Math. Nachr. **183** (1997), 173–184

Powerful Necessary Conditions for Class Number Problems

By STÉPHANE LOUBOUTIN of Caen

(Received November 24, 1994)

Abstract. We give a necessary condition for the ideal class group of a CM–field to be of exponent at most two. This condition enables us to drastically reduce the amount of relative class number computation for determination of the CM–fields of some types (e.g. the imaginary cyclic non–quadratic number fields of 2–power degrees) whose ideal class groups are of exponents at most two. We also give a necessary condition for some quartic non–CM–fields to have class number one.

1. Introduction

Lately, two class number problems on imaginary abelian number fields have been solved: 1) the determination of all imaginary abelian number fields with class number one by K. YAMAMURA in [Yam], 2) the determination of all non–quadratic 2–power degrees imaginary cyclic number fields with ideals class groups of exponent less than or equal to 2 by S. LOUBOUTIN in [Lou 7]. Using the results in [Lou 5] and this paper, we could now write down both these determinations in a much more satisfactory way than YAMAMURA and LOUBOUTIN initially adopted when they solved these determinations. In both cases, the first step is to get an explicit upper bound on the conductors of such number fields, and we explained in [Lou 5] how to get good such upper bounds. Then, we could compute the relative class numbers of all the considered imaginary abelian number fields with conductors less than this upper bound. Here, we give a necessary condition for the ideal class group of a CM–field K to have exponent at most two (Theorem 1). This necessary condition enables us to drastically reduce this amount of relative class number computation. Of course, testing whether this necessary condition holds for K is much easier and faster than computing the (relative) class number of K. Note that the use of such necessary conditions to get rid of most occurences becomes unavoidable when one deals with non abelian CM–fields, for in such cases relative class number computations are not as plain as in the abelian case (see [Lou-Oka]).

1991 *Mathematics Subject Classification.* Primary 11 R 29; Secondary 11 R 21.
Keywords and phrases. Class number, relative class number, CM–field.

Finally, we also give a necessary condition for some quartic non-CM-fields to have class number one. This necessary condition will enable us to easily solve the class number one problem for these quartic number fields.

2. Necessary conditions for class number problems for CM-fields

We gave a necessary condition for the class number of a CM-field to be one [Lou 6, Theorem D]). By a slight modification we get the following condition useful also for the exponent two class group problem.

Theorem 2.1. (cf. [Lou 6].) *Let* K *be a* CM*-field of degree* $2N$ *with maximal totally real subfield* k. *Let* d_{K} *and* d_{k} *be the absolute values of the discriminants of* K *and* k. *Let* I *be a principal ideal of* K *which is either a prime ideal of* K *ramified in* K/k, *or a power of a prime ideal of* K *which splits in* K/k. *If* k *has class number one, then the absolute norm of* I *satisfies* $N_{\mathrm{K/Q}}(\mathrm{I}) \geq d_{\mathrm{K}}/\left(4^N d_{\mathrm{k}}^2\right)$. *In particular, if* K *has class number one, then any prime* q *which splits completely in* K *satisfies* $q \geq d_{\mathrm{K}}/\left(4^N d_{\mathrm{k}}^2\right)$, *and if* k *has class number one and the ideal class group of* K *has exponent less than or equal to 2, then any prime* q *which splits completely in* K *satisfies* $q^2 \geq d_{\mathrm{K}}/\left(4^N d_{\mathrm{k}}^2\right)$.

3. Four examples

Let K be a cyclic number field of conductor f_{K}, degree $2N$ and let χ_{K} be any primitive Dirichlet character modulo f_{K} which generates the group of Dirichlet characters associated with K. Then, a prime q which does not divide f_{K} splits completely in K if and only if $\chi_{\mathrm{K}}(q) = 1$. Note that if $f_{\mathrm{K}} = p$ is some odd prime, then $\chi_{\mathrm{K}}(q) = 1$ if and only if $q^{(p-1)/(2N)} \equiv 1 \pmod{p}$ (since the multiplicative group $(\mathrm{Z}/p\mathrm{Z})^*$ is cyclic). Throughout this paper, we let h_{K} denote the class number of any number field K. If K is a CM-field, then we let h_{K}^- denote its relative class number.

3.1. First example

Theorem 2.1 may be useless, especially when the extension K/k is unramified at all the finite places, which implies $d_{\mathrm{K}} = d_{\mathrm{k}}^2$. For example Theorem 2.1 does not provide any restriction on the primes $p, q \equiv 3 \pmod{4}$ when we require the class number of the imaginary biquadratic bicyclic number field $\mathrm{Q}(\sqrt{-p}, \sqrt{-q})$ to be one.

