Journal of Number Theory 132 (2012) 1793–1806

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The class number one problem for some non-normal CM-fields of degree $2p$ ☆

Jeoung-Hwan Ahn [a], Gérard Boutteaux [b], Soun-Hi Kwon [c], Stéphane Louboutin [d,*]

[a] Department of Mathematics, Korea University, 136-701 Seoul, Republic of Korea
[b] Département GEA, IUT Bobigny, Université Paris 13, 1, rue de Chablis, 93000 Bobigny, France
[c] Department of Mathematics Education, Korea University, 136-701 Seoul, Republic of Korea
[d] Institut de Mathématiques de Luminy, UMR 6206, 163, avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France

ARTICLE INFO

Article history:
Received 12 January 2012
Accepted 23 February 2012
Available online 21 April 2012
Communicated by Michael E. Pohst

MSC:
11R29
11M20

Keywords:
CM-field
Class number
Dedekind zeta function

ABSTRACT

To date, the class number one problem for non-normal CM-fields is solved only for quartic CM-fields. Here, we solve it for a family of non-normal CM-fields of degree $2p$, $p \geqslant 3$ and odd prime. We determine all the non-isomorphic non-normal CM-fields of degree $2p$, containing a real cyclic field of degree p, and of class number one. Here, $p \geqslant 3$ ranges over the odd primes. There are 24 such non-isomorphic number fields: 19 of them are of degree 6 and 5 of them are of degree 10. We also construct 19 non-isomorphic non-normal CM-fields of degree 12 and of class number one, and 10 non-isomorphic non-normal CM-fields of degree 20 and of class number one.

1. Introduction

It is conjectured that there are only finitely many non-isomorphic CM-fields of class number equal to one (see [Bes] and the bibliography therein).

The class number one problem for the *abelian* CM-fields was completed in [Yam]. The class number one problem for the *non-abelian normal* CM-fields is almost completed (see [LK,PK] and the bibliography therein).

☆ J.-H. Ahn and S.-H. Kwon were supported by the Grant KRF-2010-0009540.

* Corresponding author.
E-mail addresses: jh-ahn@korea.ac.kr (J.-H. Ahn), gerard.boutteaux@univ-paris13.fr (G. Boutteaux), sounhikwon@korea.ac.kr (S.-H. Kwon), stephane.louboutin@univ-amu.fr (S. Louboutin).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.02.020

The class number one problem for the *non-normal* CM-fields is solved only for quartic CM-fields (see [LO94, Theorem 9]), and almost solved for sextic CM-fields (see [BL1,BL2] and [Lou08]).

Here, we solve the class number one problem in a rather general non-normal situation: for the non-normal CM-fields K of degree $2p$, $p \geqslant 3$ any odd prime, whose maximal totally real subfields are cyclic of degree p. The case $p = 3$ was considered in [BL1].

Solving the class number one problem for this general family of non-normal CM-fields of not fixed degree is to be compared with what was done for normal CM-fields: we first solved in [LO94] the class number one problem for the octic dihedral CM-fields. Then, in [LO98], we solved the class number one problem for the general dihedral CM-fields of any 2-power degree $2n = 2^m \geqslant 8$.

The main steps are

(i) to characterize such CM-fields K of odd class number (see Theorem 4),

(ii) to obtain lower bounds on their relative class numbers h_K^- to deduce the bound $p \leqslant 23$ when $h_K = 1$ (see Corollary 8),

(iii) to further improve this upper bound down to $p \leqslant 13$ by using cyclotomic units (see Corollary 10),

(iv) to further improve this upper bound down to $p \leqslant 11$ (see Corollary 11),

(v) to build a list of 12221 possible K's (see the fifth column of Table 1 below),

(vi) to use a necessary condition for the class number of K to be one to further reduce this list down to a list of 402 possible K's (see the sixth column of Table 1 below),

(vii) and finally to compute the relative class numbers of these 402 remaining CM-fields to solve our problem.

