TOKYO J. MATH.
VOL. 21, NO. 1, 1998

A Conjectural Extension of the Gross–Zagier Formula on Singular Moduli

Tim HUTCHINSON

Queen's University

(Communicated by K. Katayama)

Abstract. The values of the elliptic modular j-invariant at imaginary quadratic arguments are algebraic integers, known as singular moduli of level one. If d_1 and d_2 are imaginary quadratic discriminants, then we may consider a generalized resultant of the class polynomials of the orders of discriminant d_1 and d_2; this is the norm of the differences of singular moduli of the corresponding orders, denoted here by $J(d_1, d_2)$. These resultants are highly factorizable; Gross–Zagier established a closed formula for $J(d_1, d_2)^2$ when d_1 and d_2 are fundamental discriminants, with $(d_1, d_2)=1$. In this paper we present a conjectural extension of the Gross–Zagier formula to the case when d_1 and d_2 are not necessarily fundamental, and $(d_1, d_2)=l^e$, where l is a prime not dividing the product of the conductors of d_1 and d_2.

1. Introduction.

The values of the elliptic modular j-invariant at imaginary quadratic arguments are algebraic integers, known as singular moduli of level one. The main applications of singular moduli include the explicit construction of class fields [3] and elliptic curve primality proving [1], which is required for RSA public-key cryptography. The minimal polynomial of singular moduli corresponding to imaginary quadratic arguments of discriminant d is known as the class polynomial of $\mathcal{O}_d$ (the imaginary quadratic order of discriminant d). Let d_1 and d_2 be imaginary quadratic discriminants. Then we may consider the resultant of the class polynomials of $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$; it is defined to be the norm of the differences of two singular moduli of the corresponding orders.

More generally, for $i=1, 2$, we write h_i for the class numbers of $\mathcal{O}_{d_i}$, and w_i for the number of units in $\mathcal{O}_{d_i}$. Then we define

$$J(d_1, d_2)=\left[\prod_{s=1}^{h_1}\prod_{t=1}^{h_2}(j(\tau_s)-j(v_t))\right]^{4/w_1w_2},$$

where τ_s (respectively, v_t) runs over imaginary quadratic arguments corresponding to the form class group of $\mathcal{O}_{d_1}$ (respectively, $\mathcal{O}_{d_2}$). (Recall that a set of representatives for the

Received May 28, 1997
Revised August 27, 1997

form class group of an imaginary quadratic order of discriminant d consists of the primitive, positive definite, reduced quadratic forms of discriminant d, and that the form class group is isomorphic to the ideal class group. Also, note that when d is a fundamental discriminant, $\mathcal{O}_d$ is the ring of integers of $\mathbf{Q}(\sqrt{d})$.)

Since $w_i = 2$ when $d_i < -4$, note that when $d_1 < -4$ and $d_2 < -4$, $J(d_1, d_2)$ is the resultant discussed above. M. Deuring [6] noticed that these resultants are highly factorizable integers, and Gross–Zagier [10] established a closed formula for $J(d_1, d_2)^2$ when d_1 and d_2 are fundamental discriminants, with $(d_1, d_2) = 1$.

2. The Gross–Zagier formula.

In order to state the Gross–Zagier formula, we first need to define a component function.

Assume that $(d_1, d_2) = 1$. For primes l with $\left(\frac{d_1 d_2}{l}\right) \neq -1$, we define

$$\varepsilon(l) = \begin{cases} \left(\dfrac{d_1}{l}\right) & \text{if } (l, d_1) = 1, \\ \left(\dfrac{d_2}{l}\right) & \text{if } (l, d_2) = 1\,. \end{cases}$$

If $n = \prod_{i=1}^{r} l_i^{a_i}$ with $\left(\frac{d_1 d_2}{l_i}\right) \neq -1$ for all i, then we define $\varepsilon(n) = \prod_{i=1}^{r} \varepsilon(l_i)^{a_i}$. (The restriction on l_i is necessary to ensure that the $\varepsilon(l_i)$ are well-defined; this will be referred to in Definitions 3.1, 3.4, and 3.7, below, without stating the restriction explicitly.)

We may then define

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

where any prime divisor l of m satisfies $\left(\frac{d_1 d_2}{l}\right) \neq -1$.

There is a closed formula for $F(m)$, which not only makes computations easier but is also needed in the proof of the Gross–Zagier formula.

Proposition 2.1 [10]. *Let m be a positive integer of the form $m = (d_1 d_2 - x^2)/4$. Then*

$$F(m) = \begin{cases} p^{(a+1)(b_1+1)\cdots(b_s+1)} & \textit{if } m = p^{2a+1} p_1^{2a_1} \cdots p_r^{2a_r} q_1^{b_1} \cdots q_s^{b_s}, \textit{ where} \\ & \varepsilon(p) = \varepsilon(p_i) = -1 \textit{ and } \varepsilon(q_i) = 1 \textit{ for all } i, \\ 1 & \textit{otherwise}. \end{cases}$$

Proof. A proof is outlined by D. A. Cox in Exercises 13.15 and 13.16 of [4]. □

We are now is a position to state the Gross–Zagier formula.

