Compositio Mathematica **133:** 65–93, 2002.

Enumerating Quartic Dihedral Extensions of $\mathbb{Q}$

HENRI COHEN, FRANCISCO DIAZ Y DIAZ and MICHEL OLIVIER
Laboratoire A2X, UMR 5465 du CNRS, Université Bordeaux I, 351 Cours de la Libération, 33405 TALENCE Cedex, France. E-mail: {cohen,diaz,olivier}@math.u-bordeaux.fr

(Received: 26 January 2001; accepted in final form: 11 June 2001)

Abstract. We give an explicit Dirichlet series for the generating function of the discriminants of quartic dihedral extensions of $\mathbb{Q}$. From this series we deduce an asymptotic formula for the number of isomorphism classes of such quartic extensions with discriminant up to a given bound. On the other hand, by using essentially classical results of genus theory combined with elementary analytical methods such as the method of the hyperbola, we show how to compute exactly this number up to quite large bounds, and we give a table of selected values.

Mathematics Subject Classification (2000). 11R16, 11R29, 11R45, 11Y40.

Key words. discriminant densities, D_4-extensions.

1. Introduction and Main Results

1.1. PURPOSE OF THE PAPER

Denote by $N_4(G, X)$ the number of isomorphism classes of quartic extensions L of the field $\mathbb{Q}$ of rational numbers such that the Galois group of the Galois closure of $L/\mathbb{Q}$ is isomorphic to a transitive subgroup G of S_4. The goal of this paper is to give explicit formulas for computing $N_4(D_4, X)$, both asymptotically and exactly, where D_4 is the dihedral group of order 8. Recall that the Galois group of the Galois closure of a quartic field is isomorphic to C_4, $V_4 = C_2 \times C_2$, D_4, A_4, or S_4 with evident notation. The cases where the group G is Abelian, in other words isomorphic to C_4 or V_4, are of an elementary nature and are studied in detail in [4] and [5]. In particular, we have $N_4(C_4, X) \sim c(C_4)\, X^{1/2}$ and $N_4(V_4, X) \sim c(V_4)\, X^{1/2} \log^2 X$ for explicit constants $c(C_4)$ and $c(V_4)$ (more precise results are known, see [5]). The cases where G is isomorphic to A_4 and S_4 are much more difficult, and assuming the analytic continuation to $\mathrm{Re}(s) = 1$ of certain Dirichlet series, we can prove that $N_4(A_4, X) \sim c(A_4)\, X^{1/2} \log X$ and $N_4(S_4, X) \sim c(S_4)\, X$ for explicit constants $c(A_4)$ and $c(S_4)$. The case where G is isomorphic to D_4 is of intermediate difficulty and particularly pretty, and is the object of the present paper. Among other results we will show that $N_4(D_4, X) \sim c(D_4)\, X$ for an explicit constant $c(D_4)$. Assuming the above conjecture on S_4-extensions of $\mathbb{Q}$, this implies that the proportion of D_4-fields among all quartic fields is strictly positive, as was indicated by experimental results.

These results and conjectures also confirm heuristic predictions made by G. Malle in [11].

1.2. NOTATION

We will denote by $r_2(M)$ the 2-rank of a finite Abelian group M, in other words the $\mathbb{F}_2$-dimension of M/M^2.

For any number field k we will denote by $(r(k), i(k))$ the signature of k, so that $n = [k : \mathbb{Q}] = r(k) + 2i(k)$.

For any extension L/K of number fields, we will write $\mathfrak{d}(L/K)$ for the relative ideal discriminant of L/K.

If $\mathfrak{a}$ is a fractional ideal of K we write $\mathcal{N}(\mathfrak{a}) \in \mathbb{Q}_{>0}$ for the absolute norm of the ideal $\mathfrak{a}$.

Let G be a finite transitive permutation subgroup of S_n for some $n \geqslant 2$. We will denote by $\mathcal{F}_{K,n}(G)$ the set of K-isomorphism classes of extensions L of K of degree n such that the Galois group of the Galois closure of L/K in some fixed algebraic closure $\bar{K}$ of K is isomorphic to G. We will set

$$N_{K,n}(G, X) = |\{L \in \mathcal{F}_{K,n}(G),\ \mathcal{N}(\mathfrak{d}(L/K)) \leqslant X\}|,$$

and we let

$$\Phi_{K,n}(G, s) = \sum_{L \in \mathcal{F}_{K,n}(G)} \frac{1}{\mathcal{N}(\mathfrak{d}(L/K))^s}.$$

It is clear that, if we write $\Phi_{K,n}(G, s) = \sum_{m \geqslant 1} a_m m^{-s}$, we have $a_m \geqslant 0$ and $N_{K,n}(G, X) = \sum_{1 \leqslant m \leqslant X} a_m$, so that the Dirichlet series $\Phi_{K,n}(G, s)$ and the summatory function $N_{K,n}(G, X)$ are intimately linked via Abelian and Tauberian theorems. When $K = \mathbb{Q}$, we will omit the index K from the notation.

Finally, if d is an integer congruent to 0 or 1 modulo 4, we will denote by $L(s, d)$ the Dirichlet series associated to the quadratic character $(d/\cdot)$.

1.3. MAIN RESULTS

In this subsection, we summarize the main theoretical results of this paper. The last section of the paper is of a more algorithmic nature, and will enable us to give efficient methods for computing $N_4(D_4, X)$ for large values of X.

The first theorem that we will prove is the following:

THEOREM 1.1. *Let k be a number field. We have*

$$\Phi_{k,2}(C_2, s) = -1 + \frac{2^{-i(k)}}{\zeta_k(2s)} \sum_{\mathfrak{c}^2} \frac{\mathcal{N}(2/\mathfrak{c})}{\mathcal{N}(2/\mathfrak{c})^{2s}} \sum_{\chi} L_k(s, \chi),$$

where $\mathfrak{c}$ runs over all integral ideals of k dividing 2, χ runs over all quadratic characters of the ray class group $Cl_{\mathfrak{c}^2}(k)$ modulo $\mathfrak{c}^2$, and $L_k(s, \chi)$ is the Hecke L-function of k for the character χ.

From this theorem it is immediate to obtain the following corollary, which has been proved by a completely different method in [7].

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

COROLLARY 1.2. *By abuse of notation, write* $\zeta_k(1)$ *for the value of the residue of the Dedekind zeta function of* k *at* $s = 1$. *As* $X \longrightarrow \infty$, *we have*

$$N_{k,2}(C_2, X) \sim 2^{-i(k)} \frac{\zeta_k(1)}{\zeta_k(2)} X .$$

The most important theoretical result of this paper is the following theorem, which we will prove in Section 6:

THEOREM 1.3. *The Dirichlet series* $\Phi_4(D_4, s)$ *converges absolutely for* $\mathrm{Re}(s) > 1$ *and can be analytically continued to* $\mathrm{Re}(s) > 3/4$ *to a meromorphic function having a unique pole, at* $s = 1$, *which is simple with residue*

$$c(D_4) = \frac{1}{2} \sum_{k \in \mathcal{F}_2(C_2)} \frac{2^{-i(k)}}{d(k)^2} \frac{\zeta_k(1)}{\zeta_k(2)} = \frac{3}{\pi^2} \sum_D \frac{2^{-i(D)}}{D^2} \frac{L(1, D)}{L(2, D)} ,$$

where the last sum is over all fundamental discriminants different from 1(*i.e., discriminants of quadratic fields*), *and* $i(D) = i(\mathbb{Q}(\sqrt{D}))$, *in other words* $i(D) = 0$ *if* $D > 0$, $i(D) = 1$ *otherwise*.

From this theorem we deduce the following important corollary:

COROLLARY 1.4. *The number* $N_4(D_4, X)$ *of quartic* D_4*-extensions of* $\mathbb{Q}$ *up to isomorphism is asymptotic to* $c(D_4)\, X$, *where* $c(D_4)$ *is as above*.

Remark. Although for simplicity we will prove these results for dihedral quartic extensions of $\mathbb{Q}$, the same methods give similar but more complicated results for dihedral quartic extensions of any base field K.

1.4. CONTENTS OF THE PAPER

The plan of the paper will be as follows. In Section 2, we explain how the study of D_4-extensions can be reduced to the study of relative quadratic extensions. In Section 3, we prove Theorem 1.1, we give some applications, and we generalize to the case where one adds signature conditions. In Section 4, we describe explicitly the ray class group characters in terms of ordinary Kronecker–Jacobi symbols. This is essentially the genus theory of Gauss. We also explain how to use this to *construct* tables of relative quadratic extensions of a quadratic field. In Section 6, we deduce from the expression for $\Phi_{k,2}(C_2, s)$ the asymptotic formula for $N_4(D_4, X)$ given by Corollary 1.4. Finally, in Section 7, we obtain an efficient formula for computing *exactly* $N_4(D_4, X)$ for quite large values of X, and we give a table of such values for $X = 10^k$ with $1 \leqslant k \leqslant 17$.

2. Reduction to Relative Quadratic Extensions

If L/K is a D_4-extension, it has a unique quadratic subfield k, and we have the following lemma.

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

LEMMA 2.1. *Let L/K and L'/K be two quartic D_4-extensions of K considered to be in a fixed algebraic closure $\bar{K}$ of K, with respective quadratic subfields k and k'.*

(1) *If L and L' are K-isomorphic then $k' = k$ and L' is k-isomorphic either to L or to $\tau(L)$, where τ is an extension to L of the generator of* $\mathrm{Gal}(k/K)$.
(2) *Conversely, if $k' = k$ and if L' is k-isomorphic to L or to $\tau(L)$, then L and L' are K-isomorphic.*

Proof. For (1), if f is a K-isomorphism from L' to L the restriction f_2 of f to k' is a K-isomorphism from k' to k, hence since k and k' are subfields of $\bar{K}$ and Galois over K, $k' = k$ and $f_2 \in \mathrm{Gal}(k/K)$. If f_2 is the identity, f is a k-isomorphism (and in fact $L' = L$ since L/k is Galois), and if $f_2 = \tau$, then $\tau \circ f$ is a k-isomorphism of L' with $\tau(L)$ (so in fact $L' = \tau(L)$). Conversely, (2) is clear. □

Now recall that imprimitive quartic extensions of K can have three possible Galois groups: C_4, $V_4 = C_2 \times C_2$ and D_4. These can be combined as follows.

COROLLARY 2.2. *For any function $f(L)$ defined over K-isomorphism classes of number fields and such that the series below converge absolutely, we have the formal equality*

$$\sum_{k \in \mathcal{F}_{K,2}(C_2)} \sum_{L \in \mathcal{F}_{k,2}(C_2)} f(L) = 2 \sum_{L \in \mathcal{F}_{K,4}(D_4)} f(L) + \sum_{L \in \mathcal{F}_{K,4}(C_4)} f(L) + 3 \sum_{L \in \mathcal{F}_{K,4}(V_4)} f(L).$$

Proof. By the above lemma, the sum of the left will count twice D_4-extensions up to K-isomorphism for a given k, and two different k cannot give the same D_4-extension. A C_4-extension also contains a single k and can be obtained only once since it is Galois. Finally, a V_4-extension can be obtained once only, but for three different quadratic subfields k, proving the corollary. □

COROLLARY 2.3. (1) *We have*

$$2\Phi_{K,4}(D_4, s) + \Phi_{K,4}(C_4, s) + 3\Phi_{K,4}(V_4, s) = \sum_{k \in \mathcal{F}_{K,2}(C_2)} \sum_{L \in \mathcal{F}_{k,2}(C_2)} \frac{1}{\mathcal{N}(\mathfrak{d}(L/K))^s}.$$

(2) *We have*

$$\sum_{k \in \mathcal{F}_{K,2}(C_2)} \sum_{L \in \mathcal{F}_{k,2}(C_2)} \frac{1}{\mathcal{N}(\mathfrak{d}(L/K))^s} = \sum_{k \in \mathcal{F}_{K,2}(C_2)} \frac{1}{\mathcal{N}(\mathfrak{d}(k/K))^{2s}} \Phi_{k,2}(C_2, s).$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

(3) *Let* $N_{K,4}(I, X)$ *be defined by*

$$N_{K,4}(I, X) = \sum_{k \in \mathcal{F}_{K,2}(C_2)} \sum_{\substack{L \in \mathcal{F}_{k,2}(C_2) \\ \mathcal{N}\mathfrak{d}(L/K) \leqslant X}} 1 .$$

Then

$$N_{K,4}(I, X) = 2N_{K,4}(D_4, X) + N_{K,4}(C_4, X) + 3N_{K,4}(V_4, X).$$

(4) *We have*

$$N_{K,4}(I, X) = \sum_{\substack{k \in \mathcal{F}_{K,2}(C_2) \\ \mathcal{N}(\mathfrak{d}(k/K)) \leqslant X^{1/2}}} N_{k,2}(C_2, X/\mathcal{N}(\mathfrak{d}(k/K))^2) .$$

Proof. Statement (1) follows by applying Corollary 2.2 to the function $f(L) = \mathcal{N}(\mathfrak{d}(L/K))^{-s}$, and (2), (3), and (4) are immediate consequences of (1), of the definitions, and of the discriminant-conductor formula $\mathfrak{d}(L/K) = \mathfrak{d}(k/K)^2 \mathcal{N}_{k/K}(\mathfrak{d}(L/k))$. □

We are thus reduced to computing $\Phi_{k,2}(C_2, s)$ or, equivalently, $N_{k,2}(C_2, X)$.

