D. V. Chudnovsky G. V. Chudnovsky
H. Cohn M. B. Nathanson
Editors

Number Theory

New York Seminar 1989-1990

With 14 Figures

Springer-Verlag
New York Berlin Heidelberg London
Paris Tokyo Hong Kong Barcelona

8

Explicit Construction of the Hilbert Class Fields of Imaginary Quadratic Fields by Integer Lattice Reduction*

Erich Kaltofen[1] and Noriko Yui[2]

Abstract

Motivated by a constructive realization of generalized dihedral groups as Galois groups over $\mathbb{Q}$ and by Atkin's primality test, we present an explicit construction of the Hilbert class fields (ring class fields) of imaginary quadratic fields (orders). This is done by first evaluating the singular moduli of level one for an imaginary quadratic order, and then constructing the "genuine" (i.e., level one) class equation. The equation thus obtained has integer coefficients of astronomical size, and this phenomenon leads us to the construction of the "reduced" class equations, i.e., the class equations of the singular moduli of higher levels. These, for certain levels, turn out to define the same Hilbert class field (ring class field) as the level one class equation, and to have coefficients of small size (e.g., seven digits). The construction of the "reduced" class equations was carried out on MACSYMA, using a refinement of the integer lattice reduction algorithm of Lenstra-Lenstra-Lavász, implemented on the Symbolics 3670 at Rensselaer Polytechnic Institute.

*Erich Kaltofen was partially supported by the NSF Grant No. CCR-87-05363 and by an IBM Faculty Development Award. Noriko Yui was partially supported by the NSERC Grants No. A8566 and No. A9451, and by an Initiation Grant at Queen's University.

[1]Department of Computer Science, Rensselaer Polytechnic Institute, Troy, NY 12180, USA.
[2] Department of Mathematics, Queen's University, Kingston, Ontario, K7L3N6 Canada.

AMS(MOS)(1980) Mathematics Subject Classifications (1985) Revision. Firstly:11R37, 11Y16; Secondly : 12-04, 12F10. *Keywords*: Hilbert class fields, Ring class fields, Class equations, Singular moduli, Weber's class invariants, Generalized dihedral groups, Atkin's primality test, Integer lattice reduction algorithm.

I. INTRODUCTION

I.1 Backgrounds and the main results.

Singular moduli (class invariants) and class equations have been extensively studied over the years by many mathematicians.

In this paper, we shall discuss the explicit construction of the class equations (the defining equations of the Hilbert class fields (the ring class fields)) of imaginary quadratic fields (orders) over $\mathbb{Q}$. The "genuine" class equations having the singular moduli of the elliptic modular j-invariant as roots—the class equations of level one—have integer coefficients of astronomical size, although their constant terms and discriminants are highly divisible numbers with small prime factors (Duering [D1] and Gross-Zagier [G-Z1]; see Theorem (A2.1) below).

The main theme of this paper is to present an algorithm for the construction of the "reduced" class equations which have very small coefficients and define the same Hilbert class fields (ring class fields) over $\mathbb{Q}$ as the "genuine" ones, using a refinement of the integer lattice reduction algorithm (the L^3-algorithm), implemented with MACSYMA on the Symbolics 3670.

Let τ be a imaginary quadratic number which is a root of the quadratic equation $az^2 + bz + c = 0$ with $a, b, c \in \mathbb{Z}$. We assume that $Im\ \tau > 0$. We define the discriminant of τ to be $d = \mathrm{disc}(\tau) = b^2 = 4ac < 0$. Let $K = \mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{d})$. Let $\mathcal{O} = \mathbb{Z}\left[\frac{b+\sqrt{d}}{2}\right]$ be an imaginary quadratic order of K of class number $h(d) =: h$. Let $j(z)$ be the elliptic modular j-invariant. Then the singular modulus $j(\tau)$ for $\tau \in \mathcal{O}$ is an algebraic integer of degree h over $\mathbb{Q}$, called a class invariant of $\mathcal{O}$. The minimal polynomial, H_d, of $j(\tau)$ is know as the class equation of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, which we shall call the "genuine" class equation or the class equation of level one. The splitting field of H_d over $\mathbb{Q}$ is the field $K(j(\tau))$ which is the ring class field of conductor f over $K = \mathbb{Q}(\sqrt{d})$, where $d = d_K f^2$ with d_K a fundamental discriminant of K. By the Artin reciprocity theorem, the Galois group $\mathrm{Gal}(H_d/\mathbb{Q})$ is isomorphic to the generalized dihedral group $\mathrm{Pic}(\mathcal{O}) \rtimes C_2$ where $\mathrm{Pic}(\mathcal{O})$ denotes the ideal class group of $\mathcal{O}$.

Weber [W] considered the explicit construction of the field $K(j(\tau)) = \mathbb{Q}(\tau, j(\tau))$, $\tau \in \mathcal{O}$ using other modular functions (of higher level) $f(z)$. When $f(\tau)$ does lie in $K(j(\tau)) = \mathbb{Q}(\tau, j(\tau))$, $f(\tau)$ is also called a class invariant of $\mathcal{O}$, and its minimal polynomial, h_d, over $\mathbb{Q}$, is called the "reduced" class equation or the class equation of higher level. The polynomial h_d has small integer coefficients and (from its construction) defines the same ring class field as H_d over $\mathbb{Q}$.

Weber [W] initiated the construction of the reduced class equations of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$ with $d \equiv 1$ or $5 \pmod 8$ and carried out computations for 65 values of d; the largest class number treated by Weber was 7. Berwick [B] computed the singular moduli of degree 2 and 3. However, it was Watson who

first discussed systematically the explicit construction of class invariants and reduced class equations, in his series of papers [W1, W2, W3, W4]. Watson's algorithm was based on finding all the roots of the class equations that were to be constructed. For instance, for $d \equiv 1 (\text{mod } 8)$ (with $|d|$ prime), the Watson class equation of degree h had the single real root, $f(\sqrt{d})/\sqrt{2}$, where $f(z)$ was a Weber function (see B1.1)), and Watson described the complex roots only up to cubic conjugation. Thus, Watson had to choose from three candidates for each of the $h-1$ complex roots. The "right" choice was tested for whether the $h-1$ complex roots and the single real root added up to approximately a rational integer. However, this trial and error method required 3^{h-1} test sums. And, in fact, Watson stopped his construction at $h = 19$.

There are other methods for constructing class equations of imaginary quadratic orders. One of the methods is based on function theoretic arguments and utilizes the Schläfli modular equations. This approach was used by Schläfli, Weber [W] (§73-75), Hanna [H], and by others. Hanna [H] tabulated all of the known Schläfli modular equations, and constructed class equations of imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d < 0$, with discriminants $d > -239$. Construction of the class fields by arithmetic means was also carried out by Herz for unramified cyclic extensions of small degree, e.g., 4, 8, ... , in [B-C-H-I-S].

Recently, Cox [Cx] has written a book in which he discusses, among other things, computation of the class equations of level one, in the framework of primes of the form $x^2 + ny^2$ $(n > 0)$ (see (I.3) below).

In this paper, we take up the task of explicit construction of the "reduced" class equations of imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d = d_K f^2 < 0$ with $3 \nmid d$, from where Watson left off, by presenting an algorithm based on integer lattice reductions. The paper consists of two parts, Part A and Part B. Part A exposes the construction of the "genuine" (level one) class equations H_d by three different methods. The construction of the polynomials H_d is illustrated for the maximal order $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{-719})$ with $h = 31$. Part B is concerned with the construction of the "reduced" class equations of imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$. Geometrical aspects of the "reduced" class equations may be explained as follows. The elliptic modular function $j(z)$ gives a complex analytic isomorphism (the uniformizer) between the compact Riemann surfaces

$$j\ :\ \mathfrak{H}^*/\Gamma \longrightarrow \mathbb{P}^1(\mathbb{C}), \qquad z \longrightarrow j(z),$$

of genus zero, where

$$\mathfrak{H} = \{z \in \mathbb{C} | Im\ z > 0\},$$
$$\Gamma = PSL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\} / \pm I_2$$

and

$$\mathfrak{H}^*/\Gamma = \mathfrak{H}/\Gamma \cup \mathbb{P}^1(\mathbb{Q})\ .$$

Take a suitable subgroup G of Γ of finite index such that the associated compact Riemann surface $\mathfrak{H}^*/G = \mathfrak{H}/G \cup \{\text{cusps of } G\}$ is again of genus zero (e.g., $G = \Gamma_0(2^i) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | c \equiv 0 \pmod{2^i} \right\}$ for $i = 0, 1 - 4$). Then there is again a complex analytic isomorphism

$$u_G : \mathfrak{H}^*/G \longrightarrow \mathbb{P}^1(\mathbb{C}) \ (u_\Gamma = j)$$

which we shall call the uniformizer of higher level. Now let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d < 0, d \not\equiv 5 \pmod 8$ and $3 \nmid d$ be an imaginary quadratic order of class number h. Then the singular modulus $u_G(\tau)$ for $\tau \in \mathcal{O} \cap \mathcal{F}_G$ where $\mathcal{F}_G$ is a fundamental domain for G, is an algebraic integer of degree h over $\mathbb{Q}$, and the minimal polynomial of $u_G(\tau)$ defines the field $K(u_G(\tau))$. If $u_G(\tau) \in K(j(\tau))$, then $K(u_G(\tau))$ is isomorphic to the ring class field $K(j(\tau))$ of $\mathcal{O}$. This gives rise to the "reduced" class equation for $\mathcal{O}$. The "reduced" class equation is not always equivalent to the "genuine class" equation under Tschirnhausen transformation. Note, however, that if $\mathcal{O} \subset K = \mathbb{Q}\sqrt{d},\ d < 0$, has *odd* prime class number h, then the reduced class equation is Tschirnhausen equivalent to the genuine one (cf. (I.2.5)).

The construction of the "reduced" class equation is discussed for an arbitrary imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ using an appropriate class invariant. Put $D = d/4$ if $d \equiv 0 \pmod 4$ and $D = d$ if $d \equiv 1 \pmod 4$. Assume that D is square-free. We use the following class invariants (which differ slightly from Weber's class invariants): $f(\sqrt{D})/\sqrt{2}$ if $D \equiv 1 \pmod 8$; $f_1(\sqrt{D})^2/\sqrt{2}$ if $D \equiv 2, 6 \pmod 8$; $f(\sqrt{D})^4$ if $D \equiv 3 \pmod 8$; $f(\sqrt{D})$ if $D \equiv 5 \pmod 8$ and $f(\sqrt{D})/\sqrt{2}$ if $D \equiv 7 \pmod 8$. An algorithm for the construction of the "reduced" class equations is described in B3. Our algorithm is "generic" in the sense that the reduced class equation can be constructed for arbitrary imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ once an appropriate class invariant is provided. The idea is to construct the minimal polynomial of a class invariant (e.g., a real singular modulus) of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ using a refined integer lattice reduction algorithm. We are able to construct the "reduced" class equation up to class number $h = 43$ with this method.

Analysis of the reduced class equation is carried out in B4. The constant term of the reduced class equation is either $(-1)^h,\ \pm 1,\ \pm 2^h$ or $(-2)^h$, and no prime divisors of the discriminant can split completely in K. It is expected that there is a formula of Gross-Zagier type for the discriminant of the reduced class equations.

We tabulate in B5 the "reduced" class equation in several examples.

I.2 A motivation: The construction of integral polynomials with generalized dihedral Galois groups.

Our motivation for the study of singular moduli and class equations is impelled from constructing "nice" integral polynomials with a given finite group as Galois group. The group we wish to consider here is a

generalized dihedral group, which is a semi-direct product $G \rtimes C_2$ where G is a finite abelian group on which $C_2 = \{1, \tau\}$ acts via $\sigma^\tau = \sigma^{-1}$. When G is the cyclic group C_n of order n, $C_n \rtimes C_2$ is the usual dihedral group D_n - the group of symmetries of a regular n-gon. These groups are solvable, and hence are realizable as Galois groups over the field $\mathbb{Q}$ of rational numbers (Shafarevich). The problem is to construct a "nice" integral polynomial with a generalized dihedral group as Galois group.

Given a monic integral polynomial of degree n (odd), there are effective algorithms which determine if its Galois group over $\mathbb{Q}$ is the dihedral group D_n. Jensen and Yui [J-Y] (Thm. II.1.2) have found a characterization theorem for polynomials with dihedral Galois group D_p of prime degree p. This has been generalized by Williamson [Wi] to odd degree polynomials with dihedral Galois group D_n.

(I.2.1) Proposition. *Let f(x) be a monic irreducible polynomial of odd degree n over $\mathbb{Z}$. Let*

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{C}[x]$$

and let

$$R(x_1 - x_2, f)(x) =: \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (x - (\alpha_i - \alpha_j)) \in \mathbb{Z}[x]$$

be the resolvent polynomial. Then the splitting field of f(x) over $\mathbb{Q}$ has degree n, if and only if $R(x_1 - x_2, f)(x)$ factors into irreducible polynomials of degree n over $\mathbb{Q}$. In this situation, the necessary and sufficient conditions for Gal $(f) \cong D_n$ are

(i) *The monic irreducible factors of $R(x_1 - x_2, f)(x)$ are even polynomials and the field $K = \mathbb{Q}(\sqrt{-c})$ where c is the constant coefficient of some monic irreducible factor of $R(x_1 - x_2, f)(x)$ is quadratic over $\mathbb{Q}$ and is independent of the choice of the irreducible factor,*

(ii) *The polynomial f(x) is irreducible over K and the splitting field of f(x) over K has degree n, and*

(iii) *For some prime $p \nmid disc(f)$ which remains inert in K, $f(x)$ (mod p) factors into a linear polynomial times a product of (n-1)/2 irreducible quadratic polynomials.*

Before going into constructing polynomials with generalized dihedral Galois groups we need to settle the following question.

(I.2.2) Question. *When do two integral polynomials of degree n with the same Galois group become equivalent under Tschirnhausen transformation?*

We first observe the following general facts concerning Tschirnhausen transformation.

(I.2.3) Proposition. *Let f(x) and g(x) be irreducible polynomials of degree $n > 1$ over $\mathbb{Q}$. Let $\{\alpha_i | i = 1, \cdots, n\}$ and $\{\beta_j | j = 1, \cdots, n\}$ be the roots of f(x) and g(x) in $\mathbb{C}$, respectively. Then the following assertions hold true.*

(a) *f(x) and g(x) are equivalent under Tschirnhausen transformation, if and only if $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\beta_j)$ for some i,j.*

(b) *If f(x) and g(x) are equivalent under Tschirnhausen transformation, then f(x) and g(x) have the same splitting field over $\mathbb{Q}$.*

The converse of the assertion (b) in Proposition (I.2.3) is not always true, that is, even if $f(x)$ and $g(x)$ have the same splitting field over $\mathbb{Q}$, they are not necessarily equivalent under Tschirnhausen transformation. However, this holds true in the following special case.

(I.2.4) Proposition. *(cf. Bruen-Jensen-Yui [B-J-Y], Remark (I.2.6)). Let f(x) and g(x) be irreducible polynomials of prime degree p over $\mathbb{Q}$. Then f(x) and g(x) are equivalent under Tschirnhausen transformation, if and only if they have the same splitting field over $\mathbb{Q}$ and a solvable Galois group.*

(I.2.5) Remarks. (a) The assertion of Proposition (I.2.4) is not true, for example, for a polynomial of prime degree p having a simple group as Galois group (e.g., PSL(2,7)).