THEOREM 2.2 [10]. *Let d_1 and d_2 be imaginary quadratic, relatively prime, fundamental discriminants. Then*

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x^2 < d_1 d_2 \\ x^2 \equiv d_1 d_2 \pmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right).$$

Two proofs are given in [10], one algebraic and one analytic in approach. In the algebraic proof, it is assumed that $d_1 = -p$ for a prime p; D. Dorman [7] has extended the algebraic proof to the case stated in the theorem. The algebraic proof uses the theory of elliptic curves with complex multiplication (counting the number of isomorphisms of supersingular elliptic curves), and depends on the existence and properties of the Hilbert class field of $\mathbf{Q}(\sqrt{d_1})$.

An easy corollary of the Gross–Zagier formula gives a precise bound on the primes dividing $J(d_1, d_2)^2$.

COROLLARY 2.3 [10]. *If l is a prime dividing $J(d_1, d_2)^2$, then*

(a) $\left(\frac{d_1}{l}\right) \neq 1$ *and* $\left(\frac{d_2}{l}\right) \neq 1$,

(b) *l divides a positive integer of the form $(d_1 d_2 - x^2)/4$,*

(c) *$l \leq d_1 d_2/4$, and further,*

  (i) *if $d_1 d_2 \equiv 1 \pmod 8$, then $l < d_1 d_2/8$, and*

  (ii) *if $d_1 \equiv d_2 \equiv 5 \pmod 8$, then $l < d_1 d_2/16$.*

There are also corollaries, formulated by Kaltofen–Yui [11], which give an expression for a class polynomial evaluated at zero (with some additional restrictions, it is a perfect cube), and an expression for the discriminant of a class polynomial. These corollaries, which we will not state here, are useful for verifying the accuracy of computations of class polynomials; it is the computation of class polynomials which is needed for the construction of Hilbert class fields and for elliptic curve primality proving.

3. Extending the Gross–Zagier formula.

One would certainly like to establish a formula for $J(d_1, d_2)^2$ which holds for any two imaginary quadratic discriminants. In the case of non-fundamental discriminants, we need to consider imaginary quadratic orders, rather than just the maximal order (the ring of integers) of imaginary quadratic fields. Results of computations (carried out using GP/PARI [2]) of $J(d_1, d_2)^2$ for non-fundamental discriminants and discriminants with a non-trivial common divisor suggest an approach to this problem. In particular, Corollary 2.3, which specifies a bound on the divisors of $J(d_1, d_2)^2$, appears to hold for a larger class of discriminants; see Table 1. In fact, as we learned later from

M. Kaneko, this corollary has been established for arbitrary imaginary quadratic discriminants; we will discuss the details of the later. Since the corollary follows directly from the formula, this suggests that the Gross–Zagier formula should hold for a larger class of discriminants, given an appropriate extension of the definition of $F(m)$.

In the original case $F(m)$ is defined in terms of the function $\varepsilon(p)$. A more usable formula for $F(m)$ (and, indeed, one which is required in the proof of the Gross–Zagier formula) is given in Proposition 2.1. It does not appear possible to extend the definition of $\varepsilon(l)$ to the case $l|(d_1, d_2)$ or to the case of non-fundamental discriminants; instead, the definition of $F(m)$ will take the form of Proposition 2.1.

We shall present a conjectural formula for $J(d_1, d_2)^2$ for the case when $(d_1, d_2)=l^e$, where l is a prime not dividing the product of the conductors of d_1 and d_2. It turns out that these conditions account for about 75 percent of all possible discriminants in the range, for instance, of -500 to -3, while the conditions in the original Gross–Zagier formula account for about 30 percent. Rather than presenting the full conjecture immediately, we first present two simpler cases.

Note that when p does not divide (d_1, d_2), $\varepsilon(p)$ is well-defined, so in those cases we will continue to use the notation of $\varepsilon(p)$ (see Section 2).

3.1. A conjectural formula: $(d_1, d_2)>1$. We first relax the restriction that d_1 and d_2 must be relatively prime. Here we still assume that d_1 and d_2 are fundamental discriminants, but allow their greatest common divisor to be a prime power. (Examples of this are represented by the first eleven entries of Table 1.)

DEFINITION 3.1. Suppose that d_1 and d_2 are fundamental discriminants. If $l|(d_1, d_2)$ where l is a prime, and given m, we define $\chi=\chi(l, m)=1$ if $(l, m)>1$; otherwise let $\chi=0$. Suppose further that $\varepsilon(p)=\varepsilon(p_i)=-1$ for all i; $\varepsilon(q_i)=1$ for all i. (Note that the primes l, p, p_i, and q_i are all distinct, and that p, p_i, and q_i need to be restricted so that $\varepsilon(p)$, $\varepsilon(p_i)$, and $\varepsilon(q_i)$ are well-defined, as above). Then (for a, a_i, $b_i \geq 0$) we define

$$F(m)=\begin{cases} l^{e(b_1+1)\cdots(b_s+1)} & \text{if } m=l^e p_1^{2a_1}\cdots p_r^{2a_r} q_1^{b_1}\cdots q_s^{b_s} \ (e\geq 0)\,, \\ p^{2\chi(a+1)(b_1+1)\cdots(b_s+1)} & \text{if } m=l^e p^{2a+1} p_1^{2a_1}\cdots p_r^{2a_r} q_1^{b_1}\cdots q_s^{b_s}\,, \\ 1 & \text{otherwise}\,. \end{cases}$$

CONJECTURE 3.2. With the definition of $F(m)$ as above, the Gross–Zagier formula holds for any two imaginary quadratic, fundamental discriminants d_1 and d_2 such that (d_1, d_2) is a prime power.

