Werk

Titel: Mathematische Annalen

Verlag: Springer

Jahr: 1989

Kollektion: Mathematica

Werk Id: PPN235181684_0283

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN235181684_0283|LOG_0040

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Math. Ann. 283, 177–191 (1989)

Mathematische Annalen

Singular Moduli, Modular Polynomials, and the Index of the Closure of $\mathbb{Z}[j(\tau)]$ in $\mathbb{Q}(j(\tau))$

David R. Dorman

Department of Mathematics and Computer Science, Middleburg College, Middleburg, VT 05753, USA

1. Introduction

Let τ be an element in the upper half plane and imaginary quadratic over $\mathbb{Q}$. Then τ satisfies an integral quadratic equation $a\tau^2+b\tau+c=0$ with $a, b, c\in\mathbb{Z}$, $(a,b,c)=1$. Denote by $\operatorname{disc}\tau=d=b^2-4ac<0$ the discriminant of τ, $h=h(d)$ the order of the class group of the quadratic order $\mathcal{O}=\mathbb{Z}[(b+\sqrt{d})/2]\subset\mathbb{Q}(\sqrt{d})=K$, and $w=w(d)$ be the number of roots of unity in that order.

The value $j(\tau)$ where j is the elliptic modular function, is called a singular modulus and is an algebraic integer of degree h over $\mathbb{Q}$.

Fix two fundamental negative disriminants d_1 and d_2. Denote by w_i the number of roots of unity in the quadratic order of discriminant d_i, and let h_i denote the class number of those orders.

Three objects of study are:

1. The differences of singular moduli

$$J(d_1,d_2)=\left(\prod_{\substack{[\tau_1][\tau_2]\\ \operatorname{disc}(\tau_1)=d_1\\ \operatorname{disc}(\tau_2)=d_2}}(j(\tau_1)-j(\tau_2))\right)^{4/w_1w_2}. \tag{1.1}$$

Here $[\tau]$ denotes an equivalence class modulo $SL_2(\mathbb{Z})$.

2. The "polynomial"

$$f_d(x)=\left(\prod_{\substack{[\tau]\\ \operatorname{disc}\tau=d/g^2}}(x-j(\tau))\right)^{2/w(d/g^2)}, \tag{1.2}$$

where $[\tau]$ denotes an equivalence class mod $PSL_2[\mathbb{Z}]$. Note that

$$J(d_1,d_2)=\prod_{\substack{[\tau_1]\\ \operatorname{disc}(\tau_1)=d_1}} f_{d_2}(j(\tau_1))^{2/w(d_1)}.$$

3. The m^{th} modular polynomial, $\varphi_m(x,y)\in\mathbb{Z}[x,y]$ defined by

$$\varphi_m(j(z)-j(z'))=\prod_{\substack{\det\gamma=m\\ \bmod SL_2(\mathbb{Z})}}(j(z)-j(\gamma z')). \tag{1.3}$$

This product is taken over all equivalence classes of 2×2 matrices of determinant m, modulo the left action of $SL_2(\mathbb{Z})$.

In [8] Gross and Zagier produced a formula for $\mathrm{ord}_\ell(J(d_1, d_2))$ at a finite rational prime ℓ. Using the formula they then studied f_d and φ_m, with the application of finding the index, I, of $\mathbb{Z}[j(\tau)]$ in its integral closure in $\mathbb{Q}(j(\tau))$. These results, with general relatively prime composite discriminants, were later used in a fundamental way in their paper [7]. They gave algebraic and analytic proofs of their results. However, the algebraic proof was only for the case of prime discriminants.

In [4], generalizing the work of Gross and Zagier, we produced a formula for $\mathrm{ord}_\ell(J(d_1, d_2))$ at a finite rational prime ℓ in the case of relatively prime *composite* discriminants and gave a totally algebraic proof of our theorems. In this paper we use our earlier results and the blueprint provided by Gross and Zagier to generalize the study of φ_m and I to composite discriminants. We also produce a formula for the index I in the case of composite discriminant d.

One simply stated result is any prime λ of either $\mathbb{Q}(\sqrt{d_1})$ or $\mathbb{Q}(\sqrt{d_2})$ dividing $\varphi_m(j(\tau_1) - j(\tau_2))$ must have characteristic $\ell < md_1d_2/4$. A complete description is given in Sect. 4.

The results on the index, I, are quite technical and we must introduce some additional notation. Let d, K, and $\mathcal{O}$ be as in Sect. 1, and for non-negative integers n let $R(n)$ (resp. $r_1(n)$) the number of integral ideals (resp. integral ideals in the principal class) of $\mathcal{O}$ having norm n. Extend both functions to $\mathbb{R}$ by setting $R(x) = r_1(x) = 0$ for arguments other than non-negative integers. For each prime p, finite of infinite, let $\varepsilon_p : \mathbb{Q}_p(\sqrt{d}) \to \{\pm 1\}$ be the local character given by class field theory.

Define

$$\varrho_\ell(n) = \begin{cases} 0 & \text{if there exist two primes } p \mid d \text{ such that} \\ & \varepsilon_p((n - |d|)/n) = -1\,. \\ 2^{a(n)} & \text{otherwise, where } a(n) = \mathrm{Card}\{p \mid (n, d)\}\,. \end{cases}$$

(1.4) **Theorem.** *Let ℓ be a rational prime not dividing d. Then*

$$\mathrm{ord}_\ell(I) = \frac{1}{2} \sum_{n \geqq 0} \sum_{k \geqq 1} \varrho_\ell(n) \cdot (R(n) - r_1(n)) \cdot R\left(\frac{|d| - n}{\ell^k}\right).$$

A more precise form of this theorem extending it to all rational primes is found in Sect. 5.

As in our earlier paper the proofs depend on the interplay between the geometry of supersingular elliptic curves in characteristic ℓ and the arithmetic of orders the definite quaternion algebra ramified at ℓ and ∞. These results can be found in detail in [3, 4] and are collected, without proofs, in Sect. 2 for the convenience of the reader and to introduce notation. Section 3 presents the results of [4] that will be generalized in this paper. Sections 4 and 5 contain the main results of this paper, and Sect. 6 gives a simple example of an index computation. Section 7, the appendix, is devoted to a proof of the formula for the discriminant of $\mathbb{Q}(j(\tau))/\mathbb{Q}$. A formula for the discriminant may be well known, however we could not find it in the literature. Dummit, Gold, and Kisilevsky [5] compute the square free part of this discriminant.

2. Preliminaries

In addition to the notation already given let t be the number of distinct prime factors of the discriminant d. H will denote the Hilbert class field of $K=\mathbb{Q}(\sqrt{d})$, $G=\mathrm{Gal}(H/K)\cong \mathrm{Pic}(\mathcal{O})$, where $\mathrm{Pic}(\mathcal{O})$ is the ideal class group of K. Let χ_d be the primitive quadratic character defined mod d extended to $\mathbb{Z}$ in the usual way. For each $p|d$ let χ_p be the associated quadratic character mod p.

