ANNALES

DE

L'INSTITUT FOURIER

Henri COHEN

Enumerating quartic dihedral extensions of $\mathbb{Q}$ with signatures

Tome 53, nº 2 (2003), p. 339-377.

<http://aif.cedram.org/item?id=AIF_2003__53_2_339_0>

Ann. Inst. Fourier, Grenoble
53, 2 (2003), 339–377

ENUMERATING QUARTIC DIHEDRAL EXTENSIONS OF $\mathbb{Q}$ WITH SIGNATURES

by Henri COHEN

1. Introduction and review of known results.

1.1. Notation.

We recall the notation of [7]. Let k be a number field, considered as our base field, and let $(r(k), i(k))$ be the signature of k with $r(k)+2i(k) = [k : \mathbb{Q}]$. In the present paper k will in fact be a quadratic field (usually real), but for the moment we do not assume this. Let G be a transitive permutation subgroup of the symmetric group on n letters S_n, and let $\mathfrak{m}_\infty$ be a subset of the set of the $r(k)$ real places of k. We denote by C_n the cyclic group of order n, by $V_4 = C_2 \times C_2$ the Klein 4-group, and by D_4 the dihedral group of order 8, considered as a transitive subgroup of S_4.

Denote by $\mathcal{F}_{k,\mathfrak{m}_\infty}(G)$ 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 over k is isomorphic to G, and such that the set of real places of k which ramify (i.e., become complex) in L is exactly equal to $\mathfrak{m}_\infty$. We let

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

where as usual $\mathfrak{d}(L/k)$ denotes the relative ideal discriminant of L over k, and $\mathcal{N}$ denotes the absolute norm from k to $\mathbb{Q}$. Note that by the conductor-discriminant formula, we have $|d(L)| = |d(k)|^n \mathcal{N}(\mathfrak{d}(L/k))$, where $d(k)$ and

Keywords: Discriminant counting – Genus character – Quartic reciprocity.
Math. classification: 11R16 – 11R29 – 11R45 – 11Y40.

$d(L)$ denote the absolute discriminants of k and L respectively, so that we can also write

$$\Phi_{k,\mathfrak{m}_\infty}(G,s) = |d(k)|^{ns} \sum_{L\in\mathcal{F}_{k,\mathfrak{m}_\infty}(G)} \frac{1}{|d(L)|^s}.$$

Finally, we set

$$\begin{aligned} N_{k,\mathfrak{m}_\infty}(G,X) &= \left|\{L \in \mathcal{F}_{k,\mathfrak{m}_\infty}(G),\ \mathcal{N}(\mathfrak{d}(L/k)) \leqslant X\}\right| \\ &= \left|\{L \in \mathcal{F}_{k,\mathfrak{m}_\infty}(G),\ |d(L)| \leqslant X \cdot |d(k)|^n\}\right|. \end{aligned}$$

It is clear that $N_{k,\mathfrak{m}_\infty}(G,X)$ is the summatory function of the coefficients of the Dirichlet series $\Phi_{k,\mathfrak{m}_\infty}(G,s)$.

In the case where $k = \mathbb{Q}$, we will omit the index k from the notation. If, instead of specifying the real places which split we specify the signature (R_1, R_2) of L (with $R_1+2R_2 = n[k:\mathbb{Q}]$), we will replace the index $(k,\mathfrak{m}_\infty)$ by (k,R_1,R_2), hence simply by (R_1,R_2) when $k=\mathbb{Q}$. Finally if we do not even specify the signature, we will simply use the index (k,n), or the index n if $k=\mathbb{Q}$.

1.2. Known results.

When G is abelian and the base field is $\mathbb{Q}$, the analysis is quite elementary and it is possible to give nice explicit formulas for the Φ functions, and efficient algorithms to compute the N functions. For this, we refer to [14], [15], and [3]. For completeness, although we will not directly need them, we give here the formulas for the Φ functions for $n \leqslant 4$ since they cannot easily be found (or not be found at all) in the literature:

$$\Phi_2(C_2,s) = \left(1+\frac{1}{2^{2s}}+\frac{2}{2^{3s}}\right)\prod_{p\equiv 1 \pmod 2}\left(1+\frac{1}{p^s}\right) - 1$$

$$\Phi_{2,0}(C_2,s) = \frac{1}{2}\Phi_2(C_2,s) + \frac{1}{2}\left(1-\frac{1}{2^{2s}}\right)\prod_{p\equiv 1 \pmod 2}\left(1+\frac{(-1)^{(p-1)/2}}{p^s}\right) - \frac{1}{2}$$

$$\Phi_3(C_3,s) = \frac{1}{2}\left(1+\frac{2}{3^{4s}}\right)\prod_{p\equiv 1 \pmod 6}\left(1+\frac{2}{p^{2s}}\right) - \frac{1}{2}$$

$$\begin{aligned}\Phi_4(C_4,s) = \frac{\zeta(2s)}{2\zeta(4s)}\Bigg(&\left(1-\frac{1}{2^{2s}}+\frac{2}{2^{4s}}+\frac{4}{2^{11s}+2^{9s}}\right) \\ &\cdot \prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{3s}+p^s}\right) - \left(1-\frac{1}{2^{2s}}+\frac{2}{2^{4s}}\right)\Bigg)\end{aligned}$$

$$\Phi_{4,0}(C_4,s)=\frac{\Phi_4(C_4,s)}{2}+\frac{L(2s,(-4/\cdot))}{4\zeta(4s)}\cdot\left(\prod_{p\equiv 1\pmod 4}\left(1+\frac{2(-1)^{(p-1)/4}}{p^{3s}+p^s}\right)-1\right)$$

$$\Phi_4(V_4,s)=-\frac{\Phi_2(C_2,2s)}{2}+\frac{1}{6}\left(1+\frac{3}{2^{4s}}+\frac{6}{2^{6s}}+\frac{6}{2^{8s}}\right)\cdot\prod_{p\equiv 1\pmod 2}\left(1+\frac{3}{p^{2s}}\right)-\frac{1}{6}$$

$$\Phi_{4,0}(V_4,s)=\frac{\Phi_4(V_4,s)}{4}-\frac{\Phi_{2,0}(C_2,2s)}{2}+\frac{\Phi_2(C_2,2s)}{8}+\frac{1}{8}\left(1-\frac{1}{2^{4s}}+\frac{2}{2^{6s}}-\frac{2}{2^{8s}}\right)\cdot\prod_{p\equiv 1\pmod 2}\left(1+\frac{1+2(-1)^{(p-1)/2}}{p^{2s}}\right)-\frac{1}{8}.$$

Using the methods of [3], we can then compute the corresponding N functions very efficiently: up to 10^{25} for C_2, up to 10^{37} for C_3, up to 10^{32} for C_4, and up to 10^{36} for V_4.

When the base field is not $\mathbb{Q}$ the situation is more complicated, but can be handled with some difficulty (see [16], [8] and [9]). We will need in detail the case of $G = C_2$ which we will recall in the next section. On the other hand, when the group G is not abelian, the situation is considerably more difficult even for $k = \mathbb{Q}$. The case $G = S_3$ and $k = \mathbb{Q}$ was settled by Heilbronn–Davenport in the 1970's ([11], [12]), and the case of S_3 for general number fields was settled by Datskovsky and Wright [10]. The case $G = A_4$ is still open (although $\Phi_4(A_4,s)$ is given in [5] and a precise conjectural estimate for $N_4(A_4,X)$ is given in [6], incorrectly stated as being proved, so it is expected that the result is in sight). A lot of work has been done on the case $G = S_4$ from different directions, and the asymptotic estimate for $N_4(S_4,X)$ has now been obtained in [1] for $k = \mathbb{Q}$ (see also [17], [18], which hopefully will also be able to settle the case of general base fields k). In [7], we settled the case $G = D_4$ which is of intermediate difficulty. In particular, we obtained the following asymptotic results which we recall here for completeness, since we will not need them:

Set

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

where the sum is over discriminants D of quadratic fields of given sign and $L(s, D)$ is the Dirichlet L-function of the quadratic character $(D/.)$. Then for all $\varepsilon 0$, as $X \to \infty$ we have

$$\begin{aligned}
N_4(D_4, X) &= \left(c^+(D_4) + \frac{c^-(D_4)}{2}\right) X + O_\varepsilon(X^{3/4+\varepsilon}),\\
N_{4,0}(D_4, X) &= \frac{c^+(D_4)}{4} X + O_\varepsilon(X^{3/4+\varepsilon}),\\
N_{2,1}(D_4, X) &= \frac{c^+(D_4)}{2} X + O_\varepsilon(X^{3/4+\varepsilon}),\\
N_{0,2}(D_4, X) &= \left(\frac{c^+(D_4)}{4} + \frac{c^-(D_4)}{2}\right) X + O_\varepsilon(X^{3/4+\varepsilon}),
\end{aligned}$$

where in the last formula the term with coefficient $c^+(D_4)/4$ (resp., $c^-(D_4)/2$) counts totally complex D_4-fields having a real (resp., imaginary) quadratic subfield.

Note that we have approximately $c^+(D_4) = 0.0197113757$ and $c^-(D_4) = 0.0652292708$, hence $c^+(D_4) + c^-(D_4)/2 = 0.0523260111$.

In [7], we have also explained how to compute $N_4(D_4, X)$ *exactly* for quite large values of X (we reached $X = 10^{17}$). Apart from well-known tricks from the elementary theory of numbers, the key to this computation was the fact that the characters involved in the formula for $N_4(D_4, X)$ are all *genus characters*, hence easy to handle.

When we include signature conditions, the characters are not all genus characters, hence the formulas and algorithms become more complicated. The purpose of this paper is to give such algorithms, so as to be able to compute exactly the above quantities exactly for large X. We will again be able to reach $X = 10^{17}$, and in less than twice the time that it would have taken us without signatures (26 days on a Pentium III 600Mhz workstation). In fact, due to more efficient programming, this is faster than the time that it took us in [7] without signatures.

It is notable that the *theory* behind the algorithms that we will use is quite interesting, and involves in particular the rational quartic reciprocity law.

1.3. Reduction to quadratic extensions.

We start by giving a summary of the main results of [7] that we will need.

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

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

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.

THEOREM 1.2. — *Let $\mathfrak{n}_\infty$ be the set of real places of k not belonging to $\mathfrak{m}_\infty$. Then*

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

where δ is the Kronecker δ symbol, $\mathfrak{c}$ 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 $\mathfrak{c}^2\mathfrak{c}_\infty$.

From these theorems, it is easy to obtain formulas for the N functions. We immediately isolate the one that we will need.

COROLLARY 1.3. — *Let k be a quadratic field of discriminant D. Let $\mu_D(n)$ be the multiplicative arithmetic function such that, when p is inert $\mu_D(p^2)=-1$, when p is ramified $\mu_D(p)=-1$, when p is split $\mu_D(p)=-2$ and $\mu_D(p^2)=1$, and $\mu_D(p^k)=0$ for all other prime powers with $k\geqslant 1$. Then*

$$N_{k,2,\mathfrak{m}_\infty}(C_2,X)=-\delta_{\mathfrak{m}_\infty,\emptyset}+\frac{1}{2^{i(k)}}\sum_{1\leqslant n\leqslant X^{1/2}}\mu_D(n)S(X/n^2),$$

where

$$S(Y)=\sum_{\substack{\mathfrak{c}\mid 2\\ \mathfrak{c}_\infty\supset\mathfrak{n}_\infty}}\frac{(-1)^{|\mathfrak{c}_\infty|-|\mathfrak{n}_\infty|}}{2^{|\mathfrak{c}_\infty|}}\sum_{\chi}T_\chi(Y/\mathcal{N}(4/\mathfrak{c}^2)),$$

with

$$T_\chi(Z)=\sum_{\mathcal{N}\mathfrak{a}\leqslant Z}\chi(\mathfrak{a}).$$

The sums on χ are as above on quadratic characters of the ray class group $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}(k)$, considered as acting on ideals by the natural extension (in particular $\chi(\mathfrak{a})=0$ if $\mathfrak{a}$ is not coprime to $\mathfrak{c}$). Of course $i(k)=0$ if $D>0$ and $i(k)=1$ if $D<0$.

When $D < 0$ we necessarily have $\mathfrak{m}_\infty = \emptyset$, and the above formula is simply the formula for $N_{k,2}(C_2, X)$. In particular, there is no need to modify the algorithms given in [7] for computing these numbers, which we can thus do very efficiently.

When $D > 0$, i.e., when k is a real quadratic field, the situation is more complicated because the characters χ are not all genus characters. Recall the definition of such characters, as we used them in [7]. In this context, we say that a positive or negative integer d is a *divisor* of D if $d \mid D$ and both d and D/d are fundamental discriminants, which will automatically be coprime. If we define $\chi_d(\mathfrak{a}) = (d/\mathcal{N}\mathfrak{a})$, then this always defines a (quadratic) character on the narrow class group $Cl_{\infty_0\infty_1}(k)$, and all quadratic characters on the narrow class group are obtained in this way (exactly once if we identify d with D/d). They are called *genus characters*. In addition, they give characters on the ordinary class group if and only $d > 0$. When D is a sum of two squares, all divisors d are positive, hence all these characters are defined on the ordinary class group, and otherwise exactly half of the divisors d are positive, and only those are defined on the ordinary class group.

In addition, we know from [7] that the characters modulo a square divisor of 4, i.e., of the ray class groups $Cl_{\mathfrak{c}^2}(k)$ for $\mathfrak{c} \mid 2$, are of course first the genus characters (with $d>0$), and if either $\mathfrak{c} = 2\mathbb{Z}_k$ or $\mathfrak{c}^2 = 2\mathbb{Z}_k$ and $D \equiv 8 \pmod{16}$, also the genus characters multiplied by a single extra character of the form $(c_2/\mathcal{N}\mathfrak{a})$ with $c_2 d>0$, and $c_2 = 8$ if $D \equiv -4 \pmod{16}$, $c_2 = -4$ otherwise. These characters are very similar to the genus characters.