3. Quadratic Extensions

The aim of this section is to prove Theorem 1.1. For this, we need some preliminary results.

3.1. SOME DEFINITIONS AND BASIC RESULTS

We will need the two basic notions of *virtual unit* and *Selmer group* (see [3], § 5.2.2).

DEFINITION 3.1. We will say that an element $u \in k^*$ is a *virtual unit* if there exists an ideal $\mathfrak{q}$ such that $u\mathbb{Z}_k = \mathfrak{q}^2$ or, equivalently, if the valuations of u at all prime ideals are even. The set of virtual units is a group $V(k)$, and we will call the quotient group $S(k) = V(k)/k^{*2}$ the *Selmer group* of k.

Note that properly speaking, we should talk about 2-virtual units and the 2-Selmer group, and write $S_2(k)$ instead of $S(k)$. Since in this paper we will only deal with 2-virtual units, we will drop the index 2 as we have done above.

LEMMA 3.2. *Let* $Cl(k) = \bigoplus_{i=1}^{s} (\mathbb{Z}/d_i\mathbb{Z})\overline{\mathfrak{a}_i}$ *be the decomposition of* $Cl(k)$ *into invariant factors, with* $d_{i+1} | d_i$ *for* $1 \leqslant i < s$. *Write* $\mathfrak{a}_i^{d_i} = \alpha_i \mathbb{Z}_k$ *for some elements* $\alpha_i \in k^*$. *On the other hand, let* $r_u(k) = r(k) + i(k) - 1$ *be the unit rank of* k, *let* $(\varepsilon_i)_{1 \leqslant i \leqslant r_u}$ *be a system of fundamental units of* k, *and let* ε_0 *be a generator of the group of roots of unity in* k.

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

The Selmer group $S(k)$ is an $\mathbb{F}_2$-vector space with basis formed by the classes of the α_i for $1 \leqslant i \leqslant r_2(Cl(k))$ together with the classes of the ε_i for $0 \leqslant i \leqslant r_u$. In particular, the dimension $r_v(k)$ of $S(k)$ is equal to $r(k) + i(k) + r_2(Cl(k))$, hence its cardinality is equal to $2^{r_v(k)}$.

Proof. For the (easy) proof of this proposition, we refer to [3], Proposition 5.2.5. □

Coming back to our specific problem, we start with the following lemma.

LEMMA 3.3. *There exists a bijection between k-isomorphism classes of quadratic extensions of k and pairs $(\mathfrak{a}, \bar{u})$ satisfying the following properties:*

(1) *the ideal $\mathfrak{a}$ is integral and squarefree;*
(2) *the class of $\mathfrak{a}$ in $Cl(k)$ is the square of a class, in other words there exists $\alpha_0 \in k$ and an ideal $\mathfrak{q}$ such that $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathbb{Z}_k$;*
(3) *the class $\bar{u}$ belongs to the Selmer group $S(k)$;*
(4) *if $\mathfrak{a} = \mathbb{Z}_k$ then $\bar{u} \neq \overline{1/\alpha_0}$.*

If $(\mathfrak{a}, \bar{u})$ is such a pair and α_0 is chosen as above, the corresponding extension is $k(\sqrt{\alpha_0 u})$ for any lift of $\bar{u}$.

Proof. If L/k is a quadratic extension, we can write $L = k(\sqrt{\alpha_0})$ for some $\alpha_0 \in k^* - k^{*2}$. Let $\mathfrak{a}$ be the ideal squarefree part of α_0, in other words define $\mathfrak{a} = \prod_{v_\mathfrak{p}(\alpha_0) \equiv 1 \pmod 2} \mathfrak{p}$. By definition, there exists an ideal $\mathfrak{q}$ such that $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathbb{Z}_k$. If α_1 is another element of k defining an isomorphic extension, then $\alpha_1/\alpha_0 \in k^{*2}$, hence the squarefree part of α_1 is equal to that of α_0. Thus, the squarefree ideal $\mathfrak{a}$ is uniquely defined by the quadratic extension L/k.

Thus, fix an integral squarefree ideal $\mathfrak{a}$ such that there exists an ideal $\mathfrak{q}$ with $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathbb{Z}_k$ a principal ideal. The set of α having the same squarefree part is the set of α such that $\mathfrak{a}\mathfrak{q}_1^2 = \alpha\mathbb{Z}_k$ for some ideal $\mathfrak{q}_1$ or, equivalently, such that $(\alpha/\alpha_0)\mathbb{Z}_k = (\mathfrak{q}_1/\mathfrak{q})^2$. By definition, this means that $u = \alpha/\alpha_0$ is a virtual unit.

Finally, if u is a virtual unit, the element $u\alpha_0$ will define a quadratic extension if and only if $u\alpha_0 \notin k^{*2}$. Since u is a virtual unit this can happen only if the squarefree part $\mathfrak{a}$ of α_0 is equal to $\mathbb{Z}_k$, and in this case we must have $\bar{u}\overline{\alpha_0} \neq \bar{1}$ in $S(k)$, finishing the proof of the lemma. □

The next result is the basic tool for proving Theorem 1.1.

PROPOSITION 3.4. *Let $L = k(\sqrt{\alpha_0 u})$ be the quadratic extension of k corresponding to the pair $(\mathfrak{a}, \bar{u})$ as above where, without loss of generality, we may assume that the ideal $\mathfrak{q}$ such that $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathbb{Z}_k$ is coprime to $2\mathbb{Z}_k$, and the lift u is also chosen coprime to $2\mathbb{Z}_k$. Then $\mathfrak{d}(L/k) = 4\mathfrak{a}/\mathfrak{c}^2$, where $\mathfrak{c}$ is the largest ideal (for divisibility or, equivalently, for reverse inclusion) such that $\mathfrak{c}|2$, $(\mathfrak{c}, \mathfrak{a}) = 1$, and the congruence $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ is soluble.*

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

In the above proposition, $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ has the usual multiplicative meaning of class field theory, in other words it is equivalent to $v_\mathfrak{p}(x^2 - \alpha_0 u) \geqslant 2v_\mathfrak{p}(\mathfrak{c})$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{c}$.

Proof. This proposition is an easy consequence of Hecke's theorem giving the conductor of a cyclic Kummer extension of prime degree ℓ (see [3], Theorem 10.2.9), in this case for $\ell = 2$. Set $\alpha = \alpha_0 u$. Since u is a virtual unit, the ideal $\mathfrak{a}$ is the squarefree part of α, hence for any prime ideal $\mathfrak{p}$, $v_\mathfrak{p}(\alpha) \equiv v_\mathfrak{p}(\mathfrak{a}) \pmod 2$. We will prove the equality $\mathfrak{d}(L/k) = 4\mathfrak{a}/\mathfrak{c}^2$ by showing that for every prime ideal $\mathfrak{p}$ the valuations of both sides are equal.

We consider three cases. Assume first that $v_\mathfrak{p}(\alpha)$ is odd or, equivalently, that $\mathfrak{p}|\mathfrak{a}$. In this case Hecke's theorem mentioned above or an easy Eisenstein type argument tells us that

$$v_\mathfrak{p}(\mathfrak{d}(L/k)) = 2e(\mathfrak{p}/2) + 1 = v_\mathfrak{p}(4\mathfrak{a}) = v_\mathfrak{p}(4\mathfrak{a}/\mathfrak{c}^2),$$

since $v_\mathfrak{p}(\mathfrak{c}) = 0$ in this case. In this formula, $e(\mathfrak{p}/2)$ is the ramification index of $\mathfrak{p}$ above 2, and in particular is equal to 0 if $\mathfrak{p}$ is not above 2.

We can thus assume that $v_\mathfrak{p}(\alpha)$ is even, so that $\mathfrak{p} \nmid \mathfrak{a}$. But then Hecke's theorem or an easy argument tells us that if $\mathfrak{p} \nmid 2$ we have $v_\mathfrak{p}(\mathfrak{d}(L/k)) = 0 = v_\mathfrak{p}(4\mathfrak{a}/\mathfrak{c}^2)$.

Finally assume that $v_\mathfrak{p}(\alpha)$ is even, so that $\mathfrak{p} \nmid \mathfrak{a}$, and that $\mathfrak{p}|2$. By our choice of $\mathfrak{q}$ and u, we have in fact $v_\mathfrak{p}(\alpha) = 0$. The harder part of Hecke's theorem tells us that in this case, if the congruence $x^2 \equiv \alpha \pmod{{}^*\mathfrak{p}^t}$ has a solution for $t = 2e(\mathfrak{p}/2)$ then $\mathfrak{p}$ is unramified in L/k, so that $v_\mathfrak{p}(\mathfrak{d}(L/k)) = 0 = v_\mathfrak{p}(4\mathfrak{a}/\mathfrak{c}^2)$ since $v_\mathfrak{p}(\mathfrak{c}) = e(\mathfrak{p}/2)$ in this case, and otherwise, if $t_0 < 2e(\mathfrak{p}/2)$ is the largest value of t for which the congruence has a solution, then t_0 is odd and we have $v_\mathfrak{p}(\mathfrak{d}(L/k)) = 2e(\mathfrak{p}/2) - (t_0 - 1)$. But then by definition $v_\mathfrak{p}(\mathfrak{c}) = (t_0 - 1)/2$, hence $v_\mathfrak{p}(\mathfrak{d}(L/k)) = v_\mathfrak{p}(4\mathfrak{a}) - 2v_\mathfrak{p}(\mathfrak{c}) = v_\mathfrak{p}(4\mathfrak{a}/\mathfrak{c}^2)$, finishing the proof of the proposition. □

To apply the above proposition to our needs, we first prove a few more results.

LEMMA 3.5. *Let $\mathfrak{c}$ be an ideal dividing 2, and let $\mathfrak{a}$ be an integral ideal coprime to $\mathfrak{c}$ such that there exists an ideal $\mathfrak{q}$ also coprime to $\mathfrak{c}$ with $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathbb{Z}_k$ as above (so that, in particular, α_0 is coprime to $\mathfrak{c}$). The following two conditions are equivalent.*

(1) *There exists an element $\bar{u}$ of the Selmer group such that, for any lift u of $\bar{u}$ coprime to $\mathfrak{c}$, the congruence $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ has a solution.*
(2) *The class of $\mathfrak{a}$ in the ray class group $Cl_{\mathfrak{c}^2}(k)$ is a square.*

Proof. Note first that, by the approximation theorem, there always exists a lift of an element of the Selmer group coprime to anything we want, and that the solubility of the given congruence is independent of the chosen lift, since such lifts only differ by a square coprime to $\mathfrak{c}$. Thus, assume (1). Then $x^2 = \alpha_0 u\beta$ with $\beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}$, and since $u\mathbb{Z}_k = \mathfrak{q}_1^2$ for some ideal $\mathfrak{q}_1$, we have $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathbb{Z}_k =$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

$x^2/(\mathfrak{q}_1^2\beta)$ so that $\mathfrak{a} = \mathfrak{q}_2^2\beta'$ with $\mathfrak{q}_2 = x/(\mathfrak{q}\mathfrak{q}_1)$ and $\beta' = 1/\beta \equiv 1 \pmod{^*\mathfrak{c}^2}$, so the class of $\mathfrak{a}$ is a square in $Cl_{\mathfrak{c}^2}(k)$.

Conversely, if this is the case then there exists $\mathfrak{q}_2$ and $\beta' \equiv 1 \pmod{^*\mathfrak{c}^2}$ such that $\mathfrak{a} = \mathfrak{q}_2^2\beta'$, so that $\alpha_0\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2 = (\mathfrak{q}\mathfrak{q})^2\beta'$, hence β'/α_0 is a virtual unit u coprime to $\mathfrak{c}$, and $\alpha_0 u = \beta' \equiv 1^2 \pmod{^*\mathfrak{c}^2}$ so the congruence of the lemma has a solution, finishing the proof. □

DEFINITION 3.6. Let $\mathfrak{c}$ be an ideal dividing 2. We define the ray *Selmer group modulo* $\mathfrak{c}^2$ as the subgroup $S_{\mathfrak{c}^2}(k)$ of $S(k)$ of elements $\bar{u}$ such that for some (or, equivalently, any) lift u of $\bar{u}$ coprime to $\mathfrak{c}$ there exists a solution to the congruence $x^2 \equiv u \pmod{^*\mathfrak{c}^2}$.

We have mentioned in Lemma 3.2 that the Selmer group is an $\mathcal{F}_2$-vector space of dimension $r_v(k) = r_u(k) + 1 + r_2(Cl(k))$, hence that its cardinality is $2^{r_v(k)}$. The structure of ray Selmer groups is also easily given. We start by the following lemmas.