Associated to χ_d is an idèle character $\varepsilon: \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^*\mathbb{N}\mathbb{A}_K^* \to \mathrm{Gal}(K/\mathbb{Q})\cong\{\pm 1\}$. Thus for each prime p of $\mathbb{Q}$ there is a local character $\varepsilon_p: \mathbb{Q}_p \to \mathrm{Gal}(K/\mathbb{Q})$ associated to the extension $\mathbb{Q}_p(\sqrt{d})$. Let

$$\mathrm{Frob}\, p = \begin{cases} 1 & \text{if } p \text{ splits in } K \\ -1 & \text{if } p \text{ remains inert in } K. \end{cases}$$

Then ε_p can be evaluated on any integer n by writing $n = u \cdot p^{a_p}$ where $gcd(p,u)=1$ and letting

$$\varepsilon_p(n) = \begin{cases} \mathrm{sgn}(n) & p=\infty \\ \mathrm{Frob}\, p^{a_p} & p\nmid d \\ \chi_p(u)\chi_{d/p}(p)^{a_p} & p|d \end{cases} . \tag{2.1}$$

The ε_p can be thought of as the genus characters of K. In this language the main theorem of genus theory states

$$\prod_{p|d} \varepsilon_p(\mathbb{N}\mathfrak{a}) = 1 \quad \text{for all ideals } \mathfrak{a} \text{ in } \mathcal{O}. \tag{2.2}$$

Here $\mathbb{N}$ is the absolute norm.

Let ℓ be an inert or ramified prime in K. We now describe maximal orders containing $\mathcal{O}$ and their subrings in the definite quaternion algebra $\mathbb{D}$ defined over $\mathbb{Q}$ ramified only at ℓ and ∞. Details for the following are given in [3].

Assume ℓ is inert in K. Fix a prime q such that for all $p|d\chi_p(-\ell q)=1$. The existence of q is guaranteed by Dirichlet's Theorem. These conditions imply that $q\mathcal{O}=\mathfrak{q}\bar{\mathfrak{q}}$ and that $x^2 \equiv -\ell q \bmod p$ has two solutions for each $p|d$. For each p fix one such solution λ_p. By the Chinese Remainder Theorem we fix a *congruence solution* $\lambda \in \mathbb{Z}$ such that $\lambda \equiv \lambda_p \bmod p$. Then $\mathbb{D}=\{d, -\ell q\}$ (see Vignéras [12] p. 2 for the notation) and can be realized as the subalgebra

$$\mathbb{D} = \left\{ [\alpha,\beta] = \begin{bmatrix} \alpha & \beta \\ -\ell q\bar{\beta} & \bar{\alpha} \end{bmatrix} : \alpha,\beta \in K \right\}.$$

Here $\alpha \mapsto \bar{\alpha}$ denotes complex conjugation. Note, there is a fixed embedding of K into $\mathbb{D}$ by $\alpha \mapsto [\alpha, 0]$.

For any ideal $\mathfrak{a}$ of $\mathcal{O}$ there exists a maximal order $R(\mathfrak{a})$ in $\mathbb{D}$ containing $\mathcal{O}$ optimally, that is $\mathcal{O} \subset R(\mathfrak{a})$ and $R(\mathfrak{a}) \cap K = \mathcal{O}$. Namely let $\lambda'_p = -1^{\mathrm{ord}(\mathfrak{a})}\lambda_p$ where $\mathfrak{p}$ is the prime of $\mathcal{O}$ above p. Let λ' be the corresponding congruence solution and let $\mathscr{D}^{-1}$ be the inverse different of $\mathcal{O}$. Then

$$R(\mathfrak{a}) = R(\mathfrak{a},\lambda') = \{[\alpha,\beta] \in \mathbb{D} : a \in \mathscr{D}^{-1}, \beta \in \mathfrak{q}^{-1}\mathscr{D}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}};\ \alpha \equiv \lambda'\beta \bmod \mathcal{O}\}. \tag{2.3}$$

Observe that $R(\mathfrak{a})$ admits a filtration

$$R(\mathfrak{a})_n = \{[\alpha,\beta] \in R(\mathfrak{a}) : \beta \equiv 0 \bmod \ell^{n-1}\}. \tag{2.4}$$

That $R(\mathfrak{a})$ is maximal is proved in [3] where the following important facts concerning $R(\mathfrak{a})$ are established:

1. Any maximal order in $\mathbb{D}$ containing $\mathcal{O}$ optimally is of the form $R(\mathfrak{a})$ for some ideal $\mathfrak{a}$.

2. The conjugation relation $R(\mathfrak{a})\mathfrak{b} = \mathfrak{b}R(\mathfrak{ab})$ holds for integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$.

3. Up to conjugation by K^* there are exactly h distinct maximal orders containing $\mathcal{O}$ optimally.

A critical observation is if the ideal $\mathfrak{b} | \langle \sqrt{d} \rangle$ then $\bar{\mathfrak{b}}\mathfrak{b}^{-1} = 1$ so $R(\mathfrak{a}, \lambda')\mathfrak{b} = \mathfrak{b}R(\mathfrak{a}, \lambda'')$ where λ'' differs from λ' only in the choice of sign on the λ_p's. Thus, up to conjugacy by K^* there are 2^{t-1} orders that all look like $R(\mathfrak{a})$ except for the congruence solution. Note, we do not obtain 2^t orders since changing all the signs on the λ_p amounts to conjugating by $\sqrt{d} \in K^*$. This ambiguity will cause an obstruction as pointed out in the proof of Lemma 4.8.

Now assume ℓ is ramified in K so $\ell = p|d$. Choose a prime q such that for all $p' | d$, $p' \neq p$, $\chi_{p'}(q) = 1$ and $\chi_p(q) = -1$. Then

$$\mathbb{D} = \left\{ [\alpha, \beta] = \begin{bmatrix} \alpha & \beta \\ -q\bar{\beta} & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in K \right\}$$

and

$$R(\mathfrak{a}) = R(\mathfrak{a}, \lambda') = \{ [\alpha, \beta] \in \mathbb{D} : \alpha \in \mathfrak{p}\mathscr{D}^{-1}, \quad \beta \in \mathfrak{q}^{-1}\mathscr{D}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}};\ \alpha \equiv \lambda'\beta \bmod p',\ p' \neq p \} \tag{2.5}$$

$$R(\mathfrak{a})_n = \{ [\alpha, \beta] \in E(\mathfrak{a}) : \beta \equiv 0 \bmod \mathfrak{p}^n \}. \tag{2.6}$$

As before $\mathfrak{p}$ is the prime of K over p. The same observations and facts hold in this case as they did previously.

3. Review of Earlier Work

Some of the results and techniques from [4] are used in an essential way in what follows so we review that work with some detail now.

Let $d_1 = d$ and d_2 be another fundamental negative discriminant relatively prime to d_1. Let $w_i = w(d_i)$. Fix a finite prime v of H having characteristic ℓ and denote by $A = A_v$ the completion of the maximal, unramified, extension of the ring of v integers in H. Let $W = W_v = A[s]$ where s is a fixed element which satisfies an integral quadratic equation of discriminant d_2. Let e be the ramification index of W/A and π a uniformizer for W.

Let $j_1 = j(\tau_1)$. The algebraic integer

$$\alpha = \alpha(\tau_1, d_2) = \left(\prod_{\substack{\operatorname{disc} \tau_2 = d_2 \\ [\tau_2]}} (j_1 - j(\tau_2)) \right)^{4/w_1 w_2}, \tag{3.1}$$

lies in H, and, in fact, lies in $\mathbb{Q}(j_1)$ when $d_1, d_2 \neq -4$. Observe that $\mathbb{N}_{H/\mathbb{Q}(\sqrt{d_1})}(\alpha) = J(d_1, d_2)$. The product is taken over representative classes mod $SL_2(\mathbb{Z})$. One can, of course, try to compute $\operatorname{ord}_v(\alpha)$ for any v in H. Let E be an elliptic curve defined over W with complex multiplication by $\mathcal{O}$ and invariant $j(E) = j_1$. It is easy to show

such a curve exists, and, by a theorem of Serre and Tate [11], E has good reduction and is unique up to W isomorphism since the residue field is algebraically closed. Similarly, for each τ_2 of discriminant d_2 let E' denote the elliptic curve defined over W having complex multiplication by $\mathbb{Z}[s]$ and invariant $j(E')=j(\tau_2)$. Then

$$\mathrm{ord}_v(\alpha)=\frac{4}{ew_1w_2}\sum_{\mathrm{disc}(\tau_2)=d_2}\mathrm{ord}_\pi(j(E)-j(E')),$$

which by [8, pp. 196 and 200] gives

$$\mathrm{ord}_v(\alpha)=\frac{4}{ew_1w_2}\sum_{\mathrm{disc}(\tau_2)=d_2}\sum_{n\geqq 1}\frac{1}{2}\mathrm{Card}\{\mathrm{Iso}_{W/\pi^n}(E,E')\}.$$