(b) In order to construct integral polynomials with generalized dihedral Galois groups, we, at the moment, have to rely on singular moduli and on the construction of Hilbert class fields (ring class fields) of imaginary quadratic fields (orders). This construction, however, is not universal, that is, not all integral polynomials with generalized dihedral Galois groups can be obtained in this manner.

(c) There are other methods for constructing integral polynomials with dihedral Galois groups over $\mathbb{Q}$. For instance, Mestre [M] has utilized elliptic curves over $\mathbb{Q}$ with torsion points of order 5 (resp. 7) to realize D_5 (resp. D_7).

I.3 A motivation: The Goldwasser-Kilian-Atkin primality test.

Another motivation for constructing the "reduced" class equations stems from the Goldwasser-Kilian-Atkin primality test, discussed, for instance, by Lenstra-Lenstra [L-L] and Morain [Mo]. This primality test certifies large integers to be prime via an elliptic curve certificate as in the test by Goldwasser and Kilian ([G-K]).

Let $p > 1$ be an integer whose primality is to be tested. The test tries to choose an elliptic curve with complex multiplication by an imaginary quadratic order in order to have an efficient way of determining the number of points on the reduced elliptic curve over $\mathbb{Z}/p\mathbb{Z}$. The elliptic curve itself is then obtained

by factoring the "genuine" class equation that corresponds to the imaginary quadratic order (the ring of endomorphisms of the elliptic curve) used, modulo the number p. More precisely, Goldwasser-Kilian-Atkin's primality test is based on the following fact.

(I.3.1) Theorem. *Let $n > 0$ be an integer. Then there exists a monic irreducible integral polynomial $H_{-4n}(x)$—the genuine class equation of the imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ of discriminant $-4n$ and class number $h(-4n)$—such that if p is an odd prime dividing neither n nor the discriminant of H_{-4n}, then*

$$p = x^2 + ny^2 \text{ with } (x, y) \in \mathbb{Z}^2 \Longleftrightarrow \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and} \\ H_{-4n}(x) (\text{mod } p) \text{ has an integer solution.} \end{cases}$$

(I.3.2) The Atkin-Goldwasser Kilian primality test. *Let $p > 1$ be an integer whose primality is to be tested.*

Step 1. *Choose a fundamental discriminant $D < 0$ (among $-3, -4, \cdots$) such that p splits in the ring $\mathcal{O}_K$ of integers in $K = \mathbb{Q}(\sqrt{D})$, i.e., $p = \pi\ \pi'$ with $\pi,\ \pi' \in \mathcal{O}_K,\ \pi \neq \pi'$.*

Step 2. *For this π, compute $m = p + 1 - (\pi + \pi')$. If $m = kg$ with $k > 2$ and q a probably prime, go to Step 3; else go back to Step 1.*

Step 3. *Compute j as a root of the class equation $H_D(x)$ (mod p) or $H_{4D}(x)$ (mod p), and construct an elliptic curve E over $\mathbb{Z}/p\mathbb{Z}$ with j as its absolute invariant.*

Step 4. *For this elliptic curve E over $\mathbb{Z}/p\mathbb{Z}$ with $m = \#\ E(\mathbb{Z}/p\mathbb{Z})$, search for a rational point $P \in E(\mathbb{Z}/p\mathbb{Z})$ such that $mP = O_E$ but for the prime divisor q of m in Step 2, $\frac{m}{q}P \neq O_E$. If there is such a point P with $m > (\sqrt[4]{p} + 1)^2$, then p is prime; else p is composite.*

Step 5. *Test the primality of q in the same way.*

(I.3.3) Remark. The Goldwasser-Kilian-Atkin primality test has been implemented by Morain [Mo] (see also F. Morain: Atkin test: News from front (to appear in Proc. EUROCRYPT '89)). Morain has proved the primality of numbers with 100 to 728 digits using this algorithm.

Here we propose a modification of the Goldwasser-Kilian-Atkin primality test (see also Kaltofen-Valente-Yui [K-V-Y]). Our modification is to replace the "genuine" class equations $H_{4D}(x)$ by "reduced" class equations $h_{4D}(x)$, and, in fact, is based on the following fact.

(I.3.4) Theorem. *With the notations of Theorem (I.3.1) in force, let $h_{-4n}(x)$ be a "reduced" class equation of $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. Then*

$$p = x^2 + ny^2 \text{ with } (x, y) \in \mathbb{Z}^2 \Longleftrightarrow \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and} \\ h_{-4n}(x) \pmod{p} \text{ has an integer solution.} \end{cases}$$

(I.3.5) Remark. The above theorems (I.3.1) and (I.3.4) characterize primes p which are representable by the form $x^2 + ny^2$ $(n > 0)$. There are corresponding theorems that characterize primes which are representable by the form $x^2 + xy + \frac{1-D}{4}y^2$ with $(x, y) \in \mathbb{Z}^2$, where $D < 0,\ D \equiv 1 \pmod 4$ is a fundamental discriminant.

There exist the "genuine" class equation $H_D(x)$ or a "reduced" class equation $h_D(x)$, both of degree $h(D)$ such that if p is an odd prime dividing neither D nor the discriminant of $H_D(x)$, then

$$p = x^2 + xy + \frac{1-D}{4}\, y^2 \text{ with } (x, y) \in \mathbb{Z}^2$$

$$\iff \begin{cases} \left(\frac{D}{p}\right) = 1 \text{ and } H_D(x) \pmod p \text{ (or } h_D(x) \pmod p) \\ \text{has an integer solution.} \end{cases}$$

PART A

THE CONSTRUCTION OF THE "GENUINE" CLASS EQUATIONS*

Contents

* The announcement of this work in early stage was published in [K-Y1].

A1 Singular moduli of level one and the "genuine" class equations.

In this section, we shall recall the theoretical aspect of our computations on singular moduli of level one and class invariants. A full account of the classical theory can be found in Weber [W]. We also incorporate the recent results of Gross and Zagier [G-Z1] on singular moduli of level one, in particular, on the difference of two singular moduli, since their formulae become useful for our calculations.

(A1.1) Class numbers of imaginary quadratic orders. Let $ax^2 + bxy + cy^2,\ a, b, c\ \mathbb{Z},\ a > 0,\ GCD(a, b, c) = 1$ be a positive definite reduced primitive quadratic form of discriminant $d = b^2 - 4ac < 0$. Such a form is denoted by the symbol $[a, b, c]$. The integral matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with determinant 1 transforms $[a, b, c]$ by replacing x by $\alpha x + \beta y$ and y by $\gamma x + \delta y$ into another quadratic form $[a', b', c']$ of the same discriminant d, in which case two forms $[a, b, c]$ and $[a', b', c']$ are said to be equivalent. The class number $h(d) =: h$ is defined to be the number of such defined equivalence classes of positive definite reduced primitive quadratic forms of discriminant d. A unique reduced form for each equivalence class can be selected with

$$-a < b \le a < c \quad \text{or} \quad 0 \le b \le a = c.$$

These conditions imply that $|b| \le \sqrt{|d|/3}$, and hence the class number h is always finite.

Now let τ be a root of the quadratic equation $az^2 + bz + c = 0$ corresponding to a quadratic form $[a, b, c]$ of discriminant d. We define the discriminant of τ to be $disc(\tau) = d = b^2 - 4ac$. Put $K = \mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{d})$ and let d_K be the field discriminant of K, and put $\mathcal{O} = \mathbb{Z}[a\tau]$. Then $\mathcal{O}$ is a $\mathbb{Z}$-module of the form $\mathbb{Z}\left[\frac{-b+\sqrt{d}}{2}\right]$, and we call it an imaginary quadratic order of discriminant d. If $\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K+\sqrt{d}_K}{2}\right]$ denotes the ring of integers of K, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{-b+\sqrt{d}}{2}\right] = \mathbb{Z} + f\mathcal{O}_K$ for some integer $f \ge 1$ called the conductor of $\mathcal{O}$. $\mathcal{O}_K$ is called the maximal order of K. The form discriminant d and the field discriminant d_K are related by the identify $d = d_K f^2$. Note that d_K has no odd or even square factors except possibly 4. Put $D = d$ if $d \equiv 1 \pmod 4$ and $d/4$ if $d \equiv 0 \pmod 4$.

Now to each quadratic form $[a, b, c]$ of discriminant $d = b^2 - 4ac < 0$, we associate an ideal $\left(a, \frac{-b+\sqrt{d}}{2}\right)$ in $\mathcal{O}$. Two ideals $\mathcal{A}$ and $\mathcal{B}$ in $\mathcal{O}$ are said to be equivalent if there exist principal ideals (λ_1) and (λ_2) such that $\mathcal{A}(\lambda_1) = \mathcal{B}(\lambda_2)$. The equivalence classes of ideals in $\mathcal{O}$ are in 1-1 correspondence with the equivalence classes of quadratic forms $[a, b, c]$ of discriminant d. The ideal classes of $\mathcal{O}$ form a group, called the ideal class group, $\mathrm{Pic}(\mathcal{O})$, and the class number h therefore coincides with the order of this group.

Gauss' class number problem (find an effective algorithm for determining all imaginary quadratic orders with a given class number) has recently been solved by Goldfeld [G], and Gross and Zagier [G-Z2], independently. In particular, a complete list of imaginary quadratic orders of small class numbers are now at our disposal.

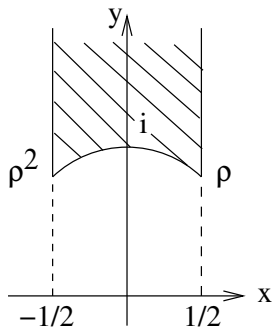

Figure 1: $i = \sqrt{-1}$, $\rho = (-1 + \sqrt{-3})/2$.

(A.1.2) Singular moduli of the elliptic modular j-invariant. Let $\Gamma = PSL_2(\mathbb{Z})$ denote the modular group:

$$PSL_2(\mathbb{Z}) \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\} / \pm I_2$$

where I_2 denotes the 2×2 identity matrix. Denote by $\mathfrak{H}$ the upper half complex plane:

$$\mathfrak{H} = \{z = x + iy \in \mathbb{C} \mid y > 0\} .$$

The modular group Γ acts on $\mathfrak{H}$ by a linear fractional transformation:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d} .$$

A fundamental domain, $\mathcal{F}$, of Γ in $\mathfrak{H}$, is defined to be a subset of $\mathfrak{H}$ such that every orbit of Γ has one element in $\mathcal{F}$, and two elements of $\mathcal{F}$ are in the same orbit if and only if they lie on the boundary of $\mathcal{F}$. Then $\mathcal{F}$ is given by the following set

$$\mathcal{F} = \{z = x + iy \in \mathfrak{H} \mid \ |z| \geq 1,\ |x| \leq \frac{1}{2}\} .$$

(Note that for any imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ with discriminant d, the class number h is equal to the number of roots of quadratic equations in $\mathcal{O} \cap \mathcal{F}$, corresponding to the positive definite primitive reduced quadratic forms of discriminant d.)

We now introduce the elliptic modular j-invariant. For each complex number z with non-negative imaginary part, let $q = e^{2\pi i z}$ and let

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \quad \sigma_3(n) = \sum_{\substack{t|n \\ t>0}} t^3 .$$

Furthermore, let

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n) = q^{\frac{1}{24}} \left(1 + \sum_{n=1}^{\infty} (-1)^n \left(q^{\frac{n(3n-1)}{2}} + q^{\frac{n(3n+1)}{2}} \right) \right) .$$

The j-invariant $j(z)$ is defined as

$$j(z) = \left(\frac{E_4(z)}{\eta(z)^8}\right)^3.$$

Put $\mathfrak{H}^*/\Gamma = \mathfrak{H}/\Gamma \cup \mathbb{P}^1(\mathbb{Q})$. Then the map

$$j \ : \ \mathfrak{H}^*/\Gamma \longrightarrow \mathbb{P}^1(\mathbb{C})$$

gives a complex analytic isomorphism of compact Riemann surfaces of genus zero, which we may call the uniformizer of level one. $j(z)$ satisfies the following properties:

(a) $j(\sqrt{d}) \in \mathbb{R}^+$ for $d < -1$; $j(\sqrt{-1}) = j(i) = 1728$, $j\left(\frac{\pm 1+\sqrt{d}}{2}\right) \in \mathbb{R}^-$ for $d < -3$ and $j\left(\frac{\pm 1+\sqrt{-3}}{2}\right) = 0$.

(b) $j(x+iy)$ and $j(-x+iy)$ are complex conjugates for any $\pm x+iy \in \mathcal{F} \cap \mathcal{O}$ where $\mathcal{O}$ is an imaginary quadratic order.

(c) $j(z)$ has the q-expansion:

$$\begin{aligned} j(q) &= \tfrac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \ \cdots \\ &= \tfrac{1}{q} + \sum_{n=0}^{\infty} a_n q^n \text{ with } a_n \in \mathbb{Z} \text{ for all n.} \end{aligned}$$

The values $j(\tau)$ for imaginary quadratic numbers $\tau \in \mathcal{O} \cap \mathcal{F}$, where $\mathcal{O}$ is an imaginary quadratic order of discriminant d, are known as singular moduli of level one. Let $\mathcal{A}_1, \cdots, \mathcal{A}_h$ be the ideal classes of the imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ of discriminant $d < 0$ and class number h. Then $j(\mathcal{A}_1), \cdots, j(\mathcal{A}_h)$ are all algebraic integers and any one of them is called a class invariant of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$. The class equation (or polynomial) of $\mathcal{O}$ is defined to be the polynomial

$$H_d(x) = (x - j(\mathcal{A}_1))(x - j(\mathcal{A}_2)) \ \cdots \ (x - j(\mathcal{A}_h)).$$

One of the most remarkable properties of singular moduli is culminated in the following theorem due to Weber, which we formulate in a most suitable form for our discussion (cf. Weber [W], Deuring [D2] or Cohn [C]).

(A1.3) Theorem. *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$ be an imaginary quadratic order of discriminant $d = d_k f^2$ and class number h. For each reduced positive primitive definite quadratic form $[a_k, b_k, c_k]$ of discriminant d, let $\tau_k = (-b_k + d)/2a_k$ be the root of the quadratic equation $a_k z^2 + b_k z + c_k = 0$, belonging to $\mathcal{F}$ for $k = 1, \cdots, h$. Then the class equation of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ defined by:*

$$H_d(x) = \prod_{k=1}^{h} (x - j(\tau_k))$$

is an integral irreducible polynomial of degree h.

Let L denote the field defined by $H_d(x)$ over $\mathbb{Q}$, and let N be its normal closure over $\mathbb{Q}$. Then N is a ring class field of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ whose Galois group over $\mathbb{Q}$ is canonically isomorphic to the generalized dihedral group, that is, the semi-direct product $Pic(\mathcal{O}) \rtimes C_2$ where $Pic(\mathcal{O})$ is the ideal class group of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$. If $f = 1$, N is the Hilbert class field of K, that is, N is the maximal unramified abelian extension of K.