3.2. Second example

Theorem 2.1 may be only slightly useful. Let $\mathrm{K} = \mathrm{kL}$ be an imaginary cyclic sextic number field. Here k is a real cyclic cubic number field, and L is an imaginary quadratic number field. Suppose $h_{\mathrm{K}} = 1$. Then $h_{\mathrm{k}} = h_{\mathrm{L}} = 1$. Hence, we have $f_{\mathrm{L}} \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$, and by considering fields with $\mathrm{k} = \mathrm{Q}(\cos(2\pi/9))$ or $f_{\mathrm{k}} = f_{\mathrm{L}}$ separately, we may assume that $f_{\mathrm{k}} = p \equiv 1 \pmod{6}$ is prime, and that p

and f_{L} are coprime. Then, $f_{\mathrm{K}} = pf_{\mathrm{L}}$, $\mathrm{K} = f_{\mathrm{L}}^3 p^4$, $d_{\mathrm{k}} = p^2$ and $d_{\mathrm{K}}/4^3 d_{\mathrm{k}}^2 = (f_{\mathrm{L}}/4)^3$. According to Theorem 2.1 and by noticing that a prime q splits in K if and only if it splits in k and L, we have that if $h_{\mathrm{K}} = 1$ then the following condition is satisfied.

$$\text{(3.1)} \qquad \begin{array}{c} \text{For any prime } q \text{ (prime to } f_{\mathrm{K}}) \text{ with } q < (f_{\mathrm{L}}/4)^3, \text{ we have} \\ (-f_{\mathrm{L}}/q)_{\mathrm{leg}} \neq +1 \text{ or } q^{(p-1)/3} \not\equiv 1 \pmod{p}. \end{array}$$

(This is useless if $f_{\mathrm{L}} \in \{3,4\}$). Here $(-f_{\mathrm{L}}/q)_{\mathrm{leg}}$ denotes the Legendre's symbol. Now, by using [Lou 5] we proved that if $h_{\mathrm{K}} = 1$, then $f_{\mathrm{K}} \leq 8000$ ([Lou 3, page 142]). Let c_{L} be the number of primes $p \equiv 1 \pmod 6$, coprime to f_{L}, such that $pf_{\mathrm{L}} = f_{\mathrm{K}} \leq 8000$, and let cn_{L} be the number of primes $p \equiv 1 \pmod 6$, coprime to f_{L}, such that $pf_{\mathrm{L}} = f_{\mathrm{K}} \leq 8000$ and (3.1) is satisfied. We have the following table.

Table 1

f_{L}	3	4	7	8	11	19	43	67	163
c_{L}	187	148	91	80	61	38	18	12	6
cn_{L}	187	148	63	54	27	0	0	0	0

Hence, the computation of the relative class numbers of these 479 number fields yields that there are exactly 17 imaginary cyclic sextic fields with class number one (see [Lou 2]).

3.3. Third example

Theorem 2.1 may be very useful. Let K be an imaginary cyclic quartic number field. Suppose that $h_{\mathrm{K}} = 1$. Then $f_{\mathrm{K}} \leq 50000$ ([Uch 2, Proposition 6]), and by considering the unique field of even conductor separately, we may assume that $f_{\mathrm{K}} = p \equiv 5 \pmod 8$ is prime. Hence, $d_{\mathrm{K}} = p^3$, $d_{\mathrm{k}} = p$. According to Theorem 2.1, if $h_{\mathrm{K}} = 1$ then the following condition is satisfied (see [Lou 6]).

$$\text{(3.2)} \qquad \text{For any prime } q \text{ with } q < p/16, \text{ we have } q^{(p-1)/4} \equiv 1 \pmod{p}.$$

Now, there are only 10 primes $p \equiv 5 \pmod 8$ less than 50000 such that (3.2) is satisfied, namely $p \in \{5, 13, 29, 37, 53, 61, 157, 173, 197, 373\}$. Hence, the computation of the relative class numbers of these 10 number fields yields that there are exactly 7 imaginary cyclic quartic fields with class number one (see [Set]).

3.4. Fourth example

(See [Lou 7]). Let K be a non-quadratic imaginary cyclic number field of 2-power degree. If the ideal class group of K has exponent less than or equal to 2, then K is in $\mathcal{F}_p$ for some prime p. Here, for each prime p, $\mathcal{F}_p$ denotes the family of non-quadratic imaginary cyclic number fields K such that $[\mathrm{K} : \mathrm{Q}] = 2N = 2^n$ for some $n \geq 2$ and such that any generator χ_{K} of the group of Dirichlet characters associated with K is factored as $\chi_{\mathrm{K}} = \chi_p \chi'$, where χ_p has order $2N$ and conductor f_p, where $f_p = 2^{n+2}$ if $p = 2$ and $f_p = p$ if p is odd, and χ' is quadratic or trivial of conductor f' prime to

p. Now, the ideal class group of K in $\mathcal{F}_p$ has exponent less than or equal to 2 if and only if $h_k = 1$ and $h_K^- = 2^{t-1}$. Here t is the number of prime ideals of the maximal real subfield k of K which ramify in the quadratic extension K/k. Now, we show that Theorem 2.1 provides useful restrictive necessary conditions for a number field K in any $\mathcal{F}_p$ to have its ideal class group of exponent less than or equal to 2.