When, as here, we add signature conditions, Corollary 1.3 shows that we need quadratic characters of the ray class groups $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}(k)$ and not only of $Cl_{\mathfrak{c}^2}(k)$. There are bad news and good news about this. The bad news are that the necessary characters χ do not all "come from $\mathbb{Q}$", in other words do not only depend on the norm of $\mathfrak{a}$, hence are more complicated. In particular they are not genus characters, and this will create complications for the computations of the sums involved.

Indeed, a crucial property of genus characters is that their L-function naturally *factors* as a product of two Dirichlet L-functions corresponding to the Dirichlet characters $(d/.)$ and $((D/d)/.)$. This property was one of the reasons that we were able to perform very efficient computations in [7]. Here this factorization will not occur exactly in this way (although we will be able to use a similar technique), so the computation will be a little more complicated.

The good news are that, in a manner analogous to the characters of $Cl_{\mathfrak{c}^2}(k)$ where we needed to introduce a *single* character $(c_2/\mathcal{N}\mathfrak{a})$ to obtain all the missing ones, the same is true here. To obtain all of the missing characters, i.e., the quadratic characters of the ray class groups $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}$ as above, it is also only necessary to add a single character which we will denote by Ψ, which of course will not be a genus character. This character will in fact only be necessary when D is a sum of two squares, otherwise it does not occur. Thus, we spend the next section studying this character.

2. The character Ψ.

Thus let $D > 1$ be a fundamental discriminant, and assume that D is a sum of two squares. We write (non uniquely) $D = a^2 + 4b^2$. For future reference note that $(a, b) = 1$. Indeed, if p is a prime dividing a and b then $p^2 \mid D$, hence $p = 2$ since D is fundamental. But then $D/4 = (a/2)^2 + 4(b/2)^2$ is congruent to a square modulo 4, hence D is not fundamental also in that case, contradiction. This implies also that b is coprime to D.

When necessary, it will be convenient to take as integral basis of $\mathbb{Z}_k$ the pair $(1, \omega)$ with $\omega = (a + \sqrt{D})/2$. The norm of ω is then equal to $-b^2$.

2.1. Some preliminary lemmas.

Recall that any fractional ideal $\mathfrak{a}$ of $\mathbb{Z}_k$ can be written in a unique way as

$$\mathfrak{a} = r_{\mathfrak{a}}\left(n_{\mathfrak{a}}\mathbb{Z} + \left(\frac{c_{\mathfrak{a}} + \sqrt{D}}{2}\right)\mathbb{Z}\right)$$

with $r_{\mathfrak{a}} \in \mathbb{Q}_{>0}$, $n_{\mathfrak{a}} \in \mathbb{Z}_{>0}$, and $c_{\mathfrak{a}}^2 \equiv D \pmod{4n_{\mathfrak{a}}}$. The ideal $\mathfrak{a}$ is primitive if and only if $r_{\mathfrak{a}} = 1$, and in that case $n_{\mathfrak{a}}$ is the absolute norm of $\mathfrak{a}$. For any ideal $\mathfrak{a}$ as above coprime to 2, we set for simplicity $d_{\mathfrak{a}}^{\pm} = (c_{\mathfrak{a}} \pm a)/2$. We need a few preliminary results.

LEMMA 2.1. — *For any ideal $\mathfrak{a}$ as above we have* $\gcd(n_{\mathfrak{a}}, d_{\mathfrak{a}}^+, d_{\mathfrak{a}}^-) = 1$, *using the above notation.*

Proof. — Assume p is a prime dividing all three integers. Then p divides $d_{\mathfrak{a}}^+ - d_{\mathfrak{a}}^- = a$ and also divides $d_{\mathfrak{a}}^+ d_{\mathfrak{a}}^- = (c_{\mathfrak{a}}^2 - a^2)/4 \equiv b^2 \pmod{n_{\mathfrak{a}}}$, hence since p divides $n_{\mathfrak{a}}$, it follows that p divides b, a contradiction since $(a, b) = 1$. □

Definition 2.2. — *We define B^+ (resp., B^-) to be the set of noninert prime ideals $\mathfrak{p}$ such that $p \mid d_{\mathfrak{p}}^+$ (resp., $p \mid d_{\mathfrak{p}}^-$), where p is the prime number below $\mathfrak{p}$ (the letter B stands for "bad").*

Lemma 2.3.

(1) *The set B^- is a set of representatives of the prime ideals (which are all split) above prime numbers dividing b for the equivalence relation $\mathfrak{p} \equiv \overline{\mathfrak{p}}$, where $\overline{\mathfrak{p}}$ is the Galois conjugate of $\mathfrak{p}$, and B^+ is the set of conjugates of elements of B^-.*

(2) *In particular the sets B^+ and B^- are finite, disjoint with the same cardinality.*

(3) *If $\mathfrak{a} = n_{\mathfrak{a}}\mathbb{Z} + ((c_{\mathfrak{a}} + \sqrt{D})/2)\mathbb{Z}$ is a primitive ideal, then $\gcd(n_{\mathfrak{a}}, d_{\mathfrak{a}}^-) = 1$ if and only if $\mathfrak{a}$ is coprime to all prime ideals of B^-. Similarly for $^+$.*

Proof. — (1) and (2) First note that if $p \mid b$ then

$$\left(\frac{D}{p}\right) = \left(\frac{a^2 + 4b^2}{p}\right) = \left(\frac{a^2}{p}\right) = 1$$

since $(a, b) = 1$, so all primes dividing b are split. Furthermore, if $\mathfrak{p} \in B^{\pm}$, then $p \mid (c_{\mathfrak{p}} \pm a)/2$ hence $p \mid (c_{\mathfrak{p}}^2 - a^2)/4 \equiv b^2 \pmod{p}$, so $p \mid b$, and conversely if $\mathfrak{p} = p\mathbb{Z} + ((c_{\mathfrak{p}} + a)/2)\mathbb{Z}$ is a prime ideal above a prime dividing b then $(c_{\mathfrak{p}}^2 - a^2)/4 \equiv b^2 \equiv 0 \pmod{p}$, so that $p \in B^- \cup B^+$. By Lemma 2.1 it is clear that the sets B^- and B^+ are disjoint. Furthermore, note that

$$d_{\overline{\mathfrak{p}}}^- = -d_{\mathfrak{p}}^+,$$

so that if $\mathfrak{p} \in B^-$ (resp., B^+), then $\overline{\mathfrak{p}} \in B^+$ (resp., B^-), proving (1). (2) follows trivially.

(3) Assume that $\gcd(n_{\mathfrak{a}}, d_{\mathfrak{a}}^-) = 1$, and let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{a}$, necessarily noninert since $\mathfrak{a}$ is primitive. If p is below $\mathfrak{p}$, i.e., is the norm of p, then $p \mid n_{\mathfrak{a}}$ hence $p \nmid d_{\mathfrak{a}}^-$. However, note that since $c_{\mathfrak{a}}^2 \equiv D \pmod{4p}$ then $p\mathbb{Z} + ((c_{\mathfrak{a}} + \sqrt{D})/2)\mathbb{Z}$ is an ideal of norm p which contains $\mathfrak{a}$, hence is equal to $\mathfrak{p}$, so that $c_{\mathfrak{p}} \equiv c_{\mathfrak{a}} \pmod{2p}$ hence $d_{\mathfrak{p}}^- \equiv d_{\mathfrak{a}}^- \pmod{p}$, so that $p \nmid d_{\mathfrak{p}}^-$, in other words $p \notin B^-$ as claimed. Conversely, if none of the prime ideal divisors of the primitive ideal $\mathfrak{a}$ are in B^-, a similar proof using the

Chinese remainder theorem shows that $\gcd(n_{\mathfrak{a}}, d_{\mathfrak{a}}^-) = 1$. The same proof is of course also valid for $^+$. □

LEMMA 2.4.

(1) *Any integral primitive ideal* $\mathfrak{a}$ *has a (nonunique) decomposition of the form* $\mathfrak{a} = \mathfrak{a}^-\mathfrak{a}^+$ *where* $\mathfrak{a}^-$ *and* $\mathfrak{a}^+$ *are coprime,* $(n_{\mathfrak{a}^-}, d_{\mathfrak{a}^-}^-) = 1$, *and* $(n_{\mathfrak{a}^+}, d_{\mathfrak{a}^+}^+) = 1$.

(2) *Let* $\mathfrak{m}$ *be a modulus, and let* $\varepsilon = \pm 1$. *Any element* $\alpha \equiv \varepsilon \pmod{^*\mathfrak{m}}$ *has a (nonunique) decomposition of the form* $\alpha = \alpha^-\alpha^+$ *where* $\alpha^- \equiv \varepsilon \pmod{^*\mathfrak{m}}$, $\alpha^+ \equiv 1 \pmod{^*\mathfrak{m}}$, $(n_{(\alpha^-)}, d_{(\alpha^-)}^-) = 1$, *and* $(n_{(\alpha^+)}, d_{(\alpha^+)}^+) = 1$ *(here for any* $\beta \in k^*$, $(\beta) = \beta\mathbb{Z}_k$ *is the principal ideal generated by* β*).*

Proof. — (1) Define

$$\mathfrak{a}^- = \prod_{\mathfrak{p} \in B^+} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \quad \text{and} \quad \mathfrak{a}^+ = \mathfrak{a}/\mathfrak{a}^- .$$

Clearly $\mathfrak{a}^-$ and $\mathfrak{a}^+$ are coprime. Since B^+ and B^- are disjoint, none of the prime ideals dividing $\mathfrak{a}^-$ belong to B^-. On the other hand, if $\mathfrak{p}$ is a prime ideal dividing $\mathfrak{a}^+$ then by definition $\mathfrak{p}$ does not belong to B^+. Thus (1) follows immediately from Lemma 2.3 (2).

(2) By the strong approximation theorem, since the sets $B^\pm$ are finite and disjoint, we can find $\alpha^- \in k^*$ satisfying the following conditions:

- $\alpha^- \equiv \varepsilon \pmod{^*\mathfrak{m}}$.
- For each $\mathfrak{p} \in B^-$ we have $v_{\mathfrak{p}}(\alpha^-) = 0$.
- For each $\mathfrak{p} \in B^+$ we have $v_{\mathfrak{p}}(\alpha^-) = v_{\mathfrak{p}}(\alpha)$.

Indeed, note that even if $\mathfrak{m}$ is not coprime to the ideals of $B^\pm$ the conditions are compatible since $\alpha \equiv \varepsilon \pmod{^*\mathfrak{m}}$. Thus, it is clear that no prime ideals dividing α^- belong to B^-. If we set $\alpha^+ = \alpha/\alpha^-$, it is also clear that no prime ideals dividing α^+ belong to B^+. We again conclude by Lemma 2.3 (2). □

2.2. Definition of Ψ.

We can now come to the theorem which allows us to define the character Ψ that we need.

THEOREM 2.5. — *Let $\mathfrak{a}$ be an ideal coprime to 2 as above, and let*

$$\Psi(\mathfrak{a})=\left(\frac{-4}{r_{\mathfrak{a}}}\right)\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}}/(n_{\mathfrak{a}},(d_{\mathfrak{a}}^-)^{\infty})}\right)\left(\frac{d_{\mathfrak{a}}^+}{(n_{\mathfrak{a}},(d_{\mathfrak{a}}^-)^{\infty})}\right).$$

(1) *If $\mathfrak{a}=r_{\mathfrak{a}}\mathfrak{a}^-\mathfrak{a}^+$ as in Lemma 2.4, then*

$$\Psi(\mathfrak{a})=\left(\frac{-4}{r_{\mathfrak{a}}}\right)\left(\frac{d_{\mathfrak{a}^-}^-}{n_{\mathfrak{a}^-}}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{n_{\mathfrak{a}^+}}\right).$$

(2) *We have $\Psi(\mathfrak{a})\neq 0$, and $d_{\mathfrak{a}}^+$ and $d_{\mathfrak{a}}^-$ can be interchanged in the definition of Ψ without changing the value of $\Psi(\mathfrak{a})$.*

(3) *Ψ is multiplicative on ideals coprime to 2.*

(4) *If $\alpha\equiv 1\pmod{{}^*4\infty_0\infty_1}$ then $\Psi(\alpha\mathfrak{a})=\Psi(\mathfrak{a})$, in other words Ψ defines a quadratic character on the ray class group $Cl_{4\infty_0\infty_1}$.*

Proof. — (1) The ideal $\mathfrak{a}/r_{\mathfrak{a}}$ being primitive, we can write $\mathfrak{a}=r_{\mathfrak{a}}\mathfrak{a}^-\mathfrak{a}^+$ as in Lemma 2.4. In particular, since $\mathfrak{a}^+$ and $\mathfrak{a}^-$ are coprime and $\mathfrak{a}/r_{\mathfrak{a}}$ is primitive, $n_{\mathfrak{a}^-}$ and $n_{\mathfrak{a}^+}$ are also coprime and we have $n_{\mathfrak{a}}=n_{\mathfrak{a}^-}n_{\mathfrak{a}^+}$, and for any $\varepsilon=\pm$ we have

$$d_{\mathfrak{a}}^{\varepsilon}\equiv d_{\mathfrak{a}^{\varepsilon}}^{\varepsilon}\pmod{n_{\mathfrak{a}^{\varepsilon}}}.$$

Thus

$$(n_{\mathfrak{a}},(d_{\mathfrak{a}}^-)^{\infty})=(n_{\mathfrak{a}^-},(d_{\mathfrak{a}}^-)^{\infty})(n_{\mathfrak{a}^+},(d_{\mathfrak{a}}^-)^{\infty})=(n_{\mathfrak{a}^+},(d_{\mathfrak{a}}^-)^{\infty}).$$

To simplify notations, set $g=(n_{\mathfrak{a}},(d_{\mathfrak{a}}^-)^{\infty})=(n_{\mathfrak{a}^+},(d_{\mathfrak{a}}^-)^{\infty})$. We thus have

$$\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}}/g}\right)\left(\frac{d_{\mathfrak{a}}^+}{g}\right)=\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}^-}}\right)\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}^+}/g}\right)\left(\frac{d_{\mathfrak{a}}^+}{g}\right)=\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}^-}}\right)\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}^+}/g}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{g}\right).$$

But by definition $d_{\mathfrak{a}}^+$ (congruent to $d_{\mathfrak{a}^+}^+$ modulo $n_{\mathfrak{a}^+}$) is also coprime to $n_{\mathfrak{a}^+}$, and for $m\mid n_{\mathfrak{a}^+}$ (which is odd) we have as usual

$$\begin{aligned}\left(\frac{d_{\mathfrak{a}}^-}{m}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{m}\right)&=\left(\frac{d_{\mathfrak{a}^+}^-}{m}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{m}\right)=\left(\frac{(c_{\mathfrak{a}^+}^2-a^2)/4}{m}\right)\\&=\left(\frac{(D-a^2)/4}{m}\right)=\left(\frac{b^2}{m}\right)=1,\end{aligned}$$

since the result is nonzero. Applying this to $m=n_{\mathfrak{a}^+}/g$, we obtain finally

$$\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}}/g}\right)\left(\frac{d_{\mathfrak{a}}^+}{g}\right)=\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}^-}}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{n_{\mathfrak{a}^+}/g}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{g}\right)=\left(\frac{d_{\mathfrak{a}}^-}{n_{\mathfrak{a}^-}}\right)\left(\frac{d_{\mathfrak{a}^+}^+}{n_{\mathfrak{a}^+}}\right)$$

as claimed.