Thus the problem is reduced to counting isomorphisms $f:E\to E' \bmod \pi^n$, or equivalently, [8, pp. 200–201] endomorphisms $s_f=f^{-1}\circ s\circ f$ of $E \bmod \pi^n$ belonging to the set

$$S_{n,v}=\begin{Bmatrix}\alpha_0\in \mathrm{End}_{W/\pi^n n}(E):\mathrm{Tr}(\alpha_0)=\mathrm{Tr}(s),\ \mathbb{N}(\alpha_0)=\mathbb{N}(s),\\ \alpha_0 \text{ induces multiplication by } s \text{ on } \mathrm{Lie}(E).\end{Bmatrix}$$

Thus, $\mathrm{ord}_v(\alpha)=\dfrac{2}{ew_1}\sum_{n\geqq 1}\mathrm{Card}\{S_{n,v}\}$.

If $\ell=\mathrm{char}(v)$ splits in K then $\mathrm{ord}_v(\alpha)=0$ since E has ordinary reduction in this case. If ℓ is inert or ramifies in K then one can hope to determine $\mathrm{ord}_v(\alpha)$ with the aid of the $R(\mathfrak{a})_n$. For simplicity we consider the case ℓ inert. An analogous sitation holds for ℓ ramified.

Deuring's theory [2] tells us that in this case there exists an integral ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $\mathrm{End}_{W/\pi^n}(E)=R(\mathfrak{a})_n$ where $R(\mathfrak{a})_n$ is given by (2.4). One then checks that an $\alpha_0\in R(\mathfrak{a})_n$ gives rise to an integer x and an integral ideal $\mathfrak{b}$ of $\mathcal{O}$, $\mathfrak{b}\sim\mathfrak{q}\mathfrak{a}^2$ solving the Diophantine equation $x^2+4\ell^{2n-1}\mathbb{N}\mathfrak{b}=d_1d_2$. However, the converse is not quite true. A solution $(x,\mathfrak{b})$ does indeed give rise to an endomorphism, however it does not necessarily end up in the original $R(\mathfrak{a})_n$ but in one of the 2^{t-1} rings conjugate to $R(\mathfrak{a})_n$ by an ideal $\mathfrak{c}|\pi$. There is no way to distinguish in which of these 2^{t-1} rings the endomorphism lies. Moreover, a single solution $(x,\mathfrak{b})$ not just one but $\mathrm{Card}\{\mathfrak{p}|(x,d_1)\}$ endomorphisms. Thus, while in principle one can factor α in H, the hopes of finding a formula for this factorization seem unobtainable by our present method. The above difficulty is overcome by descending to the subfield L of H fixed by the subgroup of G generated by the elements of order 2. Note $[H:L]=2^{t-1}$ and if u is a prime of L under v then

$$\mathrm{ord}_u(\mathbb{N}_{H/L}(\alpha))=\sum_{v'|u}\mathrm{ord}_{v'}(\alpha).$$

It turns out that a formula for $\mathrm{ord}_u(\mathbb{N}_{H/L}(\alpha))$ can be obtained and the remarkable fact is that it depends only on the genus class of $\mathfrak{q}$ but not of $\mathfrak{a}$. We remark that an analogous situation holds if $\ell=p|d_1$ but now we obtain a solution $(x,\mathfrak{b})$ to $x^2+4p\mathbb{N}\mathfrak{b}=d_1d_2$ with $x\in\mathbb{Z}$ and $\mathfrak{b}$ an integral ideal of $\mathcal{O}$ in the class of $\mathfrak{p}\mathfrak{q}\mathfrak{a}^2$. Here $\mathfrak{p}|p$.

Let $r_*(n)$ be the number of integral ideals of $\mathcal{O}$ in the class of $*$ having norm n. Then u has characteristic ℓ and we have

(3.2) **Theorem.** *Let ℓ be a rational prime and H, L, u, $\mathfrak{a}$, $\mathfrak{p}$, and $\mathfrak{q}$ be as above and in Sect. 2. Then*

$$\operatorname{ord}_u(\mathbb{N}_{H/L}(\alpha))=\begin{cases}0 & \text{if } \chi_{d_1}(\ell)=1\\ \frac{1}{2}\sum_{x\in\mathbb{Z}}\sum_{n\geqq 1}2^{a(x)}\cdot r_{\mathfrak{q}\mathfrak{a}^2}\left(\frac{d_1d_2-x^2}{4\ell^n}\right) & \text{if } \chi_{d_1}(\ell)=-1\\ \frac{1}{2}\sum_{x\in\mathbb{Z}}2^{a(x)}\cdot r_{\mathfrak{q}\mathfrak{p}\mathfrak{a}^2}\left(\frac{d_1d_2-x^2}{4p}\right) & \text{if } \ell=p|d\end{cases}$$

where $a(x)=\operatorname{Card}\{p|(x,d_1)\}$.

Proof. See [4, Propositions 3.4, 3.9, 3.11, 3.13, and Theorem 4.1]. □

4. Generalization to Modular Polynomials

From here on we fix one fundamental negative discriminant D having t distinct prime divisors and we assume $j=((D+\sqrt{D})/2)$ is a singular modulus. All notation is as before except for W which we will define later.

Assume $m\in\mathbb{Z}$ is not a perfect square. Then Kronecker's identity relating $\varphi_m(x,x)$ to $f_D(x)$ is

$$\varphi_m(x,x)=\pm\prod_{t\in\mathbb{Z};\,t^2<4m}f_{t^2-4m}(x).$$

Suppose that $m\geqq 1$ is *not* the norm of an element $(a+b\sqrt{D})/2$ in $\mathcal{O}$. Then the value $\varphi_m(j,j)\neq 0$. Thus for ℓ inert and $\mathfrak{a}$ and $\mathfrak{q}$ as defined in Sect. 2, Kronecker's identity can be use to recast the results of Theorem 3.2 as

$$\begin{aligned}\operatorname{ord}_u(\mathbb{N}_{H/L}(\varphi_m(j,j)))^{4/w^2}&=\frac{4}{w^2}\sum_{t^2\leqq 4m}\left\{\frac{1}{2}\sum_{x\in\mathbb{Z}}\sum_{n\geqq 1}2^{a(x)}r_{\mathfrak{q}\mathfrak{a}^2}\left(\frac{|D|(4m-t^2)-x^2}{4\ell^k}\right)\right\}\\&=\sum_{n\geqq 0}\sum_{k\geqq 1}2^{a(n)}r_1(n)r_{\mathfrak{q}\mathfrak{a}^2}\left(\frac{m|D|-n}{\ell^k}\right),\end{aligned}$$

where $n=(x^2-Dt^2)/4$ is the norm of an ideal in the principal class. For an ideal class $\mathfrak{b}$ define $r_{\mathfrak{b}}(0)=1/w$. If $\ell=p|D$ the last line above would read

$$=\sum_{n\geqq 0}\sum_{k\geqq 1}2^{a(n)}r_1(n)r_{\mathfrak{q}\mathfrak{p}^k\mathfrak{a}^2}\left(\frac{m|D|-n}{p^k}\right).$$

This formula can be generalized. Let $\mathfrak{b}$ be an ideal of $\mathcal{O}$ and $m\geqq 1$ an integer which is *not* the norm of an ideal in the class of $\mathfrak{b}$. Denote by $\sigma_{\mathfrak{b}}=\sigma$ be the element of $\operatorname{Gal}(H/K)$ that corresponds to $\mathfrak{b}$ under the Artin map. Then

$$\beta=\varphi_m(j,j^\sigma)^{4/w^2} \tag{4.2}$$

is an algebraic integer and we now produce a formula for $\operatorname{ord}_u(\mathbb{N}_{H/L}\beta)$.

