$\alpha = 3$
$m \equiv 3 \pmod 8$	1	0	0	0
$m \equiv 7 \pmod 8$	0	1	0	0
$m \equiv 1 \pmod 4$	0	0	1	0
$m \equiv 2 \pmod 4$	0	0	0	2
$m \equiv 12 \pmod{16}$	1	0	0	2
$m \equiv 4 \pmod{16}$	0	1	0	2
$m \equiv 8 \pmod{16}$	0	0	2	2
$m \equiv 16 \pmod{32}$	1	0	2	2
$m \equiv 0 \pmod{32}$	$\mathrm{ord}_2(m) - 5$	2	2	2

Table 3: Values of $\gamma_\alpha(2,m)$

		$\beta = 0$	$\beta = 1$
$\left(\frac{d_1}{3}\right) = -\left(\frac{d_2}{3}\right)$,	$m \equiv 2 \pmod 3$	1	0
$\left(\frac{d_1}{3}\right) = -\left(\frac{d_2}{3}\right)$,	$m \equiv 1 \pmod 3$	0	1
$\left(\frac{d_1}{3}\right) = \left(\frac{d_2}{3}\right) = +1$,	$m \equiv 1 \pmod 3$	1	0
$\left(\frac{d_1}{3}\right) = \left(\frac{d_2}{3}\right) = +1$,	$m \equiv 0 \pmod 3$	$\mathrm{ord}_3(m) - 1$	2
$\left(\frac{d_1}{3}\right) = \left(\frac{d_2}{3}\right) = -1$,	$\mathrm{ord}_3(m)$ even	1	0
$\left(\frac{d_1}{3}\right) = \left(\frac{d_2}{3}\right) = -1$,	$\mathrm{ord}_3(m)$ odd	$\frac{1}{2}\,\mathrm{ord}_3(m)$	$\frac{1}{2}$

Table 4: Values of $\gamma_\beta(3,m)$

Then the following conjectural formula fits all cases we looked at. (In particular, cases with $\mathrm{ord}_2(m)$ up to 11 were checked numerically to test the last line of Table 3.)

CONJECTURAL DECOMPOSITION LAW FOR $\mathcal{N}(f(Q_1)^r - f(Q_2)^r)$. *Let d_1 and d_2 be coprime fundamental discriminants satisfying (1). For each divisor r of 24 we have*

$$\mathcal{N}(\Phi_r(f(Q_1), f(Q_2))) = \pm \prod_x \mathfrak{F}_r\left(\frac{d_1 d_2 - x^2}{16}\right), \qquad (6a?)$$

or equivalently

$$\mathcal{N}(f(Q_1)^r - f(Q_2)^r) = \pm \prod_x \prod_{d|r} \mathfrak{F}_d\left(\frac{d_1 d_2 - x^2}{16}\right), \qquad (6b?)$$

where x runs over integers between 0 and $\sqrt{d_1 d_2}$ for which $x^2 \equiv d_1 d_2 \pmod{16}$ and the functions $\mathfrak{F}_r(m)$ for $m \in \mathbb{N}$ with $\varepsilon(m) = -1$ and r a divisor of 24 are defined as above.

Remarks. 1. It is easily checked that the congruence conditions on m in Table 3 cover all possibilities. Similarly, since numbers m of the forms $(d_1 d_2 - x^2)/16$ are always congruent to 1 or 2 modulo 3 if $(d_1/3) \neq (d_2/3)$ and to 0 or 1 modulo 3 if $(d_1/3) = (d_2/3)$, the entries in Table 4 also cover all cases.

2. Adding the entries in each row of Tables 3 and 4 and comparing with the definition of $\gamma(p, m)$, we see that $\sum_{\alpha=0}^{3} \gamma_\alpha(2, m) = \gamma(2, m)$, $\sum_{\beta=0}^{1} \gamma_\beta(3, m) = \gamma(3, m)$ in all cases and hence

$$\sum_{r|24} \gamma_r(m) = \gamma(m), \qquad \prod_{r|24} \mathfrak{F}_r(m) = \mathfrak{F}(m).$$

Therefore the formula given is compatible with equation (5?).

3. Since the entries in the last column in Table 3 are all even, the formula given implies that the norms of $\Phi_8(f(Q_1), f(Q_2))$ and $\Phi_{24}(f(Q_1), f(Q_2))$ are always perfect squares.

4. The entries in the last row of Table 4, corresponding to the case when $\ell = 3$, are half-integers. Therefore $\gamma(m)$ can be a half-integer in this case. However, this happens if and only if m has the form $3y^2$ for some $y > 0$, since the formulas for $\gamma(p, m)$ and $\gamma_\alpha(2, m)$ imply that these numbers are even if $\mathrm{ord}_p(m)$ (resp. $\mathrm{ord}_2(m)$) is odd. Thus $\mathfrak{F}_r(m)$ is an integer multiple of $\sqrt{3}$ if $m = 3y^2$ and an integer otherwise. Since the number of representations of $d_1 d_2$ as $x^2 + 48y^2$ under our assumptions on d_1 and d_2 is always even, the formula stated always yields an integral value for $\mathcal{N}(\Phi_r(f(Q_1), f(Q_2)))$, as it should.

5. The case $r = 1$ of the conjecture gives the resultant of the Weber polynomials W_{d_1} and W_{d_2} (up to sign), as given in Table 2.