(A1.4) Corollary. *Under the situation of Theorem (A1.3), assume, furthermore, that h is odd prime. Then N is the Hilbert class field of K and the Galois group $Gal(H_d/\mathbb{Q}) = Gal(N/\mathbb{Q})$ is the dihedral group D_h.*

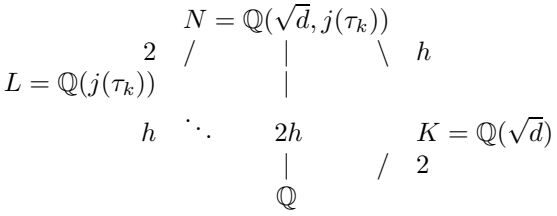

Figure 2

In the subsequent discussions, we call $H_d(x)$ the "genuine" class equation of $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$.

A2 A Theorem of Gross-Zagier on the "genuine" class equation. Let $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, and let $\mathcal{O}_K$ be the maximal order of K. For the genuine class equation $H_d(x)$ of $\mathcal{O}_K$, the growth of the coefficients is rather severe. However, the constant term $H_d(0)$ and the discriminant, $\Delta(H_d)$, are highly divisible numbers. Moreover, their prime factors do not exceed $-d$, and all prime factors of $\Delta(H_d)$ except $-d$ appear in even powers. These facts have been noticed by Deuring [D1] and Gross-Zagier [G-Z1]. Let $(—)$ denote the Legendre symbol. Deuring [D1] has shown that primes ℓ dividing $\Delta(H_d)$ are those which do not split completely in $K = \mathbb{Q}(\sqrt{d})$, i.e., $\left(\frac{d}{\ell}\right) \neq 1$. Deuring [D1] also has considered the difference $j(z) - j(z')$ for $z,\ z' \in \mathcal{F}$ belonging to two distinct quadratic fields of discriminants d and d', which are relatively prime. He has shown that no primes ℓ dividing the norm (over $\mathbb{Q}$) of the difference $j(z) - j(z')$ can split completely in $K = \mathbb{Q}(\sqrt{d})$ or in $K' = \mathbb{Q}(\sqrt{d'})$, i.e., $\left(\frac{d}{\ell}\right) \neq 1$ and $\left(\frac{d'}{\ell}\right) \neq 1$. Deuring's argument, however, does not give the exact upper bounds for prime factors appearing in $H_d(0)$ and $\Delta(H_d)$. Recently, Gross and Zagier [G-Z1] have obtained the closed formulae for $\Delta(H_d)$ and for the absolute value of the norm of the difference $j(z) - j(z')$ describing exactly which primes occur as factors.

(A2.1) Theorem. (Gross-Zagier [G-Z1]). *Let d_1 and d_2 be two fundamental discriminants. Assume that d_1 and d_2 are relatively prime. For primes ℓ with $\left(\frac{d_1 d_2}{\ell}\right) \neq -1$, denote by ϵ a strongly multiplicative*

function defined by

$$\epsilon(\ell) = \begin{cases} \left(\frac{d_1}{\ell}\right) & \text{if } (d_1, \ell) = 1 \\ \left(\frac{d_2}{\ell}\right) & \text{if } (d_2, \ell) = 1 \end{cases}$$

where (—) is the Legendre symbol. Then if $n = \prod_{i=1}^{r} \ell_i^{n_i}$ *with* $\left(\frac{d_1 d_2}{\ell_i}\right) \neq -1$ *for all* i, *we set* $\epsilon(n) = \prod_{i=1}^{r} \epsilon(\ell_i)^{n_i}$. *For a positive integer* n, *let* $\mathcal{F}$ *be the function defined by*

$$F(n) = \begin{cases} \ell^{kr_1 r_2 \cdots r_t} & \text{if } n = \ell^{2k-1} \ell_1^{2n_1} \cdots \ell_s^{2n_s} q_1^{r_1 - 1} \cdots q_t^{r_t - 1} \\ & \text{where } \epsilon(\ell) = \epsilon(\ell_i) = -1,\ \epsilon(q_i) = 1 \\ & \text{with } k,\ r_i > 1 \text{ and } n_i > 0\ ; \\ 1 & \text{if } n = \ell_1^{2k_1 - 1} \cdots \ell_s^{2k_s - 1}\ t \\ & \text{where } \epsilon(\ell_i) = -1 \text{ with } k_i \geq 1,\ s \geq 3 \\ & \text{and } t \in \mathbb{N}\ . \end{cases}$$

(a) *Put*

$$J(d_1, d_2) = \left(\prod_{s=1}^{h_1} \prod_{t=1}^{h_2} (j(\mathcal{A}_s) - j(\mathcal{B}_t)) \right)^{4/w(d_1)w(d_2)}$$

where $\{\mathcal{A}_1, \cdots, \mathcal{A}_{h_1}\}$ *(resp.* $\{\mathcal{B}_1, \cdots, \mathcal{B}_{h_2}, \}$*) is a set of ideal class representatives of* $\mathcal{O}_{K_1} \subset K_1 = \mathbb{Q}(\sqrt{d}_1)$ *(resp.* $\mathcal{O}_{K_2} \subset K_2 = \mathbb{Q}(\sqrt{d}_2)$*) and let* $w(d_1)$ *(resp.* $w(d_2)$*) denote the number of roots of unity in the ring* $\mathcal{O}_{K_1}$ *(resp.* $\mathcal{O}_{K_2}$*). Then*

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

Consequently, if ℓ *is a prime dividing* $J(d_1, d_2)^2$, *then* ℓ *is of the form* $\frac{d_1 d_2 - x^2}{4} \leq \frac{d_1 d_2}{4}$ *with* $\left(\frac{d_1}{\ell}\right) \neq 1$ *and* $\left(\frac{d_2}{\ell}\right) \neq 1$.

(b) *Let* $H_d(x)$ *be the genuine class equation of* $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$. *If* ℓ *is a prime dividing the constant term* $H_d(0)$ *of* H_d, *then* $\left(\frac{d}{\ell}\right) \neq 1$ *and* ℓ *is a divisor of* $J(d, -3)^2$. *Furthermore,* $\ell \leq 3|d|/4$.

(c) *Let* $H_d(x)$ *be the genuine class equation of* $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$. *If* ℓ *is a prime dividing the discriminant* $\Delta(H_d)$ *of* H_d, *then* $\left(\frac{d}{\ell}\right) \neq 1$ *and* $\ell \leq |d|$.

When $-d$ is a prime and the class number h of $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$ is odd prime, we have more precise information on the discriminant $\Delta(H_d)$ and the constant term $H_d(0)$ of H_d.

(A2.2) Corollary. *Let* $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $-d$ *is a prime* $\equiv 3$ *(mod 4) be the maximal order of* K *with the class number* h *an odd prime. Let* $Q_k(x, y) = a_k x^2 + b_k xy + c_k y^2$, $a_k > 1$, $k = 1, 2, \cdots, (h-1)/2$ *be the reduced positive definite primitive quadratic forms of discriminant* d. *Let* $H_d(x)$ *be the genuine class equation of* $\mathcal{O}_K \subset K = \mathcal{Q}(\sqrt{d})$. *Then the following assertions hold.*

(a) *The discriminant of* $H_d(x)$ *is given by the formula*

$$\Delta(H_d) = I^2 (-d)^{(h-1)/2}$$

where I is the index of the order $\mathbb{Z}[j]$ in the ring of integers of $\mathbb{Q}(j)$:

$$I = I_1 \cdots I_{\frac{h-1}{2}}$$

where

$$I_k = \prod_{n=1}^{-d-1} F(-d-n)^{r_k(n)}$$

with

$$r_k(n) = \frac{1}{2} \# \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid Q_k(x,y) = n\} .$$

In particular, the largest prime dividing $\Delta(H_d)$ does not exceed $-d$, and all its prime factors except $-d$ have even exponents.

(b) *Let $\tau_1, \tau_2 \in \mathcal{F}$ be imaginary quadratic integers belonging to two distinct imaginary quadratic fields of discriminant d_1 and d_2, respectively, where $-d_1$ and $-d_2$ are primes $\equiv 3$ (mod 4). Then*

$$|\mathrm{Norm}(j(\tau_1) - j(\tau_2)| = \left[\prod_{\substack{x^2 < d_1 d_2 \\ x^2 \equiv d_1 d_2 \pmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right) \right]^{w(d_1)w(d_2)/4}$$

In particular, taking $\tau_1 = \frac{1+\sqrt{d}}{2}$, $d < -4$ and $\tau_2 = \frac{1+\sqrt{-3}}{2}$ the constant term $H_d(0)$ of H_d is given up to sign by

$$H_d(0) = \pm \mid \mathrm{Norm}\left(j\left(\frac{1+\sqrt{d}}{2}\right)\right) \mid = \pm \left[\prod_{\substack{x^2 < -3d \\ x \text{ odd}}} F\left(\frac{-3d-x^2}{4}\right) \right]^3 .$$

In particular, $|H_d(0)|$ is a cube power.

(A2.3) Remarks (a) For the maximal imaginary quadratic order $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$ with discriminant d and class number h an odd prime, we have

$$sign\ (\mathrm{Norm}\left(j\left(\frac{1+\sqrt{d}}{2}\right)\right) = (-1)^t$$

where t is the number of quadratic forms $[a_k, a_k, c_k]$, $0 < a_k < c_k$ with discriminant d. In particular, if $d = -p$ with p a prime, then sign of $\mathrm{Norm}\left(j\left(\frac{1+\sqrt{d}}{2}\right)\right)$ is always negative, and hence $H_d(0) = (-1)^h \times \mathrm{Norm}\left(j\left(\frac{1+\sqrt{d}}{2}\right)\right)$ is a positive number. This can be explained as follows. The principal ideal class of $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$ corresponds to the singular modulus $j\left(\frac{1+\sqrt{d}}{2}\right)$, which is always negative (cf. A1.2)(a)). All other ideal classes appear in pairs and correspond to singular moduli $j(x + iy)$ and $j(-x + iy)$ where $\pm x + iy \in \mathcal{F} \cap \mathcal{O}_K$. Now singular moduli $j(x + iy)$ and $j(-x + iy)$ are conjugates for all values $\pm x + iy \in \mathcal{F} \cap \mathcal{O}_K$ except for those on the imaginary axis or on the boundary of $\mathcal{F}$. Singular moduli are positive on the imaginary axis, and on the lower boundary of $\mathcal{F}$, and they take negative real values on the

line $\pm\frac{1}{2}+i(\sqrt{3},\infty)$. Hence the sign of Norm $\left(j\left(\frac{1+\sqrt{d}}{2}\right)\right)$ is -1 to the power the number of roots on the line $\frac{1}{2}+i(\sqrt{3},\infty)$, which is the number t.

(b) Two proofs, one algebraic and the other analytic, have been given for Theorem (A2.1) in [G-Z1]. The algebraic proof has been, however, given only for the case of prime discriminants. Dorman [Do1] has generalized the algebraic proof to relatively prime composite discriminants d_1 and d_2. Also see [Do2].

(A2.4) The height of $\mathbf{H_d(x)}$. We define the height of $H_d(x)$ as the absolutely largest coefficient of $H_d(x)$, denoted $||H_d||$. It is observed that $||H_d|| = |H_d(0)|$, and we can give the estimate for $\log||H_d||$. For instance, from Corollary (A2.2)(b), it can be derived immediately that if $-d \equiv 3 \pmod 4$ with $|d|$ prime, then

$$\log||H_d|| = 3 \sum_{\substack{x^2 < -3d \\ x \text{ odd}}} \log F\left(\frac{-3d-x^2}{4}\right) .$$

A3 The constructions of the "genuine" class equations: A method of Kaltofen-Yui, and a method of Zagier.

We now describe the construction of the genuine class equations of the maximal imaginary quadratic orders $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$. The actual constructions are carried out for selected values of $d < 0$.

(A3.1) A method of Kaltofen-Yui. This method for computing $H_d(x)$ is rather a straightforward one. We simply evaluate singular moduli at imaginary quadratic integers in $\mathcal{F}$ corresponding to the ideal classes of $\mathcal{O}_K$. The procedure for $\mathcal{O}_K$ with *odd* prime class number cases is illustrated below in the cases that $d = d_K \equiv 1 \pmod 4$. The remaining case can be done similarly.

Step 1. *Determine the quadratic forms* $[a,b,c],\ a > 0, GCD(a,b,c) = 1$ *and* $b^2 - 4ac = d < 0$ *representing the ideal classes of* $\mathcal{O}_K$. *Calculate the roots* τ *of the quadratic equations* $az^2 + bz + c = 0$ *belonging to* $\mathcal{F}$.

(In fact, the quadratic forms are given by $[1,1,(1-d)/4],\ [a_k,\ \pm b_k,\ c_k]$ with $|b_k| \le a_k < c_k, b_k - 4a_kc_k = d,\ 1 \le k \le (h-1)/2$.) Therefore, roots τ are $(-1+\sqrt{d})/2,\ (\pm b_k + \sqrt{d})/2a_k$ for $k = 1, \cdots, (h-1)/2$.)

Step 2. *Evaluate singular moduli* $j(\tau)$ *at* $(h+1)/2$ *inequivalent imaginary quadratic numbers* $\tau = (-1+\sqrt{d})/2,\ (-b_k+\sqrt{d})/2a_k,\ k = 1, \cdots, (h-1)/2$.

(Since $j(x+iy)$ and $j(-x+iy)$ are complex conjugates for $\pm x + iy \in \mathcal{F} \cap \mathcal{O}_K$ it suffices to evaluate singular moduli over the $(h+1)/2$ values of τ.)

Step 3. *Form* $H_d(x)$*:*

$$H_d(x) = \left\{x - j\left(\frac{-1+\sqrt{d}}{2}\right)\right\} \prod_{k=1}^{(h-1)/2} \left\{x - j\left(\frac{-b_k+\sqrt{d}}{2a_k}\right)\right\}\left\{x - j\left(\frac{b_k+\sqrt{d}}{2a_k}\right)\right\} .$$

(A3.2) Remark. Some comments might be in order concerning the actual calculations. The evaluation of each singular modulus $j(\tau)$ was done to high floating point precision. We observed that the Taylor series of j evaluated at q converged extremely slowly. Therefore we evaluated the Taylor series of E_4 and η separately at q, then raised the value $\eta(q)$ to the eighth power, divided $E_4(q)$ by this result, and finally raised the quotient to the third power (cf. (A1.2)). This process yields $j(q)$ to high precision fairly quickly.

In each case there were two parameters to choose: The floating point precision and the order of the Taylor expansions. We decided to choose the same order for both E_4 and η. The constant coefficient of each polynomial turned out to be the one of largest size. Therefore we chose the floating point precision typically 20 digits more than the number of digits in that coefficient. In all cases we then could read off the correct corresponding integer from its approximation. A fact, which was already observed by Weber [W], Dering [D1] and recently been made very explicit by Gross and Zagier [G-Z1] (cf. Corollary (A2.2)(b)) asserts that the constant coefficient $H_d(0)$ must be a perfect cube. Verifying this condition proved to be a valuable test to see whether the order of the Taylor approximation was high enough. If not, we increased the order by an increment of 5 and tried again. A further confirmation for the correctness of all coefficients is to factor both $H_d(0)$ and the discriminant $\Delta(H_d)$ of H_d, whose prime factors are again predicted by a theorem of Gross and Zagier (cf. Corollary (A2.2)).