First observe by 1.2

$$\varphi_m(j,j^\sigma)^{4/w^2}=\prod_{j'}(j-j')^{4/w^2}, \tag{4.3}$$

where j' is the modular invariant of a curve E' which is m-isogenous to E^σ. Recall A is the completion of the maximal unramified extension of the v-integers of H. Now let $W=A[j']$ the field obtained by adjoining all the invariants j' of curves that are m-isogenous to E^σ. Let π be a uniformizer for W. Note if $l\nmid m$ then $W=A$ since the j' are all unramified over A. This is the case of greatest interest since $m=1$ in the later application.

Let E be an elliptic curve defined over W having complex multiplication by $\mathcal{O}$ and modular invariant $j(E)=j'$. From the definition of φ_m it follows that the factorization of β depends on determining the cardinality of

$$S_n=\{\mathrm{Iso}_{W/\pi^nW}(E,E');\ E' \text{ } m\text{-isogenous to } E\}.$$

By (1.3) and (4.3) $\mathrm{Card}(S_n)$ is related to the cardinality of the set

$$T_n=\mathrm{Hom}_{W/\pi^nW}(E,E^\sigma)_{\text{degree } m}.$$

(4.4) **Proposition.** *With the notation as above* $T_n=S_n$.

Proof. To see this let $f\in S_n$ and φ an m isogeny between E' and E^σ. Then $f\circ\varphi$ is an m isogeny for E to E^σ so $S_n\subset T_n$. On the other hand, if φ is an m isogeny for E^σ to E define $E'=E^\sigma/\ker\varphi$. Then $E\cong E'$ thus $T_n\subset S_n$. □

Since $\mathrm{ord}_v(\beta)=4/w^2\sum_{j'}\mathrm{ord}_v(j-j')$, by Proposition 2.3 in [5] $\mathrm{ord}_v(\beta)=4/w^2\sum_{n\geqq 1}\mathrm{Card}(S_n)/2$. And since $S_n=T_n$ we can use T_n in the above formula.

As mentioned in Sect. 2 the ambiguity in the congruence solution in the definition of the $R(\mathfrak{a})$ will prevent us from determining $\mathrm{ord}_v(\beta)$ in H. Instead descend to the subfield L and let u be a prime of L under v. Then

$$\mathrm{ord}_u(\mathbb{N}_{H/L}\beta)=\frac{4}{w^2}\sum_{n\geqq 1}\sum_{v'\mid u}\frac{\mathrm{Card}(T_n)}{2}. \tag{4.5}$$

The formula for (4.5) is given by

(4.6) **Theorem.** *Let m, β, L, and u be as defined above and let ℓ be a rational prime not dividing m, and let $B=\mathbb{N}_{H/L}\beta$*

1. *If $\chi_D(\ell)=1$ then $\mathrm{ord}_u(B)=0$*
2. *If $\chi_D(\ell)=-1$, then for $\mathfrak{a}$ and $\mathfrak{q}$ as in Sect. 2*

$$\mathrm{ord}_u(B)=\sum_{n\geqq 0}\sum_{k>1}2^{a(n)}r_{\mathfrak{b}^{-1}}(n)r_{\mathfrak{q}\mathfrak{a}^2}\left(\frac{m|D|-n}{\ell^k}\right).$$

3. *If $\ell=p|D$, then for $\mathfrak{a}$, $\mathfrak{q}$, and $\mathfrak{q}$ as in Sect. 2*

$$\mathrm{ord}_u(B)=\sum_{n\geqq 0}\sum_{k>1}2^{a(n)}r_{\mathfrak{b}^{-1}}(n)r_{\mathfrak{q}\mathfrak{p}^k\mathfrak{a}^2}\left(\frac{m|D|-n}{p^k}\right).$$

The proof of this theorem is broken down into 3 lemmas.

(4.7) **Lemma.** *Assume $\chi_D(\ell)=1$. Then $\mathrm{ord}_u(B)=0$ for any prime u of L of characteristic ℓ.*

Proof. By During's theory [2] $\mathrm{End}_{W/\pi^nW}E\cong\mathcal{O}$. Let $\mathfrak{b}$ be an ideal in the class of σ. By results of Serre [1] $\mathrm{Hom}_W(E,E^\sigma)\cong\mathcal{O}$ as an $\mathrm{End}_WE\cong\mathcal{O}$ module inside K. Thus

$\mathrm{Hom}_W(E, E^\sigma) = \mathrm{Hom}_{W/\pi^n W}(E, E^\sigma) = \mathcal{O}\mathfrak{b} = \mathfrak{b}$. Now assume φ is an isogeny. Then $\deg\varphi = \mathbb{N}\alpha/\mathbb{N}\mathfrak{b}$ where $\alpha \in \mathfrak{b}$. Since we are looking for isogenies of degree m it follows that $\mathbb{N}\alpha = m\mathbb{N}\mathfrak{b}$. Put $\mathfrak{c} = (\alpha)\mathfrak{b}^{-1}$. Then $\mathbb{N}\mathfrak{c} = m$. Hence $r_{\sigma^{-1}}(m) = r_\sigma(m) > 0$. This is impossible since assuming that m is not the norm of an ideal in the class of $\mathfrak{b}$ means $r_\sigma(m) = 0$. Thus $\mathrm{Card}(T_{n,v'}) = 0$; for all v' and the lemma is proved. □

(4.8) **Lemma.** *Assume $\chi_D(\ell) \neq 1$ and $\ell \nmid Dm$. Then the sum $\sum_{n \geqq 0} \sum_{v' \mid u} \frac{1}{2} \mathrm{Card}\, T_{n,v'}$ is equal to the number of solutions to the equation $\mathbb{N}\mathfrak{c} + \ell^{2k-1}\mathbb{N}\mathfrak{d} = Dm$ where $\mathfrak{c}$ and $\mathfrak{d}$ are integral ideals of $\mathcal{O}$ in the class of $\mathfrak{b}^{-1}$ and $\mathfrak{q}\mathfrak{b}\mathfrak{a}^2$ respectively. Each solution is counted with multiplicity $2^{a(\mathbb{N}\mathfrak{c})} \cdot \frac{1}{4} \cdot w^2$.*

Proof. Since $\ell \nmid Dm$, Deuring's theory tells us that there exists an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $R(\mathfrak{a})_n \cong \mathrm{End}_{W/\pi^n W}(E)$. Serre's result in this case shows that $\mathrm{Hom}_{W/\pi^n W}(E, E^\sigma) = \mathrm{End}_{W/\pi^n W}(E)\mathfrak{b}$ as an $\mathrm{End}_{W/\pi^n W}(E)$ module inside $\mathbb{D}$. Explicitly

$$\mathrm{Hom}_{W/\pi^n W}(E, E^\sigma) = \{[\alpha, \beta] \in \mathbb{D} : \alpha \in \mathscr{D}^{-1}\mathfrak{b},\ \beta \in \mathscr{D}^{-1}\mathfrak{q}^{-1}\ell^{n-1}\overline{\mathfrak{b}\mathfrak{a}}\,\mathfrak{a}^{-1};\ \alpha \equiv \beta \bmod \mathcal{O}\}.$$