Example. Take $d_1 = -71$, $d_2 = -119$, with class numbers 7 and 10, respectively. Here the absolute value of the norm of $f(Q_1) - f(Q_2)$ is $23^2 523$ (first entry of Table 2), while that of $f(Q_1)^{24} - f(Q_2)^{24}$ is

$$7^{22} 11^{28} 13^{24} 17^{8} 23^{10} 47^{3} 59^{2} 71^{2} 113^{2} 163^{2} 257^{2} 433 \cdot 523 \approx 8.1 \times 10^{128}.$$

Table 5 gives the data needed to compute these numbers (or more generally the norm of $\Phi_r(f(Q_1), f(Q_2))$ for each divisor r of 24). The table shows the prime factorizations of the numbers $m = (d_1 d_2 - x^2)/16 = (8449 - x^2)/16$, the underlined prime factor being ℓ, and gives the values of $\mathfrak{F}_r(m)$ $(r|24)$ and of their product $\mathfrak{F}(m)$.

x	m	$\mathfrak{F}_1$	$\mathfrak{F}_2$	$\mathfrak{F}_4$	$\mathfrak{F}_8$	$\mathfrak{F}_3$	$\mathfrak{F}_6$	$\mathfrak{F}_{12}$	$\mathfrak{F}_{24}$	$\mathfrak{F}$
1	$2^4\cdot 3\cdot \underline{11}$	1	1	1	1	11^2	1	11^4	11^4	11^{10}
7	$3\cdot 5^2\cdot \underline{7}$	1	1	1	1	1	1	7^6	1	7^6
9	$\underline{523}$	523	1	1	1	1	1	1	1	523
15	$2\cdot \underline{257}$	1	1	1	257^2	1	1	1	1	257^2
17	$2\cdot 3\cdot 5\cdot \underline{17}$	1	1	1	1	1	1	1	17^8	17^8
23	$3^2\cdot 5\cdot \underline{11}$	1	11^4	1	1	1	11^2	1	1	11^6
25	$3\cdot \underline{163}$	1	1	1	1	1	1	163^2	1	163^2
31	$2^2\cdot 3^2\cdot \underline{13}$	1	13	1	13^2	1	13^2	1	13^4	13^9
33	$2^2\cdot 5\cdot \underline{23}$	23^2	1	1	23^4	1	1	1	1	23^6
39	$\underline{433}$	1	1	433	1	1	1	1	1	433
41	$3^2\cdot \underline{47}$	1	47	1	1	1	47^2	1	1	47^3
47	$2\cdot 3\cdot 5\cdot \underline{13}$	1	1	1	1	1	1	1	13^8	13^8
49	$2\cdot 3^3\cdot \underline{7}$	1	1	1	7^4	1	1	1	7^4	7^8
55	$3\cdot \underline{113}$	1	1	1	1	113^2	1	1	1	113^2
57	$5^2\cdot \underline{13}$	1	1	13^3	1	1	1	1	1	13^3
63	$2^3\cdot 5\cdot \underline{7}$	1	1	7^4	7^4	1	1	1	1	7^8
65	$2^3\cdot 3\cdot \underline{11}$	1	1	1	1	1	1	11^4	11^4	11^8
71	$3\cdot \underline{71}$	1	1	1	1	1	1	71^2	1	71^2
73	$3\cdot 5\cdot \underline{13}$	1	1	1	1	13^4	1	1	1	13^4
79	$2\cdot 3\cdot \underline{23}$	1	1	1	1	1	1	1	23^4	23^4
81	$2\cdot \underline{59}$	1	1	1	59^2	1	1	1	1	59^2
87	$5\cdot \underline{11}$	1	1	1	1	1	11^2	1	1	11^2
89	$3\cdot \underline{11}$	1	1	1	1	1	1	11^2	1	11^2

Table 5: Example of a resultant computation

4. Simplification of the formula for the resultant. In the last section we gave a conjectural formula for the norm of $f(Q_1)^r - f(Q_2)^r$, $r|24$. This formula is complete and is easy to apply numerically, but has the aesthetic disadvantage that the definition of the crucial function $\mathfrak{F}_r(m)$ is given in terms of the 48 entries of Tables 3 and 4, which were found experimentally and for which no unified description was given. In this section we will find such a unified description by a series of successive simplifications; the form we obtain finally will still be a little mysterious, but will involve many fewer pieces of experimentally obtained data.

The formula for the case $r = 24$, equation (5?), was a natural enough analogue of the known equation (4b) for the level 1 case; all the mystery concerned the splitting of the arithmetic function $\mathfrak{F}$ as $\prod_{r|24}\mathfrak{F}_r$. This splitting was described by Tables 3 and 4 which gave an additive decomposition of the number $\gamma(p,m)$ for $p = 2$ and $p = 3$. We will look first at the $p = 2$ case, which is more complicated but also more homogeneous because we are always assuming that d_1 and d_2 are $\equiv 1 \pmod 8$, whereas they can take on different values modulo 3.

Recall that for each prime p dividing an integer m for which $\mathfrak{F}(m)$ is defined, there is a well-defined sign $\varepsilon(p) = \pm 1$ which is the common value of the Legendre symbols $(\frac{d_1}{p})$ and $(\frac{d_2}{p})$ if these are both non-zero. Pick a quadratic field K in which all $p|m$ with $\varepsilon(p) = +1$ split and all $p|m$ with $\varepsilon(p) = -1$ are inert. (The field K will not matter here and is just a convenient device for counting ideals. However, in §5, where we consider the case $d_1 = d_2$, the canonical choice $K = \mathbb{Q}(\sqrt{d_1})$ will play a role.) Then formula (3) says that the exponent $\gamma(m)$ in the formula $\mathfrak{F}(m) = \ell^{\gamma(m)}$ is equal to the number of decompositions

$$m = \ell^k \mathcal{N}(\mathfrak{a}) \tag{7}$$

with $\mathfrak{a}$ an integral ideal of K, because there are $a+1$ possibilities $1, 3, \ldots, 2a+1$ for k and then $(b_1+1)\cdots(b_s+1)$ possibilities for $\mathfrak{a}$. In the splitting $\gamma(m) = \prod \gamma(p,m)$, each factor $\gamma(p,m)$ $(p \neq \ell)$ counts the number of ideals of norm $p^{\mathrm{ord}_p(m)}$. In particular, $\gamma(2,m)$ $(= \nu+1$, where $2^\nu \| m)$ is the cardinality of the set $\Gamma(2,m)$ of ideals of norm 2^ν $(= \{\mathfrak{p}^\nu, \mathfrak{p}^{\nu-1}\bar{\mathfrak{p}}, \ldots, \bar{\mathfrak{p}}^\nu\}$, where $(2) = \mathfrak{p}\bar{\mathfrak{p}})$, and it is reasonable to guess that the decomposition of $\gamma(2,m)$ into four numbers $\gamma_\alpha(2,m)$ corresponds to a partition of $\Gamma(2,m)$ into four subsets $\Gamma_\alpha(2,m)$. On aesthetic grounds (and others that will appear in §5), we distribute the ideals of $\Gamma(2,m)$ according to the following scheme:

	$\alpha = 0$	$\alpha = 1$	$\alpha = 2$	$\alpha = 3$
$m \equiv 3 \pmod 8$	$\{1\}$	—	—	—
$m \equiv 7 \pmod 8$	—	$\{1\}$	—	—
$m \equiv 1 \pmod 4$	—	—	$\{1\}$	—
$m \equiv 2 \pmod 4$	—	—	—	$\{\mathfrak{p}, \bar{\mathfrak{p}}\}$
$m \equiv 12 \pmod{16}$	$\{\mathfrak{p}\bar{\mathfrak{p}}\}$	—	—	$\{\mathfrak{p}^2, \bar{\mathfrak{p}}^2\}$
$m \equiv 4 \pmod{16}$	—	$\{\mathfrak{p}\bar{\mathfrak{p}}\}$	—	$\{\mathfrak{p}^2, \bar{\mathfrak{p}}^2\}$
$m \equiv 8 \pmod{16}$	—	—	$\{\mathfrak{p}^2\bar{\mathfrak{p}}, \mathfrak{p}\bar{\mathfrak{p}}^2\}$	$\{\mathfrak{p}^3, \bar{\mathfrak{p}}^3\}$
$m \equiv 16 \pmod{32}$	$\{\mathfrak{p}^2\bar{\mathfrak{p}}^2\}$	—	$\{\mathfrak{p}^3\bar{\mathfrak{p}}, \mathfrak{p}\bar{\mathfrak{p}}^3\}$	$\{\mathfrak{p}^4, \bar{\mathfrak{p}}^4\}$
$2^\nu \| m,\ \nu \geq 5$	$\{\mathfrak{p}^{\nu-i}\bar{\mathfrak{p}}^i\}_{3\leq i\leq \nu-3}$	$\{\mathfrak{p}^{\nu-2}\bar{\mathfrak{p}}^2, \mathfrak{p}^2\bar{\mathfrak{p}}^{\nu-2}\}$	$\{\mathfrak{p}^{\nu-1}\bar{\mathfrak{p}}, \mathfrak{p}\bar{\mathfrak{p}}^{\nu-1}\}$	$\{\mathfrak{p}^\nu, \bar{\mathfrak{p}}^\nu\}$

Table 3′: The sets $\Gamma_\alpha(2,m)$

An inspection of this table shows that the column (i.e., the value of α) to which a given ideal $\mathfrak{b} = \mathfrak{p}^{\nu-i}\bar{\mathfrak{p}}^i \in \Gamma(2,m)$ is assigned depends only on the minimum of i and $\nu - i$, i.e., only on the largest power of 2 which divides $\mathfrak{b}$. Of course, this is the same as the largest power dividing the ideal $\mathfrak{a}$ in the decomposition (7) (since $\mathfrak{b}$ is the 2-primary part of $\mathfrak{a}$). Denote by $c = c(\mathfrak{a})$ the *content* of $\mathfrak{a}$, i.e., the largest rational integer such that $\mathfrak{a} = c\,\mathfrak{a}_0$ for some integral ideal $\mathfrak{a}_0$ (which is then *primitive*, i.e., not divisible by any rational integer > 1). Then the 36 entries of Table 3′ can be replaced by the following simpler description of the α which must be assigned to the decomposition (7):

$$\begin{array}{lcl}
2\nmid c & \Rightarrow & \alpha = \begin{cases} 0 & \text{if } m \equiv 3 \pmod 8 \\ 1 & \text{if } m \equiv 7 \pmod 8 \\ 2 & \text{if } m \equiv 1 \pmod 4 \\ 3 & \text{if } m \equiv 0 \pmod 2 \end{cases} \\
2\| c & \Rightarrow & \alpha = \begin{cases} 0 & \text{if } m/4 \equiv 3 \pmod 4 \\ 1 & \text{if } m/4 \equiv 1 \pmod 4 \\ 2 & \text{if } m/4 \equiv 0 \pmod 2 \end{cases} \\
4\| c & \Rightarrow & \alpha = \begin{cases} 0 & \text{if } m/16 \equiv 1 \pmod 2 \\ 1 & \text{if } m/16 \equiv 0 \pmod 2 \end{cases} \\
8| c & \Rightarrow & \alpha = \;\; 0 \quad \text{always}
\end{array}$$

This already looks much simpler and can be improved immediately to the uniform formula

$$2^\alpha = \frac{8/(8,c)}{(8/(8,c),\ m/(8,c)^2 - 3)}\,,$$

where (,) denotes greatest common divisor. But we can do more. Write m as m_0c^2 (so $m_0 = \ell^k\mathcal{N}(\mathfrak{a}_0)$ in the notation already introduced) and observe that

$$\frac{m}{(8,c)^2} = \Bigl(\frac{c}{(8,c)}\Bigr)^2 m_0 \equiv m_0 \pmod{\frac{8}{(8,c)}}$$

because $c/(8,c)$ is prime to $8/(8,c)$ and any number prime to a divisor of 8 has square congruent to 1 modulo this divisor. (This property of 8 is shared by 3 and 24 and will be used again for them.) Hence finally we can rewrite the entire content of Table 3′ by saying that we assign to each decomposition (7) the number $\alpha \in \{0,1,2,3\}$ defined by

$$2^{3-\alpha} = (8,\ c(m_0 - 3))\,, \tag{8}$$

where $\mathfrak{a} = c\,\mathfrak{a}_0$ with $\mathfrak{a}_0$ primitive and $m_0 = m/c^2 = \ell^k\mathcal{N}(\mathfrak{a}_0)$.