(A3.3) A method of Zagier (for $\mathbf{h \leq 9}$). This approach was suggested to us by D. Zagier. The idea is to use the formula of Gross and Zagier on the difference of two singular moduli, $j(\tau_1) - j(\tau_2)$ where τ_1 and τ_2 belong to two distinct maximal imaginary quadratic orders (cf. (A2.2)(b)).

We know that there are altogether 13 imaginary quadratic orders with class number 1, of which 9 are maximal (i.e., $f = 1$), and that their singular moduli are integral. The results are tabulated as follows:

d	-163	-67	-43	-27	-19	-11
f	1	1	1	3	1	1
class invariant	$-640,320^3$	$-5 \cdot 280^3$	-960^3	$-3 \cdot 160^3$	-96^3	-32^3

d	-7	-3	-4	-8	12	-16	-28
f	1	1	1	1	2	2	2
class invariant	-15^3	0	12^3	20^3	$2 \cdot 30^3$	66^3	255^3

Now take the maximal imaginary quadratic order $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{d})$ of discriminant d and class number h. Write the genuine class equation $H_d(x)$ in the form

$$H_d(x) = x^h + A_{h-1}x^{h-1} + \cdots + A_1 x + A_0 \in \mathbb{Z}[x] \ .$$

Our task is to determine the h unknowns $A_0, A_1, \cdots, A_{h-1}$ explicitly. Note that Gross-Zagier theorem is applicable only for maximal orders.

Step 1. *Evaluate the absolute value of*

$$\text{Norm}\left(j\left(\frac{1+\sqrt{d}}{2}\right)-j\left(\frac{1+\sqrt{d'}}{2}\right)\right)$$

where d' runs 9 values representing maximal imaginary quadratic orders of class number 1 (cf. the table above).

Apply the Gross and Zagier formula (Theorem (A2.1)) to get a system of 9 linear equations corresponding to $d'=-3,-4,-8,-7,\cdots,-163$:

$$H_d(0)=B_1,\ H_d(12^3)=B_2,\ H_d(20^3)=B_3,\ \cdots,\ H_d(-640,320^3)=B_9\ .$$

Step 2. *Solve the system of 9 linear equations in h unknowns.*

This linear system is solvable at most for $h(d)=h\le 9$.

A4 The construction of the "genuine" class equations via the modular equations.

This method was employed by Weber [W] and Hanna [H], and by others. However, the scope of this approach is extremely limited as the modular equations are known explicitly only up to order 19. Here we need to introduce the modular equations of order $n\ge 1$.

(A4.1) The modular equations of order n and singular moduli. Choose a positive integer $n>1$ and fix it once and for all. Denote by $GL_2^+(\mathbb{Z})$ the set of 2×2 matrices with entries in $\mathbb{Z}$ and positive determinant. If $\alpha=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in GL_2^+(\mathbb{Z})$, we say that α is primitive if $GCD(a,b,c,d)=1$. For a positive integer $n>1$, let Δ_n^* denote the subset of $GL_2^+(\mathbb{Z})$ consisting of primitive matrices with determinant n. Then $SL_2(\mathbb{Z})$ acts on Δ_n^*, and the left coset representatives of Δ_n^* modulo $SL_2(\mathbb{Z})$ are given by the set, A, of the $\psi(n)=\prod_{p|n}(1+\frac{1}{p})$ matrices, that is,

$$A=\left\{\begin{pmatrix} a & b\\ 0 & d\end{pmatrix}|a,b,d\in\mathbb{Z},\ ad=n,\ 0\le b\le d-1\right\}\ .$$

For $\alpha=\begin{pmatrix} a & b\\ 0 & d\end{pmatrix}\in A$ and for $\tau\in\mathcal{F}$, imaginary quadratic, we write $j\circ\alpha$ for

$$(j\circ\alpha)(\tau)=j\left(\frac{a\tau+b}{d}\right)\ .$$

Now we define the polynomial

$$\Phi_n(x,j)=\prod_{\alpha\in A}(x-j\circ\alpha)\ =\ \prod_{\substack{ad=n\\ 0\le b\le d-1}}\left(x-j\left(\frac{a\tau_+b}{d}\right)\right)\ .$$

This is called the modular equation of order n. It is a symmetric polynomial over $\mathbb{C}$ in x and j of degree $\psi(n)$. Furthermore, $\Phi_n(x,j)$ has coefficients in $\mathbb{Z}$. It is rather difficult to compute $\Phi_n(x,j)$ explicitly. Explicit

forms are known only up to prime order $n \leq 19$. For example, we have

$$\begin{aligned}\Phi_1(x,y) &= x - y,\\ \Phi_2(x,y) &= x^3 + y^3 - x^2y^2 + 2^4 3 \cdot 31(x^2 + xy^2) - 2^4 3^4 5^3 (x^2 + y^2)\\ &\quad + 3^4 5^3 4027 yx + 2^8 3^7 5^6 (x + y) - 2^{12} 3^9 5^9 \ .\end{aligned}$$

For $n = 5$ see Smith [Sm], and for $n = 7$ see Hermann [He] and Kaltofen and Yui [KY1]. For $n = 11$ see Kaltofen and Yui [KY2].

$\Phi_n(x,y) = 0$ defines a singular affine curve over $\mathbb{Z}$. Its resolution defines a curve of genus zero for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 16, 18$ and 25.

The polynomial $\Phi_n(x,y)$, when restricted to the diagonal, is subject to the Kronecker congruence:

$$\Phi_n(x,x) = \pm \prod_d H_d(x)^{r'(d)}$$

where the quantities in the right-hand side are defined as follows. The product is taken over all $d \in \mathbb{Z},\ d < 0$, such that $y^2 - dx^2 = 4n$ has a solution $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ with $x > 0$. Denoting by $r(d)$ the number of such solutions, the multiplicity $r'(d)$ is given by

$$r'(d) = \begin{cases} r(d) & if\ d < -4 \\ r(d)/2 & if\ d = -4 \\ r(d)/3 & if\ d = -6\ . \end{cases}$$

$H_d(x)$ is the genuine class equation for the imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ of discriminant d and degree h. Comparing the degrees of both sides, we have the Kronecker-Hurwitz class number relation:

$$\deg\ \Phi_n(x,x) = \sum_d r'(d) h(d)\ .$$

How do we make use of modular equations to construct genuine class equations $H_d(x)$? The theoretical basis is given by the following theorem of Weber (see Weber [W, §114-119]), and Cohn [C, §11]).

(A4.2) Theorem. *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$ be an imaginary quadratic order with discriminant d and conductor f. Then the genuine class equation $H_d(x)$ of $\mathcal{O}$ is the GCD (in the ring $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$) of those diagonal forms of modular equations $\Phi_n(x,x)$ for which $n = Norm(\lambda)$ for λ primitive in $\mathcal{O}$.*

More precisely, we have

$$H_{-3} = GCD(\Phi_3, \Phi_7),\ H_{-4} = GCD(\Phi_2, \Phi_5)$$

and for $d = d_K f^2$, setting $\tau = (1 + \sqrt{d_K})/2$ if $d_K \equiv 1\ (mod\ 4)$, $1 + \sqrt{d_K}/2$ if $d_K \equiv 1\ (mod\ 4)$ and $d' = Norm(f\ \tau)$,

$$H_d = \begin{cases} GCD(\Phi_{|d|}, \Phi_d,) & f\ \ odd \\ GCD(\Phi_{|d/r|}, \Phi_d,) & f\ \ even \end{cases}$$

(Here $\Phi_n := \Phi_n(x,x)$.)

Now we can describe the method for the construction of genuine class equations $H_d(x)$ for imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, using the above theorem. Since it is rather difficult to compute modular

equations, the scope of this method is rather limited, though it might be of some interest from a theoretical point of view.

Step 1. *Compute the modular equations $\Phi_{|d|}(x,y)$ and $\Phi_d,(x,y)$ if f is even, and $\Phi_{|d/4|}(x,y)$ and $\Phi_d,(x,y)$ if f is odd.*

Step 2. *Factor the diagonal forms of the modular equations determined in Step 1.*

Step 3. *Determine the greatest common factor of these diagonal forms.*

(A4.3) Illustrations. For small values of n, the factors of the diagonal form of the modular equation of order n : $\Phi_n(x,x)$ can be determined. We list them in the table below.

n	$\Phi_n(x,x)$	deg Φ_n	$H_d(x)$
2	$H_{-4}H_{-8}H^2_{-7}$	(4)	$H_{-4}(x) = x - 2^6 3^3$ $H_{-8}(x) = x - 2^6 5^3$ $H_{-7}(x) = x + 3^3 5^3$
3	$H_{-3}H_{-12}H_{-8}H^2_{-11}$	(6)	$H_{-3}(x) = x$ $H_{-11}(x) = x + 2^{15}$ $H_{-12}(x) = x - 2^4 3^3 5^3$
4	$H_{-16}H^2_{-7}H^2_{-12}H^2_{-15}$	(9)	$H_{-15}(x) = x^2 + 3^3 5^2 283x$ $\quad - 3^6 5^3 11^3$ $H_{-16}(x) = x - 2^3 3^3 11^3$
5	$H_{-20}H^2_{-4}H^2_{-11}H^2_{-16}H^2_{-19}$	(10)	$H_{-19}(x) = x + 2^{15} 3^3$ $H_{-20}(x) = x^2 - 2^7 5^3 79x$ $\quad - 2^{12} 5^3 11^3$
6	$H_{-24}H^2_{-8}H^2_{-15}H^2_{-20}H^2_{23}$	(18)	$H_{-23}(x) = x^3 + 2 \cdot 5^3 13967x^2$ $\quad - 5^6 329683x + 5^9 187^3$ $H_{-24}(x) = x^2 - 2^7 3^3 1399x$ $\quad + 2^{12} 3^6 17^3$
7	$H_{-7}H_{-28}H^2_{-3}H^2_{-12}H^2_{-19}H^2_{-24}H^2_{-27}$	(14)	$H_{-27}(x) = x + 2^{15} 3 \cdot 5^3$ $H_{-28}(x) = x - 3^3 5^3 17^3$
8	$H_{-32}H^2_{-7}H^2_{-16}H^2_{-23}H^2_{-28}H^2_{-31}$	(20)	$H_{-31}(x) = x^3 + 3^4 53 \cdot 9199x^2$ $\quad - 2 \cdot 3^7 29 \cdot 462629x$ $\quad + 3^9 11^3 17^3 23^3$
10	$H_{-24}H_{-37}H_{-36}H_{-39}H_{-40}$ $\times H^2_{-4}H^2_{-15}$	(18)	$H_{-39}(x) = x^4$ $\quad + 2^2 3^3 11 \cdot 29 \cdot 9623x^3$ $\quad - 2 \cdot 3 \cdot 71646393491x^2$ $\quad + 3^{12} 206746392899x$ $\quad 3^{15} 17^3 667^3$
11	$H_{-11}H_{-44}H^2_{-7}H^2_{-8}H^2_{-19}$ $\times H^2_{-28}H^2_{-35}H^2_{-40}H^2_{-43}$	(22)	$H_{-35}(x) = x^2 + 2^{19} 3^2 5^2 x$ $\quad - 2^{30} 5^3$ $H_{-43}(x) = x + 2^{18} 3^3 5^3$ $H_{-44}(x) = x^3 - 2^4 1709 \cdot 4105x^2$ $\quad + 2^8 3 \cdot 11^4 24049x$ $\quad - 2^{12} 11^3 17^3 29^3$

A5. The construction of the "genuine" class equations: Illustrations $\mathbf{H_{-719}(x)}$.

We illustrate our construction of the genuine class equation for the maximal imaginary quadratic order

$\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{-719})$ by a method of Kaltofen and Yui. $\mathcal{O}_K$ has discriminant $d = -719$ and class number $h(-719) = 31$. The reduced primitive positive definite quadratic forms representing the ideal classes of $\mathcal{O}_K$ are given as follows.

[a,b,c]	τ(roots of $az^2 + bz + c = 0$ belonging to $\mathcal{F} \cap \mathcal{O}_K$)
$[1, 1, 180]$	$\frac{-1+\sqrt{-719}}{2}$
$[2, \pm 1, 90]$	$\pm\frac{1+\sqrt{-719}}{4}$
$[3, \pm 1, 60]$	$\pm\frac{1+\sqrt{-719}}{6}$
$[4, \pm 1, 45]$	$\pm\frac{1+\sqrt{-719}}{8}$
$[5, \pm 1, 36]$	$\pm\frac{1+\sqrt{-719}}{10}$
$[6, \pm 1, 30]$	$\pm\frac{1+\sqrt{-719}}{12}$
$[9, \pm 1, 20]$	$\pm\frac{1+\sqrt{-719}}{18}$
$[10, \pm 1, 18]$	$\pm\frac{1+\sqrt{-719}}{20}$
$[12, \pm 1, 15]$	$\pm\frac{1+\sqrt{-719}}{24}$
$[7, \pm 3, 26]$	$\pm\frac{3+\sqrt{-719}}{14}$
$[13, \pm 3, 14]$	$\pm\frac{3+\sqrt{-719}}{26}$
$[6, \pm 5, 31]$	$\pm\frac{5+\sqrt{-719}}{12}$
$[8, \pm 7, 24]$	$\pm\frac{7+\sqrt{-719}}{16}$
$[12, \pm 7, 16]$	$\pm\frac{7+\sqrt{-719}}{24}$
$[10, \pm 9, 20]$	$\pm\frac{9+\sqrt{-719}}{20}$
$[14, \pm 11, 15]$	$\pm\frac{11+\sqrt{-719}}{28}$

The discriminant of $H_{-719}(x)$ is

$$\begin{aligned}\Delta(H_{-719}) = -11^{1080}17^{674}19^{600}23^{480}41^{258}43^{242}47^{214}53^{192}67^{144}71^{138}\\ \times 73^{132}79^{124}89^{98}97^{94}101^{96}109^{78}127^{68}131^{66}139^{58}157^{52}173^{52}\\ \times 179^{42}193^{40}197^{38}199^{32}223^{38}229^{36}233^{22}239^{32}251^{26}269^{22}271^{22}\\ \times 307^{22}313^{16}337^{16}347^{16}349^{16}353^{12}359^{24}383^{18}409^{8}419^{18}421^{4}\\ \times 431^{18}439^{16}449^{14}463^{8}467^{16}479^{20}487^{8}503^{16}509^{14}523^{8}557^{10}\\ \times 563^{12}569^{12}571^{6}593^{12}599^{16}601^{4}607^{10}619^{8}641^{8}647^{12}659^{12}\\ \times 661^{4}677^{8}683^{8}691^{6}701^{6}709^{4}719^{15}.\end{aligned}$$

The constant term of $H_{-719}(x)$ is

$$H_{-719}(0) = (11^{13}17^{8}23^{6}41^{2}47^{2}53^{2}71^{2}89^{2}173^{2}179^{2}197 \cdot 233 \cdot 383 \cdot 449 \cdot 467 \cdot 509)^{3}.$$

One can see that all primes ℓ dividing $\Delta(H_{-719})$ and $H_d(0)$ are subject to the condition that $\left(\frac{-719}{\ell}\right) \neq 1$, and that if $\ell | H_{-719}(0)$, then $\ell \leq 3 \cdot 719/4$ and if $\ell | \Delta(H_{-719})$, then $\ell \leq 719$.