Thus we must find homomorphisms $[\alpha, \beta]$ with norm equal to $m\mathbb{N}\mathfrak{b}$. Writing $\alpha = \gamma/\sqrt{D}$ with $\gamma \in \mathfrak{b}$ and $\beta = \ell^{n-1}\delta/\sqrt{D}$ where $\delta \in (\mathfrak{q}\mathfrak{a})^{-1} \cdot \overline{\mathfrak{q}\mathfrak{a}}$ the norm condition implies

$$-1(\mathbb{N}\gamma + q\ell^{2n-1}\mathbb{N}\delta)/D = m\mathbb{N}\mathfrak{b}$$

or equivalently

$$\mathbb{N}\gamma + q\ell^{2n-1}\mathbb{N}\delta = |D|\, m\mathbb{N}\mathfrak{b}. \tag{4.9}$$

Setting $\mathfrak{c} = (\gamma)/\mathfrak{b}$ and $\mathfrak{d} = (\delta)\mathfrak{q}\mathfrak{a}(\overline{\mathfrak{b}\mathfrak{a}})^{-1}$ we obtain a solution $(\mathfrak{c}, \mathfrak{d})$ to

$$\mathbb{N}\mathfrak{c} + \ell^{2n-1}\mathbb{N}\mathfrak{d} = |D|m \tag{4.10}$$

where $\mathfrak{c}$ and $\mathfrak{d}$ are integral ideals of $\mathcal{O}$ in the class of $\mathfrak{b}^{-1}$ and $\mathfrak{q}\mathfrak{b}\mathfrak{a}^2$ respectively.

On the other hand, beginning with a solution $(\mathfrak{c}, \mathfrak{d})$ to (4.10) reversing the steps in the above argument a homomorphism $[\alpha, \beta]$ is constructed in at least one of the 2^{t-1} conjugate right ideals $R(\mathfrak{a}, \lambda)_n$. However, there is no way to determine in which of these ideals the homomorphism lies. Moreover, it is possible for a single solution to contribute more than one homomorphism if $gcd(D, \mathbb{N}\mathfrak{c}) > 1$. For example, if $p = \gcd(D, \mathbb{N}\mathfrak{c})$ then reducing (4.10) mod p shows $\ell^{2n-1}\mathbb{N}\mathfrak{d} \equiv 0 \bmod p$. This implies $\delta \equiv 0 \bmod p$, hence $0 \equiv \mathbb{N}\mathfrak{c} \equiv \pm\lambda_p\delta^2 \bmod p$ is trivially satisfied with both signs on λ_p. Thus 2 homomorphisms are constructed from a single solution. Continuing in this way it is easy to see if $a(\mathbb{N}\mathfrak{c}) = \mathrm{Card}\{p \mid \gcd(D, \mathbb{N}\mathfrak{c})\}$ then $2^{a(\mathbb{N}\mathfrak{c})}$ homomorphisms are obtained from a single solution.

Both of these ambiguities are bypassed by descending to the field L where computing the $\mathrm{ord}_u(B)$ is the same as summing over all the right ideals K^* conjugate to $R(\mathfrak{a})$. This accounts for the inner summation sign.

The $\frac{1}{4} \cdot w^2$ term is 1 if $D < -4$. When $D = -3$ the generator δ of $\mathfrak{d}(\mathfrak{a}\mathfrak{q})^{-1}\overline{\mathfrak{b}\mathfrak{a}}$ and the generator γ of $\mathfrak{c}\mathfrak{b}$ can each be altered by a sixth root of unity giving $9 = \frac{1}{4} \cdot w^2$ times as many homomorphisms as expected for each solution $(\mathfrak{c}, \mathfrak{d})$. Similarly, when $D = -4$, γ and δ can each be altered by a fourth root of unity giving $4 = \frac{1}{4} \cdot w^2$ times the number of expected homomorphisms. □

The final lemma is

(4.11) **Lemma.** *Assume* $\chi_D(\ell) \neq 1$ *and* $\ell = p|D$, *but* $\ell \nmid m$. *Then the sum* $\sum_{n \geq 0} \sum_{v|u} \frac{1}{2}\mathrm{Card}(T_n)$ *is equal to the number of solutions to the equation* $\mathbb{N}\mathfrak{c} + p^{n-1}\mathbb{N}\mathfrak{d} = |D|m$, *where* $\mathfrak{c}$ *and* $\mathfrak{d}$ *are integral ideals of* $\mathcal{O}$ *in the classes of* $\mathfrak{b}^{-1}\mathfrak{p}$ *and* $\mathfrak{q}\mathfrak{b}\mathfrak{p}^n\mathfrak{a}^2$ *respectively. Each solution is counted with multiplicity* $2^{a(\mathbb{N}\mathfrak{c})} \cdot \frac{1}{4} \cdot w^2$.

Proof. For some ideal $\mathfrak{a}$ (4.6) provides a discription of $\mathrm{End}_{W/\pi^n W}(E)$. Combining this with Serre's result gives

$$\mathrm{Hom}_{W/\pi^n W}(E, E^\sigma) = \{[\alpha, \beta] \in \mathbb{D} : \alpha \in \mathfrak{p}\mathscr{D}^{-1},\ \beta \in \mathscr{D}^{-1}\mathfrak{q}^{-1}\mathfrak{p}^n\mathfrak{a}^{-1}\overline{\mathfrak{b}\mathfrak{a}};\ \alpha \equiv \lambda\beta \bmod p',\ p' \neq p\}.$$

The argument now proceeds as in the last lemma. Note in this case we can obtain an extra factor of 2 in the special case $\mathbb{N}\mathfrak{c} \equiv 0 \bmod D$ which allows a change of sign on the generator of $\mathfrak{d}$ itself. □

The proof of Theorem 4.6 is simply a matter of combining the above three lemmas.

5. An Application

One application of Theorem 4.6 is the computation of the index I of the order $\mathbb{Z}[j]$ in its integral closure in $\mathbb{Q}(j)$. When $m = 1$ and $\mathfrak{b}$ is not a principal ideal (4.1) and (4.2) give the prime factorization of $\mathbb{N}_{H/L}(j - j^\sigma)$. Norming this quantity down to K and then taking the product over all calsses $\mathfrak{b} \sim 1$ gives the discriminant of the monic polynomial, f, of degree h satisfied by j. It is also true that

$$d(\mathbb{Q}(j)) \cdot I^2 = d(f).$$

Here $d(\mathbb{Q}(j))$ is the absolute discriminant of $\mathbb{Q}(j)$ and $d(f)$ is the discriminant of f. Hence the prime factorization of I can be determined once $d(\mathbb{Q}(j))$ is known.

Write $D = D_0 \cdot D_1$ where

$$D_1 = \begin{cases} 1 & \text{if at least 2 primes congruent to } 3 \bmod 4 \text{ divide } D \\ p & \text{if } p \text{ is the unique prime congruent to } 3 \bmod 4 \text{ dividing } D \\ 4 & \text{if } 4 \| D \text{ and no primes congruent to } 3 \bmod 4 \text{ divide } D \\ 8 & \text{if } 8 \| D \text{ and no primes congruent to } 3 \bmod 4 \text{ divide } D. \end{cases}$$

We then have

(5.1) **Proposition.** $d(\mathbb{Q}(j)) = D_0^{1/2h} \cdot D_1^{1/2(h-2^{t-1})}$.

Proof. See appendix. □

We now determine I.