We now turn to the prime $p = 3$. If we assume that $d_1 \equiv d_2 \equiv 1 \pmod 3$, corresponding to our assumption $d_1 \equiv d_2 \equiv 1 \pmod 8$ for the prime 2, then the discussion is exactly like the one for $p = 2$, but very much simpler. The analogue of Table 3 in this case is just lines 3 and 4 of Table 4 and the analogue of Table 3′ says simply that the decomposition $\Gamma(3,m) = \Gamma_0(3,m) \cup \Gamma_1(3,m)$ is $\{1\} \cup \emptyset$ if $m \equiv 1 \pmod 3$ and $\{\mathfrak{q}^{\mu-i}\bar{\mathfrak{q}}^i\}_{1\le i\le\mu-1} \cup \{\mathfrak{q}^\mu,\ \bar{\mathfrak{q}}^\mu\}$ if $m \equiv 0 \pmod 3$, where $(3) = \mathfrak{q}\bar{\mathfrak{q}}$ and $3^\mu \| m$. The same discussion as for $p = 2$ lets us summarize all this in the simple formula

$$3^{1-\beta} = (3,\ c(m_0 - 1)) \qquad \text{if } d_1 \equiv d_2 \equiv 1 \pmod 3\,. \tag{9}$$

This can then be combined with (8) as

$$2^{3-\alpha}\,3^{1-\beta} = (24,\ c(m_0 + 5)) \qquad \text{if } d_1 \equiv d_2 \equiv 1 \pmod{24}\,. \tag{10}$$

If d_1 and d_2 have opposite values modulo 3, then a similar analysis using lines 1 and 2 of Table 4 (but even easier, since now $\mathrm{ord}_p(m)$ is always 0) gives $3^{1-\beta} = (3, m+1) = (3, c_0(m+1))$, which can be combined with (8) as

$$2^{3-\alpha}\, 3^{1-\beta} \;=\; (24,\, c(m_0 - 11)) \qquad \text{if } d_1 \equiv d_2 \equiv 1 \pmod 8,\ d_1 d_2 \equiv 2 \pmod 3. \tag{11}$$

Finally, if $d_1 \equiv d_2 \equiv 2 \pmod 3$, then we can interpret the last two lines of Table 4 by saying that we must assign to the decomposition (7) the value $\beta = 0$ in all cases except when $\ell = 3$ and $\mathcal{N}(\mathfrak{a})$ is prime to 3, in which case the decomposition is to be counted for both $\beta = 0$ and $\beta = 1$, with multiplicity 1/2 each.

Let us now translate this discussion into a closed formula for the norm of $f(Q_1)^r - f(Q_2)^r$. To avoid case distinctions, we consider only the case $d_1 \equiv d_2 \equiv 1 \pmod{24}$. The left-hand side of (10) is $24/r$, where r is the index of the function $\mathfrak{F}_r$ appearing in equation (6?). Comparing (6a?) and (6b?), we see that we are really interested in the function $\prod_{d|r} \mathfrak{F}_d$. But for $r|24$ the condition that $24/d = (24, c(m_0+5))$ for some divisor d of r is equivalent simply to $24 | rc(m_0+5)$. We can therefore rewrite the conjecture formulated in §3 in the following closed form:

CONJECTURAL FORMULA FOR $\mathcal{N}(f(Q_1)^r - f(Q_2)^r)$, SECOND VERSION. *Let d_1 and d_2 be coprime fundamental discriminants congruent to 1 modulo 24. Then for any prime ℓ, the power of ℓ dividing $\mathcal{N}(f(Q_1)^{24} - f(Q_2)^{24})$ is equal to the number of representations of $d_1 d_2$ in the form*

$$d_1 d_2 = x^2 \,+\, 16\,\ell^k\, \mathcal{N}(\mathfrak{a}) \tag{12}$$

with $x \geq 1$, $k \geq 1$, and $\mathfrak{a}$ an integral ideal of K; and for any $r|24$ the power of ℓ dividing $\mathcal{N}(f(Q_1)^r - f(Q_2)^r)$ is the number of such representations also satisfying

$$c(\mathfrak{a}) \left(\ell \frac{\mathcal{N}(\mathfrak{a})}{c(\mathfrak{a})^2} + 5 \right) \equiv 0 \pmod{\frac{24}{r}}, \tag{13}$$

where $c(\mathfrak{a})$ is the content of $\mathfrak{a}$.

5. Factorizations of discriminants of Weber polynomials.

In this section we discuss the case $d_1 = d_2$, so that we are concerned with the discriminant of a single Weber polynomial rather than with the resultant of two different ones. The main ideas which will be needed are already contained in §4. For simplicity we will assume that $d_1 = d_2 = -p$ is a *prime* with $-p \equiv 1 \pmod{24}$. Then the class number $h = h(-p)$ of $K = \mathbb{Q}(\sqrt{-p})$ is odd. We write the corresponding class group as $\mathrm{Pic}(\mathcal{O}_K) = \{\mathcal{A}_0, \mathcal{A}_1^{\pm 1}, \ldots, \mathcal{A}_{(h-1)/2}^{\pm 1}\}$ with $\mathcal{A}_0$ the principal class.