(2) Since $\mathfrak{a}$ is coprime to 2, so is $r_{\mathfrak{a}}$ hence $(-4/r_{\mathfrak{a}})$ is never 0. The rest follows trivially from (1). However, we can check it directly: by definition, $d_{\mathfrak{a}}^-$ is coprime to $n_{\mathfrak{a}}/g$ so the second symbol also nonzero. If the last symbol is zero, this means that $\gcd(n_{\mathfrak{a}}, d_{\mathfrak{a}}^-, d_{\mathfrak{a}}^+) > 1$, contradicting Lemma 2.1. The symmetry between $d_{\mathfrak{a}}^-$ and $d_{\mathfrak{a}}^+$ also follows from this and is left to the reader.

(3) To prove (3), we could use the formula given in (1), but we can also reason directly as follows. Since the symbol $(-4/r)$ is multiplicative, it is sufficient to prove the multiplicativity of Ψ on primitive ideals coprime to 2. Thus, for $i = 1$ and $i = 2$ let $\mathfrak{a}_i = n_i\mathbb{Z} + ((c_i + \sqrt{D})/2)\mathbb{Z}$ be two primitive ideals, with $c_i^2 \equiv D \pmod{4n_i}$, and as above set $d_i^{\pm} = (c_i \pm a)/2$. Thus, for $i = 1$ and $i = 2$ we have

$$\Psi(\mathfrak{a}_i) = \left(\frac{d_i^-}{n_i/(n_i, d_i^{-\infty})}\right)\left(\frac{d_i^+}{(n_i, d_i^{-\infty})}\right).$$

On the other hand (see for example [2]), the product $\mathfrak{a}_3 = \mathfrak{a}_1\mathfrak{a}_2$ is given by the formula

$$\mathfrak{a}_3 = d\Big(\frac{n_1 n_2}{d^2}\mathbb{Z} + \frac{c_3 + \sqrt{D}}{2}\mathbb{Z}\Big),$$

where $d = (n_1, n_2, (c_1 + c_2)/2)$ and c_3 is such that in particular $c_3 \equiv c_i \pmod{2n_i/d}$ for $i = 1, 2$ (this does not suffice to determine c_3 modulo $2n_1n_2/d^2$, but is sufficient in this proof). Hence, setting $d_3^{\pm} = (c_3 \pm a)/2$ and $n_3 = n_1n_2/d^2$, we have

$$\Psi(\mathfrak{a}_3) = \left(\frac{-4}{d}\right)\left(\frac{d_3^-}{n_3/(n_3, d_3^{-\infty})}\right)\left(\frac{d_3^+}{(n_3, d_3^{-\infty})}\right).$$

Now note the following trivial lemma whose proof is left to the reader.

LEMMA 2.6. — *Let x, y and z be arbitrary integers. Then*

(1) $(xy, z^{\infty}) = (x, z^{\infty})(y, z^{\infty})$ *(this is not true in general without the ∞ exponent).*

(2) $(x, (z + xy)^{\infty}) = (x, z^{\infty})$.

Setting $n_i' = n_i/d$, we obtain

$$\begin{aligned}\Psi(\mathfrak{a}_3) &= \left(\frac{-4}{d}\right)\left(\frac{d_3^-}{n_1'/(n_1',d_3^{-\infty})}\right)\left(\frac{d_3^-}{n_2'/(n_2',d_3^{-\infty})}\right)\left(\frac{d_3^+}{(n_3,d_3^{-\infty})}\right)\\
&= \left(\frac{-4}{d}\right)\left(\frac{d_1^-}{n_1'/(n_1',d_3^{-\infty})}\right)\left(\frac{d_2^-}{n_2'/(n_2',d_3^{-\infty})}\right)\left(\frac{d_3^+}{(n_1',d_3^{-\infty})}\right)\left(\frac{d_3^+}{(n_2',d_3^{-\infty})}\right)\\
&= \left(\frac{-4}{d}\right)\left(\frac{d_1^-}{n_1'/(n_1',d_1^{-\infty})}\right)\left(\frac{d_2^-}{n_2'/(n_2',d_2^{-\infty})}\right)\left(\frac{d_3^+}{(n_1',d_1^{-\infty})}\right)\left(\frac{d_3^+}{(n_2',d_2^{-\infty})}\right)\\
&= \left(\frac{-4}{d}\right)\left(\frac{d_1^-}{n_1'/(n_1',d_1^{-\infty})}\right)\left(\frac{d_2^-}{n_2'/(n_2',d_2^{-\infty})}\right)\left(\frac{d_1^+}{(n_1',d_1^{-\infty})}\right)\left(\frac{d_2^+}{(n_2',d_2^{-\infty})}\right)\\
&= \Psi(\mathfrak{a}_1)\Psi(\mathfrak{a}_2)P,\end{aligned}$$

where (using once again the above lemma)

$$P = \left(\frac{-4}{d}\right)\left(\frac{d_1^-}{d/(d,d_1^{-\infty})}\right)\left(\frac{d_2^-}{d/(d,d_2^{-\infty})}\right)\left(\frac{d_1^+}{(d,d_1^{-\infty})}\right)\left(\frac{d_2^+}{(d,d_2^{-\infty})}\right).$$

We must show that $P = 1$.

We first note that $(d, d_1^-, d_2^-) = 1$. Indeed, assume that p is a prime dividing all three. Then p divides

$$d_1^- d_1^+ = \frac{c_1^2 - a^2}{4} \equiv \frac{D - a^2}{4} = b^2 \pmod{n_1},$$

and $p \mid d \mid n_1$ hence $p \mid b$. On the other hand

$$a = \frac{c_1 + c_2}{2} - d_1^- - d_2^-,$$

hence p divides a, a contradiction since $(a, b) = 1$.

To simplify notation, set $e_i = (d, d_i^{-\infty})$ and $e = d/(e_1e_2) \in \mathbb{Z}$ by what we have just proved. Thus

$$\begin{aligned}P &= \left(\frac{-4}{e}\right)\left(\frac{-4}{e_1}\right)\left(\frac{-4}{e_2}\right)\left(\frac{d_1^-}{ee_2}\right)\left(\frac{d_2^-}{ee_1}\right)\left(\frac{d_1^+}{e_1}\right)\left(\frac{d_2^+}{e_2}\right)\\
&= \left(\frac{-4d_1^-d_2^-}{e}\right)\left(\frac{-4d_1^+d_2^-}{e_1}\right)\left(\frac{-4d_1^-d_2^+}{e_2}\right) = P_0P_1P_2,\end{aligned}$$

say. Let us show that $P_0 = P_1 = P_2 = 1$. First, note that

$$\frac{c_1c_2 + D}{2} = \left(\frac{c_1 + c_2}{2}\right)^2 - n_1\frac{c_1^2 - D}{4n_1} - n_2\frac{c_2^2 - D}{4n_2} \equiv 0 \pmod{d}.$$

Thus

$$-4d_1^-d_2^- = -c_1c_2 + (c_1 + c_2)a - a^2 \equiv D - a^2 \equiv b^2 \pmod{d},$$

and since $e \mid d$ and $(e,b) = 1$ (otherwise $P = 0$ which is not the case, but this can also easily be checked directly) we have $P_0 = (b^2/e) = 1$ as claimed.

For P_1, we note that

$$-4d_1^+d_2^- = \left(a + \frac{c_1 - c_2}{2}\right)^2 - \left(\frac{c_1 + c_2}{2}\right)^2 \equiv \left(a + \frac{c_1 - c_2}{2}\right)^2 \pmod{d},$$

hence again because $P \neq 0$ we have

$$P_1 = \left(\frac{(a + (c_1 - c_2)/2)^2}{e_1}\right) = 1.$$

The same proof is valid for P_2 by exchanging the indices 1 and 2. This finishes the proof of the multiplicativity of Ψ on ideals coprime to 2.

(4). By multiplicativity, we must show that if α is a totally positive element congruent to 1 modulo 4 in the multiplicative sense, then $\Psi(\alpha\mathbb{Z}_k) = 1$. Let r be the content of α, i.e., the unique positive rational number such that $\beta = \alpha/r \in \mathbb{Z}_k$ and β *primitive*, in other words $\beta/n \notin \mathbb{Z}_k$ for any integer $n1$. Since α is coprime to 2, so is r, hence we have $r \equiv \pm 1 \pmod{4}$ (as for ideals above, this makes sense even for $r \notin \mathbb{Z}$). Since $r \in \mathbb{Q}_{>0}$, r is totally positive as an element of k, so that β is totally positive and $\beta \equiv r \pmod{4}$. We must thus prove that if β is a primitive algebraic integer of $\mathbb{Z}_k$ with $\beta \equiv \varepsilon \pmod{4}$ for $\varepsilon = \pm 1$, then $\Psi(\beta\mathbb{Z}_k) = \varepsilon$.

For this, we write $\beta = \beta^-\beta^+$ as in Lemma 2.4 (2). By multiplicativity we have $\Psi(\beta\mathbb{Z}_k) = \Psi(\beta^-\mathbb{Z}_k)\Psi(\beta^+\mathbb{Z}_k)$, so it is sufficient to prove our statement for β^- and β^+. The proofs being identical (exchanging $+$ and $-$), we prove it for $\beta = \beta^-$, and we may also assume that β is primitive.

Write $\beta = (u_0 + v_0\sqrt{D})/2$, so that $\beta - \varepsilon = ((u_0 - 2\varepsilon) + v_0\sqrt{D})/2$. The condition $\beta \equiv \varepsilon \pmod{4}$ can thus be summarized by $u_0 \equiv 2\varepsilon \pmod{4}$, $v_0 \equiv 0 \pmod{4}$, and $u_0 - 2\varepsilon \equiv v_0 D \pmod{8}$. Setting $u = u_0/2$ and $v = v_0/4$, we can thus write $\beta = u + 2v\sqrt{D}$ with the sole condition $u - \varepsilon \equiv 2vD \pmod{4}$ (which implies that u is odd). Since β is primitive (and u is odd), u and v are coprime, and since β is totally positive, we have $u > 2|v|\sqrt{D}$.

Since β is primitive, the ideal $\beta\mathbb{Z}_k$ is also primitive hence

$$\beta\mathbb{Z}_k = n_\beta\mathbb{Z} + \frac{c_\beta + \sqrt{D}}{2}\mathbb{Z}$$

where $n_\beta = |\mathcal{N}(\beta)| = u^2 - 4v^2D$ (since $\beta \gg 0$) and c_β is any integer such that $(c_\beta + \sqrt{D})/2 \in \beta\mathbb{Z}_k$ or, equivalently, $((c_\beta + \sqrt{D})/2)\overline{\beta} \in n_\beta\mathbb{Z}_k$. We compute that

$$\frac{c_\beta + \sqrt{D}}{2}(u - 2v\sqrt{D}) = \frac{c_\beta u - 2vD + (u - 2vc_\beta)\sqrt{D}}{2}.$$

Since n_β is odd, the condition that this belongs to $n_\beta\mathbb{Z}_k$ is thus equivalent to $c_\beta u - 2vD \equiv 0 \pmod{n_\beta}$ and $u - 2vc_\beta \equiv 0 \pmod{n_\beta}$. Thus

$$c_\beta \equiv u(2v)^{-1} \equiv 2vDu^{-1} \pmod{n_\beta},$$

the inverses being taken modulo n_β, together with the additional condition that $c_\beta \equiv D \pmod{2}$. Note that the last two quantities are trivially checked to be congruent modulo n_β.

Since u is odd, to have the parity condition on c_β we will decree that the inverse $(2v)^{-1}$ is taken to be an inverse having the same parity as D (which is possible since n_β is odd), and so with this convention we can choose $c_\beta = u(2v)^{-1}$.