LEMMA 3.7. *To simplify notation, set* $Z_{\mathfrak{c}} = (\mathbb{Z}_K/\mathfrak{c}^2)^*$. *There exists a natural exact sequence*

$$1 \longrightarrow S_{\mathfrak{c}^2}(k) \longrightarrow S(k) \longrightarrow Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2 \longrightarrow Cl_{\mathfrak{c}^2}(k)/Cl_{\mathfrak{c}^2}(k)^2 \longrightarrow Cl(k)/Cl(k)^2 \longrightarrow 1.$$

Proof. Recall the basic exact sequence involving ray class groups

$$Z_{\mathfrak{c}} \longrightarrow Cl_{\mathfrak{c}^2}(k) \longrightarrow Cl(k) \longrightarrow 1.$$

Since tensoring by $\mathbb{F}_2$ is a right exact functor (or, of course, directly), we deduce that the sequence $Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2 \longrightarrow Cl_{\mathfrak{c}^2}(k)/Cl_{\mathfrak{c}^2}(k)^2 \longrightarrow Cl(k)/Cl(k)^2 \longrightarrow 1$ is exact. Now let $\bar{\alpha} \in Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2$ be such that the class of $\alpha\mathbb{Z}_k$ is trivial in $Cl_{\mathfrak{c}^2}(k)/Cl_{\mathfrak{c}^2}(k)^2$. This means that there exists an ideal $\mathfrak{q}$ and an element $\beta \equiv 1 \pmod{^*\mathfrak{c}^2}$ such that $\alpha\mathbb{Z}_k = \mathfrak{q}^2\beta$, so that $\alpha = \beta u$ with u a virtual unit, hence the class of α in $Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2$ is equal to that of u, proving exactness at $Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2$. Finally, the ray Selmer group $S_{\mathfrak{c}^2}(k)$ is by definition the kernel of the natural map from $S(k)$ to $Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2$, proving the lemma. □

LEMMA 3.8. *Let* $\mathfrak{c}$ *be an ideal dividing* 2. *The congruence* $x^2 \equiv 1 \pmod{^*\mathfrak{c}^2}$ *is equivalent to* $x \equiv 1 \pmod{^*\mathfrak{c}}$.

Proof. Immediate and left to the reader. □

We can now easily compute the cardinality of $S_{\mathfrak{c}^2}(k)$.

PROPOSITION 3.9. *Let* $\mathfrak{c}$ *be an ideal dividing* 2, *and set* $\mathcal{N}(\mathfrak{c}) = 2^{r_2(\mathbb{Z}_k/\mathfrak{c})}$. *Then the ray Selmer group* $S_{\mathfrak{c}^2}(k)$ *is an* $\mathbb{F}_2$*-vector space of dimension* $r_u(k) + 1 + r_2(Cl_{\mathfrak{c}^2}(k)) - r_2(\mathbb{Z}_k/\mathfrak{c})$, *or in other words its cardinality is given by*

$$|S_{\mathfrak{c}^2}(k)| = \frac{2^{r_u(k)+1+r_2(Cl_{\mathfrak{c}^2}(k))}}{\mathcal{N}(\mathfrak{c})}$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

Proof. By the above exact sequence, we have

$$|S_{\mathfrak{c}^2}(k)||Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2||Cl(k)/Cl(k)^2| = |S(k)||Cl_{\mathfrak{c}^2}(k)/Cl_{\mathfrak{c}^2}(k)^2|,$$

and since by Lemma 3.2 we know that $|S(k)| = 2^{r_u(k)+1}|Cl(k)/Cl(k)^2|$, we obtain

$$|S_{\mathfrak{c}^2}(k)| = \frac{2^{r_u(k)+1+r_2(Cl_{\mathfrak{c}}^2(k))}}{|Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2|} .$$

Now consider the squaring map from $Z_{\mathfrak{c}}$ to itself. By definition, its image is equal to $Z_{\mathfrak{c}}^2$, hence $|Z_{\mathfrak{c}}/Z_{\mathfrak{c}}^2|$ is equal to the cardinality of its kernel. Lemma 3.8 tells us that this kernel is the subgroup of classes modulo $\mathfrak{c}^2$ of elements x congruent to 1 modulo $\mathfrak{c}$. By the map $x \mapsto x - 1$, this multiplicative group is isomorphic to the additive group $\mathfrak{c}/\mathfrak{c}^2$, and we have

$$|\mathfrak{c}/\mathfrak{c}^2| = |(\mathbb{Z}_k/\mathfrak{c}^2)/(\mathbb{Z}_k/\mathfrak{c})| = \mathcal{N}(\mathfrak{c}^2)/\mathcal{N}(\mathfrak{c}) = \mathcal{N}(\mathfrak{c}) ,$$

proving the proposition. □

3.2. PROOF OF THEOREM 1.1

In the following proof, it is understood that all lifts of elements of $S(k)$ are taken to be coprime to $2\mathbb{Z}_k$, which can always be done.

Using Lemma 3.3 and its notation, we have

$$\Phi_{k,2}(C_2, s) = \sum_{(\mathfrak{a},\bar{u})} \mathcal{N}(\mathfrak{d}(k(\sqrt{\alpha_0 u})/k))^{-s} ,$$

where $(\mathfrak{a}, \bar{u})$ ranges over pairs of an ideal $\mathfrak{a}$ and an element of $S(k)$ satisfying the conditions of the lemma. By Proposition 3.4, we have $\mathfrak{d}(k(\sqrt{\alpha_0 u})/k) = 4\mathfrak{a}/\mathfrak{c}^2$, where $\mathfrak{c} = \mathfrak{c}(\alpha_0 u, \mathfrak{a})$ is given by the proposition. Note that, if $\mathfrak{a} = \mathbb{Z}_k$ and $\alpha_0 u$ is a square (which is the excluded case of Lemma 3.3 because it corresponds to the trivial extension k/k), the formula of Proposition 3.4 gives in this case $\mathfrak{d}(L/k) = \mathbb{Z}_k$ as it should. Thus,

$$\Phi_{k,2}(C_2, s) = -1 + 4^{-ns} \sum_{\substack{\mathfrak{a} \text{ squarefree} \\ \exists \mathfrak{q}, \mathfrak{a}\mathfrak{q}^2 = \alpha_0 \mathbb{Z}_k}} \mathcal{N}(\mathfrak{a})^{-s} S(\alpha_0, \mathfrak{a})$$

with

$$S(\alpha_0, \mathfrak{a}) = \sum_{\bar{u} \in S(k)} \mathcal{N}(\mathfrak{c}(\alpha_0 u, \mathfrak{a}))^{2s} = \sum_{\substack{\mathfrak{c} \mid 2 \\ (\mathfrak{c}, \mathfrak{a}) = 1}} \mathcal{N}(\mathfrak{c})^{2s} T(\alpha_0, \mathfrak{a}, \mathfrak{c}),$$

where

$$T(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\substack{\bar{u} \in S(k) \\ \mathfrak{c}(\alpha_0 u, \mathfrak{a}) = \mathfrak{c}}} 1.$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

Recall that, by Proposition 3.4 , the condition $\mathfrak{c}(\alpha_0 u, \mathfrak{a}) = \mathfrak{c}$ means that $\mathfrak{c}$ is the largest ideal dividing 2 and coprime to $\mathfrak{a}$ such that the congruence $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ is soluble. Hence, if we set

$$f(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\substack{\tilde{u} \in S(k) \\ \exists x\, x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}}} 1,$$

then for every $\mathfrak{c} \mid 2$ we have

$$f(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\substack{\mathfrak{c} \mid \mathfrak{c}_1 \mid 2 \\ (\mathfrak{c}_1, \mathfrak{a}) = 1}} T(\alpha_0, \mathfrak{a}, \mathfrak{c}_1).$$

Thus, by a form of the Möbius inversion formula applied to the functions $T(\alpha_0, \mathfrak{a}, 2/\mathfrak{c}_1)$ and $f(\alpha_0, \mathfrak{a}, 2/\mathfrak{c})$ we obtain

$$T(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\substack{\mathfrak{d} \mid 2/\mathfrak{c} \\ (\mathfrak{d}, \mathfrak{a}) = 1}} \mu(\mathfrak{d}) f(\alpha_0, \mathfrak{a}, \mathfrak{c}\mathfrak{d}),$$

hence

$$\begin{aligned} S(\alpha_0, \mathfrak{a}) &= \sum_{\substack{\mathfrak{c} \mid 2 \\ (\mathfrak{c}, \mathfrak{a}) = 1}} \mathcal{N}(\mathfrak{c})^{2s} T(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\substack{\mathfrak{c} \mid 2 \\ (\mathfrak{c}, \mathfrak{a}) = 1}} \mathcal{N}(\mathfrak{c})^{2s} \sum_{\substack{\mathfrak{d} \mid 2/\mathfrak{c} \\ (\mathfrak{d}, \mathfrak{a}) = 1}} \mu(\mathfrak{d}) f(\alpha_0, \mathfrak{a}, \mathfrak{c}\mathfrak{d}) \\ &= \sum_{\substack{\mathfrak{c}_1 \mid 2 \\ (\mathfrak{c}_1, \mathfrak{a}) = 1}} f(\alpha_0, \mathfrak{a}, \mathfrak{c}_1) \sum_{\mathfrak{c} \mid \mathfrak{c}_1} \mu(\mathfrak{c}_1/\mathfrak{c}) \mathcal{N}(\mathfrak{c})^{2s} \\ &= \sum_{\substack{\mathfrak{c} \mid 2 \\ (\mathfrak{c}, \mathfrak{a}) = 1}} f(\alpha_0, \mathfrak{a}, \mathfrak{c}) \mathcal{N}(\mathfrak{c})^{2s} \prod_{\mathfrak{p} \mid \mathfrak{c}} (1 - \mathcal{N}(\mathfrak{p})^{-2s}). \end{aligned}$$

Assume for now the following lemma:

LEMMA 3.10. *Let* $\mathfrak{a}\mathfrak{q}^2 = \alpha_0 \mathbb{Z}_k$ *as above with* $(\mathfrak{a}, \mathfrak{c}) = 1$. *Then* $f(\alpha_0, \mathfrak{a}, \mathfrak{c}) = 0$ *if the class of* $\mathfrak{a}$ *is not a square in* $Cl_{\mathfrak{c}^2}(k)$, *and otherwise* $f(\alpha_0, \mathfrak{a}, \mathfrak{c}) = |S_{\mathfrak{c}^2}(k)|$.

It follows from the formula given above for $S(\alpha_0, \mathfrak{a})$, from this lemma, and from Proposition 3.9 that

$$\begin{aligned} \Phi_{k,2}(C_2, s) &= -1 + \frac{1}{4^{ns}} \sum_{\substack{\mathfrak{a} \text{ squarefree} \\ \exists \mathfrak{q},\ \mathfrak{a}\mathfrak{q}^2 = \alpha_0 \mathbb{Z}_k}} \frac{S(\alpha_0, \mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \\ &= -1 + \frac{1}{4^{ns}} \sum_{\mathfrak{c} \mid 2} |S_{\mathfrak{c}^2}(k)| \mathcal{N}(\mathfrak{c})^{2s} \prod_{\mathfrak{p} \mid \mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^{2s}}\right) \sum_{\substack{\mathfrak{a} \text{ squarefree} \\ (\tilde{\mathfrak{a}}, \mathfrak{c}) = 1 \\ \tilde{\mathfrak{a}} \in Cl_{\mathfrak{c}^2}(k)^2}} \frac{1}{\mathcal{N}(\mathfrak{a})^s} \\ &= -1 + \frac{2^{r_u(k)+1}}{4^{ns}} \sum_{\mathfrak{c} \mid 2} \mathcal{N}(\mathfrak{c})^{2s-1} \prod_{\mathfrak{p} \mid \mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^{2s}}\right) \sum_{\chi} \sum_{\substack{\mathfrak{a} \text{ squarefree} \\ (\mathfrak{a}, \mathfrak{c}) = 1}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \end{aligned}$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

where, as in the theorem, the sum on χ is over all $2^{r_2(Cl_{\mathfrak{c}^2}(k))}$ quadratic characters of $Cl_{\mathfrak{c}^2}(k)$. We have of course used the relation $\sum_\chi \chi(\mathfrak{a}) = 0$ if the class of $\mathfrak{a}$ is not a square in $Cl_{\mathfrak{c}^2}(k)$, and equal to $2^{r_2(Cl_{\mathfrak{c}^2}(k))}$ otherwise. Now since χ is a quadratic character,

$$\sum_{\substack{\mathfrak{a}\ \text{squarefree}\\(\mathfrak{a},\mathfrak{c})=1}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{c}}(1+\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}\nmid\mathfrak{c}}\frac{1-\mathcal{N}(\mathfrak{p})^{-2s}}{1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}$$
$$= \frac{L_k(s,\chi)}{\zeta_k(2s)\prod_{\mathfrak{p}|\mathfrak{c}}(1-\mathcal{N}(\mathfrak{p})^{-2s})}.$$

Replacing, we obtain finally

$$\Phi_{k,2}(C_2,s) = -1 + \frac{2^{r_u(k)+1}}{4^{ns}\zeta_k(2s)}\sum_{\mathfrak{c}|2}\mathcal{N}(\mathfrak{c})^{2s-1}\sum_\chi L_k(s,\chi)$$
$$= -1 + \frac{1}{2^{i(k)}\zeta_k(2s)}\sum_{\mathfrak{c}|2}\mathcal{N}(2/\mathfrak{c})^{1-2s}\sum_\chi L_k(s,\chi),$$

finishing the proof of Theorem 1.1.