First, assume that p is odd. Then, $2N$ must divide $p-1$, $f_K = f_p f'$ and $f_k = f_p = p$. If χ is a non-trivial Dirichlet character modulo p of order $M \geq 2$ (dividing $p-1$) and $\epsilon \in \{-1,+1\}$, then $\chi(q) = \epsilon$ if and only if $q^{(p-1)/M} \equiv \epsilon \pmod p$. On the other hand, a prime q (prime to f_K) splits in K if and only if $\chi_K(q) = \chi_p(q)\chi'(q) = 1$, hence if and only if $\chi_p(q) = \chi'(q)$. Therefore, q splits in K if and only if $q^{(p-1)/(2N)} \equiv \chi'(q) \pmod p$. Hence, Theorem 2.1 provides us with the following restrictive necessary condition.

Theorem 3.1. *Let p be an odd prime. If K in $\mathcal{F}_p$ of degree $2N$ dividing $p-1$ has its ideal class group of exponent less than or equal to 2, then the following condition is satisfied.*

$$\text{(3.3)} \qquad \begin{array}{l} \textit{For any prime } q \textit{ (prime to } f_K = pf') \textit{ with } q^2 < p(f'/4)^N, \\ \qquad \textit{we have } q^{(p-1)/(2N)} \not\equiv \chi'(q) \pmod p. \end{array}$$

Let p be a given odd prime. Theorem 3.1 provides an efficient method to get a short list of fields which contains all the fields in $\mathcal{F}_p$ which have ideal class groups of exponents less than or equal to 2 and conductors f_K less than a prescribed upper bound. For example, if $p = 17$, in which case we must have $N \in \{2,4,8\}$, there are 26 square-free f' prime to 17 and less than 10^5 such that the necessary condition (3.3) of Theorem 3.1 is satisfied. In Table 2, we give the values of t and h_K^- of these 26 fields in $\mathcal{F}_{17}$. Note that 7 out of these 26 fields are such that $h_K^- = 2^{t-1}$. Moreover, one can check that the maximal totally real subfields of these 7 imaginary cyclic number fields have class number one. Hence, these 7 number fields K have ideal class groups of exponents less than or equal to 2. Now, by using [Lou 7], one can prove that if a number field K in $\mathcal{F}_{17}$ has its ideal class group of exponent less than or equal to 2, then $f' \leq 10^5$. Hence, we get that there are 7 number fields in $\mathcal{F}_{17}$ which have ideal class groups of exponents less than or equal to 2. In [Lou 7] we had not come up with Theorem 2.1. Hence, we had to compute the relative class numbers of all the possible fields with $f' \leq 10^5$ in order to check whether h_K^- is equal to 2^{t-1}. Thus, Theorem 3.1 considerably reduces the amount of relative class number computation. We used the formulas (see [Lou 7])

$$t - 1 = \sum_{q \mid f'} \frac{N}{\lambda(p,q,N)},$$

where

$$\lambda(p,q,N) = \operatorname{Min}\left\{i \geq 1;\ i \text{ a 2-power and } q^{i(p-1)/N} \equiv 1 \pmod p\right\},$$

and

$$h_K^- = \frac{w_K}{2^N} \prod_{k=0}^{(N/2)-1} \left| \frac{1}{2 - \bar{\chi}(2^{2k+1})} \sum_{0<a<f_K/2} \chi_p(a^{2k+1})\chi'(a) \right|^2 .$$

Here, w_K is the number of roots of unity in K.

Table 2

$N = 2$

f' =	3	4	7	8	11	15	19	20	24	31	39	47	59	71	83	84
t =	2	3	2	3	2	3	3	4	4	2	4	3	3	2	3	5
h_K^- =	10	4	2	4	34	4	52	16	16	10	16	16	116	18	212	64

$N = 4$

f' =	3	4	7	8	11	15	19
t =	2	3	2	3	2	3	3
h_K^- =	2	4	18	36	34	68	100

$N = 8$

f' =	1	5	8
t =	1	2	3
h_K^- =	1	34	388

Second, assume that $p = 2$. Then f' is odd and square-free, which implies that χ' is computed by using the Jacobi's symbol: $\chi'(q) = (q/f')_{\text{leg}}$. Then, an odd prime q splits in k/Q if and only if $\chi_K^2(q) = \chi_2^2(q) = 1$, hence if and only if $q \equiv \pm 1 \,(\mathrm{mod}\, 4N)$. Hence, Theorem 2.1 provides us with the following restrictive necessary condition.

Theorem 3.2. *If* K *in* $\mathcal{F}_2$ *of degree* $2N$ *has its ideal class group of exponent less than or equal to* 2*, then the following condition is satisfied.*

For any prime q *(prime to* $f_K = pf'$*) with* $q^2 < 2f'^N$*, we have*

$$(f'/q)_{\text{leg}} = \begin{cases} -1 & if \quad q \equiv 1, -1+4N \,(\mathrm{mod}\, 8N)\,, \\ +1 & if \quad q \equiv -1, 1+4N \,(\mathrm{mod}\, 8N)\,. \end{cases} \tag{3.4}$$

Proof. First, assume $f' \equiv 3 \,(\mathrm{mod}\, 4)$. Then χ' is odd and χ_2 even. Note that $\chi'(q) = (-f'/q)_{\text{leg}}$ and $\chi_2(q) = 1$ if and only if $q \equiv \pm 1 \,(\mathrm{mod}\, 8N)$. We then have:

(a) If $q \equiv 1 \,(\mathrm{mod}\, 8N)$, then
$$-1 = \chi_K(q) = \chi_2(q)\chi'(q) = \chi'(q) = (-f'/q)_{\text{leg}} = (f'/q)_{\text{leg}}\,.$$

(b) If $q \equiv 1 + 4N \,(\mathrm{mod}\, 8N)$, then
$$-1 = \chi_K(q) = \chi_2(q)\chi'(q) = -\chi'(q) = -(-f'/q)_{\text{leg}} = -(f'/q)_{\text{leg}}\,.$$

(c) If $q \equiv -1 \,(\mathrm{mod}\, 8N)$, then
$$-1 = \chi_K(q) = \chi_2(q)\chi'(q) = \chi'(q) = (-f'/q)_{\text{leg}} = -(f'/q)_{\text{leg}}\,.$$

(d) Finally, if $q \equiv -1 + 4N \,(\mathrm{mod}\, 8N)$, then
$$-1 = \chi_K(q) = \chi_2(q)\chi'(q) = \chi'(q) = -(-f'/q)_{\text{leg}} = (f'/q)_{\text{leg}}\,.$$

Second, assume $f' \equiv 1 \pmod 4$. Then χ' is even and χ_2 odd. Note that $\chi'(q) = (f'/q)_{\mathrm{leg}}$ and $\chi_2(q) = 1$ if and only if $q \equiv 1, -1+4N \pmod{8N}$. We then have:

(e) If $q \equiv 1 \pmod{8N}$, then
$$-1 = \chi_{\mathrm{K}}(q) = \chi_2(q)\chi'(q) = \chi'(q) = (f'/q)_{\mathrm{leg}}.$$

(f) If $q \equiv 1 + 4N \pmod{8N}$, then
$$-1 = \chi_{\mathrm{K}}(q) = \chi_2(q)\chi'(q) = -\chi'(q) = -(f'/q)_{\mathrm{leg}}.$$

(g) If $q \equiv -1 \pmod{8N}$, then
$$-1 = \chi_{\mathrm{K}}(q) = \chi_2(q)\chi'(q) = -\chi'(q) = -(f'/q)_{\mathrm{leg}}.$$

(h) Finally, if $q \equiv -1 + 4N \pmod{8N}$, then
$$-1 = \chi_{\mathrm{K}}(q) = \chi_2(q)\chi'(q) = \chi'(q) = (f'/q)_{\mathrm{leg}}.$$
□

In [Lou 7] we proved that if K in $\mathcal{F}_2$ of degree $2N \geq 4$ has its ideal class group of exponent less than or equal to 2, then $2 \leq N \leq 16$ and $f' \leq 4 \cdot 10^4$. Then, we had to compute the relative class numbers of all the possible fields to check whether h_{K}^- is equal to 2^{t-1}. Now, Theorem 3.2 enables us to drastically reduce the amount of required relative class number computation. Indeed, we easily find that there are exactly 11 pairs (N, f') with $2 \leq N \leq 16$ and $f' \leq 4 \cdot 10^4$ which satisfy the necessary conditions (3.4) of Theorem 3.2. In Table 3 below we give the values of t and h_{K}^- of these 11 fields in $\mathcal{F}_2$. Note that 5 out of these 11 fields are such that $h_{\mathrm{K}}^- = 2^{t-1}$.

Table 3

$N = 2$

$f' =$	1	3	5	7	17	61
$t =$	1	2	2	3	3	2
$h_{\mathrm{K}}^- =$	1	2	2	4	8	26

$N = 4$

$f' =$	1	3
$t =$	1	2
$h_{\mathrm{K}}^- =$	1	18

$N = 8$

$f' =$	1	3
$t =$	1	2
$h_{\mathrm{K}}^- =$	17	802

$N = 16$

$f' =$	1
$t =$	1
$h_{\mathrm{K}}^- =$	21121

Moreover, one can check that the maximal totally real subfields of these 5 imaginary cyclic number fields have class number one. Hence, these 5 number fields K have ideal class groups of exponents less than or equal to 2. Hence, we get that there are 5 number fields in $\mathcal{F}_2$ which have ideals class groups of exponents less than or equal to 2. We used the formulas (see [Lou 7])

$$t - 1 = \sum_{q \mid f'} \frac{N}{\lambda(q, N)},$$

where

$$\lambda(q, N) = \mathrm{Min}\left\{i \geq 1;\ i \text{ a } 2-\text{power and } q^i \equiv \pm 1 \pmod{4N}\right\},$$

and

$$h_{\mathrm{K}}^{-} = \frac{1}{2^{N-1}} \prod_{k=0}^{(N/2)-1} \left| \sum_{\substack{1\leq a\leq 2Nf', \\ a \text{ odd}}} \chi_2(a^{2k+1})(a/f')_{\mathrm{leg}} \right|^2 .$$