We start with some preliminary comments which apply equally to each of the modular functions $g(\tau) = j(\tau)$ or $f(\tau)^r$ $(r|24)$. We have h numbers $g(\mathcal{A})$ $(\mathcal{A} \in \mathrm{Pic}(\mathcal{O}_K))$ which lie in the Hilbert class field H and are the roots of an irreducible monic polynomial $G(X) = G(g; X) \in \mathbb{Z}[X]$ and of K (so $G(j, X) = H_d(X)$ and $G(f, X) = W_d(X)$). Because H/K is Galois and abelian, we have

$$g(\mathcal{A}\mathcal{B}) - g(\mathcal{B}) = \sigma_{\mathcal{B}}(g(\mathcal{A}) - g(\mathcal{A}_0)) \qquad (\mathcal{A}, \mathcal{B} \in \mathrm{Pic}(\mathcal{O}_K), \quad \mathcal{A} \neq \mathcal{A}_0)$$

(here $\mathcal{B} \mapsto \sigma_{\mathcal{B}}$ is the Artin map $\mathrm{Pic}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$), so the discriminant of G factors:

$$\mathrm{disc}(G) = \pm \prod_{\substack{\mathcal{A}_1,\mathcal{A}_2 \in \mathrm{Pic}(\mathcal{O}_K)\\ \mathcal{A}_1 \neq \mathcal{A}_2}} \big(g(\mathcal{A}_1) - g(\mathcal{A}_2)\big) = \pm \prod_{\substack{\mathcal{A} \in \mathrm{Pic}(\mathcal{O}_K)\\ \mathcal{A} \neq \mathcal{A}_0}} \mathcal{N}_{H/K}\big(g(\mathcal{A}) - g(\mathcal{A}_0)\big)\,.$$

Also, it is easy to show that for each $\mathcal{A} \neq \mathcal{A}_0$ we have $\mathcal{N}_{H/K}\big(g(\mathcal{A}) - g(\mathcal{A}_0)\big) = \pm I(\mathcal{A})\sqrt{-p}$ for some positive rational integer $I(\mathcal{A}) = I(g;\mathcal{A})$, so finally

$$\mathrm{disc}(G) = \pm I^2 p^{(h-1)/2}\,, \qquad I = \prod_{i=1}^{\frac{1}{2}(h-1)} I(\mathcal{A}_i)\,. \tag{14}$$

The number I, of course, has a natural interpretation as the index of the order $\mathbb{Z}[g(\mathcal{A}_0)]$ in the full ring of integers of the maximal real subfield $H^+ = \mathbb{Q}(g(\mathcal{A}_0))$ of H. The fact that it decomposes naturally into $(h-1)/2$ factors means that we have replaced our original problem of determining the discriminant of G by the more refined problem of calculating each factor $I(\mathcal{A}_i)$. We first describe the solution of this problem for the case $g = j$, since this solution was proved but not written out explicitly in [7].

The main result of [7], given here as equations (4b) and (7), says that the power of a prime ℓ dividing the norm of $j(Q_1) - j(Q_2)$ in the case $d_1 \neq d_2$ is the number of representations of $d_1 d_2$ as $x^2 + 4\ell^k \mathcal{N}(\mathfrak{b})$ with $x, k > 0$ and $\mathfrak{b}$ primitive in K (K now defined as in §4); the conjecture in §4 then says that the same is true for f^{24} instead of j if we add the requirement $2|\mathfrak{b}$ (so $\mathfrak{b} = 2\mathfrak{a}$ with $\mathfrak{a}$ satisfying (12)) and for f^r if we add the congruence condition (13). If we now set $d_1 = d_2 = -p$ (and $K = \mathbb{Q}(\sqrt{-p})$), then the expression $\frac{1}{4}(d_1 d_2 - x^2)$ factors as $\frac{1}{2}(p-x) \cdot \frac{1}{2}(p+x)$. Since the two factors are coprime, we find that ℓ^k divides one factor $\frac{1}{2}(p \pm x)$. Then $\frac{1}{2}(p \pm x) = \ell^k \mathcal{N}(\mathfrak{b}_1)$, $\frac{1}{2}(p \mp x) = \mathcal{N}(\mathfrak{b}_2)$ for uniquely determined ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$ with $\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{b}$, so we have to count the representations of p in the form

$$p = \ell^k \mathcal{N}(\mathfrak{b}_1) + \mathcal{N}(\mathfrak{b}_2) \qquad (k \geq 1,\ \mathfrak{b}_1 \text{ and } \mathfrak{b}_2 \text{ integral ideals of } K)\,. \tag{15}$$

The result of [7] was then that the power of ℓ in each factor $I(j;\mathcal{A}_i)$ in (14) is equal to the number of decompositions (15) with $\mathfrak{b}_2 \in \mathcal{A}_i$. (This is proved in Theorem 4.7 of [7] and the three following sentences, but the subsequent Corollary 4.8 gives only the result for the product I.) Now going back to our case, it is clear that the logical conjecture is:

Conjectural formula for the discriminant factors. *Let $K = \mathbb{Q}(\sqrt{-p})$ with $p \equiv 23 \pmod{24}$ and other notations as above. Then for any prime ℓ, $r|24$, and non-principal ideal class $\mathcal{A} \in \mathrm{Pic}(\mathcal{O}_K)$, the power of ℓ dividing $I(f^r;\mathcal{A})$ is equal to the number of representations of p in the form (15) with $\mathfrak{b}_1$ and $\mathfrak{b}_2$ integral ideals of K with $\mathfrak{b}_2 \in \mathcal{A}$ and $\mathfrak{b}_1\mathfrak{b}_2 = 2\mathfrak{a}$ for some integral ideal $\mathfrak{a}$ and satisfying (13).*

Remarks. 1. The special case of this conjecture when $r = 1$ and we multiply all of the $I(\mathcal{A})$ says that the power of a prime $\ell \neq p$ dividing the discriminant of the Weber polynomial $W_{-p}(X)$ equals the number of representations (15) with $\mathfrak{b}_2$ non-principal and $\mathfrak{a} = \mathfrak{b}_1\mathfrak{b}_2/2$ an integral ideal satisfying (13) with $r = 1$.

2. When we decided to realize the decomposition $\gamma(2,m) = \sum_{\alpha=0}^{3} \gamma_\alpha(2,m)$ described in Table 3 by the partition $\Gamma(2,m) = \bigcup_{\alpha=0}^{3} \Gamma_\alpha(2,m)$ given in Table 3′, the only reason we could give was that this was the most natural way available and led to the simple final formula (8). However, in the case $d_1 = d_2$ the fact that the discriminant factors as in (14) means that we can uniquely recognize the "right" way to partition the set $\Gamma(2,m)$ (and similarly $\Gamma(3,m)$) by looking at the ideal classes to which the ideals in the various subsets must belong to make the formula work out. In fact the content of Table 3′ was found in this way, by looking at the various factors of the discriminant of $G(f^r;X)$ for a large number of quadratic fields and determining the unique way of choosing the entries in the table which was compatible with the numerical data.