It remains to prove the lemma. The first statement is Lemma 3.5. For the second, assume that the class of $\mathfrak{a}$ is a square in $Cl_{\mathfrak{c}^2}(k)$ or, equivalently, that there exists $\bar{v}\in S(k)$ such that $x^2 \equiv \alpha_0 v \pmod{{}^*\mathfrak{c}^2}$ is soluble for some $x_0 \in k$. Then for any $\bar{u}\in S(k)$ the congruence $x^2 \equiv \alpha_0 u \pmod{{}^*\mathfrak{c}^2}$ is equivalent to $(x/x_0)^2 \equiv (u/v) \pmod{{}^*\mathfrak{c}^2}$, hence to $\bar{u}\in \bar{v}S_{\mathfrak{c}^2}(k)$ which has cardinality $|S_{\mathfrak{c}^2}(k)|$, thus proving the lemma. □

3.3. PROOF OF COROLLARY 1.2

It is clear that $\Phi_{k,2}(C_2,s)$ is a Dirichlet series with nonnegative coefficients, and by Theorem 1.1, this series extends to the whole complex plane into a meromorphic function. In addition, the only pole of $\Phi_{k,2}(C_2,s)$ for $\mathrm{Re}(s) > 1/2$ is at $s=1$. The L-functions $L_k(s,\chi)$ are holomorphic at $s=1$ (in fact everywhere) except if χ is the trivial character $\chi_{0,\mathfrak{c}}$ of $Cl_{\mathfrak{c}^2}(k)$, and in this case

$$L_k(s,\chi_{0,\mathfrak{c}}) = \zeta_k(s)\prod_{\mathfrak{p}|\mathfrak{c}}(1-\mathcal{N}(\mathfrak{p})^{-s}),$$

hence the residue of $L_k(s,\chi_{0,\mathfrak{c}})$ at $s=1$ is equal to

$$\zeta_k(1)\prod_{\mathfrak{p}|\mathfrak{c}}(1-1/\mathcal{N}(\mathfrak{p})).$$

Thus, the residue of $\Phi_{k,2}(C_2,s)$ at $s=1$ is equal to $2^{-i(k)}(\zeta_k(1)/\zeta_k(2))S$ with

$$S = \sum_{\mathfrak{c}|2}\mathcal{N}(2/\mathfrak{c})^{-1}\prod_{\mathfrak{p}|\mathfrak{c}}(1-1/\mathcal{N}(\mathfrak{p}))$$
$$= \sum_{\mathfrak{c}|2}\frac{\mathcal{N}(\mathfrak{c})}{\mathcal{N}(2\mathbb{Z}_k)}\frac{\phi(\mathfrak{c})}{\mathcal{N}(\mathfrak{c})} = \frac{1}{\mathcal{N}(2\mathbb{Z}_k)}\sum_{\mathfrak{c}|2}\phi(\mathfrak{c}) = 1,$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

using the immediate generalization to ideals of the formula $\sum_{d|N}\phi(d)=N$. We conclude the proof of the corollary by applying a well-known Tauberian theorem, or in this case, more simply by contour integration. □

This corollary, which deserves to be better known, is due to Datskovsky and Wright (see [7]), although their proof is totally different. This is also the case for Corollary 3.14 which we shall see below.

3.4. EXTENSIONS WITH SIGNATURES

It is easy to generalize Theorem 1.1 to the case where we want to distinguish between different signatures.

Let k be a number field of signature $(r(k), i(k))$, let $\mathfrak{m}_\infty$ be a set of real places of k, and let $\mathfrak{n}_\infty$ be the set of real places of k not belonging to $\mathfrak{m}_\infty$. We denote by $\mathcal{F}_{k,2,\mathfrak{m}_\infty}(C_2)$ the set of k-isomorphism classes of quadratic extensions k such that the places of $\mathfrak{m}_\infty$ ramify in L/k and the places in $\mathfrak{n}_\infty$ do not ramify in L/k, so that in particular $r(L)=2(r(k)-|\mathfrak{m}_\infty|)=2|\mathfrak{n}_\infty|$. We define similarly $N_{k,2,\mathfrak{m}_\infty}(C_2,X)$ and $\Phi_{k,2,\mathfrak{m}_\infty}(C_2,s)$. The result is as follows:

THEOREM 3.11. *Keep the above notation, and denote by $\delta_{a,b}$ the Kronecker δ-symbol. we have*

$$\Phi_{k,2,\mathfrak{m}_\infty}(C_2,s)=-\delta_{\mathfrak{m}_\infty,\emptyset}+\frac{(-1)^{|\mathfrak{m}_\infty|}}{2^{i(k)}\zeta_k(2s)}\times$$

$$\times\sum_{\substack{\mathfrak{c}|2\\ \mathfrak{c}_\infty\supset\mathfrak{n}_\infty}}\frac{(-1)^{|\mathfrak{c}_\infty|}}{2^{|\mathfrak{c}_\infty|}}\frac{\mathcal{N}(2/\mathfrak{c})}{\mathcal{N}(2/\mathfrak{c})^{2s}}\sum_{\chi}L_k(s,\chi),$$

where $\mathfrak{c}$ runs over all integral ideals of k dividing 2, $\mathfrak{c}_\infty$ runs through all subsets of the real places of k containing $\mathfrak{n}_\infty$, and χ runs over all quadratic characters of the ray class group $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}(k)$ modulo $\mathfrak{c}^2\mathfrak{c}_\infty$.

Proof. Since the proof is very similar to that of Theorem 1.1, we give only a sketch. The trivial extension k/k occurs if and only if $\mathfrak{m}_\infty=\emptyset$ (equivalently, the condition $\sigma(\alpha_0 u)<0$ for $\sigma\in\mathfrak{m}_\infty$ given below automatically excludes $\overline{\alpha_0 u}=\bar{1}$ if $\mathfrak{m}\neq\emptyset$). Thus,

$$\Phi_{k,2,\mathfrak{m}_\infty}(C_2,s)=-\delta_{\mathfrak{m}_\infty,\emptyset}+4^{-ns}\sum_{\substack{\mathfrak{a}\text{ squarefree}\\ \exists\mathfrak{q},\ \mathfrak{a}\mathfrak{q}^2=\alpha_0\mathbb{Z}_k}}\mathcal{N}(\mathfrak{a})^{-s}S(\alpha_0,\mathfrak{a},\mathfrak{m}_\infty)$$

with

$$S(\alpha_0,\mathfrak{a},\mathfrak{m}_\infty)=\sum_{\substack{\bar{u}\in S(k)\\ \sigma(\alpha_0 u)>0\text{ for }\sigma\in\mathfrak{n}_\infty\\ \sigma(\alpha_0 u)<0\text{ for }\sigma\in\mathfrak{m}_\infty}}\mathcal{N}(\mathfrak{c}(\alpha_0 u,\mathfrak{a}))^{2s}=\sum_{\substack{\mathfrak{c}|2\\ (\mathfrak{c},\mathfrak{a})=1}}\mathcal{N}(\mathfrak{c})^{2s}T(\alpha_0,\mathfrak{a},\mathfrak{c},\mathfrak{m}_\infty),$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

where

$$T(\alpha_0, \mathfrak{a}, \mathfrak{c}, \mathfrak{m}_\infty) = \sum_{\substack{\bar{u}\in S(k)\\ \mathfrak{c}(\alpha_0 u,\mathfrak{a})=\mathfrak{c}\\ \sigma(\alpha_0 u)>0 \text{ for } \sigma\in\mathfrak{n}_\infty\\ \sigma(\alpha_0 u)<0 \text{ for } \sigma\in\mathfrak{m}_\infty}} 1.$$

For every $\mathfrak{c}|2$ and $\mathfrak{c}_\infty \supset \mathfrak{n}_\infty$, we set

$$f(\alpha_0, \mathfrak{a}, \mathfrak{c}, \mathfrak{c}_\infty) = \sum_{\substack{\bar{u}\in S(k)\\ \exists x\, x^2\equiv\alpha_0 u \pmod{{}^*\mathfrak{c}^2}\\ \sigma(\alpha_0 u)>0 \text{ for } \sigma\in\mathfrak{c}_\infty}} 1.$$

Then for every $\mathfrak{c}|2$ we have

$$f(\alpha_0, \mathfrak{a}, \mathfrak{c}, \mathfrak{c}_\infty) = \sum_{\substack{\mathfrak{c}|\mathfrak{c}_1|2\\ (\mathfrak{c}_1,\mathfrak{a})=1}} \sum_{\mathfrak{b}_\infty\supset\mathfrak{c}_\infty} T(\alpha_0, \mathfrak{a}, \mathfrak{c}_1, \complement\mathfrak{b}_\infty),$$

where $\complement\mathfrak{b}_\infty$ is the complement of $\mathfrak{b}_\infty$ in the set of real places of k. By ideal-theoretic and set-theoretic Möbius inversion ($\sum_{A\subset B}(-1)^{|A|}$ is equal to 0 if $B\neq\emptyset$, to 1 otherwise), we obtain

$$T(\alpha_0, \mathfrak{a}, \mathfrak{c}, \mathfrak{m}_\infty) = \sum_{\substack{\mathfrak{d}|2/\mathfrak{c}\\ (\mathfrak{d},\mathfrak{a})=1}} \sum_{\mathfrak{c}_\infty\supset\mathfrak{n}_\infty} \mu(\mathfrak{d})(-1)^{|\mathfrak{c}_\infty-\mathfrak{n}_\infty|} f(\alpha_0, \mathfrak{a}, \mathfrak{c}\mathfrak{d}, \mathfrak{c}_\infty).$$

It follows as before that

$$S(\alpha_0, \mathfrak{a}, \mathfrak{m}_\infty) = \sum_{\substack{\mathfrak{c}|2\\ (\mathfrak{c},\mathfrak{a})=1}} \sum_{\mathfrak{c}_\infty\supset\mathfrak{n}_\infty} (-1)^{|\mathfrak{c}_\infty-\mathfrak{n}_\infty|} f(\alpha_0, \mathfrak{a}, \mathfrak{c}, \mathfrak{c}_\infty)\mathcal{N}(\mathfrak{c})^{2s} \prod_{\mathfrak{p}|\mathfrak{c}}(1-\mathcal{N}(\mathfrak{p})^{-2s}).$$

The analog of Lemma 3.10 tells us that $f(\alpha_0, \mathfrak{a}, \mathfrak{c}, \mathfrak{c}_\infty)$ is equal to 0 if the class of $\mathfrak{a}$ is not a square in the ray class group $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}(k)$, and is equal to $|S_{\mathfrak{c}^2\mathfrak{c}_\infty}(k)|$ otherwise, where

$$S_{\mathfrak{c}^2\mathfrak{c}_\infty}(k) = \{\bar{u}\in S(k),\ \exists x\ x^2\equiv u \pmod{{}^*\mathfrak{c}^2},\ \sigma(u)>0 \text{ for all } \sigma\in\mathfrak{c}_\infty\}.$$

A similar proof to that of Proposition 3.9 shows that

$$|S_{\mathfrak{c}^2\mathfrak{c}_\infty}| = \frac{2^{r_u(k)+1+r_2(Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}(k))}}{2^{|\mathfrak{c}_\infty|}\mathcal{N}(\mathfrak{c})}.$$

Replacing in the expression for $\Phi_{k,2,\mathfrak{m}_\infty}(C_2, s)$ we obtain the formula of the theorem.

□

COROLLARY 3.12. *Denote by* $\Phi_{k,2,\supset\mathfrak{m}_\infty}(C_2, s)$ *the Dirichlet series analogous to* $\Phi_{k,2,\mathfrak{m}_\infty}(C_2, s)$ *where we sum over quadratic extensions which ramify at*

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

the places of $\mathfrak{m}_\infty$*, and possibly also at others. With the same notation as above, we have*

$$\Phi_{k,2,\supset\mathfrak{m}_\infty}(C_2,s)=-\delta_{\mathfrak{m}_\infty,\emptyset}+\frac{1}{2^{i(k)}\zeta_k(2s)}\sum_{\substack{\mathfrak{c}|2\\ \mathfrak{c}_\infty\subset\mathfrak{m}_\infty}}\frac{(-1)^{|\mathfrak{c}_\infty|}}{2^{|\mathfrak{c}_\infty|}}\frac{\mathcal{N}(2/\mathfrak{c})}{\mathcal{N}(2/\mathfrak{c})^{2s}}\sum_\chi L_k(s,\chi),$$

where χ *runs over all quadratic characters of the ray class group* $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}(k)$ *modulo* $\mathfrak{c}^2\mathfrak{c}_\infty$.