4. Necessary conditions for some non-CM-fields

Let k be a given totally real number field with class number one, and let $(\mathrm{K}_m)_{m\in I}$ be a sequence of CM-fields with the same maximal totally real subfield k. Let q_m be the least prime which splits completely in K_m and such that at least one of the prime ideals of K_m lying above q_m is principal. Then Theorem 2.1 implies that q_m goes to infinity as d_{K_m} goes to infinity. Now, if we do not assume anymore that the K_m's are CM-fields, then we cannot expect to have a result similar to that of Theorem 2.1. Indeed, there exists a sequence $(\mathrm{K}_m)_{m\in I}$ of real quadratic number fields such that the prime $(2) = \mathcal{Q}_1\mathcal{Q}_2$ splits in each K_m with both $\mathcal{Q}_1$ and $\mathcal{Q}_2$ principal, whereas d_{K_m} goes to infinity. For example, we can take $\mathrm{K}_m = \mathrm{Q}(\sqrt{d_m})$ with

$$I = \{m\,;\ m \geq 1 \text{ and } d_m = m^2+8 \equiv 1 \pmod 8 \text{ is square-free}\}$$

as such K_m's. To get round this difficulty, we would like to know the smallest norms of the principal ideals of K_m. Hence, we would get that if K_m has class number one, then any prime p which splits completely in K_m and does not belong to a finite set known beforehand must be estimated from below by an increasing function of d_{K_m}. For example, set $\mathrm{K}_m = \mathrm{Q}(\sqrt{d_m})$ with

$$I = \{m\,;\ m \geq 1 \text{ and } d_m = m^2+2 \equiv 2,3 \pmod 4 \text{ is square-free}\}.$$

By using the continued fraction expansion of $\sqrt{d_m}$, one can prove that if the prime ideals of K_m which lie above a non inert prime p are principal, then $p = 2$ or $p \geq \sqrt{d_m} = \frac{1}{2}\sqrt{d_{\mathrm{K}_m}}$. For general number fields, instead of using continued fractions, we would use any theory of reduced ideals. See [Wil 1, Theorem 5.3, Theorem 9.1] and [Wil 2, Theorem 2.2] for such a theory and an explanation of how it provides all the principal ideals with small norms. However, as can be seen in [Wil 2], in non-quadratic cases this actual execution involves a tremendous amount of work. Therefore, we will content ourselves with an example of quartic fields where we can use a similar trick to the one used in [ACH] in a particular real quadratic case.

From now on we let $m \in \mathrm{Z}[i]$ and $\eta \in \{\pm 1, \pm i\}$ be such that $d_m = m^2 + 4\eta$ is square-free in $\mathrm{Z}[i]$ (which implies $m = a + ib$ with a and b rational integers of opposite parities) and neither real nor pure imaginary. We set $\mathrm{K}_m = \mathrm{Q}(i, \sqrt{d_m})$. Then, K_m is a non-normal quartic number field. Since $(m + \sqrt{d_m})/2$ is integral over $\mathrm{Z}[i]$ and since its relative discriminant which is equal to d_m is square-free in $\mathrm{Z}[i]$, then $\mathrm{R}_m = \mathrm{Z}\left[i, \frac{m+\sqrt{d_m}}{2}\right]$ is the ring of algebraic integers of the quartic number field K_m.

Lemma 4.1. *Assume $|d_m| \geq 156$, and let* I *be a prime ideal of* K_m *which is not inert in* $K_m/Q(i)$. *If its relative norm* $(\pi) = N_{K_m/Q(i)}(I)$ *satisfies* $|\pi| \leq \frac{1}{6}\sqrt{|d_m|}$ *then* I *is not principal.*

Proof. We note that $\epsilon_\pm = \left(m \pm \sqrt{d_m}\right)/2$ are units of R_m such that $|\epsilon_+\epsilon_-| = 1$. We set $\epsilon_m = \epsilon_+$ if $|\epsilon_+| > 1$, and $\epsilon_m = \epsilon_-$ if $|\epsilon_+| < 1$. Thus, ϵ_m is a unit in R_m such that $|\epsilon_m| > 1$. Suppose, contrary to our claim, that $I = (\alpha)$ is principal (hence, we have $\alpha \in R_m \setminus Z[i]$). Since for any $n \in Z$ we have $(\alpha) = (\epsilon_m^n \alpha)$, we may assume that $1 \leq |\alpha| < |\epsilon_m|$. Let $\alpha' = \left(x - y\sqrt{d_m}\right)/2$ be the conjugate of $\alpha = \left(x + y\sqrt{d_m}\right)/2$ (with x and y in $Z[i]$). Since $|\alpha\alpha'| = \left|N_{K_m/Q(i)}(\alpha)\right| = |\pi|$, we get

$$\begin{aligned} |y|\sqrt{|d_m|} &= |\alpha - \alpha'| \\ &\leq |\alpha| + \frac{|\pi|}{|\alpha|} < |\epsilon_m| + |\pi| \\ &\leq |\epsilon_m'| + |\epsilon_m - \epsilon_m'| + \frac{1}{6}\sqrt{|d_m|} \leq +1 + \frac{7}{6}\sqrt{|d_m|}\,. \end{aligned}$$