First let $\ell \nmid D$ so with $m = 1$ (4.10) becomes

$$\mathbb{N}\mathfrak{c} + \ell^{2k-1}\mathbb{N}\mathfrak{d} = |D|. \tag{5.2}$$

Now $\mathfrak{c} \sim \mathfrak{b}^{-1}$ and $\mathfrak{d} \sim \mathfrak{q}\mathfrak{b} \bmod \mathrm{Pic}(\mathcal{O})^2$ if and only if $\mathfrak{c} \sim \mathfrak{q}\mathfrak{d} \bmod \mathrm{Pic}(\mathcal{O})^2$, or equivalently,

$$\varepsilon_p(\mathbb{N}\mathfrak{c}\mathfrak{q}\mathfrak{d}) = 1, \tag{5.3}$$

for each genus character ε_p; $p|D$. Write $\mathbb{N}\mathfrak{c}=n$. Then (5.2) and (5.3) show

$$\mathbb{N}(\mathfrak{cqb})=nq\left(\frac{|D|-n}{\ell^{2k-1}}\right)\equiv\frac{n-|D|}{n}\cdot -q\ell \bmod \mathbb{Q}^{*2}.$$

Moreover, since q was selected so that $-q\ell$ was congruent to a square mod p for all $p|D$ condition (5.3) translates to

$$\varepsilon_p\left(\frac{n-|D|}{n}\right)=1 \quad \text{for all } p|D.$$

Observe that this condition is satisfied if $p\nmid n$ since then $(n-|D|)/n\equiv 1 \bmod p$. Moreover, since $\varepsilon_\infty((n-|D|)/n)=1$ the product formula, (2.2), implies if the above condition fails it must do so for an even number of primes dividing D.

Now assume $\ell=p|D$, so we are working with the equation

$$\mathbb{N}\mathfrak{c}+p^{k-1}\mathbb{N}\mathfrak{d}=|D|. \tag{5.4}$$

There are two cases to consider.

Case 1. Assume $n\neq 0$. Then $\mathfrak{c}\sim\mathfrak{b}^{-1}$ and $\mathfrak{d}\sim\mathfrak{qbp}^{k-1} \bmod \mathrm{Pic}(\mathcal{O})^2$. Thus $\mathfrak{c}\sim\mathfrak{qdp}^{k-1} \bmod \mathrm{Pic}(\mathcal{O})^2$, or equivalently $\varepsilon_{p'}(\mathfrak{cqdp}^{k-1})=1$ for all $p'|D$, $p'\neq p$. As above, if this condition fails it can only do so for an even number of primes dividing D.

Case 2. Assume $n=0$. Equation (5.4) becomes $p\mathbb{N}\mathfrak{d}=*D|$. Hence $\mathfrak{d}\sim\mathfrak{q} \bmod \mathrm{Pic}(\mathcal{O})^2$. But we have $\mathfrak{d}\sim\mathfrak{bqp} \bmod \mathrm{Pic}(\mathcal{O})^2$ so $\mathfrak{b}\sim\mathfrak{q} \bmod \mathrm{Pic}(\mathcal{O})^2$. Since it is required that $\mathfrak{b}\sim 1$ we have $\mathfrak{p}\sim 1$. Now if $\mathfrak{q}\sim 1$ then $\varepsilon_{p'}(q)=1$ for all $p'\neq p$. However, since $\chi_{p'}(-q)=1$ it follows that $\mathfrak{q}\sim 1$ if and only if $\chi_{p'}(-1)=1$, i.e., $p'\equiv 1 \bmod 4$.

The above analysis leads to the following definition. For each positive integer n let

$$\varrho_\ell(n)=\begin{cases}0 & \text{if there exist two primes } p|d \text{ so that}\\ & \varepsilon_p((n-|D|)/n)=-1.\\ 2^{a(n)} & \text{otherwise, where } a(n)=\mathrm{Card}\{p\mid \gcd(n,D)\}.\end{cases}$$

and for $n=0$

$$\varrho_\ell(0)=\begin{cases}0 & \text{if } p'\equiv 1 \bmod 4 \text{ for all } p'\neq p=\ell,\\ 2^t & \text{otherwise.}\end{cases}$$

Put $m=1$ and $n=\mathbb{N}\mathfrak{c}$ into (4.1) and (4.2) and take norms down to K and sum over all classes $\mathfrak{b}\sim 1$. The same result is given in both cases, namely, for any prime λ of K of characteristic ℓ

$$\mathrm{ord}_\lambda(d(f))=\sum_{n\geqq 0}\sum_{k\geqq 1}\varrho_\ell(n)\cdot(R(n)-r_1(n))\cdot R\left(\frac{|D|-n}{\ell^k}\right).$$

Combining this with Proposition 5.1 we have proved

(5.5) **Theorem.** *Let λ be a prime of K with $\mathrm{char}(\lambda)=\ell$. Then*

$$\mathrm{ord}_\lambda(I)=\frac{1}{2}\sum_{n\geqq 0}\sum_{k\geqq 1}\varrho_\ell(n)\cdot(R(n)-r_1(n))\cdot R\left(\frac{|D|-n}{\ell^k}\right)$$
$$-\frac{1}{2}\left(\frac{h}{2}\cdot\mathrm{ord}_\lambda(D_0)+\left(\frac{h-2^{t-1}}{2}\right)\cdot\mathrm{ord}_\lambda(D_1)\right) \quad \square$$

(5.6) **Corollary.** *Let ℓ be a prime in $\mathbb{Z}$.*

1. *If $\chi_D(\ell)=1$, then* $\operatorname{ord}_\ell(I)=0$.
2. *If $\chi_D(\ell)=-1$, then*

$$\operatorname{ord}_\ell(I)=\frac{1}{2}\sum_{n\geqq 0}\sum_{k\geqq 1} \varrho_\ell(n)\cdot(R(n)-r_1(n))\cdot R\left(\frac{|D|-n}{\ell^k}\right).$$

3. *If $\ell=p|D$ then*

$$\operatorname{ord}_p(I)=\frac{1}{4}\sum_{n\geqq 0}\sum_{k\geqq 1} \varrho_\ell(n)\cdot(R(n)-r_1(n))\cdot R\left(\frac{|D|-n}{p^k}\right)$$
$$-\tfrac{1}{4}(\tfrac{1}{2}\cdot h\cdot \operatorname{ord}_\lambda(D_0)+\tfrac{1}{2}(h-2^{t-1})\operatorname{ord}_\lambda(D_1)).$$

Proof. 1. is a restatement of Theorem 4.6. 2. follows immediately from the theorem since ℓ is a degree 1 prime and also there is no need for the correction term. For 3. we need only remark that $\operatorname{ord}_p(I)=\frac{1}{2}\operatorname{ord}_\lambda(I)$ in this case. □

(5.7) **Corollary.** *With ℓ as above, if the class number is odd or equal to 2 then*

$$\operatorname{ord}_\ell(I)=\sum_{n\geqq 0}\sum_{k\geqq 1} \varrho_\ell(n)\cdot\tfrac{1}{2}\cdot(R(n)-r_1(n))\cdot R\left(\frac{|D|-n}{\ell^k}\right).$$

Proof. By the above corollary we only need to check the term $\operatorname{ord}_p(I)$ when $n=0$ for $p|D$.

Case 1. h odd. Remark, this is a theorem of Gross–Zagier [6]. Here $D=-p$ where $-p\equiv 1 \bmod 4$ and so $D_0=1$ and $D_1=p$. Moreover, $2^{t-1}=1$ so

$$-\tfrac{1}{4}(\tfrac{1}{2}\cdot \mathrm{h}\cdot \operatorname{ord}_\lambda(D_0)+\tfrac{1}{2}(h-2^{t-1})\cdot \operatorname{ord}_\lambda(D_1))=-\tfrac{1}{4}(\tfrac{1}{2}(h-1)).$$

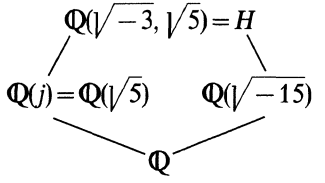
Observe that $\frac{1}{4}\varrho_\ell(0)\cdot(R(0)-r_1(0))\cdot R\left(\frac{p}{p}\right)=\frac{1}{4}(\frac{1}{2}(h-1))$. So the term corresponding to 0 in the summation cancels against the correction term for the discriminant of $\mathbb{Q}(j)$ and the corollary is proved in this case.