EXAMPLE 3.3. We shall give two computations of $|J(d_1, d_2)^2|$, based on the first case of the conjecture. (The conjecture has been checked (using GP/PARI) for $-200 \leq d_1, d_2 \leq -3$.) The factors which illustrate the conjecture (that is, those not covered by Gross–Zagier's definition of $F(m)$) are set in boldface.

TABLE 1. Values of $|J(d_1, d_2)^2|$

d_1	d_2	$\lvert J(d_1, d_2)^2\rvert$
-3	-15	$3^4 5^2 11^2$
-3	-24	$2^8 3^4 17^2$
-3	-120	$2^{16} 3^{12} 5^4 41^2 89^2$
-4	-8	$2^7 7^2$
-4	-52	$2^{16} 3^{14} 43^2$
-4	-136	$2^{28} 3^{28} 11^4 127^2$
-20	-24	$2^{56} 13^8 17^4 19^4 37^4 71^2$
-35	-155	$2^{248} 5^{24} 7^{16} 31^6 61^2 67^4 107^4 113^4 271^2$
-40	-52	$2^{56} 3^{52} 5^{12} 73^4 79^2 439^2$
-51	-195	$2^{248} 3^{64} 31^8 47^4 101^2 109^4 191^2 251^2 389^2 569^2 599^2$
-115	-195	$2^{260} 3^{48} 5^{24} 13^8 19^8 47^8 167^4 191^2 197^4 659^2 971^2 1031^2$
-3	-16	$2^2 3^2 11^2$
-3	-64	$2^2 3^4 23^2 47^2$
-4	-99	$2^{12} 7^4 19^4 83^2$
-4	-175	$3^{40} 7^6 19^2 31^2 47^4 83^4 139^2$
-7	-32	$5^{12} 7^4 13^4 31^2 47^2$
-7	-108	$3^6 5^{20} 17^4 41^4 47^4 89^2 173^2$
-7	-144	$3^{12} 7^8 19^4 31^4 47^4 59^4 83^2 131^2 227^2 251^2$
-16	-27	$2^6 3^2 59^2 83^2 107^2$
-16	-99	$2^{12} 7^8 11^6 79^4 107^2 227^2 347^2$
-3	-60	$3^4 5^2 29^2 41^2$
-3	-96	$2^8 3^8 23^2 47^2 71^2$
-3	-156	$3^{12} 17^2 53^2 101^2 113^2$
-4	-36	$2^{18} 3^3 7^4 11^2$
-8	-180	$2^{56} 5^{12} 13^8 31^4 37^4 71^2 191^2 239^2 311^2 359^2$
-8	-200	$2^{116} 5^6 7^{24} 13^{12} 23^4 29^4 31^6 37^4$
-12	-75	$2^{16} 3^{20} 5^2 11^4 17^4 23^4 29^2$
-12	-123	$2^{16} 3^{12} 5^{12} 41^2 113^2 173^2 269^2 353^2$
-12	-147	$2^{16} 3^{12} 5^{12} 11^8 17^2 23^4 29^4 41^2$
-15	-96	$3^{64} 13^{16} 37^4 41^4 43^4 67^4 71^2 89^4 191^2 239^2 311^2 359^2$
-15	-160	$3^{48} 5^{28} 29^8 43^4 67^4 71^2 73^4 101^4 149^4 239^2 311^2 431^2 479^2 599^2$

(a)
$$\begin{aligned}|J(-20,-24)^2| &= \boldsymbol{F}(\mathbf{2^3 3^1 5^1})[F(7^1 17^1)\boldsymbol{F}(\mathbf{2^2 29^1})F(3^1 37^1)\boldsymbol{F}(\mathbf{2^3 13^1})\cdot\\ &\quad F(5^1 19^1)\boldsymbol{F}(\mathbf{2^2 3^1 7^1})F(71^1)\boldsymbol{F}(\mathbf{2^3 7^1})\cdot\\ &\quad F(3^1 13^1)\boldsymbol{F}(\mathbf{2^2 5^1})]^2\\ &= \mathbf{2^{12}}[17^2\mathbf{2^4}37^2\mathbf{13^2}19^2\mathbf{2^8}71^1\mathbf{2^6}13^2\mathbf{2^4}]^2\\ &= 2^{56}13^8 17^4 19^4 37^4 71^2\end{aligned}$$