Since by assumption $d_\beta^- = (c_\beta - a)/2$ is coprime to n_β, we have

$$\Psi(\beta\mathbb{Z}_k) = \left(\frac{(u(2v)^{-1} - a)/2}{u^2 - 4v^2D}\right).$$

Since u is odd and coprime to v, $2v$ is coprime to $u^2 - 4v^2D$. In addition, since $u \equiv \varepsilon + 2vD \pmod{4}$, we have

$$u - 2av = \varepsilon + 2v(D - a) \equiv \varepsilon \pmod{4},$$

since a and D have the same parity. Thus

$$\begin{aligned}
\Psi(\beta\mathbb{Z}_k) &= \left(\frac{2(u-2av)}{u^2-4v^2D}\right)\left(\frac{2v}{u^2-4v^2D}\right) \quad \left(\text{multiply by } \left(\frac{4\cdot 2v}{u^2-4v^2D}\right) \neq 0\right)\\
&= \left(\frac{u-2av}{u^2-4v^2D}\right)\left(\frac{4v}{u^2-4v^2D}\right) \quad (\text{regroup})\\
&= \left(\frac{u-2av}{(u-2av)(u+2av)-16b^2v^2}\right)\left(\frac{4v}{u^2}\right) \quad (\text{periodicity in } 4v)\\
&= \left(\frac{\varepsilon(u-2av)}{(u-2av)(u+2av)-16b^2v^2}\right)\left(\frac{4\varepsilon}{u^2-4v^2D}\right) \quad ((u,v)=1)\\
&= \left(\frac{\varepsilon(u-2av)}{-16b^2v^2}\right) \text{ (periodicity in } \varepsilon(u-2av) \text{ and } u^2 \equiv 1 \pmod{4})\\
&= \left(\frac{4\varepsilon}{-1}\right) = \varepsilon
\end{aligned}$$

since the symbol is nonzero (so we can get rid of $16b^2v^2$), and since $u - 2avu - 2v\sqrt{D} > 0$. Thus $\Psi(\beta\mathbb{Z}_k) = \varepsilon$ as claimed, finishing the proof of the theorem. Note that we use the convention $(a/-b) = \operatorname{sign}(a)(a/b)$, which is the only reasonable one if we want to have all the nice properties coming from quadratic reciprocity, such as the periodicity in b when a is congruent to 0 or 1 modulo 4. □

Remarks.

(1) As the proof of (3) shows, it is not necessary to use the decomposition of Ψ given in (1) for proving multiplicativity directly. On the other hand, I have not been able to find a direct proof of (4) without using $\alpha^{\pm}$. This is perhaps to be expected since the construction of $\mathfrak{a}^{\pm}$ for an ideal $\mathfrak{a}$ is direct, while that of $\alpha^{\pm}$ uses the approximation theorem which is not directly "computational".

(2) If we choose the integral basis $(1,\omega)$ with $\omega=(a+\sqrt{D})/2$, then note that if $\mathfrak{a}=r_{\mathfrak{a}}(n_{\mathfrak{a}}\mathbb{Z}+((c_{\mathfrak{a}}+\sqrt{D})/2)\mathbb{Z})$, the Hermite normal form (HNF) of $\mathfrak{a}$ on the integral basis is the matrix

$$r_{\mathfrak{a}}\begin{pmatrix} n_{\mathfrak{a}} & (c_{\mathfrak{a}}-a)/2 \\ 0 & 1 \end{pmatrix}=r_{\mathfrak{a}}\begin{pmatrix} n_{\mathfrak{a}} & d_{\mathfrak{a}}^{-} \\ 0 & 1 \end{pmatrix}.$$

Thus the quantity $d_{\mathfrak{a}}^{-}=(c_{\mathfrak{a}}-a)/2$ is completely natural.

(3) It is crucial to note that the character Ψ is *not* canonical: it is attached to the decomposition $D=a^2+4b^2$ as a sum of two squares. Two such characters corresponding to different values of a differ by a (generalized) genus character, i.e., a character defined on the ray class group Cl_4. However the characters corresponding to a and to $-a$ are the same.

2.3. Conductor computations.

In order to apply Corollary 1.3, we need to enumerate the quadratic characters of $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}$ for $\mathfrak{c}\mid 2$ and $\mathfrak{c}_\infty\subset\{\infty_0,\infty_1\}$. Each such character can be written in a unique way in the form

$$\chi(\mathfrak{a})=\left(\frac{d}{\mathcal{N}\mathfrak{a}}\right)\left(\frac{c}{\mathcal{N}\mathfrak{a}}\right)\psi(\mathfrak{a}),$$

where ψ is either equal to 1 or Ψ, c is either 1, -4 or 8, and d ranges through all divisors of D. It is of course understood that $\chi(\mathfrak{a})=0$ if $\mathfrak{a}$ is not coprime to $\mathfrak{c}$.

We must compute the conductor of such a character. More precisely, we need to compute the smallest modulus of the form $\mathfrak{c}^2\mathfrak{c}_\infty$ modulo which the character can be defined. By abuse of language, we will call it the conductor of the character, although we have not checked (and do not need) that it really is the usual conductor.

When Ψ does not occur, the result is in essence given in [7], and is recalled here. The proof is in any case immediate.

Proposition 2.7. — *When 2 is not inert in k, denote by $\mathfrak{p}$ one of the prime ideals above 2 in k. We always denote by d a divisor of D, and as above we let*

$$\chi(\mathfrak{a}) = \left(\frac{d}{\mathcal{N}\mathfrak{a}}\right)\left(\frac{c}{\mathcal{N}\mathfrak{a}}\right).$$

The conductor of χ is given as follows:

(1) *The component at infinity is equal to $\infty_0\infty_1$ if $D > 0$ and $d < 0$, and is equal to 1 otherwise (i.e., when $D < 0$ or $d > 0$).*

(2) *The 2-component is equal to 1 if $c = 1$, and otherwise is equal to 4 if $D \not\equiv 8 \pmod{16}$ and to $2 = \mathfrak{p}^2$ if $D \equiv 8 \pmod{16}$.*

When the character Ψ occurs (thus only for $D0$ sum of two squares), the result is a little more subtle. We must first fix very precisely the embeddings and prime decompositions. We denote by ∞_0 the place corresponding to the real embedding of k which sends $\sqrt{D}$ to the positive square root, and by ∞_1 the other place at infinity. Furthermore, when $D \equiv 1 \pmod 8$, we can write $2\mathbb{Z}_k = \mathfrak{p}_0\mathfrak{p}_1$ for two prime ideals $\mathfrak{p}_0$ and $\mathfrak{p}_1$, and we choose

$$\mathfrak{p}_0 = 2\mathbb{Z} + \frac{-1+\sqrt{D}}{2}\mathbb{Z} \quad \text{and} \quad \mathfrak{p}_1 = 2\mathbb{Z} + \frac{1+\sqrt{D}}{2}\mathbb{Z}.$$

We then have the following result.

Proposition 2.8. — *Assume that $D = a^2 + 4b^2$ is a sum of two squares, and let*

$$\chi(\mathfrak{a}) = \left(\frac{d}{\mathcal{N}\mathfrak{a}}\right)\left(\frac{c}{\mathcal{N}\mathfrak{a}}\right)\Psi(\mathfrak{a})$$

with $c = 1$ or $c = -4$. The conductor of χ is given as follows:

(1) *The component at infinity is equal to ∞_0 if $c = 1$ and to ∞_1 if $c = -4$.*

(2) *The 2-component is equal to 4 if $D \not\equiv 1 \pmod 8$, to $\mathfrak{p}_0^2$ if $D \equiv 1 \pmod 8$ and $c = 1$, and to $\mathfrak{p}_1^2$ if $D \equiv 1 \pmod 8$ and $c = -4$.*

Proof. — Define

$$\widehat{\Psi}(\mathfrak{a}) = \Psi(\overline{\mathfrak{a}}),$$

where $\overline{\mathfrak{a}}$ is the Galois conjugate of $\mathfrak{a}$. It is clear that $\widehat{\Psi}$ is again a quadratic character of $Cl_{4\infty_0\infty_1}$ and its conductor is equal to the conjugate of the conductor of Ψ. Furthermore, we clearly have

$$\widehat{\Psi}(\mathfrak{a})\Psi(\mathfrak{a}) = \Psi(\mathcal{N}\mathfrak{a}\mathbb{Z}_k) = \left(\frac{-4}{\mathcal{N}\mathfrak{a}}\right).$$

Thus, the character χ is either of the form $\chi(\mathfrak{a}) = (d/\mathcal{N}\mathfrak{a})\Psi(\mathfrak{a})$ when $c = 1$ or of the form $\chi(\mathfrak{a}) = (d/\mathcal{N}\mathfrak{a})\widehat{\Psi}(\mathfrak{a})$ when $c = -4$. Since the conductor of $(d/\mathcal{N}\mathfrak{a})$ is equal to 1, to prove the proposition it is thus sufficient to compute the conductor of Ψ alone. By definition, we know that it divides $4\infty_0\infty_1$. We consider separately the infinite and the finite components.

Infinite part of the conductor. — The infinite part of the conductor of Ψ divides $\infty_0\infty_1$. Let us see whether Ψ can be defined modulo $4\infty_i$ for $i = 0$ or 1. Thus, we take $\alpha \equiv 1 \pmod{{}^*4}$ such that $\sigma_i(\alpha) > 0$ for the real embedding σ_i corresponding to the place ∞_i, and we must see whether or not all such α satisfy $\Psi(\alpha\mathbb{Z}_k) = 1$. As usual, without loss of generality we may assume that α is a primitive algebraic integer which is coprime to b (so as to use the simplest possible formulas). In addition, we may assume that $\mathcal{N}(\alpha) < 0$, i.e., $\sigma_{1-i}(\alpha) < 0$, otherwise the result is trivially true.

Using the computation done in the proof of Theorem 2.5 (4), we can set $\alpha = u + 2v\sqrt{D}$ with u and v coprime, $u \equiv 1 + 2vD \pmod 4$, and we have $n_\alpha = |\mathcal{N}(\alpha)| = -(u^2 - 4v^2D)$ and $c_\alpha = u(2v)^{-1} \pmod{n_\alpha}$, so that

$$\Psi(\alpha\mathbb{Z}_K) = \left(\frac{(u(2v)^{-1} - a)/2}{-(u^2 - 4v^2D)}\right).$$

Pursuing the computation done in the proof of Theorem 2.5 (4), where we saw that $u - 2av \equiv 1 \pmod 4$, and taking care of the minus sign, we obtain

$$\begin{aligned}\Psi(\alpha\mathbb{Z}_k) &= \left(\frac{u - 2av}{-(u^2 - 4v^2D)}\right)\left(\frac{4v}{-(u^2 - 4v^2D)}\right)\\ &= \left(\frac{u - 2av}{-(u - 2av)(u + 2av) + 16b^2v^2}\right)\left(\frac{4v}{-u^2}\right)\\ &= \left(\frac{u - 2av}{16b^2v^2}\right)\left(\frac{v}{-1}\right)\\ &= \operatorname{sign}(v) = \operatorname{sign}(\sigma_0(\alpha) - \sigma_1(\alpha)).\end{aligned}$$

Thus the conditions $\sigma_0(\alpha) > 0$, $\sigma_1(\alpha) < 0$ imply $\Psi(\alpha\mathbb{Z}_k) = 1$, while the conditions $\sigma_0(\alpha) < 0$, $\sigma_1(\alpha) > 0$ imply $\Psi(\alpha\mathbb{Z}_k) = -1$. Thus we see that Ψ is defined modulo $4\infty_0$ and not modulo $4\infty_1$ (hence a fortiori not modulo 4), so that the infinite part of conductor of Ψ is equal to ∞_0, as claimed.

Finite part of the conductor. — We know that the finite part of the conductor of Ψ divides 4. On the other hand, we know that it is not equal to 1 otherwise Ψ would be a genus character defined on $Cl_{\infty_0\infty_1}$ which it is not (this is trivially seen, but also follows from the computation of the component at infinity since Ψ would then be defined on $Cl_{\infty_0} = Cl$, hence a fortiori on $Cl_{4\infty_1}$ which it is not). Thus we need to see whether or not Ψ can be defined modulo $\mathfrak{p}^2\infty_0\infty_1$ for some prime ideal $\mathfrak{p}$ of norm 2. In particular we have $D \not\equiv 5 \pmod 8$. When $D \equiv 8 \pmod{16}$, we note that $3 \equiv 1 \pmod 2$ and 3 is totally positive, but $\Psi(3\mathbb{Z}_k) = -1$, so Ψ is not defined modulo $2\infty_0\infty_1$, hence the finite part of the conductor of Ψ is equal to 4 in that case. Thus, from now on assume that $D \equiv 1 \pmod 8$ and let $2\mathbb{Z}_k = \mathfrak{p}_0\mathfrak{p}_1$ with $\mathfrak{p}_0$ and $\mathfrak{p}_1$ chosen as explained above.

We easily compute that

$$\mathfrak{p}_i^2 = 4\mathbb{Z} + \frac{r_i + \sqrt{D}}{2}\mathbb{Z}$$

where r_i is defined modulo 8 so that $r_i^2 \equiv D \pmod{16}$ and $r_i \equiv (-1)^{1-i} \pmod 4$ (specifically, when $D \equiv 1 \pmod{16}$ we can take $r_0 = -1$ and $r_1 = 1$, and when $D \equiv 9 \pmod{16}$ we can take $r_0 = 3$ and $r_1 = -3$). Let $\alpha = (u_0 + v_0\sqrt{D})/2$ be totally positive such that $\alpha \equiv 1 \pmod{\mathfrak{p}_i^2}$, and without loss of generality assume also that α is coprime to b and that α is primitive. Since b is even (trivial), it follows in particular that the norm of α is odd, and we may apply the simplest formula to compute $\Psi((\alpha))$.