Case 2. $h=2$. Then $D=-pq$ where $-p\equiv q\equiv 1 \bmod 4$. So $D_0=q$ and $D_1=p$. First consider the prime p. In this situation $\varrho_\ell(0)=0$ so $\frac{1}{4}\varrho_\ell(0)\cdot(R(0)-r_1(0))\cdot R(q)=0$. But note, since $D_1=p$ then $-\frac{1}{4}(\operatorname{ord}_\lambda(q)+\operatorname{ord}_\lambda(p))=0$ so the terms cancel. Finally consider q. Here $\varrho_\ell(0)=4$ so $\frac{1}{4}\varrho_\ell(0)\cdot(R(0)-r_1(0))\cdot R(p)=\frac{1}{2}$ and $-\frac{1}{4}(\operatorname{ord}_\lambda(q)+\operatorname{ord}_\lambda(p))=-\frac{1}{2}$. Again the terms cancel and the corollary is proved. □

6. A Computational Example

A simple example will suffice to reveal the computational techniques involved in Theorem 5.5.

Let $D=-15$. The complete diagram of fields is



Thus $d(\mathbb{Q}(j))=D_0=5$ and $D_1=3$. The inert or ramified primes dividing $|D|-n$ with $0\leqq n\leqq|D|$ are 3, 5, 7, 11, and 13. 2 is the only split prime, consequently by (5.5) $\mathrm{ord}_2(I)=0$.

In the calculation of $\mathrm{ord}_3(I)$ and $\mathrm{ord}_5(I)$ we know the correction term is zero since we are in the class number 2 situation. Nevertheless, we will use Theorem 5.5 directly to illustrate how the computations are made.

Case $p=3$. Consider the table.

n	$\varrho_3(n)$	$R(n)$	$r_1(n)$	$R((15-n)/3^k)$
0	0	1	$\frac{1}{2}$	1
3	2	1	0	3
6	2	2	2	1 for $k=1$ or 2
9	2	2	2	2
12	2	3	0	1
15	0	1	1	1

Since $5\equiv 1 \bmod 4$ we have $\varrho_3(0)=\varrho_3(15)=0$. On the other hand we have $\varrho_3(3)=\varrho_3(6)=\varrho_3(9)=\varrho_3(12)=2$ since $\varepsilon_3((n-|D|)/n)\neq -1$ for at least two primes dividing D in these latter cases. Next observe that the correction term is 0 since $\mathrm{ord}_{\lambda_3}5=0$ and $\left(\frac{h-2^{t-1}}{2}\right)=0$. Note λ_3 is the unique prime of K over 3. Then from the table above and the formula in Theorem 5.5 we see

$$\mathrm{ord}_3(I)=0+\tfrac{1}{4}\cdot 2(3+0+0+0+3)=3.$$

Case $p=5$. Consider the table

n	$\varrho_5(n)$	$R(n)$	$r_1(n)$	$R((15-n)/5^k)$
0	4	1	$\frac{1}{2}$	1
5	1	1	0	2
10	1	2	2	1
15	2	1	1	1

In this case $\varrho_5(0)=4$ and $\varrho_5(5)=\varrho_5(10)=2$. The correction term in this case is $\frac{1}{4}(\mathrm{ord}_{\lambda_5}(5))=\frac{1}{2}$. λ_5 is the unique prime above 5. Then the table and (5.5) imply $\mathrm{ord}_5(I)=\frac{1}{4}(4\cdot\frac{1}{2}+2\cdot 1\cdot 2+0)-\frac{1}{2}=1$.

Case $p=7$. The table is

n	$\varrho_7(n)$	$R(n)$	$r_1(n)$	$R((15-n)/7^k)$
1	1	1	1	2
8	1	4	0	1

and $\mathrm{ord}_7(I)=\frac{1}{2}\cdot 4=2$.

Case $p=11$. Our table has one entry

n	$\varrho_{11}(n)$	$R(n)$	$r_1(n)$	$R((15-n)/11^k)$
4	1	3	3	1

Thus, $\operatorname{ord}_{11}(I)=\frac{1}{2}\cdot 0=0$.

Case $p=13$. Our table has one entry

n	$\varrho_{13}(n)$	$R(n)$	$r_1(n)$	$R((15-n)/13^k)$
2	1	2	0	1

Thus, $\operatorname{ord}_{13}(I)=\frac{1}{2}\cdot 2=1$.

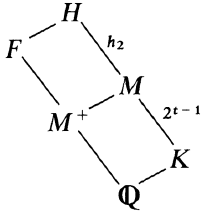
So we find $I=3^3\cdot 5\cdot 7^2\cdot 13$.

7. Appendix

We now compute the absolute disriminant of $\mathbb{Q}(j)$ over $\mathbb{Q}$.

To simplify notation set $F=\mathbb{Q}(j)$ and for any extension of fields B/A let $d(B/A)$ denote the discriminant of that extension. If $A=\mathbb{Q}$ it will be dropped from the notation. All other notation will be as in the previous sections.

Consider the diagram of fields



Here $h_2=h/2^{t-1}$, M is the genus field of K, and M^+ is the composition of all the real quadratic subfields contained in H. This last condition is equivalent to the fact that M^+ is the totally real subfield of M, hence the $^+$ in the notation. Using the norm-discriminant formula the following equalities can be read from the diagram

$$d(F)^2\mathbb{N}_{F/\mathbb{Q}}(d(H/F))=d(H)=d(K)^h\mathbb{N}_{K/\mathbb{Q}}(d(H/K)).$$

Now $d(K)=D$ and $d(H/K)=1$ since H is unramified over K. Thus the above equations reduce to

$$d(F)^2\mathbb{N}_{F/\mathbb{Q}}(d(H/F))=D^h.$$

Hence we can compute $d(F)$ once we compute $\mathbb{N}_{F/\mathbb{Q}}(d(H/F))$.

Now consider the field M^+. That M^+ is actually contained in F is shown in Rohrlich [9] where he also proves

(7.1) **Proposition.** *The following are equivalent.*

a. *There are at least two primes congruent to* $3 \bmod 4$ *which divide* D;

b. *the extension* M/M^+ *is unramified outside infinity,*

c. *the extension* H/F *is unramified outside infinity.*

Recall $D = D_0 \cdot D_1$ where

$$D_1 = \begin{cases} 1 & \text{if at least 2 primes congruent to 3 mod 4 divide } D \\ p & \text{if } p \text{ is the unique prime congruent to 3 mod 4 dividing } D \\ 4 & \text{if } 4 \| D \text{ and no primes congruent to 3 mod 4 divide } D \\ 8 & \text{if } 8 \| D \text{ and no primes congruent to 3 mod 4 divide } D \end{cases}$$

and

(5.1). **Proposition.** $d(\mathbb{Q}(j)) = D_0^{1/2h} \cdot D^{1/2(h-2^{t-1})}$.

Proof. Case 1. Assume at least two primes congruent to 3 mod 4 divide D. Rohrlich's proposition shows $d(H/F) = 1$, so $d(F) = D^{1/2h}$ as claimed.