We point out that up to point (iii) we do not use any software dedicated to number theory. However, from point (iv) we need any software dedicated to number theory that can compute a system of fundamental units of real cyclic fields of prime degree $p \leqslant 13$.

Throughout this paper, we adopt the following notation.

If k is a number field of degree $n \geqslant 1$, then d_k, $\rho_k = d_k^{1/n}$, A_k, h_k and $\zeta_k(s)$ are the absolute value of the discriminant of k, its root discriminant, its ring of algebraic integers, its class number and its Dedekind zeta function.

If k is abelian, then f_k denotes its conductor. For K/k an abelian extension, $\mathcal{F}_{K/k}$ is the finite part of its conductor.

If K is a CM-field with maximal totally real subfield $K^+ = k$, $Q_K \in \{1, 2\}$ is the Hasse unit index of K, the class number h_k of k divides the class number h_K of K, and the *relative class number* $h_K^- = h_K/h_k$ of K is a positive integer that divides h_K.

2. The simplest non-normal $2p$-CM-fields

The aim of this section is to characterize in Theorem 4 the non-normal CM-fields K of degree $2p \geqslant 6$ of odd class number whose maximal totally real subfields $K^+ = k$ are cyclic of degree $p \geqslant 3$. We point out that R. Okazaki proved (unpublished) that the class number h_K of a CM-field K of degree $2n \geqslant 6$, $n \geqslant 3$ odd, is odd if and only if its relative class number h_K^- is odd.

Proposition 1. *Let K be a CM-field of degree $2n$, $n > 1$ odd. Let k denote its maximal totally real subfield (of degree n). At least one prime ideal of k is ramified in the quadratic extension K/k. Therefore, $d_K \geqslant 3d_k^2$ and the narrow class number h_k^+ of k divides the class number h_K of K. Consequently, h_K is odd if and only if the narrow class number h_k^+ of k is odd and a unique prime ideal $\mathcal{Q}$ of k is ramified in the quadratic extension K/k.*

Proof. Let χ be the quadratic character associated with the quadratic extension K/k. According to class field theory (e.g., see [Neu, Chapter VII, §6]), there exists a primitive quadratic character χ_0 on the multiplicative group $(A_k/\mathcal{F}_{K/k})^*$ such that $\chi((\alpha)) = \nu(\alpha)\chi_0(\alpha)$ for $\alpha \in A_k$, where $\nu(\alpha) \in \{\pm 1\}$ is the sign of the norm $N_{k/\mathbf{Q}}(\alpha)$ of $\alpha \neq 0$. In particular, if K/k were unramified at all the finite places of k, then we would obtain $1 = \chi((-1)) = \nu(-1) = (-1)^n$ and n would be even, a contradiction. Conversely, assume that h_k^+ is odd. Since K is a totally imaginary number field which is a quadratic extension of the totally real number field k of odd narrow class number, then, the 2-rank of the ideal class group of K is equal to $t-1$, where t denotes the number of prime ideals of k which are ramified in the quadratic extension K/k (see [CH, Lemma 13.7]). Hence h_K is odd if and only if exactly one prime ideal $\mathcal{Q}$ of k is ramified in the quadratic extension K/k. $\square$

Remark 2. Here is another proof of the first assertion which does not use class field theory (from the referee). If no ideal of k were ramified in K/k, there would exist a totally negative element $\alpha \in k$ with $K = k(\sqrt{\alpha})$, with (α) coprime with (2), with $(\alpha) = \mathcal{A}^2$ a square of a fractional ideal of k and with $\alpha \equiv 1 \pmod{4}$ (e.g., see [He, Theorem 120]). Taking norms down to $\mathbf{Q}$, we would obtain $N(\alpha) = -N(\mathcal{A})^2 \equiv 1 \pmod 4$, a contradiction.