A simple computation shows that the above conditions are equivalent to $u_0 > |v_0|\sqrt{D}$, $u_0 \equiv 2 + v_0 r_i \pmod 8$, u_0 and v_0 even, and $(u_0/2, v_0/2) = 1$ with $u_0/2 \not\equiv v_0/2 \pmod 2$. Setting $u = u_0/2$ and $v = v_0/2$, this is equivalent to $u > |v|\sqrt{D}$, $u \equiv 1 + vr_i \pmod 4$, and $(u, v) = 1$ (the condition $u \not\equiv v \pmod 2$ is automatically satisfied since r_i is odd). A similar computation to that made for the infinite part shows that

$$\Psi((\alpha)) = \frac{(uv^{-1} - a)/2}{u^2 - Dv^2} = \left(\frac{u - av}{u^2 - v^2 D}\right)\left(\frac{2v}{u^2 - v^2 D}\right).$$

We consider the two symbols separately. Note that a is odd and u and v are of opposite parity hence $u - av$ is odd, and is positive since $u > |v|\sqrt{D}$. Thus, let $\varepsilon = \pm 1$ such that $\varepsilon(u - av) \equiv 1 \pmod 4$. Since we have assumed $(u, v) = 1$ and α coprime to b, we have

$$\begin{aligned}\left(\frac{u - av}{u^2 - v^2 D}\right) &= \left(\frac{u - av}{(u - av)(u + av) - 4v^2 b^2}\right)\\ &= \left(\frac{\varepsilon(u - av)}{(u - av)(u + av) - 4v^2 b^2}\right)\left(\frac{\varepsilon}{u^2 - v^2 D}\right)\\ &= \left(\frac{\varepsilon(u - av)}{-1}\right)\left(\frac{4\varepsilon}{u^2 - v^2}\right) = \varepsilon\varepsilon^v = \varepsilon^{v+1},\end{aligned}$$

where the equality $(4\varepsilon/(u^2 - v^2)) = \varepsilon^v$ immediately follows from the fact that u and v are of opposite parity. Thus, when v is odd this symbol is equal to 1. When v is even we have $u - av \equiv 1 + v(r - a) \equiv 1 \pmod 4$ since $r - a$ is even, hence $\varepsilon = 1$, so the symbol is equal to 1 in every case.

Consider now the second symbol. When v is even, $2v \equiv 0 \pmod 4$ and v^2D is divisible by $2v$, hence $(2v/(u^2 - v^2D)) = 1$. Thus, assume v odd, hence u even. From $u \equiv 1 + vr_i \pmod 4$ we obtain $u^2 - v^2D \equiv 1 + 2vr_i \pmod 8$. Let $\varepsilon = \pm 1 = (-1)^{(v-1)/2}$ such that $\varepsilon v \equiv 1 \pmod 4$. We thus have

$$\Big(\frac{2v}{u^2 - v^2D}\Big) = \Big(\frac{2}{u^2 - v^2D}\Big)\Big(\frac{v}{u^2 - v^2D}\Big) = \Big(\frac{2}{1 + 2vr_i}\Big)\Big(\frac{v}{u^2 - v^2D}\Big)$$
$$= \Big(\frac{2}{1 + 2vr_i}\Big)\Big(\frac{\varepsilon v}{u^2 - v^2D}\Big)\Big(\frac{4\varepsilon}{u^2 - v^2D}\Big) = \varepsilon\Big(\frac{2}{1 + 2vr_i}\Big).$$

We separate the two cases $\mathfrak{p}_0$ and $\mathfrak{p}_1$. For $\mathfrak{p}_0$, we have $r_i \equiv -1 \pmod 4$, hence

$$\Big(\frac{2v}{u^2 - v^2D}\Big) = \varepsilon\Big(\frac{2}{1 - 2v}\Big) = (-1)^{(v-1)/2}\Big(\frac{2}{1 - 2v}\Big).$$

This depends only on v modulo 4, and we thus see that it is equal to 1 for all v. It follows that $\Psi((\alpha)) = 1$ in that case, as was to be proved. For $\mathfrak{p}_1$, we have $r_i \equiv 1 \pmod 4$, hence

$$\Big(\frac{2v}{u^2 - v^2D}\Big) = \varepsilon\Big(\frac{2}{1 + 2v}\Big) = (-1)^{(v-1)/2}\Big(\frac{2}{1 + 2v}\Big).$$

This is always equal to -1, hence $\Psi((\alpha)) = -1$ in that case, showing that Ψ cannot be defined modulo $\mathfrak{p}_1^2\infty_0\infty_1$. This terminates the proof of the proposition. □

We will see in Section 2.5 that these two propositions immediately give us all the quadratic characters that we will need.

Since the finite part of the conductor of Ψ and associated characters is different from 4 when $D \equiv 1 \pmod 8$, it is necessary to compute the value of the extension of Ψ on ideals $\mathfrak{a}$ which are coprime to $\mathfrak{p}_0$ but not necessarily to $\mathfrak{p}_1$ (which by abuse of notation we will still denote by Ψ), hence which may have even norm. The result is as follows.

PROPOSITION 2.9. — *Assume that $D = a^2 + 4b^2 \equiv 1 \pmod 8$, let $\mathfrak{a}$ be an ideal coprime to $\mathfrak{p}_0$, and set as usual $\mathfrak{a} = r_{\mathfrak{a}}(n_{\mathfrak{a}}\mathbb{Z} + ((c_{\mathfrak{a}} + \sqrt{D})/2)\mathbb{Z})$. Define $v_{\mathfrak{a}} = v_2(n_{\mathfrak{a}})$, the 2-adic valuation of $n_{\mathfrak{a}}$ and*

$$\mathfrak{b} = r_{\mathfrak{a}}\Big(\frac{n_{\mathfrak{a}}}{2^{v_{\mathfrak{a}}}}\mathbb{Z} + \frac{c_{\mathfrak{a}} + \sqrt{D}}{2}\mathbb{Z}\Big).$$

Then $\mathfrak{b}$ is a primitive ideal coprime to 2, $\mathfrak{a} = \mathfrak{p}_1^{v_\mathfrak{a}}\mathfrak{b}$, and we have

$$\Psi(\mathfrak{a}) = \Psi(\mathfrak{p}_1)^{v_\mathfrak{a}}\Psi(\mathfrak{b}) \quad \textit{with} \quad \Psi(\mathfrak{p}_1) = \left(\frac{2}{a}\right)(-1)^{b/2}.$$

Proof. — Since $\mathfrak{a}$ is coprime to $\mathfrak{p}_0$ and $\mathcal{N}\mathfrak{p}_1 = 2$, $r_\mathfrak{a}$ is coprime to 2 and we have

$$v_{\mathfrak{p}_1}(\mathfrak{a}) = v_2(\mathcal{N}\mathfrak{a}) = v_2(n_\mathfrak{a}) = v_\mathfrak{a}.$$

On the other hand, since $n_\mathfrak{a}/2^{v_\mathfrak{a}}$ is odd, it is clear that $\mathfrak{a} = \mathfrak{p}_1^{v_\mathfrak{a}}\mathfrak{b}$ where $\mathfrak{b}$ is as in the proposition. The given formula follows by multiplicativity. Thus the only work to be done is to compute $\Psi(\mathfrak{p}_1)$. For this, we choose $\alpha = (u-\sqrt{D})/2$, where u is a large positive integer such that $u \equiv 2-r_0 \pmod 8$, where r_0 is defined as above in the computation of the finite part of the conductor. It is clear that for u sufficiently large α is totally positive, and $u \equiv 2 - r_0 \pmod 8$ hence $\alpha \equiv 1 \pmod{\mathfrak{p}_0^2}$. Furthermore α is clearly primitive, and since $r_0^2 \equiv D \pmod{16}$ and $r_0 \equiv -1 \pmod 4$, we have

$$n_\alpha = \mathcal{N}(\alpha) = \frac{u^2 - D}{4} \equiv \frac{4 - 4r_0 + r_0^2 - D}{4} \equiv 1 - r_0 \equiv 2 \pmod 4.$$

It follows that α is divisible by $\mathfrak{p}_1$ but not by $\mathfrak{p}_1^2$. Thus, if we write $\alpha\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{b}$, then $\mathfrak{b}$ is coprime to 2 and $\Psi(\alpha\mathbb{Z}_k) = 1$, so that $\Psi(\mathfrak{p}_1) = \Psi(\mathfrak{b})$. We have $\mathfrak{b} = \alpha\mathfrak{p}_0/2$, and an explicit Hermite Normal Form computation gives

$$\mathfrak{b} = \frac{u^2 - D}{8}\mathbb{Z} + \frac{-u + \sqrt{D}}{2}\mathbb{Z}.$$

However, we have the following lemma whose easy proof is left to the reader:

LEMMA 2.10. — *Let a, b, c, and m be integers such that $(a, b, c) = 1$ and either c or $a + b$ is odd. Then there exists x such that $(ax^2 + bx + c, m) = 1$.*

Using this lemma, if necessary by changing u modulo 8, we may assume that $(u^2 - D)/8$ (which is odd) is coprime to b, so as to use the simplest formula for $\Psi(\mathfrak{b})$. Thus

$$\Psi(\mathfrak{p}_1) = \Psi(\mathfrak{b}) = \left(\frac{(-u - a)/2}{(u^2 - D)/8}\right).$$

Since $u \equiv 2 - r_0 \equiv -1 \pmod 4$, to perform the computation more easily we change if necessary a into $-a$ so that $a \equiv -1 \pmod 4$, hence $(-u-a)/2$ will be odd. However $r_0^2 \equiv D \equiv a^2 \pmod{16}$ and $r_0 \equiv a \equiv -1 \pmod 4$ together imply that $r_0 \equiv a \pmod 8$, hence

$$\frac{-u - a}{2} \equiv \frac{-2 + r_0 - a}{2} \equiv -1 \pmod 4.$$

Furthermore, since u is large, $(-u-a)/2$ is negative. We thus obtain

$$\begin{aligned}\Psi(\mathfrak{p}_1) &= \left(\frac{-4}{(u^2-D)/8}\right)\left(\frac{(u+a)/2}{(u^2-D)/2}\right)\\ &= \left(\frac{-4}{(u^2-D)/8}\right)\left(\frac{(u+a)/2}{(u-a)(u+a)/2-2b^2}\right)\\ &= \left(\frac{-4}{(u^2-D)/8}\right)\left(\frac{(u+a)/2}{2}\right).\end{aligned}$$

Since $u \equiv 2-r_0 \equiv 2-a \pmod 8$, we can write $u \equiv 2-a+8\delta \pmod{16}$ for $\delta = 0$ or 1. Thus,

$$\frac{u^2-D}{8} \equiv \frac{1-a}{2} + 2\left(\frac{b}{2}\right)^2 + 2a\delta \pmod 4$$

and of course $(u+a)/2 \equiv 1+4\delta \pmod 8$. It follows that

$$\Psi(\mathfrak{p}_1) = (-1)^{(a+1)/4+(b/2)^2+a\delta}(-1)^{\delta} = (-1)^{(a+1)/4}(-1)^{b/2} = \left(\frac{2}{a}\right)(-1)^{b/2}$$

as claimed. Note that this last formula is invariant under the possible change a into $-a$ that we made at the beginning. □

2.4. Ψ and the quartic reciprocity law.

Quite surprising and important for us is that when the norm of the primitive ideal $\mathfrak{a}$ is a sum of two squares, then $\Psi(\mathfrak{a})$ is *independent* of the ideal $\mathfrak{a}$ of norm $n_{\mathfrak{a}}$ and can be given by quite a different formula. The fact that this formula coincides with the initial definition is a consequence of the *rational quartic reciprocity law*.

We begin by the following lemmas.

LEMMA 2.11. — *Let n be an odd positive integer and set*

$$a(n) = \sum_{\substack{\mathcal{N}\mathfrak{a}=n\\ \mathfrak{a}\ \text{integral}}} \Psi(\mathfrak{a}).$$

Then

(1) *If n is not a sum of two squares, we have $a(n) = 0$.*

(2) *If n is a sum of two squares, write $n = n'n''$ where n' and n'' are coprime and the primes dividing n'' are exactly the prime divisors of n which are both split in k and congruent to 3 modulo 4. Then*

$$a(n) = \Bigl(\sum_{\mathcal{N}\mathfrak{a}=n'} 1\Bigr)\Psi(\mathfrak{a}) = \Bigl(\sum_{m\mid n'}\left(\frac{D}{m}\right)\Bigr)\Psi(\mathfrak{a}),$$

where $\mathfrak{a}$ is any primitive integral ideal of norm n'.

Proof. — Recall that an integer n is a sum of two squares if and only if its prime divisors congruent to 3 modulo 4 have an even exponent in n. It is clear that $a(n)$ is a multiplicative function Thus it is enough to compute $a(p^k)$ for $k \geqslant 1$. We will use the crucial result (which is in fact the only property of Ψ that we use) that for an odd integer m we have $\Psi(m\mathbb{Z}_k) = (-4/m)$, which follows trivially from the definition. Let $k \geqslant 1$. We consider three cases.

(1) If p is inert, then $a(p^k) = 0$ if k is odd while

$$a(p^k) = \Psi(p^{k/2}\mathbb{Z}_k) = \left(\frac{-4}{p}\right)^{k/2}$$

if k is even. In particular if k is odd (whether $p \equiv 3 \pmod 4$ or not) we have $a(p^k) = 0$, and if k is even we have $a(p^k) =^{\cdot} 1 \cdot \Psi(\mathfrak{a})$ for $\mathfrak{a} = p^{k/2}\mathbb{Z}_k$ the unique ideal above p, corresponding to the given formula.

(2) If p is ramified, then $p \mid D$, and since D is a sum of two squares we must have $p \equiv 1 \pmod 4$, so there is no condition for a sum of two squares. In addition, it is clear that $a(p^k) = 1 \cdot \Psi(\mathfrak{p}^k)$ where $\mathfrak{p}$ is the unique ideal above p, corresponding once again to the given formula.