COROLLARY 3.13. *Denote by* $\Phi_{k,2,\subset\mathfrak{m}_\infty}(C_2,s)$ *the Dirichlet series analogous to* $\Phi_{k,2,\mathfrak{m}_\infty}(C_2,s)$ *where we sum over quadratic extensions which are unramified at the real places of* k *not belonging to* $\mathfrak{m}_\infty$*, and possibly also at some places of* $\mathfrak{m}_\infty$*. With the same notation as above, we have*

$$\Phi_{k,2,\subset\mathfrak{m}_\infty}(C_2,s)=-1+\frac{1}{2^{i(k)+|\mathfrak{m}_\infty|}\zeta_k(2s)}\sum_{\mathfrak{c}|2}\frac{\mathcal{N}(2/\mathfrak{c})}{\mathcal{N}(2/\mathfrak{c})^{2s}}\sum_\chi L_k(s,\chi),$$

where χ *runs over all quadratic characters of the ray class group* $Cl_{\mathfrak{c}^2\mathfrak{n}_\infty}(k)$ *modulo* $\mathfrak{c}^2\mathfrak{n}_\infty$.

Proof. Both of these corollaries are simply obtained by summing the formula of Theorem 3.11 over all $\mathfrak{m}'_\infty\supset\mathfrak{m}_\infty$ and $\mathfrak{m}'_\infty\subset\mathfrak{m}_\infty$ respectively, and using the Möbius inversion formula for sets mentioned above. Theorem 1.1 is clearly the special case of the second corollary when we choose $\mathfrak{m}_\infty$ to be the complete set of real places of k. □

COROLLARY 3.14. *In what follows, it is understood that* X *tends to infinity.*

(1) *The number of quadratic extensions* L *of* k *such that* $\mathcal{N}(\mathfrak{d}(L/k))\leqslant X$ *for which the set of real places of* k *ramified in* L/k *is equal to* $\mathfrak{m}_\infty$ *is asymptotic to*

$$\frac{1}{2^{r(k)+i(k)}}\frac{\zeta_k(1)}{\zeta_k(2)}X.$$

Note that this expression is independent of $\mathfrak{m}_\infty$.

(2) *The number of quadratic extensions* L *of* k *such that* $\mathcal{N}(\mathfrak{d}(L/k))\leqslant X$ *for which the set of real places of* k *ramified in* L/k *contains* $\mathfrak{m}_\infty$ *is asymptotic to*

$$\frac{1}{2^{|\mathfrak{m}_\infty|+i(k)}}\frac{\zeta_k(1)}{\zeta_k(2)}X.$$

(3) *The number of quadratic extensions* L *of* k *such that* $\mathcal{N}(\mathfrak{d}(L/k))\leqslant X$ *for which the set of real places of* k *ramified in* L/k *is contained in* $\mathfrak{m}_\infty$ *is asymptotic to*

$$\frac{1}{2^{|\mathfrak{n}_\infty|+i(k)}}\frac{\zeta_k(1)}{\zeta_k(2)}X.$$

(4) *The number of quadratic extensions* L *of* k *such that* $\mathcal{N}(\mathfrak{d}(L/k))\leqslant X$ *and of signature* (R,I) *is asymptotic to*

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

$$\frac{\binom{r(k)}{R/2}}{2^{r(k)+i(k)}}\frac{\zeta_k(1)}{\zeta_k(2)}X.$$

Proof. Setting $\mathfrak{c}_\infty = \mathfrak{n}_\infty \cup \mathfrak{d}_\infty$ in Theorem 3.11 and using the above-mentioned Tauberian theorem, we find that in case (1) the number of required quadratic extensions is asymptotic to BX with

$$B = \frac{\zeta_k(1)}{2^{r(k)+3i(k)+|\mathfrak{n}_\infty|}\zeta_k(2)}\left(\sum_{\mathfrak{c}|2}\mathcal{N}\mathfrak{c}\prod_{\mathfrak{p}|\mathfrak{c}}\left(1-\frac{1}{\mathcal{N}\mathfrak{p}}\right)\right)\left(\sum_{\mathfrak{d}_\infty\subset\mathfrak{m}_\infty}\frac{(-1)^{|\mathfrak{d}_\infty|}}{2^{|\mathfrak{d}_\infty|}}\right).$$

Since $\mathcal{N}\mathfrak{c}\prod_{\mathfrak{p}|\mathfrak{c}}(1-1/\mathcal{N}\mathfrak{p}) = \phi(\mathfrak{c})$ the first sum is equal to $\mathcal{N}(2) = 2^n = 2^{r(k)+2i(k)}$.

The second sum is equal to

$$\sum_{0\leqslant k\leqslant|\mathfrak{m}_\infty|}\binom{|\mathfrak{m}_\infty|}{k}(-1/2)^k = 1/2^{|\mathfrak{m}_\infty|}.$$

Putting everything together gives the first assertion of the corollary. The second and third follow immediately by summing over all supersets or all subsets of $\mathfrak{m}_\infty$ respectively, and the last assertion follows by summing over all subsets $\mathfrak{m}_\infty$ of the set of real places of k of cardinality equal to $r(k) - R/2$. □

Remark. Although we have done so only for the places at infinity, it is easy to specify also the decomposition behavior of a finite number of places of k, or even the isomorphism type of a finite number of localizations of k. The asymptotic expression is always of the form $r\cdot\zeta_k(1)/\zeta_k(2)X$ for a suitable nonzero rational number r. □

4. Description of the Ray Class Quadratic Characters

In the preceding section we have seen how to deduce from the Dirichlet series $\Phi_{k,2}(C_2, s)$ asymptotic information on the number $N_{k,2}(C_2, X)$ of quadratic extensions of k with absolute discriminant bounded by X. From now on, we will restrict to the case where k is a quadratic field. We want to obtain more explicit information on the series $\Phi_{k,2}(C_2, s)$, and from this we will be able to give an asymptotic formula for $N_4(D_4, X)$ as well as *exact* formulas for $N_{k,2}(C_2, X)$ and $N_4(D_4, X)$ (for example, we will be able to compute $N_4(D_4, 10^{17})$).

In this section we fix the quadratic field k, and denote by D its discriminant, so that $k = \mathbb{Q}(\sqrt{D})$. We will describe explicitly the quadratic characters of $Cl_{\mathfrak{c}^2}(k)$ for $\mathfrak{c}|2$, which are the characters that we need in the explicit formula which we have given for $\Phi_{k,2}(C_2, s)$ (Theorem 1.1).

The contents of this section are in essence due to Gauss and can easily be proved. Many of the results can be found in the literature, for instance in [9], [12] and [13]. Thus, we simply state the results and leave most of the proofs to the reader.

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

4.1. GENUS THEORY AND QUADRATIC CHARACTERS

LEMMA 4.1. *A fundamental discriminant D can be written in a unique way (up to permutation of factors) as $D = p_1 \dots p_t$, where $t = \omega(D)$ is the number of prime divisors of D and the p_i are distinct so-called* prime discriminants, *in other words $p_i = (-1)^{(p-1)/2}p$ for an odd prime p or $p_i = -4$, -8, or 8.*

If $D \equiv 0 (\mathrm{mod}\, 4)$, we will always assume that p_1 is even.

DEFINITION 4.2. Let I be a subset of $\{1, 2, \dots, t\}$. The number

$$d_I = \prod_{i \in I} p_i$$

will be called the divisor of D associated with I. When we speak of "a" divisor of D, it will always mean a divisor associated with a subset of $\{1, 2, \dots, t\}$.

Note that a divisor of D is always a fundamental discriminant (including 1).

LEMMA 4.3. *Let d_I be a divisor of D.*

(1) *If $\alpha \in k^*$ and $\alpha\mathbb{Z}_k$ is coprime to $d_I\mathbb{Z}_k$, we have $(d_I/\mathcal{N}(\alpha)) = 1$.*
(2) *If $\mathfrak{a}$ is a fractional ideal of k coprime to $D\mathbb{Z}_k$, we have $(D/\mathcal{N}(\mathfrak{a})) = 1$.*

In the above, we multiplicatively extend to rational numbers and fractional ideals the coprimeness condition and the Legendre–Kronecker symbol.

If $D > 0$, we will denote by ε a fundamental unit, in other words a generator of the free part of the unit group of $k = \mathbb{Q}(\sqrt{D})$.

COROLLARY 4.4. *If $D > 0$ has a negative divisor then $\mathcal{N}(\varepsilon) = 1$.*

PROPOSITION 4.5. *Let d_I be a divisor of D, assumed to be positive if $D > 0$. Let $\mathcal{C} \in Cl(k)$ and $\mathfrak{a}$ be an integral ideal belonging to $\mathcal{C}$ and coprime to $d_I\mathbb{Z}_k$ (such ideals always exist). Set $\chi_I(\mathcal{C}) = (d_I/\mathcal{N}(\mathfrak{a}))$. Then*

(1) *the value of $\chi_I(\mathcal{C})$ is independent of the choice of the integral ideal $\mathfrak{a}$ coprime to $d_I\mathbb{Z}_k$;*
(2) *χ_I is a quadratic character of $Cl(k)$;*
(3) *$\chi_I = \chi_J$ if and only if $I = J$ or $I = \{1, \dots, t\} - J$;*
(4) *every quadratic character of $Cl(k)$ is equal to χ_I for some I.*

Remark. When $D > 0$, Corollary 4.4 tells us that the condition $d_I > 0$ is automatically satisfied if $\mathcal{N}(\varepsilon) = -1$, hence is only necessary when $\mathcal{N}(\varepsilon) = 1$.

We also need to compute the value of characters χ_I for the class of *any* integral ideal $\mathfrak{a}$, not only those coprime to $d_I\mathbb{Z}_k$. For this, recall that if a and b are two

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

nonzero integers, (a, b^∞) denotes the limit of (a, b^n) as $n \to \infty$, in other words $(a, b^\infty) = \prod_{p|(a,b)} p^{v_p(a)}$.

The result is as follows.

PROPOSITION 4.6. *With the above notation, for any integral ideal* $\mathfrak{a}$*, we have*

$$\chi_I(\bar{\mathfrak{a}}) = \left(\frac{d_I}{\mathcal{N}(\mathfrak{a})/(\mathcal{N}(\mathfrak{a}), d_I^\infty)}\right)\left(\frac{D/d_I}{(\mathcal{N}(\mathfrak{a}), d_I^\infty)}\right).$$

4.2. EXPLICIT DESCRIPTION OF SOME RAY CLASS QUADRATIC CHARACTERS

We start by the following proposition, which is an immediate consequence of Theorem 1.1, but of course can also be proved directly.

PROPOSITION 4.7. *We have*

$$r_2(Cl_4(k)) = r_2(Cl^+(k)) + i(k),$$

where $Cl^+(k)$ *denotes the narrow class group of* k.

Proof. We count in two different ways the number of k-isomorphism classes of quadratic relative extensions L/k which are unramified outside the infinite places. On the one hand, by class field theory, this is equal to the number of subgroups of index 2 of the narrow class group $Cl^+(k)$, hence to $2^{r_2(Cl^+(k))} - 1$. On the other hand, by Theorem 1.1, it is equal to the constant term of $\Phi_{k,2}(C_2, s)$, hence to

$$-1 + 2^{-i(k)} \sum_\chi 1,$$

where χ runs over all quadratic characters of the ray class group $Cl_4(k)$, and so

$$2^{r_2(Cl^+(k))} - 1 = -1 + 2^{r_2(Cl_4(k))-i(k)},$$

from which the proposition follows. □

Using the same method, but this time by applying Corollary 3.13 instead of Theorem 1.1, we obtain more generally the following proposition which we will not need.

PROPOSITION 4.8. *Let* $\mathfrak{m}_\infty$ *be a subset of the set of real places of* k *and let* $\mathfrak{n}_\infty$ *be the set of real places not belonging to* $\mathfrak{m}_\infty$*. We have*

$$r_2(Cl_{4\mathfrak{n}_\infty}(k)) = r_2(Cl_{\mathfrak{m}_\infty}(k)) + i(k) + |\mathfrak{n}_\infty|.$$

Note that the above two propositions are special cases of much more general 'reflection theorems' ('Spiegelungssätze'), see [10].

Using Proposition 4.7, we can describe explicitly the quadratic characters of $Cl_4(k)$.

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

PROPOSITION 4.9. *The quadratic characters χ of $Cl_4(k)$ are either characters coming from $Cl(k)$, in other words $\chi = \chi_I$ for some divisor d_I of D assumed to be positive if $D > 0$, or of the form $\chi = \psi\chi_I$ with d_I a divisor of D, $\psi(\mathcal{C}) = (c_2/\mathcal{N}(\mathfrak{a}))$, where $\mathfrak{a}$ is an ideal belonging to the ray class $\mathcal{C}$ (hence of odd norm), and where c_2 and d_I satisfy the following:*

(1) *if $D \not\equiv -4 \pmod{16}$, $c_2 = -4$ and d_I is negative if $D > 0$;*
(2) *if $D \equiv -4 \pmod{16}$, $c_2 = 8$ and d_I is positive if $D > 0$.*

Remarks. (1) If $D > 0$ has no negative divisor, we cannot have $D \equiv -4 \pmod{16}$ (otherwise -4 would be a negative divisor), hence all the quadratic characters of $Cl_4(k)$ come from those of $Cl(k)$. In all other cases, we have twice as many.

(2) In case (1), if $D > 0$ the character χ_I corresponding to d_I is *not* a character on $Cl(k)$ but only on the narrow class group $Cl^+(k)$.