Proposition 3. *Let K be a non-normal CM-field of degree $2p$ whose maximal totally real subfield k is cyclic of prime degree $p \geqslant 3$ and conductor f_k. Assume that h_K is odd, stick to the notation introduced in Proposition* 1 *and let $q \geqslant 2$ denote the rational prime such that $\mathcal{Q} \cap \mathbf{Z} = q\mathbf{Z}$. Then,* (i) *The number of complex roots of unity in K is equal to* 2, *$Q_K = 1$ and*

$$h_K^- = \frac{2}{(2\pi)^p}\sqrt{\frac{d_K}{d_k}\frac{\mathrm{Res}_{s=1}(\zeta_K(s))}{\mathrm{Res}_{s=1}(\zeta_k(s))}};$$

(ii) *$K = K_{k,\mathcal{Q}} := k(\sqrt{-\alpha_{\mathcal{Q}}})$ for any totally positive algebraic integer $\alpha_{\mathcal{Q}} \in k$ such that $\mathcal{Q}^{h_k^+} = (\alpha_{\mathcal{Q}})$*; (iii) *$\mathcal{F}_{K/k} = \mathcal{Q}^{e(q)}$ with $e(q) \geqslant 1$ odd*; (iv) *q splits completely in k*; (v) *$e(q) = 1$ and $q \equiv 3 \pmod 4$ if $q > 2$, and $e(q) = 3$ if $q = 2$. Hence, $d_K = d_k^2\tilde{q} = f_k^{2(p-1)}\tilde{q}$, where $\tilde{q} = N_{k/\mathbf{Q}}(\mathcal{F}_{K/k})$ (hence, $\tilde{q} = q$ if $q > 2$ and $\tilde{q} = 2^3$ is $q = 2$), and*

$$h_K^- = \frac{\sqrt{\tilde{q}}}{\pi}\left(\frac{\sqrt{f_k}}{2\pi}\right)^{p-1}\frac{\mathrm{Res}_{s=1}(\zeta_K(s))}{\mathrm{Res}_{s=1}(\zeta_k(s))}. \tag{1}$$

Proof. We set $h = h_k^+$, which is odd (Proposition 1). Let U_k and U_k^+ be the groups of units and totally positive units of the ring of algebraic integers of k, respectively. Since h_k^+ is odd, we have $U_k^+ = U_k^2$.