PART B

THE CONSTRUCTION OF THE "REDUCED" CLASS EQUATIONS

Contents

B1 The "reduced" class equations.

Let $H_d(x)$ be the "genuine" (level one) class equation of an imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ with class number $h(d) =: h$. We now describe a procedure for constructing a monic integral irreducible polynomial, $h_d(x)$, of degree h with very small coefficients, which defines the same ring class field as $H_d(x)$ over $\mathbb{Q}$. The theoretical basis of this construction is due to Weber [W]. Watson carried out these constructions for selected imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ with class numbers ≤ 19 in his series of papers $[W_1, W_2, W_3, W_4]$.

We review here the Weber-Watson theory, which we modify slightly to suit our purposes. Our choice of the class invariants differs slightly from those of Weber [W].

(B1.1) The Weber functions. Let $q = e^{2\pi i z}$ with $Im\ z > 0$ and $|q| < 1$. Put

$$f(z) = q^{-1/48} \prod_{m=1}^{\infty} (1 + q^{m-1/2}),$$

$$f_1(z) = q^{-1/48} \prod_{m=1}^{\infty} (1 - q^{m-1/2}),$$

and

$$f_2(z) = \sqrt{2}\ q^{1/24} \prod_{m=1}^{\infty} (1 + q^m).$$

These functions are known as the "Weber" functions. They are expressed in terms of the eta function $\eta(z)$ (cf. (A1.2)) as follows:

$$f(z) = \frac{e^{-\pi i/24}\eta((z+1)/2)}{\eta(z)}\ ,$$

$$f_1(z) = \frac{\eta(z/2)}{\eta(z)} \quad \text{and} \quad f_2(z) = \sqrt{2}\ \frac{\eta(2z)}{\eta(z)}\ .$$

The function f_2 induces a complex analytic isomorphism

$$f_2 : \mathfrak{H} * /\Gamma_0(2) \longrightarrow \mathbb{P}^1(\mathbb{C})$$

of compact Riemann surfaces of genus zero where $\Gamma_0(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma | c \equiv 0 \pmod 2 \right\}$ is a subgroup of Γ of index 3. These functions are interconnected by the relations

$$\begin{aligned} f^8(z) &= f_1^8(z) + f_2^8(z)\ , \\ f(z)f_1(z)f_2(z) &= \sqrt{2}\ , \\ f(z)f_2\left(\tfrac{1+z}{2}\right) &= e^{\pi i/24}\sqrt{2}\ , \end{aligned}$$

and

$$f_1(z)f_2\left(\frac{z}{2}\right) = \sqrt{2}\ .$$

The elliptic modular j-invariant $j(z)$ is expressed as rational functions of $f^{24}(z), -f_1^{24}(z)$ and $-f_2^{24}(z)$, respectively. Indeed, we have

$$j(z) = \frac{\{f^{24}(z)-16\}^3}{f^{24}(z)} = \frac{\{f^{24}(z)+16\}^3}{f_1^{24}(z)} = \frac{\{f_2^{24}(z)+16\}^3}{f_2^{24}(z)} \ .$$

These identities imply that $f^{24}(z), -f_1^{24}(z), -f_2^{24}(z)$ are the roots of the cubic equation

$$(x-16)^3 - xj(z) = 0 \ .$$

Equivalently, if we put

$$\gamma_2(z) = j^{1/3}(z) = \sqrt[3]{j(z)} \ ,$$

then $f^8(z),\ -f_1^8(z)$ and $-f_2^8(z)$ are the roots of the equation

$$x^3 - \gamma_2(z)x - 16 = 0$$

Put

$$D = \begin{cases} d/4 & \text{if } d \equiv 0 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

and assume that D is a square-free.

(B1.2) Theorem (cf. Weber [W, §19]; Watson [W4]). *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $d \equiv 1 \ (mod\ 8)$ and $3 \nmid d$, be an imaginary quadratic order of discriminant d and class number h. Let $\{\mathcal{A}_1, \cdots, \mathcal{A}_h\}$ be a complete set of representatives of the ideal classes of $\mathcal{O}$, and let*

$$H_d(x) = \prod_{k=1}^{h} (x - j(\mathcal{A}_k))$$

be the genuine class equation of $\mathcal{O}$. Put

$$\overline{H}_d(x) := x^h H_d((x-16)^3/x).$$

Then the following assertions hold true.

(a) $\overline{H}_d(x) = \prod_{k=1}^{h} \left\{(x-16)^3 - xj(\mathcal{A}_k)\right\}$ *, and it is a monic integral polynomial of degree $3h$ over $\mathbb{Q}$.*

(b) *$\overline{H}_d(x)$ has a monic irreducible integral polynomial, $\overline{h}_d(x)$, of degree h as its factor. Moreover, $\overline{h}_d(x)$ is the minimal polynomial of $2^{12} f^{-24}(\sqrt{d}) = -f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{R}$ with the constant term $\overline{h}_d(0) = -1$.*

(c) *The quotient $\overline{H}_d(x)/\overline{h}_d(x)$ is a monic integral irreducible polynomial of degree $2h$ over $\mathbb{Q}$.*

(d) *If $\overline{h}_d(x) = \prod_{k=1}^{h} (x - \alpha_k) \in \mathbb{C}[x]$, then for suitable choice of h 24^{th} roots of $\alpha_k, k = 1, \cdots, h$, the polynomial*

$$h_d(x) := x^h \prod_{k=1}^{h} \left(\frac{1}{x} - \sqrt[24]{\alpha_k}\right)$$

is a monic irreducible polynomial of degree h over $\mathbb{Q}$, which is the minimal polynomial of $f(\sqrt{d})/\sqrt{2}$ or its reciprocal. Furthermore, the constant term $h_d(0)$ is equal to -1. Therefore, every root of $h_d(x)$ is a unit.

(e) *$h_d(x)$ defines the same ring class field as $H_d(x)$ over $\mathbb{Q}$.*

Consequently, $Gal(h_d/\mathbb{Q})$ is the generalized dihedral group, that is, the semi-direct product $Pic(\mathcal{O}) \rtimes C_2$. In particular, if h is odd prime, then $Gal(h_d/\mathbb{Q}) \cong D_h$.

Proof. (a) We have

$$\overline{H}_d(x) = \prod_{k=1}^{h} \{(x-16)^3 - xj(\mathcal{A}_k)\} .$$

Note that the equation $(x-16)^3 - xj(z) = 0$ has three distinct roots $f^{24}(\tau), -f_1^{24}(\tau)$ and $-f_2^{24}(\tau)$. It then follows that $\overline{H}_d(x)$ has the roots $f^{24}(\mathcal{A}_k)$, $-f_1^{24}(\mathcal{A}_k)$, $-f_2^{24}(\mathcal{A}_k)$, $k = 1, \cdots, h$. $\overline{H}_d(x)$ is obviously a monic integral polynomial, since $H_d(x)$ is. It has degree $3h$ over $\mathbb{Q}$.

(b) We note that the principal ideal class, say $\mathfrak{A}_1$, of $\mathcal{O}$ is represented by the quadratic form $[1, -1, (1-d)/4]$ whose root in $\mathcal{F} \cap \mathcal{O}$ is $\frac{1+\sqrt{d}}{2}$. Now one of the Weber's formula

$$f(z) f_2\left(\frac{1+z}{2}\right) = e^{\pi i/24}\sqrt{2}$$

with $z = \frac{1+\sqrt{d}}{2}$ yields the identity

$$f(\sqrt{d}) f_2\left(\frac{1+\sqrt{d}}{2}\right) = e^{\pi i/24}\sqrt{2} .$$

This implies that $2^{12} f^{-24}(\sqrt{d}) = -f_2^{24}(\mathcal{A}_1)$ is a root of $\overline{H}_d(x)$. Now the fact that $f(\sqrt{d})/\sqrt{2}$ is a class invariant of $\mathcal{O}$, implies that a complete set of conjugates of $2^{12} f^{-24}(\sqrt{d}) = -f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right)$ consists of exactly h algebraic integers chosen from the pool of algebraic integers

$$\{f^{24}(\mathcal{A}_k), -f_1^{24}(\mathcal{A}_k), -f_2^{24}(\mathcal{A}_k) \ ; \ k = 1, \cdots, h\}$$

in such a way that each member of the ideal class of $\mathcal{O}$ can occur once and only once. In other words, if $f^{24}(\mathcal{A}_i)$ occurs as a conjugate, neither $-f_1^{24}(\mathcal{A}_i)$ nor $-f_2^{24}(\mathcal{A}_i)$ with the same ideal $\mathcal{A}_i$ can be conjugates. Let $\overline{h}_d(x)$ be the minimal polynomial of $2^{12} f^{-24}(\sqrt{d})$. Then $\overline{h}_d(x)$ is a monic integral irreducible polynomial of degree h over $\mathbb{Q}$.

If h is odd, $j\left(\frac{1+\sqrt{d}}{2}\right)$ is the only real root of $H_d(x)$. Since $j\left(\frac{1+\sqrt{d}}{2}\right) \in \mathfrak{R}^-$ and since $j\left(\frac{1+\sqrt{d}}{2}\right) < 8^2$, the function $\frac{(x-16)^3}{x}$ is monotonic. Accordingly, $(x-16)^3 - xj\left(\frac{1+\sqrt{d}}{2}\right) = 0$ has only one real root. Evaluating all three roots $f^{24}(\tau)$, $-f_1^{24}(\tau)$ and $-f_2^{24}(\tau)$ at $\tau = \frac{1+\sqrt{d}}{2}$, we can conclude that $-f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right)$ is the only real root of the equation $(x-16)^3 - xj\left(\frac{1+\sqrt{d}}{2}\right) = 0$. Therefore, $-f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right) = 2^{12} f^{-24}(\sqrt{d})$ is the only real root of $\overline{H}_d(x)$. If h is even, $H_d(x)$ may have even numbers of real roots, one of which is $2^{12} f^{-24}(\sqrt{d})$.

To prove the assertion on the constant term $\overline{h}_d(0)$, we study the quotient $\overline{H}_d(x)/\overline{h}_d(x)$. In the given situation, there always exist quadratic forms $[2, \pm 1, (1-d)/8]$ besides $[1, -1, (1-d)/4]$. The quadratic

equation corresponding to the former quadratic form has roots $\frac{\pm 1+\sqrt{d}}{4}$, and $\frac{1+\sqrt{d}}{4}$ is just half of the root of the quadratic equation corresponding to the latter form. Then from the formula of Weber: $f_1(z)f_2\left(\frac{z}{2}\right)=\sqrt{2}$, it follows that $\overline{H}_d(x)$ always possesses pairs of roots

$$x_1=-24_1(\tau) \text{ and } x_2=-f_2^{24}(\tau/2)$$

with the relation $x_1x_2=2^{12}$. This means that $\overline{H}_d(x)$ has pairs of roots, each pair connected with the above relation. Therefore, the quotient $\overline{H}_d(x)/\overline{h}_d(x)$ has the form

$$\begin{aligned}\overline{H}_d(x)/\overline{h}_d(x) &= \prod_{k=1}^{h}\{(x-x_{1,k})(x-x_{2,k})\}\\ &= \prod_{k=1}^{h}\left\{x^2-(x_{1,k}+x_{2,k})x+2^{12}\right\}.\end{aligned}$$

The constant term of $\overline{H}_d(x)/\overline{h}_d(x)$ is 2^{12h}. From the definition of $\overline{H}_d(x)$, we see immediately that the constant term of $\overline{H}_d(x)$ is $\overline{H}_d(0)=-16^{3h}=-2^{12h}$. Therefore, we have $\overline{h}_d(0)=-1$.

(c) We have only to show the irreducibility of $\overline{H}_d(x)/\overline{h}_d(x)$. We have the identities

$$\begin{aligned}f^{24}\left(\tfrac{1+\sqrt{d}}{2}\right)f_1^{24}\left(\tfrac{1+\sqrt{d}}{2}\right)f_2^{24}\left(\tfrac{1+\sqrt{d}}{2}\right)&=2^{12}\ ,\\ f_1^{24}\left(\tfrac{1+\sqrt{d}}{2}\right)f_2^{24}\left(\tfrac{1+\sqrt{d}}{4}\right)&=2^{12}\ ,\end{aligned}$$

and

$$f^{24}(\sqrt{d})f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right)=-2^{12}\,.$$

From these, we obtain the identity

$$(*)\qquad 2^{12}f^{-24}(\sqrt{d})=-f^{-24}\left(\frac{1+\sqrt{d}}{2}\right)f_2^{24}\left(\frac{1+\sqrt{d}}{4}\right)\ .$$

We know that $2^{12}f^{-24}(\sqrt{d})=-f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right)$, which is the only real root of $\overline{H}_d(x)$, is a class invariant of $\mathcal{O}\subset K$, so that its minimal polynomial $\overline{h}_d(x)$ is irreducible of degree h over $\mathbb{Q}$. Therefore, all roots of $\overline{H}_d(x)/\overline{h}_d(x)$ are imaginary whose product is equal to 2^{12}. One of such pairs is $f_1^{24}\left(\frac{1+\sqrt{d}}{2}\right)$ and $f_2^{24}\left(\frac{1+\sqrt{d}}{4}\right)$. Then the relation(*) implies that the Galois group $\mathrm{Gal}(\overline{h}_d/K)$ act transitively on the set of roots of $\overline{H}_d(x)/\overline{h}_d(x)$. As the $\mathrm{Gal}(\overline{h}_d/K)$-orbit of $f_2^{24}\left(\frac{1+\sqrt{d}}{4}\right)$ has length h, $\overline{H}_d(x)/\overline{h}_d(x)$ must be irreducible of degree $2h$ over $\mathbb{Q}$.

(d) This follows from the fact that $f(\sqrt{d})/\sqrt{2}$ is a class invariant of $\mathcal{O}$. In fact, $x^h\overline{h}_d\left(\frac{1}{x}\right)$ has h roots which are conjugates of $f^{24}(\sqrt{d})/2^{12}$. This guarantees that for a suitable choice of the 24^{th} roots of reciprocal roots of $\overline{h}_d(x)$, the resulting polynomial $h_d(x)$ is integral and irreducible of degree h and $\mathbb{Q}$. The assertion on $h_d(0)$ follows from (b).

(e) From the construction, $H_d(x)$ and $h_d(x)$ have the same splitting field over $\mathbb{Q}$, which is the ring class field of $\mathcal{O}$.

For the cases $d \equiv 5 \pmod 8$, we have the following results.

(B1.3) Theorem. *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $d \equiv 5 \pmod 3$ and $3 \nmid d$ be an imaginary quadratic order of discriminant d and class number h. Then $f(\sqrt{d})$ is a class invariant of $\mathcal{O}$, and its minimal polynomial, which is of degree $3h$ over $\mathbb{Q}$, is the "reduced" class equation $h_d(x)$ of $\mathcal{O}$.*

Furthermore, the constant term is equal to $(-2)^h$.