$(l=2;\, p_i=13;\, q_i=3, 5, 7, 29)$

(b)
$$\begin{aligned}|J(-40,-52)^2| &= \boldsymbol{F}(\mathbf{2^3 5^1 13^1})[F(3^1 173^1)\boldsymbol{F}(\mathbf{2^2 3^1 43^1})F(7^1 73^1)\cdot\\ &\quad \boldsymbol{F}(\mathbf{2^3 3^2 7^1})F(3^2 5^1 11^1)\boldsymbol{F}(\mathbf{2^2 11^2})F(3^1 157^1)\cdot\\ &\quad \boldsymbol{F}(\mathbf{2^3 3^1 19^1})F(439^1)\boldsymbol{F}(\mathbf{2^2 3^1 5^1 7^1})F(3^1 7^1 19^1)\cdot\end{aligned}$$

$$\begin{aligned}
&\boldsymbol{F(2^3 47^1)}F(3^3 13^1)\boldsymbol{F(2^2 3^4)}F(5^1 59^1)\cdot\\
&\boldsymbol{F(2^3 3^1 11^1)}F(3^1 7^1 11^1)\boldsymbol{F(2^2 7^2)}F(3^1 53^1)\cdot\\
&\boldsymbol{F(2^3 3^1 5^1)}F(79^1)\boldsymbol{F(2^2 3^2)}]^2\\
=&\boldsymbol{5^4}[3^2\boldsymbol{1^1}73^2\boldsymbol{2^6}5^2\boldsymbol{2^6}3^2\boldsymbol{3^4}439^1\boldsymbol{1^1}3^4\boldsymbol{2^6}3^4\boldsymbol{2^2}\cdot\\
&5^2\boldsymbol{3^4}3^4\boldsymbol{2^6}3^2\boldsymbol{1^1}79^1\boldsymbol{2^2}]^2\\
=&2^{56}3^{52}5^{12}73^4 79^2 439^2
\end{aligned}$$

$(l=2; p_i=3, 5, 43; q_i=7, 11, 13, 47)$

3.2. A conjectural formula: non-fundamental discriminants. We next reintroduce the restriction that $(d_1, d_2)=1$, but allow the possibility that d_1 or d_2 is non-fundamental. (Examples of this are represented by the middle nine entries of Table 1.) For our purposes, a discriminant D is said to be fundamental if it is the discriminant of an imaginary quadratic field. That is, given a discriminant D, we may write

$$D=\mathfrak{f}^2 d_K\,,$$

where $\mathfrak{f}$ is the conductor of D and d_K is the discriminant of an imaginary quadratic field, $\mathbf{Q}(\sqrt{D})$. Then D is non-fundamental if and only if $\mathfrak{f}>1$. In our case, we will write $\mathfrak{f}_i$ for the conductor of d_i. As before, $F(m)$ will depend on the values of $\varepsilon(p)$, where p is a prime divisor of m. In the present case, we must also distinguish between primes p which divide $\mathfrak{f}_1\mathfrak{f}_2$ and such that $\varepsilon(p)=-1$; primes q which divide $\mathfrak{f}_1\mathfrak{f}_2$ and such that $\varepsilon(q)=1$; and primes which do not divide $\mathfrak{f}_1\mathfrak{f}_2$. Notation for this is introduced below.

Definition 3.4. Let $\mathfrak{f}_i$ be the conductor of d_i. Suppose $\varepsilon(p)=\varepsilon(p_i)=-1$ for all i, $\varepsilon(q_i)=1$ for all i, where p, p_i, and q_i do not divide $\mathfrak{f}_1\mathfrak{f}_2$. We write $\mathfrak{f}_p$ for a prime dividing $\mathfrak{f}_1\mathfrak{f}_2$ with $\varepsilon(\mathfrak{f}_p)=-1$, and $\mathfrak{f}_q$ for a prime dividing $\mathfrak{f}_1\mathfrak{f}_2$ with $\varepsilon(\mathfrak{f}_q)=1$. (Note that the primes l, p, p_i, q_i, $\mathfrak{f}_p$, and $\mathfrak{f}_q$ are all distinct, and that p, p_i, q_i, $\mathfrak{f}_p$, and $\mathfrak{f}_q$ need to be restricted so that $\varepsilon(p)$, $\varepsilon(p_i)$, $\varepsilon(q_i)$, $\varepsilon(\mathfrak{f}_p)$, and $\varepsilon(\mathfrak{f}_q)$ are well-defined, as above). Then (for $n, r_i\geq 1$; $a, a_i, b_i\geq 0$) we define

$$F(m)=\begin{cases} p^{2^t(a+1)(b_1+1)\cdots(b_s+1)} & \text{if}\quad m=p^{2a+1}\mathfrak{f}_{q_1}^{r_1}\cdots\mathfrak{f}_{q_t}^{r_t}p_1^{2a_1}\cdots p_k^{2a_k}q_1^{b_1}\cdots q_s^{b_s}\,,\\ \mathfrak{f}_p^{2^t(b_1+1)\cdots(b_s+1)} & \text{if}\quad m=\mathfrak{f}_p^n\mathfrak{f}_{q_1}^{r_1}\cdots\mathfrak{f}_{q_t}^{r_t}p_1^{2a_1}\cdots p_k^{2a_k}q_1^{b_1}\cdots q_s^{b_s}\,,\\ 1 & \text{otherwise}\,. \end{cases}$$

Conjecture 3.5. With the definition of $F(m)$ as above, the Gross–Zagier formula holds for any two imaginary quadratic discriminants d_1 and d_2 such that $(d_1, d_2)=1$.