(3) If p is split as $p\mathbb{Z}_k = \mathfrak{p}\overline{\mathfrak{p}}$, then

$$\Psi(\overline{\mathfrak{p}}) = \left(\frac{-4}{p}\right)\Psi(\mathfrak{p}).$$

Thus

$$a(p^k) = \Psi(\mathfrak{p})^k \sum_{0 \leqslant j \leqslant k} \left(\frac{-4}{p}\right)^j,$$

hence if $p \equiv 3 \pmod 4$ we have $a(p^k) = 0$ when k is odd and $a(p^k) = \Psi(\mathfrak{p})^k = 1$ when k is even. When $p \equiv 1 \pmod 4$, we have

$$a(p^k) = (k+1) \cdot \Psi(\mathfrak{p})^k,$$

which corresponds to the given formula and finishes the proof of the lemma.

Although not needed, note also that n'' is a square. □

To state the main result of this section, we first recall that b is coprime to D. Thus if we set

$$i = \begin{cases} -a(2b)^{-1} & \text{if } D \equiv 1 \pmod 4 \\ -(a/2)b^{-1} & \text{if } D \equiv 0 \pmod 4 \end{cases}$$

(inverses of course taken modulo D, which exist in both cases), then it is clear that $(2i)^2 \equiv -4 \pmod{D}$, whence the notation (note that when D is even we have only $i^2 \equiv -1 \pmod{D/4}$; evidently it is impossible to have $i^2 \equiv -1 \pmod{4}$, a fortiori modulo D; in any event, we will only use $2i$ in that case so this does not matter). Note that the choice of the minus sign is only for aesthetic reasons, see below.

The main theorem of this section is the following.

THEOREM 2.12. — *For any odd positive integer n, and with the above choice of $2i$ (see remark below), we have*

$$a(n) = \sum_{x^2+4y^2=n} \left(\frac{D}{x+2iy}\right),$$

where the pair (x, y) is identified with the pair $(-x, -y)$ (but not with the pairs $(-x, y)$ and $(x, -y)$).

Proof. — The representations of n as a sum of two squares being multiplicative, in the same way as the symbol $(D/(x+2iy))$, it follows that both sides are multiplicative functions of n. In addition, by Lemma 2.11 both sides vanish when n is not a sum of two squares. Thus we may assume that $n = p^k$ for some prime p. Assume first that $p \equiv 3 \pmod{4}$, so that in particular p is unramified and k is even. In this case the only solution to $x^2 + 4y^2 = p^k$ is given by $y = 0$ and $x = p^{k/2}$, so that the right hand side is equal to $(D/p)^{k/2}$. On the other hand, by Lemma 2.11 the left hand side is equal to $(-1)^{k/2}$ if p is inert and to 1 if p is split, which is indeed equal to $(D/p)^{k/2}$.

From now on, assume that $p \equiv 1 \pmod{4}$, and write

$$p = u^2 + 4v^2 \equiv (u + 2iv)(u - 2iv) \pmod{D}$$

(where $2i$ is of course the number defined above modulo D). The decompositions $p^k = x^2 + 4y^2$ are in one-to-one correspondence with exponents j with $0 \leqslant j \leqslant k$ under the formula $x + 2iy = (u + 2iv)^j (u - 2iv)^{k-j}$. This of course corresponds to the $k + 1$ ideals above p^k *in the field* $\mathbb{Q}(i)$, not in k. Assume first that p is unramified. We then have

$$\left(\frac{D}{u-2iv}\right) = \left(\frac{D}{u+2iv}\right)\left(\frac{D}{p}\right),$$

so the right hand side is equal to

$$\left(\frac{D}{u+2iv}\right)^k \sum_{0\leqslant j\leqslant k} \left(\frac{D}{p}\right)^j.$$

When p is inert, this is equal to 0 when k is odd and to 1 when k is even, corresponding to the formula given for $a(n)$ in Lemma 2.11.

When p is split, this is equal to $(k+1)(D/(u+2iv))^k$, which is equal to $k+1$ when k is even, hence equal to $a(n)$, and to $(k+1)(D/(u+2iv))$ when k is odd. We must thus prove that in this case $\Psi(\mathfrak{p}) = (D/(u+2iv))$, and this is of course the heart of the matter. For the moment let us postpone this.

When p is ramified, then p divides D so p divides either $u+2iv$ or $u-2iv$, but not both, otherwise p would divide u which is absurd. For example, let us choose v so that p divides $u-2iv$ and hence does not divide $u+2iv$. Thus since $x+2iy \equiv (u+2iv)^j(u-2iv)^{k-j} \pmod{D}$ and $p \mid D$, it follows that $(D/(x+2iy)) = 0$ for $0 \leqslant j < k$, hence the right hand side is equal to

$$\left(\frac{D}{u+2iv}\right)^k.$$

Since the left hand side is equal to $\Psi(\mathfrak{p})^k$, as in the split case we must thus prove that $\Psi(\mathfrak{p}) = (D/(u+2iv))$.

The theorem is thus reduced to the following proposition.

PROPOSITION 2.13. — *Let $p \equiv 1 \pmod{4}$ be a prime number, and write $p = u^2 + 4v^2$, where when $p \mid D$ the signs of u or v are chosen so that $p \nmid u + 2iv$. Assume that there exists an integer c such that $c^2 \equiv D \pmod{4p}$. Then*

$$\left(\frac{(c\pm a)/2}{p}\right) = \left(\frac{D}{u+2iv}\right),$$

where the ± sign is chosen so that $p \nmid (c \pm a)/2$ (such a choice is always possible, and if both are possible any one can be taken).

Proof. — Assume first that $D = q$ is a prime congruent to 1 modulo 4 and different from p. By a version of the rational quartic reciprocity law given in [13], Theorem 5.7, we know (with our notations) that in suitable number fields we have

$$\left(\frac{(\sqrt{q}\pm c)/2}{p}\right) = \left(\frac{u+v\sqrt{-4}}{q}\right),$$

thus giving the result by replacing $\sqrt{q}$ by c, $\sqrt{-4}$ by $2i$, and applying the quadratic reciprocity law (q being positive and congruent to 1 modulo 4). Note that the result in that case is also equal to

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4.$$

When $D = q = p$, the proposition clearly reduces to the equality

$$\left(\frac{2a}{p}\right) = \left(\frac{p}{2a}\right)$$

which is true by quadratic reciprocity since $p \equiv 1 \pmod 4$.

When $D = 8$, we choose $2i = -4$ and the proposition is thus equivalent to

$$\left(\frac{\sqrt{2}+1}{p}\right) = \left(\frac{8}{u-2v}\right)$$

for any prime $p \equiv 1 \pmod 8$. By a special case of Scholz's biquadratic reciprocity law (see [13] Proposition 5.8) and by [13] Proposition 5.4, we have

$$\left(\frac{\sqrt{2}+1}{p}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4 = (-1)^{(p-1)/8}\left(\frac{2}{p}\right)_4 = (-1)^{(p-1)/8+v/2}.$$

We must thus simply check that when $p \equiv 1 \pmod 8$, i.e., when v is even we have

$$\frac{p-1}{8} + \frac{v}{2} \equiv \frac{(u-2v)^2-1}{8} \pmod 2,$$

which is an immediate verification.

Finally, for arbitrary D it is immediately checked that both sides of the equality of the proposition are multiplicative in D, hence the proposition follows in general. □

Remarks.

(1) As we have already mentioned, the character Ψ is not canonical, but depends on the particular choice of decomposition $D = a^2 + 4b^2$. The same is true in Theorem 2.12: the sum $a(n)$ depends on Ψ, and the quantity $2i$ occurring in the right hand side (equal to $-ab^{-1}$) also depends on this decomposition. The theorem would thus not be correct for another choice of i.

(2) The choice of $2i = -ab^{-1}$ (instead of $2i = ab^{-1}$) is due to the fact that if we write $p = c^2 + 4d^2$ in the above proposition (which we have not done to avoid notational confusions with the letters c and d already used with a different meaning), then the right hand side of the formula reads

$$\left(\frac{D}{c+2id}\right) = \left(\frac{D}{c-ab^{-1}d}\right) = \left(\frac{D}{b}\right)\left(\frac{D}{ad-bc}\right)$$

and the $ad - bc$ is more reminiscent of the rational quartic reciprocity law.

The case of even norms can be handled very simply thanks to the following supplementary proposition.

PROPOSITION 2.14. — *Let $D = a^2 + 4b^2 \equiv 1 \pmod 8$, and let $i = -a(2b)^{-1}$ as above. Then*

$$\Psi(\mathfrak{p}_1) = \left(\frac{2}{a}\right)(-1)^{b/2} = \left(\frac{D}{1+i}\right).$$

Proof. — By [13], we know that for any prime $p = a^2 + 4b^2 \equiv 1 \pmod 4$ we have

$$\left(\frac{2}{p}\right)_4 = i^{ab}.$$

It is easy to see that this formula extends by multiplicativity to any $D = a^2 + 4b^2 \equiv 1 \pmod 4$, and when $D \equiv 1 \pmod 8$, b is even so that this reduces to

$$\left(\frac{2}{D}\right)_4 = (-1)^{b/2}.$$

On the other hand, it is clear that

$$\left(\frac{2}{a}\right) = (-1)^{(a^2-1)/8} = (-1)^{(D-1)/8} = i^{(D-1)/4} = \left(\frac{i}{D}\right)_4.$$

Thus,

$$\Psi(\mathfrak{p}_1) = \left(\frac{2}{a}\right)(-1)^{b/2} = \left(\frac{2i}{D}\right)_4 = \left(\frac{(1+i)^2}{D}\right)_4 = \left(\frac{1+i}{D}\right) = \left(\frac{D}{1+i}\right)$$

using quadratic reciprocity, since D is positive and congruent to 1 modulo 8, proving the proposition. □

COROLLARY 2.15. — *Let $D = a^2 + 4b^2 \equiv 1 \pmod 8$, and denote by abuse of notation by Ψ the character extended to $Cl_{\mathfrak{p}_0^2\infty_0\infty_1}$. For any (odd or even) positive integer n we have*

$$a_2(n) = \sum_{\mathcal{N}\mathfrak{a}=n} \Psi(\mathfrak{a}) = \sum_{\substack{x^2+y^2=n\\ x\geqslant 0,\ y>0}} \left(\frac{D}{x+iy}\right).$$

Proof. — Indeed, by the above proposition, we have

$$a_2(n) = \sum_{x^2+y^2=n} \left(\frac{D}{x+iy}\right)$$

where (because of multiplication of $x + iy$ by the units of $\mathbb{Z}[i]$) we must identify the pair (x, y) with the pairs $(-x, -y)$, $(-y, x)$ and $(y, -x)$. The result follows by choosing a suitable system of representatives for this equivalence relation. Of course, when n is odd, we can decide instead as we have done above that y is even, and in that case we recover the identification of the theorem. □

2.5. The quadratic characters of $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}$.

As we will see in the next theorem, all the characters of $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}$ for $\mathfrak{c} \mid 2$ and $\mathfrak{c}_\infty \subset \{\infty_0, \infty_1\}$ can be written in a unique way in the form

$$\chi(\mathfrak{a}) = \left(\frac{d}{\mathcal{N}\mathfrak{a}}\right)\left(\frac{c}{\mathcal{N}\mathfrak{a}}\right)\psi(\mathfrak{a}),$$

where ψ is either equal to 1 or belongs to a 2-element set which can be either $\{1, \Psi\}$ or $\{1, \widehat{\Psi}\}$, where

$$\widehat{\Psi}(\mathfrak{a}) = \Psi(\overline{\mathfrak{a}}),$$

c is either equal to 1 or belongs to a 2-element set $\{1, c_2\}$, and d ranges through all divisors of D such that the sign of cd is either equal to positive (written $s = 1$) or arbitrary (written $s = \pm 1$). The result thus only depends on the ranges of c, s, and ψ, hence can be written as follows.