(3) In the special case where $D > 0$, $D \equiv 24 \pmod{32}$, then $D/(-8) \equiv 1 \pmod 4$, hence -8 is a negative divisor of D. It follows that, as d_I ranges through the positive divisors of D the characters $(\frac{-8d_I}{\cdot})$ range through the characters χ_J with $d_J < 0$, and on the other hand $\left(\frac{32}{n}\right) = \left(\frac{8}{n}\right)$ for all n. It follows that, if desired, this special case can be included in case (2).

Finally, we need to give an explicit description of the quadratic characters of the ray class groups $Cl_{\mathfrak{c}^2}(k)$ for moduli $\mathfrak{c}$ dividing 2. We have already given this description for $\mathfrak{c} = \mathbb{Z}_k$ and $\mathfrak{c} = 2\mathbb{Z}_k$, so we may assume that $\mathfrak{c}$ is not equal to these two moduli. If $D \equiv 5 \pmod 8$ there are no others, hence we will assume that $D \equiv 1 \pmod 8$ or $D \equiv 0 \pmod 4$. Finally, since we have seen that the group of quadratic characters of $Cl(k)$ is of index at most equal to 2 in that of $Cl_4(k)$, the group of quadratic characters of $Cl_{\mathfrak{c}^2}(k)$ must be equal to one of the two, according to the following result.

PROPOSITION 4.10. *Let $\mathfrak{c}$ be an integral ideal of $k = \mathbb{Q}(\sqrt{D})$ dividing 2 and different from $\mathbb{Z}_k$ and $2\mathbb{Z}_k$. With a slight abuse of language, the group of quadratic characters of $Cl_{\mathfrak{c}^2}(k)$ is equal to that of $Cl(k)$ if $D \equiv 1 \pmod 8$ or $D \equiv -4 \pmod{16}$, and to that of $Cl_4(k)$ if $D \equiv 8 \pmod{16}$.*

It follows from the results of this section that for any ideal $\mathfrak{c}$ dividing 2, a quadratic character χ of $Cl_{\mathfrak{c}^2}(k)$ is of the form $\chi(\bar{\mathfrak{a}}) = (c_2 d_I/\mathcal{N}(\mathfrak{a}))$ for an ideal $\mathfrak{a}$ in the class chosen coprime to d_I (and of course to $\mathfrak{c}$), where d_I is a divisor of D (of suitable sign if $D > 0$) and $c_2 = 1$, 4, -4, or 8. Note that we choose $c_2 = 4$ in some cases so as to exclude ideals $\mathfrak{a}$ such that $\mathfrak{a}$ is not coprime to $\mathfrak{c}$.

As a final result of this section, we note that the functions $L_k(s, \chi)$ which occur in Theorem 1.1 can be expressed very simply as follows (recall that we denote by $L(s, d)$ the ordinary Dirichlet series for the quadratic character $(\frac{d}{n})$).

PROPOSITION 4.11. *Let χ be a character corresponding to (d_I, c_2) as above. We have*

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

$$L_k(s,\chi) = L(s, c_2 d_I) L(s, c_2' D/d_I),$$

where $c_2' = c_2$ *except when* $D \equiv 1 \pmod 8$ *and* $\mathfrak{c} = \mathfrak{p}_2$ *is a prime ideal above 2, in which case* $c_2 = 4$ *and* $c_2' = 1$.

5. Constructing Tables of Relative Quadratic Extensions of a Quadratic Field

Although the main purpose of this paper is to explain how to *count* relative quadratic and quartic dihedral extensions, if we want also to *construct* tables of such extensions, we need to make tables of pairs $(\mathfrak{a}, \bar{u})$ as in Lemma 3.3 and of the corresponding elements α_0. As we have seen in the proof of Theorem 1.1, we must construct tables of squarefree ideals $\mathfrak{a}$ of norm less than or equal to a given bound Y, whose class is a square in a ray class group $Cl_{\mathfrak{c}^2}(k)$ for some ideal $\mathfrak{c}$ dividing 2. To make tables of squarefree ideals is most efficiently done by using standard sieving methods. We must, then choose among such ideals those whose class is a square in $Cl_{\mathfrak{c}^2}(k)$.

Using the standard orthogonality relations already used in the proof of Theorem 1.1, we know that

$$\sum_{\chi} \chi(\bar{\mathfrak{a}}) = \begin{cases} 2^{r_2(Cl_{\mathfrak{c}^2}(k))}, & \text{if } \bar{\mathfrak{a}} \in Cl_{\mathfrak{c}^2}(k)^2, \\ 0, & \text{otherwise,} \end{cases}$$

where the sum on χ is over quadratic characters of $Cl_{\mathfrak{c}^2}(k)$. Thus, the ideals we are interested in are those for which the sum is nonzero. However, since we have a complete explicit description of the quadratic characters, and since in addition we have seen that $\chi(\mathfrak{a})$ depends only on $\mathcal{N}(\mathfrak{a})$ as long as $\mathfrak{a}$ is kept coprime to $\mathfrak{c}$, the test above is easily performed. For example, in the ordinary class group $Cl(k)$, we simply check whether the expression

$$\sum_{d_I \mid D} \left(\frac{d_I}{\mathcal{N}(\mathfrak{a})/(\mathcal{N}(\mathfrak{a}), d_I)} \right) \left(\frac{D/d_I}{(\mathcal{N}(\mathfrak{a}), d_I)} \right)$$

is nonzero, where the sum runs over the divisors of D which are positive if $D > 0$, taking only one in a pair $(d_I, D/d_I)$ (note that in our case we have $(\mathcal{N}(\mathfrak{a}), d_I^\infty) = (\mathcal{N}(\mathfrak{a}), d_I)$). In the ray class groups $Cl_{\mathfrak{c}^2}(k)$, we must also sum over suitable integers c_2 (at most two) according to what we have seen above, and restrict to ideals coprime to $\mathfrak{c}$.

To find the set of elements $\bar{u}$, we must compute an $\mathbb{F}_2$-basis of the Selmer group $S(k)$ (once this is done, it is immediate to obtain a basis of the ray Selmer groups $S_{\mathfrak{c}^2}(k)$ for $\mathfrak{c} \mid 2$). For this, we use the following proposition.

PROPOSITION 5.1. *Let* $D = d(k) = p_1 \cdots p_t$ *be the decomposition of* D *into prime discriminants as in Lemma* 4.1*, where we choose* p_1 *even if* $D \equiv 0 \pmod 4$.

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

(1) *If D has a negative divisor (this includes the case $D < 0$) and $D \not\equiv -4 \pmod{16}$, the classes modulo squares of -1 and the p_i for $1 \leqslant i \leqslant t-1$ form an $\mathbb{F}_2$-basis of $S(k)$.*

(2) *If $D \equiv -4 \pmod{16}$ (in which case D has the negative divisor -4), the classes modulo squares of -1, 2, and the p_i for $2 \leqslant i \leqslant t-1$ form an $\mathbb{F}_2$-basis of $S(k)$.*

(3) *Otherwise, in other words if $D > 0$ has no negative divisors, there exists integers a and b such that $D = a^2 + 4b^2$. Then the classes modulo squares of -1, $(a + \sqrt{D})/2$ and the p_i for $1 \leqslant i \leqslant t-1$ form an $\mathbb{F}_2$-basis of $S(k)$.*

Note that, since the p_i are unique only up to ordering, choosing the p_i for $1 \leqslant i \leqslant t-1$ simply means that we must take all but one of the p_i.

Proof. Since $p_i | D$, it is clear that $p_i \mathbb{Z}_k$ is equal to the square of a prime ideal, or to the fourth or sixth power if $p_i = -4$ or $p_i = \pm 8$ respectively. Thus the p_i (and of course also -1) are virtual units. In addition, when $D \equiv 0 \pmod 4$ and, in particular, when $D \equiv -4 \pmod{16}$, 2 is also a virtual unit. Let us look for a relation between the classes of these elements modulo squares. Set $q_i = p_i$ for $2 \leqslant i \leqslant t$, and $q_1 = p_1$ if $D \not\equiv -4 \pmod{16}$, $q_1 = 2$ otherwise. Let I be a subset of $\{1, \ldots, t\}$. It is clear that an element of $\mathbb{Q}$ is a square in k if and only if it is either a square in $\mathbb{Q}$ or D times a square in $\mathbb{Q}$. Thus, a relation of the type $\prod_{i \in I} q_i = \pm x^2$ with $x \in k$ is equivalent to $\prod_{i \in I} q_i = \pm y^2$ or to $\prod_{i \in I} q_i = \pm D y^2$ for some $y \in \mathbb{Q}$. Since the q_i are pairwise coprime the first relation can occur only if $I = \emptyset$ and the sign is $+$. It is easy to see that the second relation can be written $\prod_{j \in J} p_j = \pm y^{-2}$ with $J = \{1, \ldots, t\} - I$, and again this can occur only if $J = \emptyset$, hence $I = \{1, \ldots, t\}$, again with the $+$ sign. It follows that the only nontrivial relation between the $t+1$ given classes of virtual units is the relation

$$\prod_{1 \leqslant i \leqslant t} \overline{q_i} = \overline{(\sqrt{D})^2} = \bar{1}$$

if $D \not\equiv -4 \pmod{16}$, or the relation

$$-\prod_{2 \leqslant i \leqslant t} \overline{q_i} = \overline{(\sqrt{D/4})^2} = \bar{1}$$

if $D \equiv -4 \pmod{16}$, hence the $\mathbb{F}_2$-subspace of $S(k)$ generated by these classes is of dimension equal to t.

On the other hand, Lemma 3.2 tells us that $S(k)$ is of dimension equal to t, except when D does not have any negative divisor (hence in particular $D > 0$), in which case its dimension is equal to $t+1$. This proves (1).

Thus, we assume that D does not have any negative divisor. Since we have a subspace of codimension 1, we simply need to find an element of $S(k)$ which does not belong to our subspace. Since all the elements of our subspace are classes of ordinary integers, their norms are all squares hence positive, so it suffices to exhibit an element of $S(k)$ of negative norm. By assumption, all the p_i are equal either to 8 or to primes congruent to 1 modulo 4, hence are sums of two squares. By multiplicativity of such

numbers, D is also a sum of two squares, and an immediate congruence argument shows that one can choose a and b as in the proposition.

If we set $\alpha = (a + \sqrt{D})/2$, we see that α is an algebraic integer of norm equal to $(a^2 - D)/4 = -b^2$, hence equal to the negative of a square. This evidently shows that the class of α modulo squares cannot belong to our subspace. On the other hand it is clear that α cannot be divisible by inert or ramified prime ideals, and that for a prime ideal $\mathfrak{p}$ above a split prime number p, we have $v_{\mathfrak{p}}(\alpha) = v_p(\mathcal{N}(\alpha)) = 2v_p(b)$, hence is even. It follows that α is the virtual unit that we are looking for, finishing the proof of the proposition. □

It is important to note that the integers a and b needed in case (3) of the proposition can be found very efficiently (see [2], Algorithm 1.5.2).

At the end of these quite simple computations we have the list of suitable pairs $(\mathfrak{a}, \bar{u})$. To find an explicit equation for the corresponding D_4-extension, we must compute an element α_0 and an ideal $\mathfrak{a}_0$ such that $\mathfrak{a}\mathfrak{a}_0^2 = \alpha_0\mathbb{Z}_k$. For this, we proceed as follows. We first find the content of $\mathfrak{a}$, in other words the largest positive integer $a \in \mathbb{Z}$ such that $\mathfrak{a}' = \mathfrak{a}/a$ is still an integral ideal. This can be done very simply. Then $\mathfrak{a}'$ is a *primitive* squarefree ideal, and in particular its norm $N = \mathcal{N}(\mathfrak{a}')$ is squarefree. Using an algorithm due initially to Legendre, but much improved since (see [6]), whose speed is analogous to that of the Euclidean algorithm, we can find nonzero integers x, y and z such that $x^2 - Dy^2 = \pm 4Nz^2$ and $(x, y, z) = 1$. Once a solution is found, it is immediate to find all solutions up to multiplication by a virtual unit. For such a solution, we set $\beta = (x + y\sqrt{D})/2$ if N is odd or $\beta = (x + y\sqrt{D})/4$ if N is even. Then β is a primitive algebraic integer, and it is immediately checked that for at least one β, for every prime ideal $\mathfrak{p}$ we will have $v_{\mathfrak{p}}(\beta) \equiv v_{\mathfrak{p}}(\mathfrak{a}') \pmod 2$. Thus $\alpha_0 = ua\beta$ for some virtual unit u, and since $\mathfrak{a}_0$ can be taken at will, we can choose $\alpha_0 = a\beta$.

To conclude, we see that the explicit computation of the equations of D_4-extensions can be done with no extra work than factoring the discriminants of the quadratic fields which occur.

6. Asymptotic Formulas for D_4-Extensions

We now have all the tools necessary for computing $N_4(D_4, X)$, both numerically and asymptotically. We start in this section by proving the asymptotic result.

6.1. REDUCTION TO IMPRIMITIVE EXTENSIONS

Although what we will do in this section can be done in general, we continue to assume that $K = \mathbb{Q}$, hence that k is a quadratic field. Our aim in this section is to prove Theorem 1.3.