Example. We illustrate the conjecture and remarks by one example. Take $p = 47$, with class number 5. Here the discriminant of the Weber polynomial $W_{-p}(X) = G(f,X)$ is uninteresting (compare Table 1), but the polynomials $G(j;X)$ and $G(f^r;X)$ for $r > 1$ have non-trivial discriminants. For instance, the polynomial $G(j,X)$ is

$$x^5 + 2257834125\,x^4 - 9987963828125\,x^3 + 5115161850595703125\,x^2 \\ - 1498247285082861328125O\,x + 16042929600623870849609375$$

whose discriminant factors as $47^2 I(j,\mathcal{B})^2 I(j,\mathcal{B}^2)^2$ with

$$I(j,\mathcal{B}) = 5^{15}11^2 13^5 19^4 23^2 29\cdot 31\cdot 41\,, \qquad I(j,\mathcal{B}^2) = 5^{15}11^7 13^5 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 43\,,$$

where $\mathcal{B}$ is ideal class of the prime ideal $\mathfrak{p}_2 = \left(2, \frac{1+\sqrt{-47}}{2}\right)$, and similarly the discriminant of the polynomial $G(f^r,X)$ for $g = f^r$ with $r|24$ factors as $47^2 I(g,\mathcal{B})^2 I(g,\mathcal{B}^2)^2$ with $I(g,\mathcal{A})$ given by:

g	f	f^2	f^3	f^4	f^6	f^8	f^{12}	f^{24}
$I(g,\mathcal{B})$	1	1	11	19	$5\cdot 11$	$5^2\cdot 19$	$5^3 11\cdot 19$	$5^5 11\cdot 13^2 19\cdot 23$
$I(g,\mathcal{B}^2)$	1	5	1	5	5	$5\cdot 31$	$5^3 11$	$5^5 11\cdot 23\cdot 31$

To explain these numbers in terms of the formula explained in this section, we must look at each decomposition of p in the form (15) with $\ell < p$ a prime quadratic non-residue of p. There are $(p-1)/2 = 23$ decompositions of p as $B_1 + B_2$ with B_1, $B_2 > 0$, $(B_1/p) = -1$, $(B_2/p) = +1$, and for each such decomposition a unique prime quadratic non-residue ℓ of p dividing B_1 to an odd power (since the smallest product of three prime non-residues of p is $715 > p$) and various representations of B_1/ℓ and B_2 as norms of ideals of $K = \mathbb{Q}(\sqrt{-p})$. Rather than making a table of all cases, we give all the details for the prime $\ell = 11$; the other primes ℓ work similarly and yield the numbers given in the above table.

The 25 decompositions of p in the form (15) with $\ell = 1$ all have $k = 1$ and are given by

$$\begin{aligned}
&\mathfrak{b}_1 = (1), && \mathfrak{b}_2 \in \{\mathfrak{p}_2^2\mathfrak{p}_3^2,\, 2\mathfrak{p}_3^2,\, \bar{\mathfrak{p}}_2^2\mathfrak{p}_3^2,\, 3\mathfrak{p}_2^2,\, (6),\, 3\bar{\mathfrak{p}}_2^2,\, \mathfrak{p}_2^2\bar{\mathfrak{p}}_3^2,\, 2\bar{\mathfrak{p}}_3^2,\, \bar{\mathfrak{p}}_2^2\bar{\mathfrak{p}}_3^2\}\,; \\
&\mathfrak{b}_1 \in \{\mathfrak{p}_2,\, \bar{\mathfrak{p}}_2\}, && \mathfrak{b}_2 = (5)\,; \\
&\mathfrak{b}_1 \in \{\mathfrak{p}_3,\, \bar{\mathfrak{p}}_3\}, && \mathfrak{b}_2 \in \{\mathfrak{p}_2\mathfrak{p}_7,\, \bar{\mathfrak{p}}_2\mathfrak{p}_7,\, \mathfrak{p}_2\bar{\mathfrak{p}}_7,\, \bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_7\}\,; \\
&\mathfrak{b}_1 \in \{\mathfrak{p}_2^2,\, (2),\, \bar{\mathfrak{p}}_2^2\}, && \mathfrak{b}_2 \in \{\mathfrak{p}_3,\, \bar{\mathfrak{p}}_3\}\,,
\end{aligned}$$

where $\mathfrak{p}_3$ and $\mathfrak{p}_7$ are prime ideals of norm 3 and 7, respectively, and $\bar{\mathfrak{p}}_p$ ($p = 2, 3, 7$) denote the conjugates of $\mathfrak{p}_p$. We can choose the ideals $\mathfrak{p}_3$ and $\mathfrak{p}_7$ to belong to the ideal classes $\mathcal{B}^2$ and $\mathcal{B}$, respectively, since K contains integers of norm 12 and 14. Then we find that of the 25 cases listed there are 7 for which $\mathfrak{b}_2$ is principal, 2 for which $\mathfrak{b}_2$ belongs to the class $\mathcal{B}$ (and of course equally many with $\mathfrak{b}_2 \in \mathcal{B}^4$), and 7 with $\mathfrak{b}_2 \in \mathcal{B}^2$ (or $\mathcal{B}^3$). This explains the powers 11^2 and 11^7 in the numbers $I(j, \mathcal{B})$ and $I(j, \mathcal{B}^2)$ given above.