Example 3.6. As above, we give two computations of $|J(d_1, d_2)^2|$, based on the conjecture in this case. Again, the conjecture has been checked for $-200\leq d_1, d_2\leq -3$, and the relevant factors (those which illustrate the conjecture) have been set in boldface.

(a) $$\begin{aligned}|J(-7,-108)^2|=&\boldsymbol{F(3^3 7^1)}[\boldsymbol{F(2^2 47^1)}F(5^1 37^1)\boldsymbol{F(2^2 3^2 5^1)}F(173^1)\cdot\\ &\boldsymbol{F(2^2 42^1)}\boldsymbol{F(3^2 17^1)}\boldsymbol{F(2^5 5^1 7^1)}F(5^3)\boldsymbol{F(2^2 3^3)}\cdot\end{aligned}$$

$$
\begin{aligned}
&F(89^1)\boldsymbol{F}(\mathbf{2^2 17^1})\boldsymbol{F}(\mathbf{3^2 5^1})\boldsymbol{F}(\mathbf{2^2 5^1})]^2\\
&=\mathbf{3^2}[\mathbf{47^2}5^2\mathbf{1^1}173^1\mathbf{41^2 1^1 5^4}5^2\mathbf{3^2}89^1\mathbf{17^2 1^1 5^2}]^2\\
&=3^6 5^{20} 17^4 41^4 47^4 89^2 173^2
\end{aligned}
$$

$(\mathfrak{f}_p=3;\ \mathfrak{f}_q=2;\ p_i=5,\ 17,\ 41,\ 47;\ q_i=7)$

(b)
$$
\begin{aligned}
|J(-16,-27)^2| &= \boldsymbol{F}(\mathbf{2^2 3^3})[F(107^1)\boldsymbol{F}(\mathbf{2^3 13^1})\boldsymbol{F}(\mathbf{3^2 11^1})\boldsymbol{F}(\mathbf{2^2 23^1})\cdot\\
&\quad F(83^1)\boldsymbol{F}(\mathbf{2^3 3^2})F(59^1)\boldsymbol{F}(\mathbf{2^2 11^1})\boldsymbol{F}(\mathbf{3^3})\mathrm{F}(2^3)]^2\\
&=\mathbf{1^1}[107^1\mathbf{2^2 1^1 1^1}83^1\mathbf{1^1}59^1\mathbf{1^1 3^1 2^1}]^2\\
&=2^6 3^2 59^2 83^2 107^2
\end{aligned}
$$

$(\mathfrak{f}_p=2,\ 3;\ p_i=11,\ 23;\ q_i=13)$

3.3. Full conjecture. We now combine the above two cases; that is, we allow d_1 and d_2 to be non-fundamental and have a non-trivial common divisor. We continue to assume that if d_1 and d_2 have a common divisor, then it is a prime power, l^e. If $\mathfrak{f}_i$ is the conductor of d_i, then we also assume that $(\mathfrak{f}_1\mathfrak{f}_2, l)=1$. (Examples of this are represented by the last eleven entries of Table 1.)

In certain special cases, to be specified below, it turns out that extending the definition of $F(m)$ is not enough. In these cases an extra factor occurs in $J(d_1, d_2)^2$. Fortunately, this factor has a (conjectural) closed formula, suggested by considering the definition of $J(d_1, d_2)$.

DEFINITION 3.7. Let $\mathfrak{f}_i$ be the conductor of d_i. We assume that (d_1, d_2) is a power of a prime l, where $(\mathfrak{f}_1\mathfrak{f}_2, l)=1$.

Given m, we define $\chi=\chi(l,m)=1$ if $(l,m)>1$; otherwise let $\chi=0$. Suppose $\varepsilon(p)=\varepsilon(p_i)=-1$ for all i, and $\varepsilon(q_i)=1$ for all i, where p, p_i and q_i do not divide $\mathfrak{f}_1\mathfrak{f}_2$. We write $\mathfrak{f}_p$ for a prime dividing $\mathfrak{f}_1\mathfrak{f}_2$ with $\varepsilon(\mathfrak{f}_p)=-1$, and $\mathfrak{f}_q$ for a prime dividing $\mathfrak{f}_1\mathfrak{f}_2$ with $\varepsilon(\mathfrak{f}_q)=1$. (Note that the primes l, p, p_i, q_i, $\mathfrak{f}_p$, and $\mathfrak{f}_q$ are all distinct, and that p, p_i, q_i, $\mathfrak{f}_p$, and $\mathfrak{f}_q$ need to be restricted so that $\varepsilon(p)$, $\varepsilon(p_i)$, $\varepsilon(q_i)$, $\varepsilon(\mathfrak{f}_p)$, and $\varepsilon(\mathfrak{f}_q)$ are well-defined, as above). Then (for n, $r_i\geq 1$; a, a_i, $b_i\geq 0$) we define