THEOREM 2.16. — *Denote by C (resp., S, resp., P) the range of values of c (resp., s, resp., ψ), all having only one or two elements. Denote by $\mathfrak{p}$ a prime ideal above 2 in k when 2 is not inert. Then the quadratic characters of $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}$ for $\mathfrak{c} \mid 2$ and $\mathfrak{c}_\infty \subset \{\infty_0, \infty_1\}$ are summarized by the following diagrams:*

- *If $D < 0$ then $P = 1$, hence we give the pair (C, S):*

	$D \equiv 5 \pmod 8$	$D \equiv 1 \pmod 8$	$D \equiv 8 \pmod{16}$	$D \equiv 12 \pmod{16}$
Cl	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{\mathfrak{p}^2}$	$(\emptyset,\emptyset)$	$(1,1)$	$(\{1,-4\},1)$	$(1,1)$
Cl_4	$(\{1,-4\},1)$	$(\{1,-4\},1)$	$(\{1,-4\},1)$	$(\{1,8\},1)$

- *If $D > 0$ is not a sum of two squares, then $P = 1$, hence we give* *the pair* (C, S)*:*

	$D \neq a^2+4b^2$ $5 \pmod 8$	$D \neq a^2+4b^2$ $1 \pmod 8$	$D \neq a^2+4b^2$ $8 \pmod{16}$	$D \neq a^2+4b^2$ $12 \pmod{16}$
Cl	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{\infty_\imath}$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{\infty_0\infty_1}$	$(1,\pm1)$	$(1,\pm1)$	$(1,\pm1)$	$(1,\pm1)$
$Cl_{\mathfrak{p}^2}$	$(\emptyset,\emptyset)$	$(1,1)$	$(\{1,-4\},1)$	$(1,1)$
$Cl_{\mathfrak{p}^2\infty_\imath}$	$(\emptyset,\emptyset)$	$(1,1)$	$(\{1,-4\},1)$	$(1,1)$
$Cl_{\mathfrak{p}^2\infty_0\infty_1}$	$(\emptyset,\emptyset)$	$(1,\pm1)$	$(\{1,-4\},\pm1)$	$(1,\pm1)$
Cl_4	$(\{1,-4\},1)$	$(\{1,-4\},1)$	$(\{1,-4\},1)$	$(\{1,8\},1)$
$Cl_{4\infty_\imath}$	$(\{1,-4\},1)$	$(\{1,-4\},1)$	$(\{1,-4\},1)$	$(\{1,8\},1)$
$Cl_{4\infty_0\infty_1}$	$(\{1,-4\},\pm1)$	$(\{1,-4\},\pm1)$	$(\{1,-4\},\pm1)$	$(\{1,8\},\pm1)$

• *If* $D > 0$ *is a sum of two squares, then the sign indication* s *is superfluous since all divisors* d *of* D *are positive, hence we give here the pair* (C, P) *instead. We choose* ∞_0 *to be the place corresponding to the embedding from* k *into* $\mathbb{R}$ *sending* $\sqrt{D}$ *to the positive square root, and* ∞_1 *to be the other one.*

	$D = a^2+4b^2$ $5 \pmod 8$	$D = a^2+4b^2$ $1 \pmod 8$	$D = a^2+4b^2$ $8 \pmod{16}$
Cl	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{\infty_\imath}$	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{\infty_0\infty_1}$	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{\mathfrak{p}^2}$	$(\emptyset,\emptyset)$	$(1,1)$	$(1,1)$
$Cl_{\mathfrak{p}^2\infty_\imath}$	$(\emptyset,\emptyset)$	$*$	$(1,1)$
$Cl_{\mathfrak{p}^2\infty_0\infty_1}$	$(\emptyset,\emptyset)$	$*$	$(\{1,-4\},1)$
Cl_4	$(1,1)$	$(1,1)$	$(1,1)$
$Cl_{4\infty_0}$	$(1,\{1,\Psi\})$	$(1,\{1,\Psi\})$	$(1,\{1,\Psi\})$
$Cl_{4\infty_1}$	$(1,\{1,\widehat{\Psi}\})$	$(1,\{1,\widehat{\Psi}\})$	$(1,\{1,\widehat{\Psi}\})$
$Cl_{4\infty_0\infty_1}$	$(\{1,-4\},\{1,\Psi\})$	$(\{1,-4\},\{1,\Psi\})$	$(\{1,-4\},\{1,\Psi\})$

In the above diagram, the special cases for $D \equiv 1 \pmod 8$ *marked with a* $*$ *must be treated with special care as follows. Let* $2\mathbb{Z}_k = \mathfrak{p}_0\mathfrak{p}_1$ *be the prime ideal decomposition of* 2*, where the numbering is chosen so that*

$$\mathfrak{p}_0 = 2\mathbb{Z} + \frac{-1+\sqrt{D}}{2}\mathbb{Z} \quad \text{and} \quad \mathfrak{p}_1 = 2\mathbb{Z} + \frac{1+\sqrt{D}}{2}\mathbb{Z}$$

(here the $\sqrt{D}$ *is the same as that used for defining* Ψ*, in other words* $2\omega - a$ *if we take* $(1, (a+\sqrt{D})/2)$ *as integral basis). Then we have the following*

supplementary diagram, which fills in the $*$ *cases of the above diagram:*

	$D=a^2+4b^2$ 1 (mod 8)
$Cl_{\mathfrak{p}_0^2\infty_0}$	$(1,\{1,\Psi\})$
$Cl_{\mathfrak{p}_0^2\infty_1}$	$(1,1)$
$Cl_{\mathfrak{p}_1^2\infty_0}$	$(1,1)$
$Cl_{\mathfrak{p}_1^2\infty_1}$	$(1,\{1,\widehat{\Psi}\})$
$Cl_{\mathfrak{p}_0^2\infty_0\infty_1}$	$(1,\{1,\Psi\})$
$Cl_{\mathfrak{p}_1^2\infty_0\infty_1}$	$(1,\{1,\widehat{\Psi}\})$

Proof. — The case $D<0$ (and also the case $D>0$ with no infinite component) has been dealt with in [7], hence we assume that $D>0$.

For any number field k, denote by $\mathfrak{m}_\infty$ a subset of the set of real places of k, by $\mathfrak{n}_\infty$ the set of real places not belonging to $\mathfrak{m}_\infty$, and by $i(k)$ the number of complex places of k. By [7] Proposition 4.9, we know that

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

where r_2 denotes the 2-rank.

In our case, we have $i(k)=0$, and if t denotes the number of distinct prime numbers dividing D, we know by genus theory that

$$r_2(Cl_{\infty_0\infty_1})=t-1 \quad\text{and}\quad r_2(Cl)=t-1-\delta,$$

where $\delta=1$ if D is not a sum of 2 squares, $\delta=0$ otherwise. The genus characters (i.e., the quadratic characters of $Cl_{\infty_0\infty_1}$ or of Cl) are classical and by [7], we also have a complete description of the quadratic characters modulo 4.

To prove the above theorem, it is thus sufficient to exhibit the characters modulo $4\infty_0\infty_1$ and to compute their conductors. We consider two cases.

- D is not a sum of 2 squares. Then our rank formula gives

$$r_2(Cl_{4\infty_0\infty_1})=t.$$

Thus, we have the $t-1$ independent genus characters $(d/\mathcal{N}\mathfrak{a})$ for all prime discriminant divisors $d\mid D$ but one (in the sense explained above), and the additional independent character $(c_2/\mathcal{N}\mathfrak{a})$ given in [7], in other words with $c_2=-4$ if $D\not\equiv -4 \pmod{16}$ and $c_2=8$ if $D\equiv -4 \pmod{16}$. The conductors of these characters are easily computed and have been given in Proposition 2.7, and give the second diagram of the theorem.

- $D = a^2 + 4b^2$ is a sum of 2 squares. Then our rank formula gives
$$r_2(Cl_{4\infty_0\infty_1}) = t + 1.$$

Thus, we have the same t independent characters as above, and we need an additional one to obtain the rank $t+1$. This is of course the character Ψ, which we have shown to be well defined on the ray class group $Cl_{4\infty_0\infty_1}$ and which is easily seen to be $\mathbb{F}_2$-multiplicatively independent of the t others. This gives the last line of the diagram. As in the previous case, the rest of the diagram is filled by computing explicitly the conductors of the characters, which we have done in Proposition 2.8, finishing the proof of Theorem 2.12. Note of course that the main part of the proof was the computation of the conductors, performed in Propositions 2.7 and 2.8. □

Remark. — Since there are so many special cases in this theorem, it is easy to make an error. We have checked the correctness of the above tables in two ways. First, by computing thousands of numerical examples in *each* entry of the tables, and checking that the 2-rank of the corresponding ray class group is exactly equal to the number of quadratic characters.

Second, by using the above tables as explained in this paper to compute the number of D_4-extensions with signatures, and comparing the results with results obtained in an independent manner, for example using the number field tables of [5].

3. Computational methods and results.

To compute $N_{k,2,\mathfrak{m}_\infty}(C_2, X)$, we use Corollary 1.3, which reduces to the computation of the sums $T_\chi(Z)$ for the quadratic characters χ of $Cl_{\mathfrak{c}^2\mathfrak{c}_\infty}$, which are given by the above theorem. When the character does not involve Ψ, these sums can be efficiently computed using the method explained in [7], which works in this slightly more general setting without change (the essential point is the use of the method of the hyperbola). When the character χ involves Ψ, then we first note that sums on Ψ and on $\widehat{\Psi}$ are equal, since the map sending an ideal to its Galois conjugate is a bijection on ideals of fixed norm. Furthermore, using Theorem 2.12 and Corollary 2.15, these sums are reduced to the computation of
$$\sum_{\substack{x^2+4y^2\leqslant X\\ x \text{ odd}}} \left(\frac{D/d}{x+2iy}\right)\left(\frac{d}{x-2iy}\right)$$

(where we choose $y \geqslant 0$ and $x \geqslant 1$ if $y = 0$) and of

$$\sum_{\substack{x^2+y^2\leqslant X\\ x\geqslant 0,\ y>0}} \left(\frac{D/d}{x+iy}\right)\left(\frac{d}{x-iy}\right)$$

(when $D \equiv 1 \pmod 8$)). It is not necessary (and not really possible nor useful) to use the method of the hyperbola on what is in fact a *circle* problem. On the other hand, to speed up the computation by orders of magnitude, it is essential to use the following method. We start by summing on y (for $y \leqslant \sqrt{X}/2$ in the first sum, and $y \leqslant \sqrt{X}$ in the second), and we then sum on $|x| \leqslant \sqrt{X-4y^2}$ in the first sum, and on $0 \leqslant x \leqslant \sqrt{X-y^2}$ in the second. To compute these sums, we use the following lemma, which insures that we never sum more than $D/2$ terms:

LEMMA 3.1. — *Let D and d be as above, in particular positive fundamental discriminants such that D/d is a fundamental discriminant coprime to d, and let y, z be integers.*

(1)

$$\sum_{0\leqslant x<D} \left(\frac{D/d}{x+y}\right)\left(\frac{d}{x+z}\right) = 0.$$

(2) *Let $\varepsilon = 0$ or $\varepsilon = 1$. Then*

$$\sum_{\substack{0\leqslant x<D\\ x\equiv\varepsilon \pmod 2}} \left(\left(\frac{D/d}{x+y}\right)\left(\frac{d}{x-y}\right)+\left(\frac{D/d}{x-y}\right)\left(\frac{d}{x+y}\right)\right) = k\left(\frac{D}{y}\right),$$

where $k = 0$ if $D \equiv 0 \pmod 4$ and $k = (-1)^\varepsilon$ if $D \equiv 1 \pmod 4$.

Proof. — (1) Since D/d and d are coprime, we can find m such that

$$y + m(D/d) \equiv z \pmod d$$

($m = (z-y)(D/d)^{-1} \pmod d$)). Thus

$$\sum_{0\leqslant x<D} \left(\frac{D/d}{x+y}\right)\left(\frac{d}{x+z}\right) = \sum_{0\leqslant x<D} \left(\frac{D/d}{x+y+m(D/d)}\right)\left(\frac{d}{x+y+m(D/d)}\right)$$
$$= \sum_{0\leqslant x<D} \left(\frac{D}{x+y+m(D/d)}\right) = 0$$

since the sum of a nontrivial character over a period is equal to zero.

(2) Here, we set $z = -y$. Using the same $m = (-2y)(D/d)^{-1} \pmod{d}$ as in (1), we find in the same way

$$\sum_{\substack{0 \leqslant x < D \\ x \equiv \varepsilon \pmod 2}} \left(\frac{D/d}{x+y}\right)\left(\frac{d}{x-y}\right) = \sum_{\substack{0 \leqslant x < D \\ x \equiv \varepsilon \pmod 2}} \left(\frac{D}{x+t}\right)$$

with $t = y + m(D/d)$. Similarly,

$$\sum_{\substack{0 \leqslant x < D \\ x \equiv \varepsilon \pmod 2}} \left(\frac{D/d}{x-y}\right)\left(\frac{d}{x+y}\right) = \sum_{\substack{0 \leqslant x < D \\ x \equiv \varepsilon \pmod 2}} \left(\frac{D}{x-t}\right)$$

for the same t (this would not be true if z was not equal to $-y$).

Thus, if we set

$$S_\varepsilon(t) = \sum_{\substack{0 \leqslant x < D \\ x \equiv \varepsilon \pmod 2}} \left(\frac{D}{x+t}\right),$$

the sum to be computed is equal to $S_\varepsilon(t) + S_\varepsilon(-t)$.

We clearly have $S_0(t) + S_1(t) = 0$.

Assume first that $D \equiv 0 \pmod 4$. Then

$$S_0(t) = \sum_{\substack{t \leqslant x \leqslant t+D \\ x \equiv t \pmod 2}} \left(\frac{D}{x}\right) = - \sum_{\substack{t \leqslant x \leqslant t+D \\ x \equiv t+1 \pmod 2}} \left(\frac{D}{x}\right)$$

since the sum over a period is zero. When t is even, all the terms in the first sum are zero, while when t is odd, all the terms in the second sum are zero, giving the result in that case. In fact this proves the stronger result valid only when $D \equiv 0 \pmod 4$:

$$\sum_{\substack{0 \leqslant x < D \\ x \equiv \varepsilon \pmod 2}} \left(\frac{D/d}{x+y}\right)\left(\frac{d}{x+z}\right) = 0.$$

Assume now that $D \equiv 1 \pmod 4$. Changing x into $D - x$, we have

$$\begin{aligned} S_\varepsilon(t) &= \sum_{\substack{1 \leqslant x \leqslant D \\ x \equiv 1-\varepsilon \pmod 2}} \left(\frac{D}{D-x+t}\right) = \sum_{\substack{1 \leqslant x \leqslant D \\ x \equiv 1-\varepsilon \pmod 2}} \left(\frac{D}{x-t}\right) \\ &= S_{1-\varepsilon}(-t) + \left(\frac{D}{t}\right)\delta_{D,1-\varepsilon} - \left(\frac{D}{t}\right)\delta_{0,1-\varepsilon} \\ &= -S_\varepsilon(-t) + (-1)^\varepsilon\left(\frac{D}{t}\right), \end{aligned}$$

where $\delta_{a,b} = 1$ if a and b have the same parity, 0 otherwise.