Finally, of the 25 decompositions (15), there are only 5 with $\mathfrak{b}_1\mathfrak{b}_2$ divisible by 2, and of these there are one each with $\mathfrak{b}_2$ belonging to the ideal classes $\mathcal{B}$ or $\mathcal{B}^2$. This explains why the exponent of 11 in $I(f^{24}, \mathcal{B})$ and $I(f^{24}, \mathcal{B}^2)$ is 1. For the decomposition having $\mathfrak{b}_2 \in \mathcal{B}$, namely $\mathfrak{b}_1 = (1)$, $\mathfrak{b}_2 = 2\bar{\mathfrak{p}}_3^2$, the ideal $\mathfrak{a} = \mathfrak{b}_1\mathfrak{b}_2/2$ is primitive of norm 9, so the number occurring on the left-hand side of (13) is 104, which is divisible by $24/r$ if and only if r is a multiple of 3, explaining why the factor 11^1 occurs in $I(f^r, \mathcal{B})$ in these cases. Similarly, for the decomposition for which $\mathfrak{b}_2 \in \mathcal{B}^2$, namely $\mathfrak{b}_1 = (2)$, $\mathfrak{b}_2 = \mathfrak{p}_3$, we have that $\mathfrak{a}$ is primitive of norm 3, so the left-hand side of (13) is 38, which is divisible by $24/r$ only for $r = 12$ and 24.

6. Weber polynomials for other discriminants. In theory one could repeat the analysis of the previous sections for discriminants congruent to 5 (mod 8), 0 (mod 4), or 0 (mod 3), obtaining (conjectural) formulas for the conjugation behavior of the singular Weber moduli and for the norms of their differences. The results in general would be less sharp than in the case of discriminants satisfying (1) since, as mentioned in the introduction, one cannot usually get class invariants by going all the way from j to f but has to take a modular function on some intermediate group. We will restrict ourselves to giving some partial discussion of the two cases

A. $d \equiv 5 \pmod 8$ (so that 2 is inert) but still $\not\equiv 0 \pmod 3$, and

B. $d \equiv 1 \pmod 8$ as before but now $3|d$.

In both cases we will end up in small extension fields of the Hilbert class field $H = \mathbb{Q}(\sqrt{d})(j_0)$ and its real subfield $H^+ = \mathbb{Q}(j_0)$, $j_0 = j\left(\frac{1+\sqrt{d}}{2}\right)$.

A. If $d \equiv 5 \pmod 8$, then the correct class invariant is $f(\sqrt{d})$ rather than $\sqrt{2}/f(\sqrt{d})$ as before. It generates the same number field as $j_0 = j(\sqrt{d})$ (this was conjectured by Weber [11, §127] and proved by Schertz [9]), but this field no longer coincides with H^+ since now $h(4d)$ equals $3h(d)$ rather than $h(d)$ as in the case $d \equiv 1 \pmod 8$. Instead, $f(\sqrt{d})$ satisfies a cubic equation of the form

$$X^3 - 2\lambda X^2 + 2\mu X - 2 = 0$$

with λ and μ integers in H^+. (In particular, $f(\sqrt{d})^3/2$ is a unit.) The other two roots of this equation are $\sqrt{2}/f\left(\frac{\pm b+\sqrt{d}}{2}\right)$ where $b \equiv 0 \pmod 3$ and $\frac{b^2-d}{4} \equiv 1 \pmod{16}$, so the numbers λ and μ can be obtained easily, using an analogue of the proposition in §1 to find the numerical values of their conjugates. These two numbers have relatively small height and generate H^+, so we again get reasonable equations for generating the class field. Examples are given in Table 6. In all cases either $\theta = \lambda$ or $\theta = \mu$ (or $\theta = 0$ if $h = 1$) generates H^+, but the cases $d = -83$ and $d = -427$ show that neither λ nor μ alone always

$\lvert d\rvert$	$h(d)$	λ	μ	minimal polynomial of $\theta \in H^+$
11	1	1	1	X
19	1	0	-1	X
35	2	θ	θ	$X^2 - X - 1$
43	1	1	0	X
59	3	θ	$\theta^2 - \theta$	$X^3 - 2X^2 - 1$
67	1	1	-1	X
83	3	1	θ	$X^3 - X^2 - 3X + 4$
91	2	1	θ	$X^2 + X - 3$
107	3	θ	$(\theta^2 - \theta - 2)/2$	$X^3 - X - 4$
115	2	θ	θ	$X^2 - 3X + 1$
131	5	θ	$(-\theta^3 + \theta^2 - \theta + 2)/2$	$X^5 - 2X^4 + X^3 - 4X^2 + 7X - 4$
139	3	θ	$(\theta^2 - \theta - 2)/2$	$X^3 - X^2 - 2X - 4$
155	4	θ	$-1 - \theta$	$X^4 - X^3 - 3X - 1$
163	1	3	2	X
179	5	θ	$(\theta^2 - \theta - 2)/2$	$X^5 - 5X^3 - 16X^2 - 16X - 8$
187	2	θ	θ	$X^2 - 3X - 2$
211	3	θ	$-\theta$	$X^3 - 3X^2 + X - 2$
235	2	$-\theta + 3$	θ	$X^2 - X - 1$
403	2	$-2\theta - 2$	θ	$X^2 + 5X + 3$
427	2	θ	-1	$X^2 - 7X - 3$

Table 6: Class fields for discriminants $d \equiv 5 \pmod 8$

works. We do not know whether there is a universal combination of λ and μ which always generates the class field.

Note that, since the Galois group of $H/\mathbb{Q}$ is solvable (dihedral), we could have given a closed formula for the generator θ in the last column instead of its minimal polynomial over $\mathbb{Q}$. For instance, the θ for $d = -155$ has the minimal polynomial $X^2 - \frac{1+\sqrt{5}}{2}X + \frac{1-\sqrt{5}}{2}$ over $\mathbb{Q}(\sqrt{5})$ (the real subfield of the genus field of $\mathbb{Q}(\sqrt{d})$) and is given explicitly by $\theta = \dfrac{1+\sqrt{5}}{4} + \sqrt{\dfrac{-1+5\sqrt{5}}{8}}$, while the θ for $d = -107$ is $\dfrac{\sqrt[3]{6\sqrt{3}+\sqrt{107}} + \sqrt[3]{6\sqrt{3}-\sqrt{107}}}{\sqrt{3}}$.