We thus get $0 < |y| < \frac{1}{\sqrt{156}} + \frac{7}{6} < \sqrt{2}$, which implies $|y| = 1$ and $y \in \{\pm 1, \pm i\}$. We may clearly assume that $y = 1$. We thus have $|x^2 - m^2 - 4\eta| = 4|\pi|$. Hence, $x \neq \pm m$, which implies $|x \pm m| \geq 1$. Since

$$|x - m|^2 + |x + m|^2 = 2\left(|x|^2 + |m|^2\right) \geq 2\,|m|^2\,,$$

then $|x - m| \geq |m|$ or $|x + m| \geq |m|$. We thus get

$$4|\pi| \geq |x - m|\,|x + m| - 4 \geq |m| - 4 \geq \sqrt{|d_m| - 4} - 4 > \frac{2}{3}\sqrt{|d_m|}$$

(if $|d_m| \geq 156$). This contradicts our hypothesis, and the Lemma follows. □

Theorem 4.2. *If $h_{K_m} = 1$, then the following conditions are satisfied*

(4.1) *For any prime $q \equiv 3 \pmod 4$ with $q^2 \leq \frac{1}{36}|d_m|$, we have $\left(|d_m|^2/q\right)_{\text{leg}} = -1$;*

(4.2) *For any prime $p \equiv 1 \pmod 4$ with $p \leq \frac{1}{36}|d_m|$, we have $\left(|d_m|^2/p\right)_{\text{leg}} = 1$*

and

$$((\alpha x + \beta y)/p)_{\text{leg}} = ((\alpha x - \beta y)/p)_{\text{leg}} = -1,$$

where $p = x^2 + y^2$ with $x, y \in Z$, y even and $d_m = \alpha + i\beta$ where $\alpha, \beta \in Z[i]$.

Proof. Since both conditions (4.1) and (4.2) are empty when $|d_m| < 156$, we may assume that $|d_m| \geq 156$. If a prime q is congruent to 3 modulo 4, it is inert in $Q(i)$. If $(|d_m|^2/q)_{\text{leg}} \neq -1$, then q is not inert in $K_m/Q(i)$ (see [Lou 4, Theorem 5(a)]). Hence, there exists a non-inert prime ideal $\mathcal{Q}$ of R_m such that $N_{K_m/Q(i)}(\mathcal{Q}) = (q)$. According to Lemma 4.1, if $h_{K_m} = 1$ then $|\pi| = q > \frac{1}{6}\sqrt{|d_m|}$. If a prime p is congruent to 1 modulo 4, it splits as $(p) = (\pi)(\bar{\pi})$ in $Q(i)/Q$ with $\pi = x + iy$ and x and y as in the Theorem. If $(|d_m|^2/p)_{\text{leg}} \neq 1$, then $\left((\alpha x + \beta y)/p\right)_{\text{leg}} \neq -1$ or $\left((\alpha x - \beta y)/p\right)_{\text{leg}} \neq -1$, and π or $\bar{\pi}$, respectively, is not inert in $\mathrm{K}_m/\mathrm{Q}(i)$ (see [Lou 4, Theorem 5(b)]). Hence, there exists a non-inert prime ideal $\mathcal{P}$ of R_m such that $N_{\mathrm{K}_m/\mathrm{Q}(i)}(\mathcal{P}) = (\pi)$ or $(\bar{\pi})$. According to Lemma 4.1, if $h_{\mathrm{K}_m} = 1$ then $|\pi| = |\bar{\pi}| = \sqrt{p} > \frac{1}{6}\sqrt{|d_m|}$. □

Remark 4.3. There is no use considering the splitting in $\mathrm{K}_m/\mathrm{Q}(i)$ of the prime ideal $(1+i)$ of $\mathrm{Q}(i)$ lying above 2. Indeed, this prime ideal is inert in $\mathrm{K}_m/\mathrm{Q}(i)$ (see [Lou 8, page 135]).

Corollary 4.4. *Let $m \in \mathrm{Z}[i]$ and $\eta \in \{\pm 1, \pm i\}$ be such that $d_m = m^2 + 4\eta$ is square-free in $\mathrm{Z}[i]$ (which implies $m = a + ib$ with a and b rational integers of opposite parities) and neither real nor pure imaginary. Then, the class number of the non normal quartic number field $\mathrm{K}_m = \mathrm{Q}(i, \sqrt{d_m})$ is equal to one if and only if K_m is isomorphic to one of the 14 K_m's which appear in the following Table 4.*

Table 4

$m =$	1	$2+i$	$2+i$	$-3+2i$	3	$2+3i$	$1+4i$
$\eta =$	i	1	i	i	i	1	1
$d_m =$	$1+4i$	$7+4i$	$3+8i$	$5-8i$	$9+4i$	$-1+12i$	$-11+8i$
$\lvert d_m\rvert^2 =$	17	65	73	89	97	145	185
$m =$	$-4+i$	$3+2i$	$-4+3i$	5	$2+5i$	$6+i$	$5+4i$
$\eta =$	i	i	i	i	1	i	1
$d_m =$	$15-4i$	$5+16i$	$7-20i$	$25+4i$	$-17+20i$	$35+16i$	$13+40i$
$\lvert d_m\rvert^2 =$	241	281	449	641	689	1481	1769