We start the proof by noticing that Corollary 2.3 tells us that if we set

$$\Phi(s) = \sum_{k \in \mathcal{F}_2(C_2)} \frac{1}{d(k)^{2s}} (\Phi_{k,2}(C_2, s) + 1),$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

we have

$$\Phi_4(D_4,s)=\frac{1}{2}\left(\Phi(s)-\sum_D\frac{1}{D^{2s}}-\Phi_4(C_4,s)-3\Phi_4(V_4,s)\right)$$
$$=\frac{1}{2}(\Phi(s)-\Phi_2(C_2,2s)-\Phi_4(C_4,s)-3\Phi_4(V_4,s)).$$

However, it is well-known and easy to show (see for example [5]) that

$$\Phi_2(C_2,2s)=-1+\left(1-\frac{1}{2^{2s}}+\frac{2}{2^{4s}}\right)\frac{\zeta(2s)}{\zeta(4s)},$$
$$\Phi_4(C_4,s)=\frac{\zeta(2s)}{2\zeta(4s)(1+2^{-2s})}\left(\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}+\frac{4}{2^{11s}}\right)\prod_{p\equiv1\pmod 4}\left(1+\frac{2}{p^{3s}+p^s}\right)-\right.$$
$$\left.-\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}\right)\right),$$

and

$$\Phi_4(V_4,s)=\frac{1}{6}\left(1+\frac{3}{2^{4s}}+\frac{6}{2^{6s}}+\frac{6}{2^{8s}}\right)\prod_{p\equiv1(\mathrm{mod}\,2)}\left(1+\frac{3}{p^{2s}}\right)-$$
$$-\frac{1}{2}\left(1+\frac{1}{2^{4s}}+\frac{2}{2^{6s}}\right)\prod_{p\equiv1\pmod 2}\left(1+\frac{1}{p^{2s}}\right)+\frac{1}{3}.$$

Thus by absolute convergence, these three functions can be analytically continued to holomorphic functions on the half plane $\mathrm{Re}(s)>1/2$. To prove the theorem, it is thus sufficient to prove it for the function $\Phi(s)$.

6.2. PROOFS OF THEOREM 1.3 AND OF COROLLARY 1.4

For simplicity, write for the moment D instead of $d(k)$. By Theorem 1.1 and Proposition 4.11, we have

$$\Phi_{k,2}(C_2,s)+1=\frac{2^{-i(k)}}{\zeta_k(2s)}\sum_{\mathfrak{c}|2\mathbb{Z}_k}\mathcal{N}(\mathfrak{c})^{1-2s}\sum_{d_I,c_2}L(s,c_2d_I)L(s,c_2'D/d_I)$$

with evident notation.

If $d_I\neq1$ and $d_I\neq D$, the functions $L(s,c_2d_I)$ and $L(s,c_2'D/d_I)$ can both be analytically continued to $\mathbb{C}$ into holomorphic functions, and by [8], Théorème 8.1, we know that both these functions as well as their derivatives can be bounded for $\mathrm{Re}(s)>3/4$ by $c_\varepsilon\cdot(|Ds|)^{1/4+\varepsilon}$ for any $\varepsilon>0$, where c_ε is a constant depending only on ε (hence independent of D, d_I, c_2 and, of course, of s).

If $d_I=1$ then $c_2'D/d_I=c_2'D$ is never a square, so the function $L(s,c_2'D/d_I)$ is again holomorphic on all of $\mathbb{C}$ and the same bound applies, while the function $L(s,c_2d_I)$ may have a simple pole at $s=1$ (if $c_2=1$ or $c_2=4$), but then the above-mentioned bounds apply to $L(s,c_2d_I)$ minus its polar part, and to its derivative. The same

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

applies symmetrically to $d_I = D$ (recall that d_I and D/d_I give the same character). Finally, note that the sum on d_I and c_2 involves at most 4 times the number of divisors of D, hence has $O(|D|^{\varepsilon})$ terms for any $\varepsilon > 0$, and that $\zeta_k(2s)$ is trivially uniformly bounded from below in any compact subset of $\mathrm{Re}(s) > 1/2$.

If we denote by $R(k)$ the residue of $\Phi_{k,2}(C_2, s)$ at $s = 1$ (which we recall below), we have thus proved that $\Phi_{k,2}(C_2, s) - R(k)/(s-1)$ extends to a holomorphic function in $\mathrm{Re}(s) > 1/2$, hence in particular in $\mathrm{Re}(s) \geqslant 3/4$, and that both itself and its derivative are bounded in absolute value by $O_{\varepsilon}(|d(k)s|^{1/2+\varepsilon})$ for any $\varepsilon > 0$, where the O_{ε}-constant depends only on ε. It follows that the series $\sum_k |d(k)|^{-2s}(\Phi_{k,2}(C_2, s) - R(k)/(s-1))$ is absolutely convergent in $|d(k)|$ for $\mathrm{Re}(s) > 3/4$, and defines a holomorphic function.

Finally, the proof of Corollary 1.2 tells us that $R(k) = 2^{-i(k)}\zeta_k(1)/\zeta_k(2)$, proving the first formula for $c(D_4)$ in Theorem 1.3, and the second follows by replacing $\zeta_k(s)$ by $\zeta(s)L(s, d(k))$. □

Remark. It is possible that the above proof can be modified so as to prove that $\Phi(s)$ extends meromorphically to the half-plane $\mathrm{Re}(s) > 1/2$ with a simple pole at $s = 1$, but we do not need this for the following corollary, which is a strengthening of Corollary 1.4.

COROLLARY 6.1. *For all $\varepsilon > 0$ we have*

$$N_4(D_4, X) = c(D_4)\, X + O_{\varepsilon}(X^{3/4+\varepsilon})$$

where, as above,

$$c(D_4) = \frac{3}{\pi^2} \sum_D \frac{2^{-i(D)}}{D^2} \frac{L(1, D)}{L(2, D)},$$

and the sums on D are over discriminants D of quadratic fields.

Proof. Since the Dirichlet series $\Phi_4(D_4, s)$ converges absolutely for $\mathrm{Re}(s) > 1$, has nonnegative coefficients, and since $\Phi_4(D_4, s) - c(D_4)/(s-1)$ can be analytically continued to $\mathrm{Re}(s) > 3/4$, standard contour integration techniques give the corollary. □

Remarks. (1) This corollary is one of the main theoretical results of this paper. The best previous result was that of Baily [1], who showed that $c_1 X \leqslant N_4(D_4, X) \leqslant c_2 X$ for suitable constants c_1 and c_2.

(2) It is possible to formally transform the formula for $c(D_4)$ into the expression

$$\frac{3}{\pi^2} \sum_{n \geqslant 1} \frac{1}{n^2} \sum_{D|n} 2^{-i(D)} \left(\frac{D}{n/|D|}\right) \phi(n/|D|).$$

However, the justifications for the necessary interchanges of summations are not immediate, so we have not proved that $c(D_4)$ is indeed equal to this new expression,

although numerically it seems to be the case. In any event, the only advantage of this new expression is that the L-functions have disappeared, but it seems to be much less useful from a computational point of view. On the other hand, we know that the formula of the corollary converges like $O(1/|D|^{2-\varepsilon})$ for all $\varepsilon > 0$, hence has a remainder term of the order of $O(1/|D|^{1-\varepsilon})$.

(3) Because of this, it is quite difficult to compute $c(D_4)$ numerically. We have approximately $c(D_4) = 0.0523260113$, where the last two digits may be wrong. It would be interesting to know whether there exists another expression for this constant which would make it much easier to compute, for example as a linear combination of Euler products.

(4) It is immediate to extend the above corollary to the case of relative D_4-extensions of an arbitrary base number field: one obtains

$$N_{K,4}(D_4, X) = c_K(D_4)\, X + O_\varepsilon(X^{1-\alpha+\varepsilon})$$

for some strictly positive α depending only on the degree of K, with

$$c_K(D_4) = \sum_{[k:K]=2} \frac{1}{2^{r_2(k)+1}\mathcal{N}(\mathfrak{d}(k/K))^2} \frac{\zeta_k(1)}{\zeta_k(2)},$$

where the sum is over all isomorphism classes of quadratic extensions k of K.

In a manner analogous to what we have done for quadratic extensions with signatures, we can generalize Corollary 6.1 to the case where we specify the signature. We omit the proof, which is essentially identical.

PROPOSITION 6.2. *Denote by $N_{R,I}(D_4, X)$ the number of quartic D_4-extensions of $\mathbb{Q}$ up to isomorphism with signature (R, I). In addition, in the totally complex case $(R, I) = (0, 2)$, denote by $N^+_{0,2}(D_4, X)$ (resp., $N^-_{0,2}(D_4, X)$) those having a real (resp., imaginary) quadratic subfield. Finally, set*

$$c(D_4)^\pm = \frac{3}{\pi^2} \sum_{\mathrm{sign}(D)=\pm} \frac{1}{D^2} \frac{L(1, D)}{L(2, D)},$$

where the sum is over discriminants D of quadratic fields of given sign. Then for all $\varepsilon > 0$, as $X \to \infty$ we have

$$N_{4,0}(D_4, X) = \frac{c(D_4)^+}{4} X + R, \quad N_{2,1}(D_4, X) = \frac{c(D_4)^+}{2} X + R,$$
$$N^+_{0,2}(D_4, X) = \frac{c(D_4)^+}{4} X + R, \quad N^-_{0,2}(D_4, X) = \frac{c(D_4)^-}{2} X + R,$$

where $R = O_\varepsilon(X^{3/4+\varepsilon})$, and of course $N_{0,2}(D_4, X) = N^+_{0,2}(D_4, X) + N^-_{0,2}(D_4, X)$ and $c(D_4) = c(D_4)^+ + c(D_4)^-/2$.

We have approximately $c(D_4)^+ = 0.019711375$ and $c(D_4)^- = 0.065229272$, where the last digit may be wrong.

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

7. An Efficient Formula for $N_{k,2}(C_2, X)$

We will now give an exact and efficient formula for computing $N_4(D_4, X)$. By the reductions made above, it is sufficient to do this for $N_{k,2}(C_2, X)$, where k is a quadratic field, and as usual $N_{k,2}(C_2, X)$ is the number of k-isomorphism classes of quadratic extensions L/k such that $\mathcal{N}(\mathfrak{d}(L/k)) \leqslant X$. We denote as usual by $D = d(k)$ the discriminant of k.

7.1. REDUCTION TO THE SUMS T_χ

From Theorem 1.1, since $1/\zeta_k(2s) = \sum_{\mathfrak{b}} \mathcal{N}(\mathfrak{b})^{-2s}$, it is clear that we have

$$N_{k,2}(C_2, X) = -1 + 2^{-i(k)} \sum_{\mathcal{N}(\mathfrak{b}) \leqslant X^{1/2}} \mu(\mathfrak{b}) S(X/\mathcal{N}(\mathfrak{b})^2),$$

where

$$S(Y) = \sum_{\mathfrak{c}|2} \mathcal{N}(2/\mathfrak{c}) \sum_{\chi} T_\chi(\mathfrak{c}, Y/\mathcal{N}(4/\mathfrak{c}^2)),$$

the sum runs over all quadratic characters of $Cl_{\mathfrak{c}^2}(k)$, and

$$T_\chi(\mathfrak{c}, Z) = \sum_{\substack{\mathcal{N}(\mathfrak{a}) \leqslant Z \\ (\mathfrak{a},\mathfrak{c})=1}} \chi(\overline{\mathfrak{a}}),$$

where we denote by $\bar{\mathfrak{a}}$ the class of $\mathfrak{a}$ in the ray class group $Cl_{\mathfrak{c}^2}(k)$.

We first treat the outer sum. It is clear that

$$\sum_{\mathcal{N}(\mathfrak{b}) \leqslant X^{1/2}} \mu(\mathfrak{b}) S(X/\mathcal{N}(\mathfrak{b})^2) = \sum_{n \leqslant X^{1/2}} \mu_D(n) S(X/n^2),$$

where

$$\mu_D(n) = \sum_{\mathcal{N}(\mathfrak{b})=n} \mu(\mathfrak{b}).$$

We have the following lemma:

LEMMA 7.1. *With the above notation, $\mu_D(n)$ is the multiplicative arithmetic function such that for prime powers p^k with $k \geqslant 1$, we have*

(1) *if p is inert, $\mu_D(p^2) = -1$ and $\mu_D(p^k) = 0$ otherwise;*
(2) *if p is ramified, $\mu_D(p) = -1$ and $\mu_D(p^k) = 0$ otherwise;*
(3) *if p is split, $\mu_D(p) = -2$, $\mu_D(p^2) = 1$ and $\mu_D(p^k) = 0$ otherwise.*

Proof. This is clear since

$$\sum_{n \geqslant 1} \frac{\mu_D(n)}{n^s} = \frac{1}{\zeta_k(s)} = \prod_p \left((1 - p^{-s}) \left(1 - \left(\frac{D}{p} \right) p^{-s} \right) \right). \qquad \square$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

Coming back to the sum $S(Y)$ and distinguishing between different cases, we have the following proposition.