B. We now consider the case when $d \equiv 1 \pmod 8$ but $3|d$. Then the class number h of $\mathbb{Q}(\sqrt{d})$ is divisible by 2, the Hilbert class field H contains the biquadratic field $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$, and its subfield H^+ has degree $h/2$ over the real quadratic field $\mathbb{Q}(\sqrt{-d/3})$. Let ε be the fundamental unit of this latter field. The number $\alpha = \sqrt{2}/f(\sqrt{d})$ has degree $3h$ rather than h over $\mathbb{Q}$ and only its cube lies in H^+. However, in all the examples we looked at, it was the case that (for an appropriate choice of ε)

$$\alpha^{3h}/\varepsilon = \text{cube (of a unit) in } H^+\,. \qquad (16_?)$$

Suppose that this is true. Then we have the following two possibilities:

i) If the class number h is $\equiv \pm 1 \pmod 3$, then (16?) implies that $\alpha/\varepsilon^{\pm 1/3}$ belongs to H^+, so again we get relatively small generators of the class field. As an example, take $d = -159$, with $h = 10$. Then the minimal polynomial of α^3 over $\mathbb{Q}$ is

$$X^{10} - X^9 + X^8 + 7X^7 + 63X^6 + 121X^5 + 219X^4 + 196X^3 + 146X^2 + 47X - 1\,,$$

with discriminant $3^{12}11^2 17^4 53^5 59^2 79^2$, while that of $\alpha/\varepsilon^{1/3}$, where $\varepsilon = (7+\sqrt{53})/2$, is

$$X^{10} - 3X^9 + 7X^8 - 2X^7 + 15X^6 + 18X^5 - 37X^4 - 60X^3 - 27X^2 - 2X + 1$$

with discriminant $3^8 53^5 79^2 223^2$, which is somewhat better. However, the discriminant of H^+ is $3^4 53^5$ and this field contains an element with the much simpler minimal polynomial $X^{10} - X^9 + 2X^8 + 7X^7 + X^6 - 15X^5 - 5X^4 + 8X^3 + 5X^2 - 5X + 1$ of discriminant $3^8 19^2 53^5$, so the polynomials obtained from α^3 and $\alpha/\varepsilon^{1/3}$ are — as is to be expected — not as good as the ones obtained directly from α in the case $3\nmid d$.

ii) On the other hand, if h is divisible by 3 then (16?) no longer lets us obtain an equation of degree h for α by dividing by $\varepsilon^{\pm 1/3}$. Instead, it says that H^+ contains the sextic field $\mathbb{Q}(\varepsilon^{1/3})$. Then α^3, which has degree h over $\mathbb{Q}$, can also be given by an equation of degree $h/2$ over $\mathbb{Q}(\varepsilon)$ and by an equation of degree $h/6$ over $\mathbb{Q}(\varepsilon^{1/3})$. For instance, the generator $x = (\sqrt{2}/f(\sqrt{d}))^3$ of H^+ for $d = -87$ (class number 6) satisfies the equations

$$\begin{aligned} &x^6 + x^5 + 4x^4 - 4x^3 + 11x^2 + 13x - 1 = 0\,, \\ &x^3 - (2+\varepsilon^{-1})x^2 + (3-\varepsilon^{-1})x - \varepsilon^{-1} = 0\,, \\ &3x + (2\varepsilon^{5/3} + \varepsilon^{4/3} + \varepsilon - 10\varepsilon^{2/3} - 7\varepsilon^{1/3} - 3) = 0 \end{aligned}$$

where $\varepsilon = (5+\sqrt{29})/2$. Similarly, the generator x for $d = -231$ ($h = 12$) satisfies

$$3x^2 - (6\eta^5 - \eta^4 - 53\eta^2 + 9\eta - 2)\,x + (2\eta^5 - 2\eta^4 + \eta^3 - 19\eta^2 + 17\eta - 2) = 0$$

where $\eta = \varepsilon^{1/3}$, $\varepsilon = (9+\sqrt{77})/2$.

Acknowledgements. The first author was partially supported by a Natural Sciences and Engineering Research Council of Canada grant, as well as Senior Research Fellowships at Newnham College and the Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, and by the Newton Institute. The paper was completed at the Max-Planck-Institut für Mathematik, Bonn.

References

[1] Atkin, O. and Morain, F., Elliptic curves and primality proving, preprint, University of Illinois at Chicago, 1989.

[2] Berwick, W.E.H., Modular invariants expressible in terms of quadratic and cubic irrationalities, Proc. London Math. Soc. **28** (1928), pp. 53-69.

[3] Birch, B., Weber's class invariants, Mathematika **16** (1969), pp. 283–294.

[4] Cohn, H., *Introduction to the Construction of Class Fields*, Cambridge studies in advanced mathematics **6**, Cambridge University Press 1985.

[5] Cox, D., *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, 1989.

[6] Deuring, M., Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung, Comm. Math. Helvetici **19** (1946), pp. 74–82.

[7] Gross; B. and Zagier, D., On singular moduli, J. Reine Angew. Math. **355** (1985), pp. 191–220.

[8] Kaltofen, E., and Yui, N., Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction, Number Theory, New York Seminars 1989–90, Springer-Verlag (1991), pp. 149–202.

[9] Schertz, R., Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_2, γ_3, J. Reine Angew. Math. **286/287** (1976), pp. 46–74.

[10] Watson, G.N., Singular moduli (3), Proc. London Math. Soc. **40**, (1936), pp. 83–142.

[11] Weber, H., *Lehrbuch der Algebra*, Bd. III, Braunschweig, 1908.

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

Don Zagier
Max-Planck-Institut für Mahematik
Gottfried-Claren-Straße 26
53225 Bonn, Germany
email: zagier@mpim-bonn.mpg.de