$$
F(m)=\begin{cases}
l^{e(2^t)(b_1+1)\cdots(b_s+1)} & \text{if } m=l^e\mathfrak{f}_{q_1}^{r_1}\cdots\mathfrak{f}_{q_t}^{r_t}p_1^{2a_1}\cdots p_k^{2a_k}q_1^{b_1}\cdots q_s^{b_s}\ (e\geq 1)\,,\\
p^{2\chi+t(a+1)(b_1+1)\cdots(b_s+1)} & \text{if } m=l^e p^{2a+1}\mathfrak{f}_{q_1}^{r_1}\cdots\mathfrak{f}_{q_t}^{r_t}p_1^{2a_1}\cdots p_k^{2a_k}q_1^{b_1}\cdots q_s^{b_s}\ (e\geq 0)\,,\\
\mathfrak{f}_p^{2^t(b_1+1)\cdots(b_s+1)} & \text{if } m=\mathfrak{f}_p^n\mathfrak{f}_{q_1}^{r_1}\cdots\mathfrak{f}_{q_t}^{r_t}p_1^{2a_1}\cdots p_k^{2a_k}q_1^{b_1}\cdots q_s^{b_s}\,,\\
\mathfrak{f}_p^{2\chi+t(b_1+1)\cdots(b_s+1)} & \text{if } m=l^e\mathfrak{f}_p^{2n+1}\mathfrak{f}_{q_1}^{r_1}\cdots\mathfrak{f}_{q_t}^{r_t}p_1^{2a_1}\cdots p_k^{2a_k}q_1^{b_1}\cdots q_s^{b_s}\ (e\geq 0)\,,\\
1 & \text{otherwise}\,.
\end{cases}
$$

Further, if $d_2=\mathfrak{f}_2^2 d_1$, where d_1 is a fundamental discriminant and $\mathfrak{f}_2$ is the power of a prime $p_{\mathfrak{f}}$, then we define

$$\delta=p_{\mathfrak{f}}^{8h_1/w_1w_2}\,.$$

(Otherwise, let $\delta=1$.)

CONJECTURE 3.8. With the definition of $F(m)$ and δ as above, the following modified Gross–Zagier formula holds for any imaginary quadratic discriminants d_1 and d_2 such that (d_1, d_2) is a power of a prime l, where $(l, \mathfrak{f}_1\mathfrak{f}_2)=1$:

$$J(d_1, d_2)^2 = \pm\delta \prod_{\substack{x^2<d_1d_2\\ x^2\equiv d_1d_2 \pmod 4}} F\left(\frac{d_1d_2-x^2}{4}\right).$$

EXAMPLE 3.9. The full conjecture has been checked with GP/PARI for $-200\leq d_1, d_2\leq -3$. We now give two computations of $|J(d_1, d_2)^2|$, based on the full conjecture. The factors not covered by Gross–Zagier's definition of $F(m)$ or the definitions in the last two cases are set in boldface. Note that example (a) illustrates the factor of δ. In this particular example, δ is a quadratic non-residue (that is, $\varepsilon(\delta)=-1$), but this is not always the case; in fact, if $d_1=-3$, then δ is not necessarily an integer. (Note, however, that the need for δ is relatively rare.)

(a)
$$\begin{aligned}|J(-4,-36)^2| &= \boldsymbol{\delta}\mathbf{F(2^2 3^2)}[F(5^1 7^1)F(2^5)F(3^3)F(2^2 5^1)F(11^1)]^2\\ &= \mathbf{3\cdot 1^1}[7^2 2^5 3^3 2^4 11^1]^2\\ &= 2^{18}3^3 7^4 11^2\end{aligned}$$
$(l=2;\ \mathfrak{f}_p=3;\ h_1=1;\ w_1=4;\ w_2=2)$

(b)
$$\begin{aligned}|J(-12,-147)^2| &= \mathbf{F(3^2 7^2)}[F(2^3 5^1 11^1)F(19^1 23^1)\mathbf{F(2^4 3^3)}\,\cdot\\ &\quad F(5^2 17^1)F(2^5 13^1)F(3^4 5^1)F(2^3 7^2)\,\cdot\\ &\quad F(13^1 29^1)\mathbf{F(2^3 3^2 5^1)}F(11^1 31^1)F(2^6 5^1)\,\cdot\\ &\quad F(3^3 11^1)F(2^4 17^1)F(5^1 7^2)\mathbf{F(2^3 3^3)}\,\cdot\\ &\quad F(5^1 37^1)F(2^3 19^1)F(3^2 13^1)F(2^4 5^1)F(41^1)]^2\\ &= \mathbf{3^4}[1^1 23^2 \mathbf{1^1} 17^1 2^2 5^2 2^2 29^2 \mathbf{1^1} 11^2 1^1 11^2 1^1 5^2 \mathbf{2^2}\,\cdot\\ &\quad 5^2 2^2 3^4 1^1 41^1]^2\\ &= 2^{16}3^{12}5^{12}11^8 17^2 23^4 29^4 41^2\end{aligned}$$
$(l=3;\ \mathfrak{f}_p=2;\ \mathfrak{f}_q=7;\ p_i=5)$