PROPOSITION 7.2. *Keep the above notation, and write* $\sum_{\chi,1}$ (*resp.,* $\sum_{\chi,4}$) *for a sum over all quadratic characters of* $Cl(k)$ (*resp.,* $Cl_4(k)$). *In each case, denote by* $\mathfrak{p}_2$ *a prime ideal above* 2.

(1) *If* $D \equiv 5 \pmod 8$, *then*

$$S(Y) = \sum_{\chi,4} T_\chi(2\mathbb{Z}_k, Y) + 4 \sum_{\chi,1} T_\chi(\mathbb{Z}_k, Y/16).$$

(2) *If* $D \equiv 1 \pmod 8$, *then*

$$S(Y) = \sum_{\chi,4} T_\chi(2\mathbb{Z}_k, Y) + 4 \sum_{\chi,1} T_\chi(\mathfrak{p}_2, Y/4) + 4 \sum_{\chi,1} T_\chi(\mathbb{Z}_k, Y/16).$$

(3) *If* $D \equiv 8 \pmod{16}$, *then*

$$S(Y) = \sum_{\chi,4} T_\chi(2\mathbb{Z}_k, Y) + 2 \sum_{\chi,4} T_\chi(\mathfrak{p}_2, Y/4) + 4 \sum_{\chi,1} T_\chi(\mathbb{Z}_k, Y/16).$$

(4) *If* $D \equiv -4 \pmod{16}$, *then*

$$S(Y) = \sum_{\chi,4} T_\chi(2\mathbb{Z}_k, Y) + 2 \sum_{\chi,1} T_\chi(\mathfrak{p}_2, Y/4) + 4 \sum_{\chi,1} T_\chi(\mathbb{Z}_k, Y/16).$$

Proof. This immediately follows from the definition of $S(Y)$ and from Proposition 4.10. In the case $D \equiv 1 \pmod 8$, we have in fact a contribution from $\mathfrak{p}_2$ as well as a contribution from the conjugate ideal $\bar{\mathfrak{p}}_2$, but these contributions are clearly equal. Note that we make a useful abuse of notation by writing, for example, $\sum_{\chi,1} T_\chi(\mathfrak{p}_2, Y/4)$: although χ is a character of $Cl(k)$, it is in fact considered as a character of $Cl_{\mathfrak{p}_2^2}(k)$, in other words by convention it vanishes on ideals not coprime to $\mathfrak{p}_2$. □

Remark. Thanks to our study of quadratic characters and their L-series, the sums on χ appearing in the above proposition are completely explicit: more precisely, since we can write $\chi = \chi_I\left(\frac{c_2}{\cdot}\right)$, they are of the form $\sum_{d_I,c_2}$, where d_I ranges through the divisors of D modulo the equivalence $d_I \sim D/d_I$, c_2 ranges in the set $\{1\}$ (for $\sum_{\chi,1}$), or in the set $\{4, -4\}$ (for $\sum_{\chi,4}$ and $D \not\equiv -4 \pmod{16}$, or in the set $\{4, 8\}$ (for $\sum_{\chi,4}$ and $D \equiv -4 \pmod{16}$), with the additional restriction $c_2 d_I > 0$ if $D > 0$.

COROLLARY 7.3. *If* $\mu_D(n)$ *is the arithmetic function described in Lemma* 7.1 *and* $S(Y)$ *is given by the above proposition, we have*

$$N_{k,2}(C_2, X) = -1 + 2^{-i(k)} \sum_{1 \leqslant n \leqslant X^{1/2}} \mu_D(n) S(X/n^2).$$

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

Remark. As we will do below for the sums T_χ, we may transform this using the method of the hyperbola into the formula

$$N_{k,2}(C_2, X) = -1 + 2^{-i(k)}\Bigg(\sum_{1 \leqslant n \leqslant E} \mu_D(n) S(X/n^2) + \\ + \sum_{1 \leqslant m \leqslant X/E^2} S(m) \sum_{\max\left(\left(\frac{X}{m+1}\right)^{1/2}, E\right) < n \leqslant \left(\frac{X}{m}\right)^{1/2}} \mu_D(n)\Bigg),$$

valid for $1 \leqslant E \leqslant X^{1/2}$. Since however the bound X is often not very large, this brings only a small improvement. □

7.2. AN EFFICIENT FORMULA FOR T_χ

By what we have seen above, to each character χ of $Cl_{\mathfrak{c}^2}(k)$ is attached a pair of integers (d_I, c_2), as well as an auxiliary integer c_2' defined in Proposition 4.11. This allows us to give an efficient explicit formula for computing $T_\chi(\mathfrak{c}, Y)$.

PROPOSITION 7.4. *Let* $\mathfrak{c}$ *be an ideal dividing* 2*, let* χ *be a character of* $Cl_{\mathfrak{c}^2}(k)$*, and let* (d_I, c_2) *be a pair of integers corresponding to* χ *as above. For any* d *congruent to* 0 *or* 1 *modulo* 4*, set*

$$U(d, Z) = \sum_{1 \leqslant n \leqslant Z} \left(\frac{d}{n}\right).$$

Then for any real number E *such that* $1 \leqslant E \leqslant Y$*, we have*

$$T_\chi(\mathfrak{c}, Y) = \sum_{1 \leqslant m \leqslant E} \left(\frac{c_2 d_I}{m}\right) U(c_2' D/d_I, Y/m) + \\ + \sum_{1 \leqslant m \leqslant Y/E} \left(\frac{c_2' D/d_I}{m}\right) U(c_2 d_I, Y/m) - U(c_2 d_I, E) U(c_2' D/d_I, Y/E).$$

Proof. By Proposition 4.11, we know that

$$L_k(s, \chi) = L(s, c_2 d_I) L(s, c_2' D/d_I),$$

where $c_2' = c_2$ except when $D \equiv 1 (\mathrm{mod}\ 8)$, $\mathfrak{c} = \mathfrak{p}_2$, hence $c_2 = 4$, in which case $c_2' = 1$. Since by definition $T_\chi(\mathfrak{c}, Y)$ is the summatory function of the coefficients of this L-series, it follows immediately that

$$T_\chi(\mathfrak{c}, Y) = \sum_{1 \leqslant m \leqslant Y} \left(\frac{c_2 d_I}{m}\right) \sum_{1 \leqslant n \leqslant Y/m} \left(\frac{c_2' D/d_I}{n}\right).$$

A standard application of the method of the hyperbola (see for example [4]) gives immediately the formula of the proposition. □

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

To use this formula in the most efficient way, we must explain how to compute $U(d, Z)$ and how to choose E (which will *not* be chosen equal to $Y^{1/2}$ in general).

Note first that if $d \equiv 0 \pmod{16}$, we always have $(d/n) = ((d/4)/n)$, hence we can replace d by $d/4$. Now d can be a square only if $d = c_2 d_I$, $d_I = 1$ and $c_2 = 1$ or $c_2 = 4$, or symmetrically if $d = c_2' D/d_I$, $d_I = D$, $c_2' = 1$ or $c_2' = 4$, hence only if $d = 1$ or $d = 4$. If $d = 1$, we have $U(d, Z) = \lfloor Z \rfloor$, while if $d = 4$, we have $U(d, Z) = \lfloor (Z+1)/2 \rfloor$. In all other cases, d is not a square, hence $U(d, Z)$ is periodic of period dividing $|d|$. Thus, we write $Z = q|d| + r$ with $|r| \leqslant |d|/2$, hence if $r \geqslant 0$ we have $U(d, Z) = U(d, r)$ while if $r < 0$, it is easy to see that we have $U(d, Z) = -\text{sign}(d) U(d, |r| - 1)$. Thus, we have at most $|d|/2$ terms to compute.

To fix a representative in an equivalence class $\{d_I, D/d_I\}$, let us choose for the sake of discussion $|d_I| < |D|^{1/2}$ (the results would be identical with any other choice). Since we can reasonably consider the time for computing Legendre symbols to be constant, it follows that the time for computing $T_\chi(\mathfrak{c}, Y)$ by the above proposition is of the order of $((c_2'|D/d_I|)E + (c_2|d_I|)(Y/E))/2$, which is minimized for $E = (d_I^2 (c_2/c_2') Y/|D|)^{1/2}$. This can in fact be slightly improved if $c_2 d_I$ is a square, since in that case the computation of $U(c_2 d_I, Z)$ is faster. The improvement is small and implementation dependent, however.

7.3. A TABLE OF $N_4(D_4, 10^k)$

We can now combine all of the above to compute efficiently $N_4(D_4, X)$. More precisely, we use Corollary 2.3 (3), together with the formulas given for example in [4] and [5] for $N_4(C_4, X)$ and $N_4(V_4, X)$, to reduce to the case of imprimitive

Table I.

X	$N_4(C_4, X)$	$N_4(V_4, X)$	$N_4(D_4, X)$	$N_4(I, X)$
10^1	0	0	0	0
10^2	0	0	0	0
10^3	1	8	24	73
10^4	10	47	413	977
10^5	32	243	4764	10289
10^6	113	1014	50496	104147
10^7	363	4207	516399	1045782
10^8	1168	16679	5205848	10462901
10^9	3732	64316	52225424	104647528
10^{10}	11930	242710	522889160	1046518380
10^{11}	38045	901557	5231249258	10465241232
10^{12}	120925	3306085	52321107488	104652254156
10^{13}	383500	11982067	523242546935	1046521423571
10^{14}	1215198	43017383	5232538688240	10465207643827
10^{15}	3848219	153156284	52325790887461	104652045091993
10^{16}	12180240	541382988	523259337279192	1046520310887588
10^{17}	38542706	1901705324	5232598410033780	10465202563726238

https://doi.org/10.1023/A:1016310902973 Published online by Cambridge University Press

extensions. We use Corollary 2.3 (4) to reduce to the computation of $N_{k,2}(C_2, X)$ for a finite number of quadratic fields k. We use Corollary 7.3 together with Lemma 7.1 and Proposition 7.2 to reduce to the computation of $T_\chi(\mathfrak{c}, Y)$ for certain characters χ and ideals $\mathfrak{c}|2$. Finally, we use Proposition 7.4 together with the subsequent discussion to compute $T_\chi(\mathfrak{c}, Y)$ efficiently.

In addition, we can use some small simplifications. For example, it is easy to show that if $X \leqslant 2$ then $N_{k,2}(C_2, X) = 2^{\omega(d(k))-1} - 1$, where $\omega(d(k)) = t$ is the number of distinct prime divisors of $d(k)$. This is essentially the content of Proposition 4.7, together with the fact that a conductor cannot be divisible by a prime ideal of norm equal to 2.

Since it is also easily checked by the explicit formula or directly that we have $T_\chi(2\mathbb{Z}_k, Y) = 1$ for $Y \leqslant 2$, the same corollary shows that $S(Y) = 2^{\omega(d(k))-1+i(k)}$ for $Y \leqslant 2$.

The above two improvements are not completely marginal, since the bounds X in $N_{k,2}(C_2, X)$ or Y in $S(Y)$ are frequently very small.

Putting all this on a computer, we have computed the values of $N_4(D_4, 10^k)$ for $1 \leqslant k \leqslant 17$. The computation of $N_4(D_4, 10^{17})$ took almost 33 days CPU time on a Pentium III 600 Mhz workstation. We give the results in the Table I where, for completeness, we also give the corresponding results for $N_4(C_4, X)$, $N_4(V_4, X)$, and $N_4(I, X)$ (where $N_4(I, X) = N_4(C_4, X) + 3N_4(V_4, X) + 2N_4(D_4, X)$, see Section 2). More complete tables of $N_4(C_4, X)$ and $N_4(V_4, X)$, which are much easier to compute, can be found in [5].

References

1. Baily, A.: On the density of discriminants of quartic fields, *J. reine angew. Math.* **315** (1980), 190–210.
2. Cohen, H.: *A Course in Computational Algebraic Number Theory* (third printing), Grad. Texts in Math. 138, Springer, New York, 1996.
3. Cohen, H.: *Advanced Topics in Computational Number Theory*, Grad. Texts Math. 193, Springer, New York, 2000.
4. Cohen, H.: Comptage exact de discriminants d'extensions abéliennes, *J. Theor. Nombres Bordeaux* **12** (2000), 379–397.
5. Cohen, H., Diaz y Diaz, F. and Olivier, M.: Counting discriminants of number fields, Preprint.
6. Cremona, J. and Rusin, D.: Efficient solution of rational conics, Preprint.
7. Datskovsky, B. and Wright, D. J.: Density of discriminants of cubic extensions, *J. reine angew. Math.* **386** (1988), 116–138.
8. Ellison, W. (with M. Mendès-France): *Les nombres premiers*, Hermann, Paris, 1975.
9. Fröhlich, A. and Taylor, M.: *Algebraic Number Theory*, Cambridge Stud. Adv. Math. 27, Cambridge Univ. Press, 1991.
10. Gras, G.: Théorèmes de réflexion, *J. Théor. Nombres Bordeaux* **10** (1998), 399–499.
11. Malle, G.: On the distribution of Galois groups, *J. Number Theory*, to appear.
12. Redei, L. and Reichardt, H.: Die Anzahl der durch 4 teilbaren Invarian-ten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.* **170** (1933), 69–74.
13. Zagier, D.: *Zetafunktionen und quadratische Körper*, Hochschultext, Springer, Berlin, 1981.