Proof. Since $\mathrm{Q}(i, \sqrt{d_m}) = \mathrm{Q}(i, \sqrt{-d_m})$ is isomorphic to $\mathrm{Q}(i, \sqrt{\bar{d}_m}) = \mathrm{Q}(i, \sqrt{-\bar{d}_m})$, we may assume that $d_m = m^2 + 4$ with $m = a + ib$ such that $a \geq 1$ and $b \geq 1$, or $d_m = m^2 + 4i$ with $m = a + ib$ such that $|a| > b \geq 0$. We give a proof only for the case $d_m = m^2 + 4i$. Note that the 2-rank of the ideal class group of K_m is equal to $t - 1$ (in the case $d_m = m^2 + 4$, use [Lou 1, Corollaire 10] to compute the 2-rank of the ideal class group of K_m), where t is the number of irreducible factors of d_m in $\mathrm{Z}[i]$ (note that $N_{\mathrm{K}_m/\mathrm{Q}(i)}((m + \sqrt{d_m})/2) = -i$ and use [Lou 1, Théorème 3]). Hence, h_{K_m} is odd if and only if $|d_m|^2$ is prime. According to [Lou 8, Theorem 2], if $h_{\mathrm{K}_m} = 1$ then $|d_m| \leq 10^5$. Now, Table 5 provides us with the class numbers of the K_m's in the 51 occurences of the d_m's such that $d_m = m^2 + 4i$ and $|d_m|^2 \leq 10^{10}$ is prime (with a and b as above) and such that the necessary conditions for class number one given in Theorem 4.2 are satisfied. Since $\epsilon_{\mathrm{K}_m} = (m + \sqrt{d_m})/2$ is the fundamental unit of K_m (see [Sch]), then the class number h_{K_m} of K_m is easily computed by using the method developed in [Lou 4].

Table 5

m	d_m	$\|d_m\|^2$	h_{K_m}	m	dm	$\|d_m\|^2$	h_{K_m}
1	$1+4i$	17	1	$-11+2i$	$117-40i$	15289	3
$2+i$	$3+8i$	73	1	$11+4i$	$105+92i$	19489	11
$-3+2i$	$5-8i$	89	1	$-9+8i$	$17-140i$	19889	3
3	$9+4i$	97	1	$-12+i$	$143-20i$	20849	5
$-4+i$	$15-4i$	241	1	$9+8i$	$17+148i$	22193	5
$3+2i$	$5+16i$	281	1	$-11+6i$	$85-128i$	23609	11
$-4+3i$	$7-20i$	449	1	$12+3i$	$135+76i$	24001	5
5	$25+4i$	641	1	$-12+5i$	$119-116i$	27617	5
$-6+i$	$35-8i$	1289	3	$12+5i$	$119+124i$	29537	5
$6+i$	$35+16i$	1481	1	$-10+9i$	$19-176i$	31337	7
$-6+3i$	$27-32i$	1753	3	$-13+4i$	$153-100i$	33409	7
$5+4i$	$9+44i$	2017	3	$12+9i$	$63+220i$	52369	9
7	$49+4i$	2417	3	$14+7i$	$147+20i$	61609	7
$7+2i$	$45+32i$	3049	5	$-16+7i$	$207-220i$	91249	9
$-6+5i$	$11-56i$	3257	3	$-14+11i$	$75-304i$	98041	11
$-7+4i$	$33-52i$	3793	3	$-17+6i$	$253-200i$	104009	7
$6+5i$	$11+64i$	4217	3	$18+i$	$323+40i$	105929	7
$-7+6i$	$13-80i$	6569	3	$15+10i$	$125+304i$	108041	7
9	$81+4i$	6577	5	$18+7i$	$275+256i$	141161	7
$-8+5i$	$39-76i$	7297	5	$-19+6i$	$325-224i$	155801	7
$9+2i$	$77+40i$	7529	3	$17+12i$	$145-404i$	184241	9
$-9+4i$	$65-68i$	8849	5	$-21+2i$	$437-80i$	197369	11
$10+3i$	$91+64i$	12377	3	$18+11i$	$203+400i$	201209	9
$-9+6i$	$45-104i$	12841	3	$-21+4i$	$425-164i$	207521	9
$8+7i$	$15+116i$	13681	3	$22+9i$	$403+400i$	322409	9
11	$121+4i$	14657	5				

According to Table 5, Corollary 4.4 is proved. □

5. Conclusion

Theorem 2.1 would also have drastically simplified the determination in [HHRW] of the imaginary cyclic quartic fields with class number 2.