4. Corollaries and applications of the conjectural formula.

The motivation for our approach to this extension of the Gross–Zagier formula was Corollary 2.3; one then might ask if this corollary holds under the new hypotheses. Experimentally, the answer appears to be yes; for example, see Table 1. In fact, as M. Kaneko has pointed out, it has been established as a theorem (independently of any Gross–Zagier type formula), for any two imaginary quadratic discriminants.

THEOREM 4.1. *Let d_1 and d_2 be imaginary quadratic discriminants. If l is a prime dividing $J(d_1, d_2)^2$, then*

(a) $\left(\frac{d_1}{l}\right)\neq 1$ *and* $\left(\frac{d_2}{l}\right)\neq 1$,

(b) *l divides a positive integer of the form* $(d_1d_2-x^2)/4$,

(c) $l\leq d_1d_2/4$, *and further,*

(i) *if* $d_1d_2\equiv 1 \pmod 8$, *then* $l<d_1d_2/8$, *and*

(ii) *if* $d_1\equiv d_2\equiv 5 \pmod 8$, *then* $l<d_1d_2/16$.

Proof. Part (a) is due to M. Deuring [5]; this fact was made explicit by N. Elkies [9]. Part (b) was proved by M. Kaneko [12, Theorem 2], and part (c) follows from part (b). □

The theorem would also be a fairly easy corollary of the conjectural formula; the proof of Corollary 2.3, following hints given in [4, Exercise 13.17], is independent of the assumptions about d_1 and d_2. Thus the theorem provides further justification for our approach of using the original Gross–Zagier formula; indeed, it also suggests that a similar approach should yield a formula for $J(d_1, d_2)^2$ when d_1 and d_2 are any two imaginary quadratic discriminants. (Recall that the conditions on d_1 and d_2 under discussion here account for about 75 percent of possible discriminants.)

Perhaps more significant, it is worth noting that at least one of the corollaries which have applications for the computation of class polynomials (formulated by Kaltofen–Yui [11] and mentioned at the end of Section 2) also follows from our conjectural formula. (Again, however, we need to omit the few cases involving a non-trivial δ.)

Conjecture 4.2. Let τ_1, τ_2 be imaginary quadratic integers belonging to two distinct imaginary quadratic fields with discriminants $d_1\equiv d_2\equiv 1 \pmod 4$, where $(d_1, d_2)=l^e$ and l does not divide the product of the conductors of d_1 and d_2. Assume further that d_1 and d_2 are not of the form $d_2=\mathfrak{f}_2^2 d_1$, where d_1 is a fundamental discriminant and $\mathfrak{f}_2$ (the conductor of d_2) is a power of a prime. Then

(a)
$$|J(d_1, d_2)|=\left[\prod_{\substack{0<x<\sqrt{d_1d_2}\\ x\text{ odd}}} F\left(\frac{d_1d_2-x^2}{4}\right)\right]^{w_1w_2/4}.$$

(b) If $H_d(x)$ is the class polynomial of $\mathcal{O}_d$, an imaginary quadratic order such that $d\equiv 1 \pmod 4$, then
$$H_d(0)=\pm\left[\prod_{\substack{0<x<\sqrt{-3d}\\ x\text{ odd}}} F\left(\frac{-3d-x^2}{4}\right)\right]^3.$$
In particular, $|H_d(0)|$ is a perfect cube.

As mentioned at the end of Section 2, this conjecture is useful in verifying the accuracy of computations of class polynomials. It also seems likely that a version of the corollary giving an expression for the discriminant of a class polyonimial (see

[11]) holds in the generalized case, but we have not investigated this.

Thus if the conjectural formula is correct, this would provide a method of verifying computations of class polynomials for a larger class of discriminants than the one provided for by the original Gross–Zagier formula (and these computations, in turn, have applications in the construction of class fields and in elliptic curve primality proving, as mentioned above).

Perhaps more interesting is the fact that the formula may be helpful in the consideration of "higher level" cases. The Gross–Zagier formula arises from a study of singular moduli of level one; the elliptic modular j-function is invariant under the action of $\Gamma=\Gamma_0(1)=\mathrm{PSL}_2(\mathbf{Z})$. Yui–Zagier [13] have considered class polynomials arising from the Weber function $\mathfrak{f}(\tau)$, rather than the j-invariant; $\mathfrak{f}^{24}(\tau)$ is an invariant for $\Gamma_0(2)$. These polynomials are considerably simpler than the class polynomials corresponding to level one. Yui–Zagier have considered the singular moduli of the 24th roots of this invariant, and have obtained a conjectural Gross–Zagier type formula, which turns out to be considerably more complicated than the Gross–Zagier formula for level one. Yui–Zagier's conjectural formula for level two, however, uses the Gross–Zagier formula for level one, so it may be possible to extend the Yui–Zagier formula to a larger class of discriminants by using the conjectural formula presented here.