Thus, our sum is equal to

$$(-1)^{\varepsilon}\Big(\frac{D}{t}\Big) = (-1)^{\varepsilon}\Big(\frac{D}{y+m(D/d)}\Big) = (-1)^{\varepsilon}\Big(\frac{D/d}{y}\Big)\Big(\frac{d}{-y}\Big) = (-1)^{\varepsilon}\Big(\frac{D}{y}\Big)$$

as claimed. □

In the sequel, we fix y, and to simplify notation we set

$$f(x) = \Big(\frac{D/d}{x+y}\Big)\Big(\frac{d}{x-y}\Big),$$

so that

$$f(-x) = \Big(\frac{D/d}{x-y}\Big)\Big(\frac{d}{x+y}\Big),$$

and we also set $f^+(x) = f(x) + f(-x)$.

COROLLARY 3.2. — *Let*

$$S(X) = \sum_{\substack{|x|\leqslant X\\ x\equiv 1 \pmod 2}} f(x) \quad \text{and} \quad S_2(X) = \sum_{0\leqslant x\leqslant X} f(x).$$

Then

(1) *Write $X = qD + r$ with $0 \leqslant r < D$. Then*

$$S(X) = \sideset{}{'}\sum_{\substack{0\leqslant x\leqslant r\\ x\equiv qD+1 \pmod 2}} f^+(x) \quad \text{and} \quad S_2(X) = \sum_{0\leqslant x\leqslant r} f(x) = S_2(r),$$

where $\sum'$ indicates that the term $x = 0$, if present, must be counted with coefficient $1/2$ (i.e., $f(0)$ instead of $f^+(0)$).

(2) *Let $\varepsilon = 0$ or $\varepsilon = 1$, and assume $0 \leqslant r < D$ as in (1). Then*

$$\sideset{}{'}\sum_{\substack{0\leqslant x\leqslant r\\ x\equiv \varepsilon \pmod 2}} f^+(x) = -\sideset{}{'}\sum_{\substack{0\leqslant x< D-r\\ x\equiv D-\varepsilon \pmod 2}} f^+(x) \quad \text{and} \quad S_2(r) = -\sum_{0< x< D-r} f(-x).$$

Proof. — (1) Note first that Lemma 3.1 (2) can be rewritten

$$\sum_{\substack{0\leqslant x< D\\ x\equiv \varepsilon \pmod 2}} f^+(x) = (-1)^{\varepsilon}\Big(\frac{D}{4y}\Big).$$

Write $x = jD + n$. We thus have

$$\begin{aligned}S(X) &= \sum_{\substack{0\leqslant x\leqslant X\\ x\equiv 1 \pmod 2}} f^+(x)\\
&= \sum_{0\leqslant j\leqslant q-1}\ \sum_{\substack{jD\leqslant x<(j+1)D\\ x\equiv 1 \pmod 2}} f^+(x) + \sum_{\substack{qD\leqslant x\leqslant qD+r\\ x\equiv 1 \pmod 2}} f^+(x)\\
&= \sum_{0\leqslant j\leqslant q-1}\ \sum_{\substack{0\leqslant x<D\\ x\equiv jD+1 \pmod 2}} f^+(x) + \sum_{\substack{0\leqslant x\leqslant r\\ x\equiv qD+1 \pmod 2}} f^+(x)\\
&= \left(\frac{D}{4y}\right)\sum_{0\leqslant j\leqslant q-1}(-1)^{jD+1} + \sum_{\substack{0\leqslant x\leqslant r\\ x\equiv qD+1 \pmod 2}} f^+(x).\end{aligned}$$

When qD is even, we thus have

$$S(X) = \sum_{\substack{0\leqslant x\leqslant r\\ x\equiv 1 \pmod 2}} f^+(x),$$

while when qD is odd, we have

$$S(X) = -\left(\frac{D}{y}\right) + \sum_{\substack{0\leqslant x\leqslant r\\ x\equiv 0 \pmod 2}} f^+(x),$$

proving the first formula. The formula for $S_2(X)$ follows trivially from Lemma 3.1 (1).

(2) We write

$$\begin{aligned}\sum_{\substack{0\leqslant x\leqslant r\\ x\equiv \varepsilon \pmod 2}}{}' f^+(x) &= \sum_{\substack{0\leqslant x<D\\ x\equiv \varepsilon \pmod 2}}{}' f^+(x) - \sum_{\substack{r<x<D\\ x\equiv \varepsilon \pmod 2}} f^+(x)\\
&= \left((-1)^\varepsilon\left(\frac{D}{4}\right) - \frac{1+(-1)^\varepsilon}{2}\right)\left(\frac{D}{y}\right) - \sum_{\substack{0<x<D-r\\ x\equiv D-\varepsilon \pmod 2}} f^+(x)\end{aligned}$$

since $f^+(D-x) = f^+(x)$. By considering the four different cases (D and ε odd or even), we see that this is equal to

$$-\sum_{\substack{0\leqslant x<D-r\\ x\equiv D-\varepsilon \pmod 2}}{}' f^+(x)$$

as claimed.

The second sum is done similarly and is simpler:

$$S_2(r)=\sum_{0\leqslant x\leqslant r} f(x)=\sum_{0\leqslant x<D} f(x)-\sum_{r<x<D} f(x)=-\sum_{0<x<D-r} f(-x)$$

proving the corollary. □

Thus, using (1) and (2) when $r\geqslant D/2$, we can always reduce the computation of the sums S and S_2 to sums of at most $D/2$ terms. Note also that for $y=0$, we use the equalities

$$\sum_{\substack{1\leqslant x\leqslant X\\ x\equiv 1 \pmod 2}}\left(\frac{D}{x}\right)=\sum_{\substack{1\leqslant x\leqslant r\\ x\equiv qD+1 \pmod 2}}\left(\frac{D}{x}\right)=-\sum_{\substack{1\leqslant x<D-r\\ x\equiv qD+1+D \pmod 2}}\left(\frac{D}{x}\right)$$

which immediately follow from the above corollary. There is of course no $\sum'$ since $\left(\frac{D}{0}\right)=0$.

Putting all this on .a computer, we have computed the values of $N_{r_1,r_2}(D_4,10^k)$ for $1\leqslant k\leqslant 17$. The computation of $N_{r_1,r_2}(D_4,10^{17})$ (for all pairs (r_1,r_2)) required in total 26 days CPU time on a Pentium III 600Mhz workstation. We give the results in the following table where, for completeness, we also give the corresponding results for $N_{r_1,r_2}(C_4,X)$, $N_{r_1,r_2}(V_4,X)$, and $N_{r_1,r_2}(I,X)$, where

$$N_{r_1,r_2}(I,X)=N_{r_1,r_2}(C_4,X)+3N_{r_1,r_2}(V_4,X)+2N_{r_1,r_2}(D_4,X).$$

In signature $(0,2)$, we separate the cases where the quartic fields contain a real quadratic field from those which contain a complex quadratic field. In that case, we have

$$N^+_{0,2}(I,X)=2N^+_{0,2}(D_4,X)+N_{0,2}(V_4,X)+N_{0,2}(C_4,X)$$

and

$$N^-_{0,2}(I,X)=2N^-_{0,2}(D_4,X)+2N_{0,2}(V_4,X).$$

More complete tables of $N_{r_1,r_2}(C_4,X)$ and $N_{r_1,r_2}(V_4,X)$, which are much easier to compute, can be found in [4]. For the reader's convenience, we also recall the corresponding tables without signature.

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

X	$N_{4,0}(C_4,X)$	$N_{4,0}(V_4,X)$	$N_{4,0}(D_4,X)$	$N_{4,0}(I,X)$
10^1	0	0	0	0
10^2	0	0	0	0
10^3	0	0	1	2
10^4	6	6	25	74
10^5	15	42	379	899
10^6	59	196	4486	9619
10^7	182	876	47562	97934
10^8	586	3603	486314	984023
10^9	1867	14249	4903607	9851828
10^{10}	5966	54940	49188349	98547484
10^{11}	19017	207295	492454432	985549766
10^{12}	60456	769284	4926654580	9855677468
10^{13}	191736	2814497	49274156836	98556948899
10^{14}	607589	10181802	492769145545	985569444085
10^{15}	1924160	36478693	4927790007755	9855691375749
10^{16}	6090130	129620531	49278249627160	98556894206043
10^{17}	19271385	457321963	492783730187748	985568851612770

X	$N_{2,1}(D_4, X)$	$N_{2,1}(I, X)$
10^1	0	0
10^2	0	0
10^3	6	12
10^4	93	186
10^5	968	1936
10^6	9772	19544
10^7	98413	196826
10^8	984708	1969416
10^9	9852244	19704488
10^{10}	98546786	197093572
10^{11}	985536549	1971073098
10^{12}	9855572218	19711144436
10^{13}	98556488881	197112977762
10^{14}	985567509497	1971135018994
10^{15}	9855683662056	19711367324112
10^{16}	98556864596086	197113729192172
10^{17}	985568739794773	1971137479589546

X	$N_{0,2}(C_4, X)$	$N_{0,2}(V_4, X)$	$N_{0,2}(D_4, X)$	$N_{0,2}(I, X)$
10^1	0	0	0	0
10^2	0	0	0	0
10^3	1	8	17	59
10^4	4	41	295	717
10^5	17	201	3417	7454
10^6	54	818	36238	74984
10^7	181	3331	370424	751022
10^8	582	13076	3734826	7509462
10^9	1865	50067	37469573	75091212
10^{10}	5964	187770	375154025	750877324
10^{11}	19028	694262	3753258277	7508618368
10^{12}	60469	2536801	37538880690	75085432252
10^{13}	191764	9167570	375411901218	750851496910
10^{14}	607609	32835581	3754202033198	7508503180748
10^{15}	1924059	116677591	37542317217650	75084986392132
10^{16}	6090110	411762457	375424223055946	750849687489373
10^{17}	19271321	1444383361	3754245940051259	7508496232523922

X	$N^{+}_{0,2}(D_4, X)$	$N^{+}_{0,2}(I, X)$	$N^{-}_{0,2}(D_4, X)$	$N^{-}_{0,2}(I, X)$
10^1	0	0	0	0
10^2	0	0	0	0
10^3	0	9	17	50
10^4	27	99	268	618
10^5	395	1008	3022	6446
10^6	4512	9896	31726	65088
10^7	47708	98928	322716	652094
10^8	486531	986720	3248295	6522742
10^9	4904276	9860484	32565297	65230728
10^{10}	49190647	98575028	325963378	652302296
10^{11}	492464630	985642550	3260793647	6522975818
10^{12}	4926673909	9855945088	32612206781	65229487164
10^{13}	49274235813	98557830960	326137665405	652293665950
10^{14}	492769387400	985572217990	3261432645798	6522930962758
10^{15}	4927790822970	9855700247590	32614526394680	65229286144542
10^{16}	49278252225484	98556922303535	326145970830462	652292765185838
10^{17}	492783738112277	985568939879236	3261462201938982	6522927292644686

BIBLIOGRAPHY

[1] M. BHARGAVA, Higher Composition Laws, PhD Thesis, Princeton Univ., June 2001.

[2] H. COHEN, A Course in Computational Algebraic Number Theory (fourth corrected printing), Graduate Texts in Math., 138, Springer-Verlag, 2000.

[3] H. COHEN, Comptage exact de discriminants d'extensions abéliennes, J. Th. Nombres Bordeaux, 12 (2000), 379–397.

[4] H. COHEN, F. DIAZ Y DIAZ and M. OLIVIER, Counting discriminants of number fields, preprint.

[5] H. COHEN, F. DIAZ Y DIAZ and M. OLIVIER, Construction of tables of quartic fields using Kummer theory, Proceedings ANTS IV, Leiden (2000), Lecture Notes in Computer Science 1838, Springer-Verlag, 257–268.

[6] H. COHEN, F. DIAZ Y DIAZ and M. OLIVIER, Counting discriminants of number fields of degree up to four Proceedings ANTS IV, Leiden (2000), Lecture Notes in Computer Science 1838, Springer-Verlag, 269–283.

[7] H. COHEN, F. DIAZ Y DIAZ and M. OLIVIER, Enumerating quartic dihedral extensions of $\mathbb{Q}$, Compositio Math., 133 (2002), 65–93.

[8] H. COHEN, F. DIAZ Y DIAZ et M. OLIVIER, Densité des discriminants des extensions cycliques de degré premier, C.R. Acad. Sci. Paris, 330 (2000), 61–66.

[9] H. COHEN, F. DIAZ Y DIAZ and M. OLIVIER, On the Density of Discriminants of Cyclic Extensions of Prime Degree, J. reine angew. Math., 550 (2002), 169–209.

[10] B. DATSKOVSKY and D. J. WRIGHT, Density of discriminants of cubic extensions, J. reine angew. Math., 386 (1988), 116–138.

[11] H. DAVENPORT and H. HEILBRONN, On the density of discriminants of cubic fields I, Bull. London Math. Soc., 1 (1969), 345–348.

[12] H. DAVENPORT and H. HEILBRONN, On the density of discriminants of cubic fields II, Proc. Royal. Soc. A, 322 (1971), 405–420.

[13] F. LEMMERMEYER, Reciprocity laws, Springer Monographs in Math., Springer-Verlag (2000).

[14] S. MÄKI, On the density of abelian number fields, Thesis, Helsinki, 1985.

[15] S. MÄKI, The conductor density of abelian number fields, J. London Math. Soc., 47-2 (1993), 18–30.

[16] D. J. WRIGHT, Distribution of discriminants of abelian extensions, Proc. London Math. Soc., 58-3 (1989), 17–50.

[17] D. J. WRIGHT and A. YUKIE, Prehomogeneous vector spaces and field extensions, Invent. Math., 110 (1992), 283–314.

[18] A. YUKIE, Density theorems related to prehomogeneous vector spaces, preprint.

Manuscrit reçu le 9 octobre 2001,
accepté le 16 mai 2002.

Henri COHEN,
Université Bordeaux I
Laboratoire A2X, U.M.R. 5465 du C.N.R.S.
351 Cours de la Libération
33405 Talence Cedex (France).
cohen@math.u-bordeaux.fr