In [Lou 9] we proved that there are only finitely many cubic number fields K with negative discriminants d_K and given class number h such that their rings of algebraic integers are equal to $Z[\epsilon]$ for some unit ϵ of K. We also explained how to get the explicit upper bound $|d_K| \leq c h^2 \log^4(1+h)$ (for some effective large constant c) on the absolute values of these discriminants of the numbers fields. We could not determine all these fields with class number one because we did not find a restrictive necessary condition which would have enabled us to sieve efficiently these fields up to that large previous upper bound on $|d_K|$. We raise the problem: Prove a result similar to that of Lemma 4.1 which would imply that if K ranges over the cubic number fields with negative discriminants such that their rings of algebraic integers are equal to $Z[\epsilon]$ for some unit ϵ of K, then the least norm of the principal prime ideals of K tends to infinity with $|d_K|$?

In [Lou 10] we make use of a result similar to that of Lemma 4.1 to get lower bounds on the exponents of the ideals class groups of pure cubic number fields.

References

[ACH] Ankeny, N. C., Chowla, S., and Hasse, H.: On the Class Number of the Real Subfield of a Cyclotomic Field, J. reine angew. Math. **217** (1965), 217-220

[HHRW] Hardy, K., Hudson, R. H., Richman, D., and S. Williams, K.: Determination of all Imaginary Cyclic Quartic Fields with Class Number 2, Trans. Amer. Math. Soc. **311** (1989), 1-55

[Lou 1] Louboutin, S.: Norme Relative de l'Unité Fondamentale et 2-Rang du Groupe des Classes d'Idéaux de Certains Corps Biquadratiques, Acta Arith. **58** (1991), 273-288

[Lou 2] Louboutin, S.: Minoration au Point 1 des Fonctions L et Détermination des Corps Sextiques Abéliens Totalement Imaginaires Principaux, Acta Arith. **62** (1992), 109-124

[Lou 3] Louboutin, S.: Zéros Réels des Fonctions Zêta et Minorations de Nombres de Classes. Application à la Majoration des Discriminants de Certains Types de Corps de Nombres, Séminaire de Théorie des Nombres, Paris 1991-92, 135-152

[Lou 4] Louboutin, S.: L-Functions and Class Numbers of Imaginary Quadratic Fields and of Quadratic Extensions of an Imaginary Quadratic Field, Math. Comp. **59** (1992), 213-230

[Lou 5] Louboutin, S.: Lower Bounds for Relative Class Numbers of CM-Fields, Proc. Amer. Math. Soc. **120** (1994), 425-434

[Lou 6] Louboutin, S.: On the Class Number One Problem for Non-Normal Quartic CM-Fields, Tôhoku Math. J. **46** (1994), 1-12

[Lou 7] Louboutin, S.: Determination of all Nonquadratic Imaginary Cyclic Number Fields of 2-Power Degrees with Ideal Class Groups of Exponents ≤ 2, Math. Comp. **64** (1995), 323-340

[Lou 8] Louboutin, S.: The Exponent 2 Class Group Problem for non Galois over Q Quartic Fields, J. Number Theory **49** (1994), 133-141

[Lou 9] Louboutin, S.: Class-Number Problems for Cubic Number Fields, Nagoya Math. J. **138** (1995), 199-208

[Lou 10] Louboutin, S.: Une Remarque sur l'Exposant du Groupe des Classes d'Idéaux des Corps Cubiques, C. R. Acad. Sci. Paris **320** (1995), Série I, 1161-1163

[LMW] LOUBOUTIN, S., MOLLIN, R. A. and WILLIAMS, H. C.: Class Groups of Exponent Two in Real Quadratic Fields, Advances in Number Theory, Proc. Third Conf. Canad. Number Theory Assoc., August 18–24, 1991, Kingston Clarendon Press. Oxford (1993), pp 499–513

[Lou-Oka] LOUBOUTIN, S., and OKAZAKI, R.: Determination of All Non-Normal Quartic CM-Fields and of All Non-Abelian Normal Octic CM-Fields with Class Number One, Acta Arith. **67** (1994), 47–62

[Sch] SCHARLAU, R.: The Fundamental Unit in Quadratic Extensions of Imaginary Quadratic Fields, Arch. Math. (Basel) **34** no. 6 (1980), 534–537

[Set] SETZER, B.: The Determination of All Imaginary, Quartic Abelian Number Fields with Class-Number 1, Math. Comp. **35** (1980), 1383–1386

[Uch 1] UCHIDA, K.: Class Numbers of Imaginary Abelian Number Fields I, Tôhoku Math. J. **23** (1971), 97–104

[Uch 2] UCHIDA, K.: Imaginary Abelian Number Fields with Class Number One, Tôhoku Math. J. **24** (1972), 487–499

[Wil 1] WILLIAMS, H. C.: Continued Fractions and Number-Theoretic Computations, Rocky Mountain J. Math. **15** (1985), 621–655

[Wil 2] WILLIAMS, H. C.: The Period Lenght of Voronoi's Algorithm for Certain Cubic Orders, Publ. Math. **37** (1990), 245–265

[Yam] YAMAMURA, K.: The Determination of the Imaginary Abelian Number Fields with Class Number One, Math. Comp. **62** (1994), 899–921

Université de Caen,
Département de Mathématiques
Esplanade de la Paix
14032 Caen Cedex, France
email:
louboutí@math.unicaen.fr