We consider the case $d \equiv 0 \pmod 8, d < 0$. Put $D = d/4$ and let $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$ be the imaginary quadratic order of discriminant d and class number h. The results differ depending on D is even or odd.

(B1.4) Theorem. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$, $D < 0, D = \frac{d}{4} \equiv 2$ or $6 \pmod 8$ and $3 \nmid D$ be an imaginary quadratic order of discriminant d and class number h. Then $f_1(\sqrt{D})^2/\sqrt{2}$ is a class invariant of $\mathcal{O}$, and its minimal polynomial, which is of degree h over $\mathbb{Q}$, is the "reduced" class equation $h_d(x)$ of $\mathcal{O}$.*

Furthermore, the constant term $h_d(0)$ is equal to ± 1.

(B1.5) Theorem. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$, $d < 0$, $D = \frac{d}{4} \equiv 3 \pmod 8$ and $3 \nmid D$ be an imaginary quadratic order of discriminant d and class number h. Then $f(\sqrt{D})^4$ is a class invariant of $\mathcal{O}$, and its minimal polynomial, which is of degree h over $\mathbb{Q}$, is the "reduced" class equation $h_d(x)$ of $\mathcal{O}$.*

Furthermore, the constant term $h_d(0)$ is equal to $\pm 2^h$.

(B1.6) Theorem. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$, $D < 0$, $D = \frac{d}{4} \equiv 7 \pmod 8$ and $3 \nmid D$ be an imaginary quadratic order of discriminant d and class number h. Then $f(\sqrt{D})^2/\sqrt{2}$ is a class invariant of $\mathcal{O}$, and its minimal polynomial, which is of degree h over $\mathbb{Q}$, is the "reduced" class equation $h_d(x)$ of $\mathcal{O}$.*

Furthermore, the constant term $h_d(0)$ is equal to $(-1)^h$.

(B1.7) The cases when $3|d$. (cf. Schertz [S].) Let $\mathcal{O}$ be an imaginary quadratic order in $K = \mathbb{Q}(\sqrt{d})$, $d < -3$ with $3|d$. Write $\mathcal{O} = [1, \tau]$ where

$$\tau = \begin{cases} \sqrt{d}/2 & if \quad d \equiv 0 \pmod 4 \\ \frac{3+\sqrt{d}}{2} & if \quad d \equiv 1 \pmod 4 \end{cases}$$

Then $K(j^{1/3}(\tau))$ is the ring class field of the imaginary quadratic order $\mathcal{O}' = [1, 3\tau]$, and it is an algebraic extension of degree 3 of the ring class field of $\mathcal{O}$. Furthermore, $\mathbb{Q}(j^{1/3}(\tau) = \mathbb{Q}(j(3\tau))$.

Consequently, the minimal polynomial of the class invariant $j^{1/3}(\tau)$ has degree $3h$ rather than h over $\mathbb{Q}$. In other words, there is no algebraic relation of degree h over $\mathbb{Z}$ among the singular moduli of imaginary quadratic orders with discriminants divisible by 3, and the smallest algebraic relation is of degree $3h$.

B2 The method of Weber-Watson on the construction of the "reduced" class equations.

B2.1 A method of Weber-Watson. We describe the Weber-Watson construction of the "reduced" class equations for an imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d \equiv 1 \pmod 8$ and $3 \nmid d$ with class number h. For each reduced positive definite primitive quadratic form $[a_k, b_k, c_d]$ of discriminant d, let

$\tau_k = (-b_k + \sqrt{d})/2a_k$ be the root of the quadratic equation $a_k z^2 + b_k z + c_k = 0$, belonging to $\mathcal{F}$, for $k = 1, \cdots, h$.

Step 1. *Let $f(z)$, $f_1(z)$ and $f_2(z)$ be the Weber functions. Evaluate*

$$f^{24}(\tau_k),\ -f_1^{24}(\tau_k),\ -f_2^{24}(\tau_k)$$

at h imaginary quadratic numbers $\tau_k = (-b_k + \sqrt{d})/2a_k$ for $k = 1, \cdots, h$ corresponding to $Pic(\mathcal{O})$.

(Step 2 - Step 6 are the reduction processes.)

Step 2. *From the set of $3h$ numbers constructed in Step 1, discard $2h$ pairs of numbers whose products are equal to 2^{12}. Construct an equation of degree h, one of whose roots is $f_2^{24}\left(\frac{1+\sqrt{d}}{2}\right)$. Denote by $\prod_{k=1}^{h}(x-\alpha_k) = 0$ the equation thus obtained.*

Step 3. *Compute the cube roots $\sqrt[3]{\alpha_k}$ for $k = 1, \cdots, h$. From the set of $3h$ numbers, select the "proper" h cube roots in such a way that one of the cube roots is $f_2^8\left(\frac{1+\sqrt{d}}{2}\right)$. The "proper" selection of h cube roots is tested by the condition that $\sum_{k=1}^{h} \sqrt[3]{\alpha_k}$ becomes a rational integer. There are $3^{(h-1)/2}$ sums to be tested. Denote by $\prod_{r=1}^{h}(x - \sqrt[3]{\alpha_r}) = 0$ the equation with integer coefficients thus produced.*

Step 4. *Compute the square roots of $\sqrt[3]{\alpha_r}$ for $r = 1, \cdots, h$. From the set of $2h$ numbers, make the "correct" selection of h sixth roots in such a way that one of the roots is $f_2^4\left(\frac{1+\sqrt{d}}{2}\right)$. The "correct" selection is tested by the condition that the sum $\sum_{s=1}^{h} \sqrt[6]{\alpha_s}$ becomes a rational integer. There are $2^{(h-1)/2}$ sums to be tested. Denote by $\prod_{s=1}^{h}(x - \sqrt[6]{\alpha_s}) = 0$ the equation with integer coefficients thus obtained.*

Step 5. *Repeat the same procedure as in Step 4 to get the "correct" h twelfth roots $\sqrt[12]{\alpha_s}$ in such a way that one of the roots is $f_2^2\left(\frac{1+\sqrt{d}}{2}\right)$. The resulting equation must have integer coefficients of degree h. There are $2^{(h-1)/2}$ sums to be tested. Denote by $\prod_{t=1}^{h}(x - \sqrt[12]{\alpha_t}) = 0$ the equation thus obtained.*

Step 6. *Repeat the same procedure as in Step 5 to get the "correct" h twenty-fourth roots $\sqrt[24]{\alpha_t}$ in such as way that one of the roots is $f_2\left(\frac{a+\sqrt{d}}{2}\right)$. To get the equation of degree h with integer coefficients, there are $2^{(h-1)/2}$ sums to be tested.*

The equation thus produced is nothing but $h_d(x) = 0$ or its reciprocal $x^h h_d(1/x) = 0$.

The correct selection processes in Step 3 - Step 6 require exponential computational time.

(B2.2) A refinement of the method of Weber-Watson.

Step 1. *Construct the genuine class equation $H_d(x)$ for an imaginary quadratic order $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d \equiv 1\ (mod\ 8)$ and $3 \nmid d$ with class number h.*

Step 2. *Make the change of variable* $x \to (x-16)^3/x$ *in* $H_d(x)$. *Factor out the integral irreducible polynomial of degree* h *from* $x^h H_d((x-16)^3/x)$, *and call it* $h_d^*(x)$.

Step 3. *Repeat the same Steps 3-6 of (B2.1) for* $h_d^*(x)$.

The difference from the method of Weber-Watson is that we replace the first two steps by the construction of the genuine class equations. However, by doing this, we don't gain any computational time.

B3 The construction of the "reduced" class equations by integer lattice reduction.

Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d < 0$ be an imaginary quadratic order of discriminant $d = d_k f^2,\ 3 \nmid d$ and class number h. Let $f(z),\ f_1(z)$ and $f_2(z)$ be the Weber functions. They are modular functions of higher level. Consider the values $f(\tau),\ f_1(\tau)$ and $f_2(\tau)$ at imaginary quadratic arguments τ belonging to an imaginary quadratic order $\mathcal{O}$. Then under certain circumstances, these values do lie in the field $\mathbb{Q}(\tau,\ j(\tau))$. When that happens, $f(\tau),\ f_1(\tau)$ and $f_2(\tau)$ are also called class invariants of $\mathcal{O}$.

Here we describe an algorithm for the construction of "reduced" class equations of imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d = d_k f^2 < 0$ with $3 \nmid d$. Put

$$D = \begin{cases} d/4 & if \quad d \equiv 0 \pmod 4 \\ d & if \quad d \equiv 1 \pmod 4 \end{cases}$$

Our algorithm of constructing the "reduced" class equations is generic in the sense that it works for arbitrary imaginary quadratic order with D square-free, if a real class invariant of $\mathcal{O}$ is provided.

(B3.1) The Class Invariants. The class invariants for imaginary quadratic orders $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d = d_K f^2 < 0$ with $3 \nmid d$ are listed as follows. ($D = d/4$ if $d \equiv 0 \pmod 4$, d if $d \equiv 1 \pmod 4$).

D or d	the class invariant of $\mathcal{O}$
$d \equiv 1 \pmod 8$	$f(\sqrt{d})/\sqrt{2}$
$d \equiv 5 \pmod 8$	$f(\sqrt{d}$
$D \equiv 2 \pmod 8$	$f_1(\sqrt{D})^2/\sqrt{2}$
$D \equiv 3 \pmod 8$	$f(\sqrt{D})^4$
$D \equiv 6 \pmod 8$	$f_1(\sqrt{D})^2/\sqrt{2}$
$D \equiv 7 \pmod 8$	$f(\sqrt{D})^2/\sqrt{2}$

Our class invariants differ slightly from those of Weber [W, §127].

The following theorem will govern the algorithm for constructing the reduced class equations.

(B3.2) Theorem. *Let* $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d < 0$ *be an imaginary quadratic order with discriminant* $d,\ 3 \nmid d$ *and class number* h. *Let* $h_d(x) := x^h + a_{h-1}x^{h-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *be the reduced class equation of* $\mathcal{O}$. *Let* $||h_d||$ *denote the Euclidean norm of* h_d:

$$||h_d|| := \sqrt{1 + a_{h-1}^2 + \cdots + a_0^2}.$$

For any real number α, let $\{\alpha\}$ denote the closest integer to α. Let ζ be a real root of $h_d(x)$, and let C be a real constant such that

$$C \geq 2^{(h+1)^2} ||h_d||_2^{2h+1} \frac{|\zeta|^h - 1}{|\zeta| - 1} .$$

Consider the $h+2$ dimensional lattice spanned by the columns of

$$L = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ C & \{C\zeta\} & \{C\zeta^2\} & \cdots & \{C\zeta^h\} \end{pmatrix} .$$

Then the only short vector in this lattice, that is, a vector of Euclidean length within a factor of $2^{h/2}$ of the shortest vector in the lattice, is the vector

$$L \times \begin{pmatrix} a_0 \\ \vdots \\ a_{h-1} \\ 1 \end{pmatrix}$$

Proof. See [Sc], [K-L-L], [K1], and [Ka].

(B3.3) The algorithm. We now can describe our algorithm. We first approximate a real root ζ of $h_d(x)$ to sufficiently high floating point precision using the class invariant of $\mathcal{O}$ in the table in (B3.1). We obtain the values of the Weber functions f, f_1 and f_2 by their relations to the η function given in (B1.1). We approximate the η function by its Taylor series in q given in (A1.2). Notice that we use a Horner evaluation scheme for the truncated series (see the Macsyma code listed below). One also must choose a floating point precision, in Macsyma, the variable FPPREC. We chose this precision typically $50 + h \log_{10}(C\zeta)$.

The lattice reduction algorithm of [L-L-L] can now produce a short vector for the lattice L in the above theorem (B3.2). This vector will contain as its first $h+1$ components the coefficients of $h_d(x)$. However, it turns out that the estimate for C is likely to be much too large among the multipliers that still guarantee that the reduction algorithm produces the correct answer. Therefore, we chose C individually and tried. If the discriminant of the candidate polynomial exhibited the factorization pattern predicted, in particular, if it splits into primes no larger than $-d$, we knew that the short vector corresponded to the polynomial $h_d(x)$. Otherwise we increased C and tried again. In the code listed below, C is chosen $10^{LLLPREC}$, and for our large cases we incremented LLLPREC by 25 for each new attempt.

Finally, the lattice reduction algorithm itself needs mention. We used a version where the $\mu_{i,j}$ are kept as pairs of integral numerators $K_{i,j}$ and denominators d_j (cf. [L-L-L], 1.29). This replaces the numerator and denominator reduction by the greatest common divisor in the rational number arithmetic by exact integer division. Furthermore, we used special formulae to compute the initial quantities $k_{i,j}$ and d_j, i.e.,

the Gram-Schmidt orthonormalization, of the lattice L in the above theorem (B3.2) (cf. [K-McG] and [K1]). We also experimented with selected other improvement, such as modular number arithmetic [K1]. We also experimented with selected other improvement, such as modular number arithmetic [K2], but none of these significantly improved the performance of the algorithm.

Following is a table of discriminants, together with the needed LLLPREC and the total time it took on our Symbolics 3670 to compute $h_d(x)$. For all computations used a Taylor approximation of η to order 126. Actually, the time for the computation of an approximation of ζ for larger class numbers is insignificant compared to the time for the lattice reduction. We also list the number of times the lattice reduction algorithm swaps two basis vectors (Step (2) of Fig. 1 in [L-L-L]), which is a good machine-independent measure of the complexity of our method.

D or d	h	d(mod 8)	D(mod 8)	LLLPREC	# Swaps	CPU-TIME
-221	16		3	100	2135	1830 secs.
-194	20		6	100	2804	2210 secs.
-209	20		7	100	2847	2450 secs.
-326	22		2	100	3141	2940 secs.
-647	23	1		100	3267	2760 secs.
-419	9	5		100	4186	5320 secs.
-887	29	1		100	4224	4940 secs.
-719	31	1		100	4681	5860 secs.
-1487	37	1		150	8326	26700 secs.
-1151	41	1		150	9575	32100 secs.
-1847	43	1		175	11674	56600 secs.

Here $D = d$ if $d \equiv 1 \pmod 4$ and $d/4$ if $d \equiv 0 \pmod 4$.