5. Possible approaches to a proof.

Ideally, to prove the conjectural formula, we would like to be able to follow the proof of the original Gross–Zagier formula, changing details as necessary. While it may be possible to use the overall structure of the original proof, there appear to be some obstacles to simply mimicking it, which we outline below.

The fact that the expression for $F(m)$ is divided into five cases, involving five types of primes $(l, \mathfrak{f}_p, \mathfrak{f}_q, p, q)$, rather than the original three and two (p, q), respectively, causes immediate difficulties. At best, in a proof of this conjecture, each type of prime would need to be treated separately; additional theory would certainly be needed. It may also be problematic that $F(m)$ is not well-defined in terms of order, with respect to $\mathfrak{f}_p$ or $\mathfrak{f}_q$ (for example, $F(\mathfrak{f}_p^5)=F(\mathfrak{f}_p^3)=\mathfrak{f}_p$).

It is not clear how to treat the case of non-trivial common divisors of d_1 and d_2, since several arguments in the original proof require that assumption; the methods of Dorman [7] in extending the original proof to composite d_1 may shed some light on this.

To prove the formula for non-fundamental discriminants, it seems clear that one would need to consider non-maximal orders. In the original proof, Gross–Zagier use the Hilbert class field of $K=\mathbf{Q}(\sqrt{d_1})$. It may be possible to use the theory of ring class fields; recall that the ring class field of a quadratic order of discriminant d is merely the Hilbert class field of $\mathbf{Q}(\sqrt{d})$ when d is fundamental. We have not investigated this approach in any detail, but one would lose the convenient property, used in the original proof, that the Hilbert class field of K is the maximal, unramified extension of K.

However, if one were to try to follow the original algebraic proof in proving the conjecture, using the ring class field would appear to be the correct approach. A potential tool for such an approach has been suggested by R. Murty; in a paper by D. Zagier [14], an analogue of the Legendre symbol for non-fundamental discriminants is described.

ACKNOWLEDGEMENTS. This paper is an adaptation of a portion of my master's thesis. It is a pleasure to thank Prof. N. Yui, my supervisor, not only for her help and encouragement during my studies at Queen's University, but also for carefully reading and commenting on drafts of this paper. I would also like to thank Prof. R. Murty, Prof. M. Kaneko, and the referee for their helpful comments and corrections.

References

[1] A. O. L. ATKIN and F. MORAIN, Elliptic curves and primality proving, Math. Comp. **61** (1993), 29–68.

[2] C. BATUT, D. BERNARDI, H. COHEN and M. OLIVER, *GP/PARI*, Version 1.38, 1993, available by anonymous ftp from ftp.u-bordeaux.fr in directory /pub/Local/Math/Software/pari. (UNIX implementation, run on Sparc 20 using SunOS 5.5.)

[3] A. BOREL, S. CHOWLA, C. S. HERZ, K. IWASAWA and J-P. SERRE, *Seminar on Complex Multiplication*, Lecture Notes in Math. **21** (1966), Springer.

[4] D. A. COX, *Primes of the Form* x^2+ny^2, Wiley (1989).

[5] M. DEURING, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

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

[7] D. R. DORMAN, Special values of the elliptic modular function and factorization formulae, J. Reine Angew. Math. **383** (1988), 207–220.

[8] D. R. DORMAN, Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves, *Number Theory: Proceedings of the International Number Theory Conference held at Université Laval in 1987* (J.-M. de Koninck and C. Levesque, eds.), Walter de Gruyter (1989), 108–116.

[9] N. D. ELKIES, The existence of infinitely many supersingular primes for every elliptic curve over **Q**, Invent. Math. **89** (1987), 561–567.

[10] B. H. GROSS and D. B. ZAGIER, On singular moduli, J. Reine Angew. Math. **355** (1985), 191–220.

[11] E. KALTOFEN and N. YUI, Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction, *Number Theory, New York Seminar, 1989–1990* (D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson, eds.), Springer (1991), 149–202.

[12] M. KANEKO, Supersingular j-invariants as singular moduli mod p, Osaka J. Math. **26** (1989), 849–855.

[13] N. YUI and D. ZAGIER, On the singular values of Weber modular functions, Math. Comp. **66** (1997), 1645–1662.

[14] D. ZAGIER, Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields, *Modular Functions of One Variable VI* (Proc. Second Internat. Conf. Univ. Bonn, 1976), Lecture Notes in Math. **627** (J.-P. Serre and D. Zagier, eds.), Springer (1977), 105–169.

Present Address:
505 CLARENCE AVE. S., APT. 304, SASKATOON, SK, S7H 2C8, CANADA.
e-mail: tim.hutchinson@usask.ca