Before embarking on cases 2 and 3 we make some observations. Let p be the unique prime *not* congruent to 3 mod 4 dividing D. By class field theory p splits into $h/2$ prime factors in H, each of degree 2. Corresponding to each of these factors there is an inertia subgroup of $\mathrm{Gal}(H/\mathbb{Q})$ each of order 2. Since H/F is ramified at p at least one of these subgroups corresponds to $\mathrm{Gal}(H/F)$. Let $\langle\sigma\rangle$ be this subgroup. To determine $d(H/F)$ we need to see precisely how many of the other inertia subgroups are equal to $\langle\sigma\rangle$. By Galois theory this is equivalent to finding the order of the normalizer of $\langle\sigma\rangle$ in $\mathrm{Gal}(H/\mathbb{Q})$. We know $\mathrm{Gal}(H/\mathbb{Q}) = \mathrm{Gal}(H/K) \rtimes \langle\sigma\rangle$, with the action of σ given by $\sigma g \sigma^{-1} = g^{-1}$ for all $g \in \mathrm{Gal}(H/K)$. Thus the centralizer of σ in $\mathrm{Gal}(H/\mathbb{Q})$ – which is the same as the normalizer in this case – is

$$\mathscr{Z}(\sigma) = \{\sigma^n g : n = 0, 1 \text{ and } g \in \mathrm{Gal}(H/K),\ g^2 = 1\}.$$

Thus $\mathrm{Card}(\mathscr{Z}(\sigma)) = 2^t$. Thus the number of distinct quadratic subfields of H is $[H:\mathbb{Q}]/\mathrm{Card}(\mathscr{Z}(\sigma)) = 2h/2^t = h/2^{t-1}$. Consequently the number of ramified primes dividing the different $\mathscr{D}_{H/F}$ is $\dfrac{h/2}{h/2^{t-1}} = 2^{t-2}$.

Now onto cases 2 and 3 where we calculate the $\mathrm{ord}_{\mathfrak{p}_i}(\mathscr{D})$ for any of the primes $\mathfrak{p}_i$ dividing $\mathscr{D}^{H/F}$. We have the formula

$$\text{(Serre [10, p. 64])};\ \mathrm{ord}_{\mathfrak{p}_i}(\mathscr{D}_{H/F}) = \sum_{n \geqq 0} \mathrm{Card}(\mathrm{Gal}(H/F)_n) - 1.$$

Where $\mathrm{Gal}(H/F)_n$ denotes the n^{th} higher ramification group of $\mathrm{Gal}(H/F)$.

Case 2. Let p be odd. Then H/F is tamely ramified at p so $\mathrm{Card}(\mathrm{Gal}(H/F)_n) = 1$ for $n \geqq 0$. Hence for all $\mathfrak{p}_i$

$$\mathscr{D}_{H/F} = \prod_{i=1}^{2^{t-2}} \mathfrak{p}_i.$$

Consequently $d(H/F) = \prod_{i=1}^{2^{t-2}} \mathfrak{p}_i$, for those $\mathfrak{p}_i | p$.

Since each $\mathfrak{p}_i$ is of degree 2 it follows that $\mathbb{N}_{F/\mathbb{Q}}(d_{H/F}) = (p^2)^{2^{t-2}} = p^{2^{t-1}}$. Thus $d_F^2 = D^h / p^{2^{t-1}}$ hence $d_F = D_0^{1/2h} \cdot p^{1/2(h-2^{t-1})}$ as claimed.

Remark. If $D = p$ we find $d_F = p^{(h-1)/2}$ which was obtained by Gross in [5].

Case 3. Let $p = 2$. Then H/F has wild ramification at 2 and we must compute the higher ramification groups. Since $\mathrm{Gal}(H/F)$ is a subgroup of $\mathrm{Gal}(H/\mathbb{Q})$ we have $\mathrm{Gal}(H/F)_n = \mathrm{Gal}(H/\mathbb{Q})_n \cap \mathrm{Gal}(H/F)$. So the question is reduced to computing the

higher ramification groups for $\mathrm{Gal}(H/\mathbb{Q})$. These can be computed using Herbrand's Theorem from the knowledge of $\mathrm{Gal}(H/K)_n$ and $\mathrm{Gal}(K/\mathbb{Q})_n$.

Let $\mathcal{G}=\mathrm{Gal}(H/\mathbb{Q})$, $\mathcal{H}=\mathrm{Gal}(H/K)$, and $G=\mathrm{Gal}(K/\mathbb{Q})$. Since H/K is unramified $\mathcal{H}_n=0$ for $n\geqq 0$. If $4\|D$ then $G=G_0=G_1\supsetneq_2 G_2=0$. And if $8\|D$ the $G=G_0=G_1=G_2\supsetneq_2 G_3=0$. Following the notation of Serre [10, p. 73] we have the transition formula

$$\varphi_{H/K}(u)=\int_0^u (\mathcal{H}_0:\mathcal{H}_t)^{-1}\mathrm{d}t=\int_0^u 1\,dt=u.$$

So in particular $\varphi_{H/K}(n)=n$ for any integer $n\geqq 0$. Herbrand's Theorem gives $G_n=(\mathcal{G}/\mathcal{H})_n=(\mathcal{G}_n\mathcal{H})/\mathcal{H}$. So $\mathrm{Gal}(H/\mathbb{Q})_n=\mathrm{Gal}(K/\mathbb{Q})_n$ for all $n\geqq 0$. Using this fact it is easy to see that

$$\mathcal{D}_{H/F}=\prod_{i=1}^{2^{t-2}}\mathfrak{p}_i^a;\quad \text{where}\quad a=\begin{cases}2 & \text{if}\quad 4\|D\\ 3 & \text{if}\quad 8\|D\end{cases}.$$

A computation similar to that in case 2 reveals $d(\mathbb{Q}(j))=D_0^{1/2h}\cdot D_1^{1/2(h-2^{t-1})}$ as claimed. □

Acknowledgements. It is a pleasure to thank Benedict H. Gross for generously sharing his ideas with me and his encouragement during this investigation.

References

1. Borel, A., Chowla, S., Herz, C.S., Iwasawa, K., Serre, J.-P.: Seminar on Complex Multiplication. (Lecture Notes in Math. Vol. 21). Berlin Heidelberg New York: Springer 1966
2. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Semin. Hamb. **14**, 197–272 (1941)
3. Dorman, D.R.: Global orders in definite guaternion algebras as endomorphism rings for reduced CM elliptic curve. Proceedings of Conférence internationale de theorie des nombres (to appear)
4. Dorman, D.R.: Special values of the elliptic modular function and factorization formulae. J. Reine Angew. Math. **383**, 207–220 (1988)
5. Dummit, D.S., Gold, R., Kisilevsky, H.: The field generated by the discriminant of the class invariants of an imaginary quadratic field. Can. Math. Bull. **26**, 280–282 (1983)
6. Gross, B.H.: Arithmetic on elliptic curves with complex multiplication. (Lectures Notes in Math. Vol. 776). Berlin Heidelberg New York: Springer 1980
7. Gross, B.H., Zagier, D.B.: Heegner points and derivatives of L-Series. Invent. Math. **84**, 225–320 (1986)
8. Gross, B.H., Zagier, D.B.: On singular moduli. J. Reine Angew. Math. **355**, 191–220 (1985)
9. Rohrlich, D.E.: Elliptic curves with good reduction everywhere. J. Lond. Math. Soc. **25**, 216–222 (1982)
10. Serre, J.-P.: Local fields. Grad. Texts in Math. 67. Berlin Heidelberg New York: Springer 1979
11. Serre, J.-P., Tate, J.T.: Good reduction of abelian varities. Ann. Math. **88**, 492–517 (1968)
12. Vignéras, M.-F.: Arithmétique des algèbres de quaternions. (Lecture Notes in Math. Vol. 800). Berlin Heidelberg New York: Springer 1980

Received June 16, 1987