(B3.4) Algorithm (continued). Following is the listing of the Macsyma functions used to compute the equation. These functions require a callable lattice reduction algorithm.

```
/* -*- Mode: MACSYMA -*- */
eta(z):=block([q,q2,q3,q4,q5,q6,q7,q8,q9,q11,q13,q15,q17,eta],
      q: bfloat(exp(rectform(2*%pi*%i*z))),
      /* Horner evaluation of 1+sum((-1)^n*(q^(n(3*n-1)/2)+q^(n(3*n+1)/2)),n).
         This is currently done to order O(q^127). */
      q2: rectform(q^2), q3: rectform(q2*q), q4: rectform(q2*q2),
      q5: rectform(q3*q2), q6: rectform(q3*q3), q7: rectform(q5*q2),
      q8: rectform(q4*q4), q9: rectform(q4*q5), q11: rectform(q5*q6),
      q13: rectform(q6*q7), q15: rectform(q7*q8), q17: rectform(q8*q9),
      eta: rectform(q8*(rectform(q17*(-q9-1)+1)+1)),
      eta: rectform(q11*rectform(q6*rectform(q13*rectform(q7*rectform(q15*
           eta-1)-1)+1)+1)),
      eta: rectform(q4*rectform(q9*rectform(q5*rectform(
           eta - 1) - 1) + 1)),
      eta: rectform(q5*rectform(q3*rectform(q7*rectform(
           eta + 1) - 1) - 1) + 1),
      eta: rectform(q*rectform(q*rectform(q3*rectform(q2*
           eta + 1) - 1) - 1) + 1),
      rectform(eta*q^(1/24)))$
/* The Weber functions. */
f0(z):=block(
      /* Weber's f(z) */
      t1: bfloat(rectform(exp(-%pi*%i/24))),
      t2: eta((z+1)/2),
```

```
      t3: eta(z),
      realpart(rectform(t1*t2/t3)))$
f1(z):=rectform(eta(z/2)/eta(z))$
f2(z):=rectform(bfloat(sqrt(2))*eta(2*z)/eta(z))$
quadforms(m):=block(
   /* Compute all primitive reduced quadratic forms of Q(sqrt m), m < 0,
      squarefree. Quadforms returns a list [[a1,b1,c1],...,[ah,bh,ch]]
      where ai*x^2+bi*x*y+ci*y^2 are the reduced forms and h is the
      class number. */
   [a, b, c, ac, d, f],
   if remainder(-m,4)=3 then d: m else d: 4*m,
   f: [],
   for b: 0 thru sqrt(-d/3) do
       if remainder(b^2-d,4)=0 then
          (ac: (b^2-d)/4,
           for a: max(1, b) thru sqrt(ac) do
               (if remainder(ac, a)=0 then
                   (c: quotient(ac, a),
                    f: endcons([a,b,c], f),
                    if b # 0 and b < a and a < c then f: endcons([a,-b,c],f))
          )    ),
    return(f))$
rootlatt(r, d, rp):=block([lat, lcol, redlat, f, i],
    /* Find the minimal polynomial for the bfloat root r of degree d using
LLL; */
    /* rp is the multiplier to be used in the last row for LLL to converge
       to the root. */
    /* This function only sets up the lattice. */
    lat: ident(d+1),
    lcol: zeromatrix(1,d+1),
    for i: 0 thru d do lcol[1,i+1]: entier(rp*r^i),
    lat: addrow(lat, lcol),
    return(lat))$
watson(d):=block([h, /* classnumber of Q[sqrt(d)] */
                  rr, /* real root of the Watson equation */
                  L, /* lattice for rr */
                  f, i, delta],
     /* This function (currently) needs the following global settings: */
     /*    FPPREC: The floating point precision in the real root
computation */
     /*    LLLPREC: The multiplier used in the lattice construction */
     h: length(quadforms(d)),
     if verbose then print("Classnumber of ",d," is ",h),
     /* Computation of the singular moduli, the real roots of the reduced
equ's. */
     if remainder(d,8) = -7 then rr: bfloat(f0(sqrt(d))/sqrt(2)),
     if remainder(d,8) = -6 then rr: bfloat(f1(sqrt(d))^2/sqrt(2)),
     if remainder(d,8) = -2 then rr: bfloat(f1(sqrt(d))^2/sqrt(2)),
     if remainder(d,8) = -1 then rr: bfloat(f0(sqrt(d))^2/sqrt(2)),
     if remainder(d,8) = -3 then (rr: bfloat(f0(sqrt(d))), h: 3*h),
     if remainder(d,8) = -5 then rr: bfloat(f0(sqrt(d))^4),
     /* All other cases are not maximal orders */
     if verbose then print("Real root found:",rr),
     L: rootlatt(rr,h,10^LLLPREC),
     if verbose then print("Lattice: ",L),
     if verbose then print("Starting lattice reduction"),
     /* Call the lattice reduction algorithm (coded in Lisp) */
     LL: latticereduction(L,true), /* second argument true indicates to use
                                      special Gram-Schmidt code */
     if verbose then print("Done lattice reduction"),
     if verbose then print("Reduced Lattice",LL),
     f: 0, for i: 1 thru h+1 do f: f+LL[i,1]*x^(i-1),
     delta: poly_discriminant(f,x),
     /* Test whether discriminant of field divides discriminant of equation */
     if remainder(delta, d) # 0 then
     print("Failed to find classequation, increase order for eta, FPPREC,
or LLLPREC")
     else if verbose then print("Discriminant ",factor(delta)),
     return(f))$
```

B4 Analysis of the "reduced" class equations.

Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d = d_K f^2 < 0,\ 3 \nmid d$ be an imaginary quadratic order of discriminant d with class number h. As we have seen in Theorem (A2.1)(1), the constant term and the discriminant of the level one class equation $H_d(x)$ are highly divisible numbers. In fact, if ℓ is a prime dividing $H_d(0)$, then $\left(\frac{d}{\ell}\right) \neq 1$ and $\ell \leq \frac{3|d|}{4}$, and if ℓ is a prime dividing the discriminant $\Delta(H_d)$, then $\left(\frac{d}{\ell}\right) \neq 1$ and $\ell \leq |d|$.

We have the corresponding results for the constant term and the discriminant of the higher level class equation $h_d(x)$.

(B4.1) Theorem. *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d}),\ d < 0,\ d \equiv 1\ (mod\ 8)$ and $3 \nmid d$ be an imaginary quadratic order with discriminant d and with class number h. Let $h_d(x)$ denote the "reduced" class equation of $\mathcal{O}$ constructed in (B1.1). Then,*

(a) $h_d(0) = (-1)^h$

(b) *If ℓ is a prime dividing the discriminant $\Delta(h_d)$ of h_d, then $\left(\frac{d}{\ell}\right) \neq 1$ and $\ell \leq |d|$.*

Furthermore,

$$\Delta(h_d) = i^2(-d)^{\frac{h-1}{2}}$$

where i is the index of the order $\mathbb{Z}[f_2]$ in the ring of integers of $\mathbb{Q}(f_2(\tau)),\ \tau \in \mathcal{O}$ where $f_2(z)$ is the Weber function defined in (B1.1), and i divides the index I of Theorem (A2.1)(1), and hence $\Delta(h_d)|\Delta(H_d)$.

(B4.2) Example. Let $H_d(x)$ be the genuine class equation of $\mathcal{O}$. By a theorem of Gross-Zagier, $H_d(0)$ and the discriminant $\Delta(H_d)$ factor very highly with prime factors smaller than or equal to $-d$. It remains to clarify why the reduced equation $h_d(x)$ loses almost all the factors appearing in $H_d(0)$ and $\Delta(H_d)$. For example, consider the genuine and reduced class equations of the maximal imaginary quadratic order $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{-271})$. $\mathcal{O}_K$ has class number $h(-271) = h = 11$. As our computations show, $H_{-271}(x)$ has

$$H_{-271}(0) = (3^{11}23^2 29^2 47 \cdot 71 \cdot 113 \cdot 131 \cdot 173 \cdot 191 \cdot 197)^3$$

and

$$\begin{aligned}\Delta(H_{-271}) = \quad & -3^{732}13^{110}19^{70}23^{48}29^{38}43^{30}47^{20}59^{22}71^{10}73^{12}97^8 \\ & \times 101^8 107^6 109^6 113^6 127^8 131^{10} 137^4 149^4 173^4 181^4 191^8 \\ & \times 197^2 199^4 227^6 239^6 251^6 257^4 263^4 269^2 271^5.\end{aligned}$$

While the reduced class equation $h_{-271}(x)$ has

$$h_{-271}(0) = -1$$

and

$$\Delta(h_{-271}) = -3^6 13^2 19^2 271^5\ .$$

(B4.3) The discriminants of the reduced class equations. Let d_1 and d_2 be fundamental discriminants of quadratic forms. Let $g(z)$ denote one of the class invariants defined in (B3.1). Suppose that

$\tau_1, \tau_2 \in \mathcal{F}$ belong to two distinct imaginary quadratic fields of discriminants d_1 and d_2, respectively. Then the absolute value of the norm of difference $g(\tau_1) - g(\tau_2)$, i.e.,

$$|\mathrm{Norm}(g(\tau_1) - g(\tau_2))|$$

is a highly divisible number, and its prime factors ℓ satisfy the conditions

$$\left(\frac{d_1}{\ell}\right) \neq 1 \text{ and } \left(\frac{d_2}{\ell}\right) \neq 1,$$

and $|\mathrm{Norm}(g(\tau_1) - g(\tau_2))|$ divides $|\mathrm{Norm}(j(\tau_1) - j(\tau_2)|$.

It is expected that there is a Gross-Zagier type formula for the discriminants $\Delta(h_d)$ of the reduced class equations $h_d(x)$.

On the height $||h_d||$ of the reduced class equation $h_d(x)$, we have the following results.

(B4.4) Proposition. *Let $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $d_K f^2$ and $3 \nmid d$ be an imaginary quadratic order with class number h. Let $D = d/4$ if $d \equiv 0 \pmod 4$ and d if $d \equiv 1 \pmod 4$. Let $h_d(x)$ be the reduced class equation of $\mathcal{O}$ and let $ht(h_d) = \log ||h_d||$ be its height. If $h_d(x) = \prod (x - \alpha_i) \in \mathbb{C}[x]$, let $M = \prod_i \max(1, |\alpha_i|)$. Then $M \geq 1$.*

(a) *Assume that $d \equiv 1 \pmod 8$. Then $h_d(x)$ is of degree h with the constant term $(-1)^h$, and*

$$ht(h_d) \leq h \log 2 + \log h + \log M.$$

(b) *Assume that $d \equiv 5 \pmod 8$. Then $h_d(x)$ is of degree $3h$ with the constant term $(-2)^h$, and*

$$ht(h_d) \leq (3h) \log 2 + \log(3h) + \log M$$

(c) *Assume that $D = \frac{d}{4} \equiv 2, 6$ or $7 \pmod 8$. Then $h_d(x)$ is of degree h with the constant term ± 1, and*

$$ht(h_d) \leq h \log 2 + \log h + \log M.$$

(d) *Assume that $D = \frac{d}{4} \equiv 3 \pmod 8$. Then $h_d(x)$ is of degree h with the constant term $\pm 2^h$, and*

$$ht(h_d) \leq h \log 2 + \log h + \log M \ .$$

Proof. If $h_d(x)$ is of degree h, write

$$h_d(x) = x^h + a_{h-1}x^{h-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \ .$$

Then

$$||h_d|| \leq \sqrt{1 + a_{h-1}^2 + \cdots + a_1^2 + a_0^2} \leq 1 + \sum_{i=0}^{h-1} |a_i| \ .$$

Furthermore, for each i,

$$|a_i| \leq \left(\begin{array}{c} h-1 \\ i \end{array} \right) M + \left(\begin{array}{c} h-1 \\ i-1 \end{array} \right) \leq \left(\begin{array}{c} h \\ i \end{array} \right) M < 2^h M \ .$$

(a) *In this case,* $a_0 = (-1)^h$ *and*

$$||h_d|| \leq 2 + \sum_{i=1}^{h-1} |a_i| \leq 2 + (h-1)2^h M < 2^h M \ .$$

(b) *In this case* $h_d(x)$ *is of degree* $3h$.

Write

$$h_d(x) = x^{3h} + a_{3h-1}x^{3h-1} + \cdots + a_1 x + (-2)^h \in \mathbb{Z}[x] \ .$$

Then

$$\begin{aligned} ||h_d|| &\leq 1 + 2^h + \sum_{i=1}^{3h-1} |a_i| \leq 1 + 2^h + (3h-1)2^{3h} M \\ &\leq 3h \cdot 2^{3h} M \ . \end{aligned}$$

(c) *In this case,* $a_0 = (-1)^h$ *and*

$$||h_d|| \leq 2 + \sum_{i=1}^{h-1} |a_i| \leq 2 + (h-1)2^h M < h2^h M \ .$$

(d) *In this case,* $a_0 = \pm 2^h$ *and*

$$\begin{aligned} ||h_d|| &\leq 1 + 2^h + \sum_{i=1}^{h-1} |a_i| \leq 1 + 2^h + (h-1)2^h M \\ &\leq h\ 2^h M \ . \end{aligned}$$

B5 Tables of the "reduced" class equations.

We tabulate selected examples of the "reduced" class equations.

Table 1: The reduced class equation for $d \equiv 1 \pmod 8$

d	h	$h_d(X)$	$\Delta(h_d)$
-647	23	$X^{23} - 20X^{22} + 3X^{21} + 37X^{20} + 46X^{19} - 2X^{18} - 151X^{17} - 384X^{16} - 610X^{15} - 849X^{14} - 995X^{13} - 955X^{12} - 798X^{11} - 596X^{10} - 378X^9 - 202X^8 - 75X^7 + 21X^5 + 19X^4 + 13X^3 + 3X^2 - 2X - 1$	$-5^{22}11^6 19^4 37^4 \times 199^2 439^2 647^{11}$
-887	29	$X^{29} - 32X^{28} - 98X^{27} - 95X^{26} + 265X^{25} + 6X^{24} - 13X^{23} - 247X^{22} + 268X^{21} - 349X^{20} + 413X^{19} - 405X^{18} + 574X^{17} - 839X^{16} + 866X^{15} - 953X^{14} + 951X^{13} - 820X^{12} + 758X^{11} - 628X^{10} + 447X^9 - 336X^8 + 217X^7 - 115X^6 + 70X^5 - 29X^4 + 7X^3 - 7X^2 - X - 1$	$5^{16}17^6 23^8 29^2 31^8 \times 89^2 97^6 103^2 211^2 \times 439^2 563^2 691^2 887^{14}$
-719	31	$X^{31} - 26X^{30} + 53X^{29} + 68X^{28} - 168X^{27} - 176X^{26} + 161X^{25} + 172X^{24} - 175X^{23} - 440X^{22} - 341X^{21} - 169X^{20} - 293X^{19} - 255X^{18} - 57X^{17} - 9X^{16} - 114X^{15} - 157X^{14} - 21X^{13} + 68X^{12} + 59X^{11} + 20X^{10} + 37X^9 + 29X^8 + 36X^7 + 24X^6 + 20X^5 - X^4 - 11X^3 - 11X^2 - 4X - 1$	$-11^4 17^{10} 19^2 23^2 \times 41^2 43^2 71^2 73^8 79^4 \times 97^2 127^2 139^4 271^2 \times 523^2 619^2 719^{15}$
-1487	37	$X^{37} - 110X^{36} + 7X^{35} - 1660X^{34} + 2145X^{33} - 3216X^{32} + 5894X^{31} - 5958X^{30} + 1958X^{29} - 3622X^{28} + 1289X^{27} + 149X^{26} - 2612X^{25} + 2051X^{24} + 922X^{23} - 450X^{22} - 3003X^{21} + 575X^{20} + 597X^{19} - 2300X^{18} + 67X^{17} + 870X^{16} + 192X^{15} - 1075X^{14} + 151X^{13} + 180X^{12} - 400X^{11} - 335X^{10} + 72X^9 + 31X^8 - 97X^7 - 97X^6 - 26X^5 - 38X^4 - 42X^3 - 24X^2 - 6X - 1$	$5^{42} 13^{10} 19^{10} 29^8 41^8 \times 53^2 59^4 61^4 89^2 \times 157^4 191^2 257^4 \times 331^2 337^2 463^2 \times 523^2 619^4 1039^2 \times 1163^2 1291^2 1487^{18}$
-1151	41	$X^{41} - 64X^{40} + 242X^{39} - 128X^{38} + 67X^{37} - 1356X^{36} - 1996X^{35} + 1602X^{34} + 1673X^{33} + 4366X^{32} - 273X^{31} - 6530X^{30} - 197X^{29} + 10X^{28} + 1681X^{27} + 716X^{26} - 2057X^{25} + 885X^{24} + 2067X^{23} + 291X^{22} - 1309X^{21} - 210X^{20} - 327X^{19} + 197X^{18} + 144X^{17} - 100X^{16} - 33X^{15} + 207X^{14} + 33X^{13} - 229X^{12} + 128X^{11} - 26X^{10} + 49X^9 + 32X^8 - 50X^7 - 59X^6 + 65X^5 + 3X^4 - 20X^3 - 2X^2 + 5X - 1$	$13^{28} 17^{16} 19^{12} 23^4 \times 31^4 41^4 61^6 71^2 73^2 \times 97^4 127^2 137^2 191^4 \times 251^2 281^2 367^2 \times 379^2 431^2 571^4 \times 751^2 827^2 1051^2 \times 1151^{20}$
-1847	43	$X^{43} - 196X^{42} - 13X^{41} - 4673X^{40} + 5250X^{39} - 20238X^{38} + 13122X^{37} - 38978X^{36} + 9561X^{35} - 42114X^{34} + 5753X^{33} - 25633X^{32} - 3134X^{31} - 7110X^{30} - 11340X^{29} - 12064X^{28} - 303X^{27} - 4565X^{26} + 570X^{25} + 443X^{24} + 5283X^{23} - 1129X^{22} - 1067X^{21} - 268X^{20} + 1033X^{19} - 732X^{18} + 606X^{17} + 1854X^{16} - 1112X^{15} - 900X^{14} + 142X^{13} - 725X^{12} - 768X^{11} + 440X^{10} + 375X^9 - 185X^8 - 42X^7 + 17X^6 - 172X^5 - 170X^4 - 44X^3 + 2X^2 - X - 1$	$-5^{60} 17^{10} 19^8 31^8 \times 43^2 47^{10} 53^8 61^4 \times 73^4 83^2 109^2 127^6 \times 149^4 257^4 401^4 \times 409^2 499^2 659^4 \times 823^2 883^2 1063^2 \times 1171^2 1399^2 \times 1459^2 1523^2 1847^{21}$

Table 2: The reduced class equation for $d \equiv 5 \pmod 8$

d	h	$h_d(X)$	$\Delta(h_d)$
-179	5	$X^{15} - 20X^{13} - 62X^{12} - 76X^{11} - 32X^{10} + 16X^9 + 8X^8 - 64X^7 - 160X^6 - 176X^5 - 96X^4 - 16X^3 + 32X^2 - 32$	$-2^{94} 11^2 79^2 179^7$
-587	7	$X^{21} - 24X^{20} + 12X^{19} - 186X^{18} - 236X^{17} - 192X^{16} - 652X^{15} - 1464X^{14} - 528X^{13} - 1272X^{12} - 1952X^{11} + 384X^{10} + 688X^9 - 896X^8 + 2112X^7 + 2208X^6 - 960X^5 + 960X^3 - 1664X^2 + 256X - 128$	$2^{198} 5^{16} 13^2 23^4 41^2 \times 97^2 139^2 263^2 331^2 \times 587^{10}$

-419	9	$X^{27}-18X^{26}+54X^{25}-58X^{24}-16X^{23}-192X^{22}+608X^{21}-752X^{20}+800X^{19}-1376X^{18}+2592X^{17}-2752X^{16}+3680X^{15}-5696X^{14}+5568X^{13}-7616X^{12}+8192X^{11}-9728X^{10}+11008X^{9}-8960X^{8}+13312X^{7}-10240X^{6}+8704X^{5}-9216X^{4}+3328X^{3}-4608X^{2}+1536X-512$	$-2^{318}11^{6}17^{4}19^{6}\times 31^{2}89^{2}127^{2}163^{2}\times 211^{2}223^{2}419^{13}$

Table 3: The reduced class equation for $d=4D$ with $D\equiv 2 \pmod 8$

D	h	$h_d(X)$	$\Delta(h_d)$
-62	8	$X^8-2X^7-13X^6-30X^5-36X^4-30X^3-13X^2-2X+1$	$-2^{20}5^{4}31^{3}$
-86	10	$X^{10}-8X^9+2X^8-18X^7+9X^6-4X^5-9X^4-18X^3-2X^2-8X-1$	$2^{49}13^{4}43^{4}$
-134	14	$X^{14}-12X^{13}-34X^{12}-66X^{11}-37X^{10}-76X^9-3X^8-126X^7+3X^6-76X^5+37X^4-66X^3+34X^2-12X-1$	$2^{85}7^{4}29^{2}41^{4}67^{6}$
-206	20	$X^{20}-30X^{19}-13X^{18}+118X^{17}+204X^{16}-794X^{15}+141X^{14}+1238X^{13}-753X^{12}-948X^{11}+1656X^{10}-948X^9-753X^8+1238X^7+141X^6-794X^5+204X^4+118X^3-13X^2-30X+1$	$-2^{162}13^{12}29^{8}47^{4}103^{9}$
-326	22	$X^{22}-88X^{21}+674X^{20}-1970X^{19}+2377X^{18}-1348X^{17}+913X^{16}-3458X^{15}+2578X^{14}-4108X^{13}+233X^{12}-6504X^{11}-233X^{10}-4108X^9-2578X^8-3458X^7-913X^6-1348X^5-2377X^4-1970X^3-674X^2-88X-1$	$2^{217}7^{8}17^{8}61^{4}73^{4}\times 83^{4}89^{4}137^{4}163^{10}$

Table 4: The reduced class equation for $d=4D$ with $D\equiv 3 \pmod 8$

D	h	$h_d(X)$	$\Delta(h_d)$
-53	6	$X^6-46X^5+48X^4-600X^3-192X^2-736X-64$	$2^{54}5^{6}53^{3}$
-221	16	$X^{16}-2380X^{15}-51556X^{14}-274960X^{13}-12528X^{12}-10574592X^{11}+5908352X^{10}-21593600X^9-30432768X^8+86374400X^7+94533632X^6+676773888X^5-3207168X^4+281559040X^3-211173376X^2+38993920X+65536$	$2^{404}7^{20}11^{4}13^{12}17^{16}\times 29^{8}31^{4}61^{4}113^{4}\times 149^{2}181^{4}$

Table 5: The reduced class equation for $d = 4D$ with $D \equiv 6 \pmod 8$

D	h	$h_d(X)$	$\Delta(h_d)$
-26	6	$X^6 - 2X^5 - 2X^4 + 2X^2 - 2X - 1$	$2^{12}13^3$
-146	16	$X^{16} - 22X^{15} + 99X^{14} - 190X^{13} + 177X^{12} - 88X^{11} - 34X^{10} + 228X^9 - 374X^8 + 228X^7 - 34X^6 - 88X^5 + 177X^4 - 190X^3 + 99X^2 - 22X + 1$	$-2^{111}17^4 23^4 73^8$
-194	20	$X^{20} - 26X^{19} - 23X^{18} - 190X^{17} - 36X^{16} - 190X^{15} + 103X^{14} - 230X^{13} - 81X^{12} - 132X^{11} + 584X^{10} - 132X^9 - 81X^8 - 230X^7 + 103X^6 - 190X^5 - 36X^4 - 190X^3 - 23X^2 - 26X + 1$	$-2^{181}17^8 41^4 47^4 97^{10}$

Table 6: The reduced class equation for $d = 4D$ with $D \equiv 7 \pmod 8$

D	h	$h_d(X)$	$\Delta(h_d)$
-193	4	$X^4 - 26X^3 - 22X^2 - 26X + 1$[*]	$-2^{12}3^2 193^2$
-41	8	$X^8 - 5X^7 + 7X^6 - 12X^5 + 14X^4 - 12X^3 + 7X^2 - 5X + 1$	$-2^{16}41^4$
-89	12	$X^{12} - 5X^{11} - 21X^{10} - 50X^9 - 65X^8 - 81X^7 - 70X^6 - 81X^5 - 65X^4 - 50X^3 - 21X^2 - 5X + 1$	$-2^{62}89^6$
-209	20	$X^{20} - 34X^{19} + 93X^{18} - 124X^{17} + 292X^{16} - 420X^{15} - 69X^{14} - 710X^{13} - 1289X^{12} - 752X^{11} - 2168X^{10} - 752X^9 - 1289X^8 - 710X^7 - 69X^6 - 420X^5 + 292X^4 - 124X^3 + 93X^2 - 34X + 1$	$2^{166}11^{14}17^4 19^{10} \times 23^4 97^4$

[*]This polynomial has appeared in D. Shanks: *Dihedral quartic approximations and series for* π, J. Number Theory 14, No. 3, (1982), pp. 397–423.

ACKNOWLEDGMENTS

We wish to thank all colleagues who commented on earlier versions of this paper. We are, especially, indebted to Harvey Cohn for his encouragement and interest, David Cox for his constructive criticisms, David and Gregory Chudnovsky for their bringing the works of Watson to our attention, and Don Zagier for his generous help in constructing "genuine" and "reduced" class equations. And last but not least, we thank François Morain for his critical and constructive comments, in particular, on the Atkin primality test.

Susan G. Clark has kindly retyped this paper in LaTeX (added on February 22, 2001).

References

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

[B-C-H-I-S] Borel, A., Chowla, S., Herz, C.S., Iwasawa, K., and Serre, J.P., Seminar on Complex Multiplication, Lecture Notes in Mathematics 21 (1966), Springer-Verlag.

[B-J-Y] Bruen, A., Jensen, C. U., and Yui, N., Polynomials with Frobenius groups of prime degree as Galois Groups II, Journal of Number Theory 24 (1986), pp. 305-359.

[C] Cohn, H., Introduction to the Construction of Class Fields, Cambridge Studies in Advanced Mathematics 6, Cambridge University Press, 1985.

[Cx] Cox, David, Primes of the form $x^2 + ny^2$: From Fermat to Class Field Theory and Complex Multiplication, John Wiley and Sons (1989) (to appear). [1989, xiv+351 pp.]

[D1] Deuring, M., Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung, Commentarii Mathematici Helvetici 19 (1946), pp. 74-82.

[D2] ———————, Die Klassenkörper der komplexen Multiplikation, Enzyklopädie Math. Wiss, 12 (Book 10, Part II), Teubner, Stuttgart 1958.

[Do1] Dorman, D., Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(z)]$ in $\mathbb{Q}(j(z))$, Math. Ann. 283 (1989), pp. 177-191.

[Do2] Dorman, D., Special values of the elliptic modular function and factorization formulae, J. Reine Angew. Math. 383 (1988), pp. 207-220.

[G] Goldfeld, D., Gauss' class number problem for imaginary quadratic fields, Bull. American Math. Soc. (New Series) 13 (1985), pp. 23-37.

[G-K] Goldwasser, S., and Kilian, J., Almost all primes can be quickly certified, Proc. 18th Annual ACM Symp. on Theory of Computing (1986), pp. 316-329.

[G-Z1] Gross, B., and Zagier, D., On singular moduli, J. Reine Angew. Math. 355 (1985), pp. 191-220.

[G-Z2] Gross, B., and Zagier, D., Heegner points and derivatives of L-series, Invent. math. 84 (1986), pp. 225-320.

[H] Hanna, M., The modular equations, Proc. London Math. Soc. (2) 28 (1928), pp. 46-52.

[He] Hermann, O., Über die Berechnung der Fouriercoeffizienten der Funktion $j(\tau)$, J. Reine Angew. Math. 274 (1973), pp. 187-195.

[J-Y] Jensen, C. U., and Yui, N., Polynomials with D_p as Galois group, Journal of Number Theory 15 (1982), pp. 347-375.

[K1] Kaltofen, E., On the complexity of finding short vectors in integer lattices, Proc. EUROCAL '83, Lecture Notes in Computer Science 162 (1983), pp. 236-244, Springer-Verlag.

[K2] Kaltofen, E., Polynomial Factorization 1982-1986, Tech. Report 86-19, Dept. Comp. Sci., Rensselaer Polytech. Ins., Sept. (1986).

[K-V-Y] Kaltofen, E., Valente, T., and Yui, N., An improved Las Vegas primality test, ISSAC '89, Portland, Oregon (1989) (to appear). [pp 26-33]

[K-Y1] Kaltofen, E., and Yui, N., Explicit construction of the Hilbert class fields of imaginary quadratic fields with class numbers 7 and 11, EUROSAM '84, Lecture Notes in Computer Science 174 (1984), pp. 310-320, Springer-Verlag.

[K-Y2] Kaltofen, E., and Yui, N., On the modular equations of order 11, Proc. of the 1984 MACSYMA Users Conference (1984), pp. 472-485, General Electric.

[Ka] Kannan, R., Algebraic geometry of numbers, in Annual Review in Computer Science 2, edited by J. F. Traub (1987), pp. 231-67, Annual Reviews Inc.

[K-L-L] Kannan, R., Lenstra, A.K., and Lová, L., Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers, Math. Comp. 50, (1988), pp. 235-250.

[K-McG] Kannan, R. and McGeoch, L. A., Basis reduction and the evidence for transcendence of certain numbers, Manuscript (1984).

[L-L-L] Lenstra, A.K., Lenstra, H.W., and Lovász, L., Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), pp. 515-534.

[L-L] Lenstra, A.K. and Lenstra, H.W., Algorithms in Number Theory, Handbook of Theoretical Computer Science (1989) (to appear).

[M] Mestre, J.F., Courves elliptiques et groupes de classes d'ideaux de certains corps quadratiques, J. Reine Angew. Math. 343 (1983), pp. 23-35.

[Mo] Morain, F., Implementation of the Goldwasser-Kilian-Atkin primality testing algorithm, University of Limoges, INRIA, preprint (1988).

[S] Schertz, R., Die singularen Werte der Weberschen Funktionen, f, f_1, f_2, γ_2, γ_3, J. Reine Angew. Math. 286/287 (1976), pp. 46-47.

[Sc] Schönhage, A., Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm, Proc. ICALP '84, Lecture Notes in Computer Science 172 (1984), pp. 436-447, Springer-Verlag.

[Sm] Smith, H. J. S., Note on the modular equation for the transformation of the third order, Proc. London Math. Soc. 10 (1878), pp. 87-91.

[W1] Watson, G. N., Singular moduli (1), Quart. J. Math. 3 (1932), pp. 81-98.

[W2] Watson, G. N., Singular moduli (2), ibid. 3 (1932), pp. 189-212.

[W3] Watson, G. N., Singular moduli (3), Prod. London Math. Soc. 40 (1936), pp. 83-142.

[W4] Watson, G. N., Singular moduli (4), Acta Arithmetica 1 (1935), pp. 284-323.

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

[Wi] Williamson, C. J., Odd degree polynomials with dihedral Galois groups, Thesis, Berkeley (1989).

Original hand-typed paper ends on page 202.