1. We have $Q_K = (U_K : U_k)$. If we had $Q_K = 2$, then we would have $K = k(\sqrt{-\epsilon})$ for some $\epsilon \in U_k^+ = U_k^2$ and $K = k(\sqrt{-1})$ would be a cyclic number field of degree $2p$. A contradiction. Hence, $Q_K = 1$. As in Section 10 below, one could also use [Lou96, Proposition 6] and the oddness of h_K^- to deduce that $Q_K = 1$. For the formula for h_K^-, see [Was, Chapter 4].
2. Since $\mathcal{Q}$ is the only prime ideal of k which is ramified in the quadratic extension $K/k = k(\sqrt{-\alpha})/k$, where α is some totally positive algebraic integer of k, there exists some integral ideal $\mathcal{I}$ of k such that $(\alpha) = \mathcal{I}^2\mathcal{Q}^l$, with $l \in \{0,1\}$, which implies $\alpha^h = \epsilon\alpha_{\mathcal{I}}^2\alpha_{\mathcal{Q}}^l$ for a totally positive generator $\alpha_{\mathcal{I}}$ of $\mathcal{I}^h$ and some $\epsilon \in U_k^+$. Since $U_k^+ = U_k^2$, we have $\epsilon = \eta^2$ for some $\eta \in U_k$ and $K = k(\sqrt{-\alpha}) = k(\sqrt{-\alpha^h}) = k(\sqrt{-\alpha_{\mathcal{Q}}^l})$. If we had $l = 0$ then $K = k(\sqrt{-1})$ would be a cyclic field of degree $2p$. A contradiction. Therefore, $l = 1$ and $K = k(\sqrt{-\alpha_{\mathcal{Q}}})$.
3. Since $\mathcal{Q}$ is the only prime ideal of k ramified in the quadratic extension K/k, there exists $e \geqslant 1$ such that $\mathcal{F}_{K/k} = \mathcal{Q}^e$. Since $K/k = k(\sqrt{-\alpha_{\mathcal{Q}}})/k$ is quadratic, $(4\alpha_{\mathcal{Q}}) = \mathcal{I}^2\mathcal{F}_{K/k}$ some integral ideal $\mathcal{I}$ of k (see [LYK, Proposition 1]). Hence, $(4\alpha_{\mathcal{Q}}) = (2)^2\mathcal{Q}^h = \mathcal{I}^2\mathcal{F}_{K/k} = \mathcal{I}^2\mathcal{Q}^e$ and e is odd.
4. If $(q) = \mathcal{Q}$ is inert in k, then $K = k(\sqrt{-q^h}) = k(\sqrt{-q})$. If $(q) = \mathcal{Q}^p$ is ramified in k, then $K = k(\sqrt{-\alpha_{\mathcal{Q}}}) = k(\sqrt{-\alpha_{\mathcal{Q}}^p}) = k(\sqrt{-q^h}) = k(\sqrt{-q})$. In both cases, K would be abelian. A contradiction. Hence, q splits in k.
5. According to class field theory, there exists a primitive quadratic characters χ_0 on the multiplicative groups $(A_k/\mathcal{Q}^e)^*$ which satisfy $\chi_0(\epsilon) = \nu(\epsilon)$ for all $\epsilon \in U_k$. In particular, $\chi_0(-1) = \nu(-1) = (-1)^p = -1$ and χ_0 is odd. Since we have a canonical isomorphism from $\mathbf{Z}/q^e\mathbf{Z}$ onto $A_k/\mathcal{Q}^e$, there exists an odd primitive quadratic character on the multiplicative group $(A_k/\mathcal{Q}^e)^*$, e odd, if

and only if there exists an odd primitive quadratic character on the multiplicative group $(\mathbf{Z}/q^e\mathbf{Z})^*$, e odd, hence if and only if [$q=2$ and $e=3$] or [$q\equiv 3 \pmod 4$ and $e=1$], in which cases there exists only one such odd primitive quadratic character modulo $\mathcal{Q}^e$, which we denote by $\chi_{\mathcal{Q}}$. □

Clearly, $\mathcal{Q}$ is ramified in the quadratic extension $K_{k,\mathcal{Q}}/k$. However, $K_{k,\mathcal{Q}}/k$ could also be ramified at primes ideals of k above the rational prime 2. We define *a simplest non-normal 2p-CM-field* as being a $K_{k,\mathcal{Q}}$ such that $\mathcal{Q}$ is the only prime ideal of k ramified in the quadratic extension $K_{k,\mathcal{Q}}/k$. Hence, the simplest non-normal $2p$-CM-fields are the non-normal CM-fields of degree $2p$ of odd class numbers and whose maximal real subfields are cyclic of degree p. We are now in a position to characterize these CM-fields:

Theorem 4. *A number field K is a non-normal CM-field of degree $2p$, of odd class number and of maximal totally real subfield a cyclic field k of prime degree $p\geqslant 3$ if and only if the narrow class number h_k^+ of k is odd and $K=K_{k,\mathcal{Q}}:=k(\sqrt{-\alpha_{\mathcal{Q}}})$, where $\alpha_{\mathcal{Q}}$ is any totally positive algebraic integer of k such that $\mathcal{Q}^{h_k^+}=(\alpha_{\mathcal{Q}})$, with $\mathcal{Q}$ a prime ideal of k above a prime $q\not\equiv 1 \pmod 4$ which splits completely in k and for which the odd primitive quadratic modular character $\chi_{\mathcal{Q}}$ on $(A_k/\mathcal{Q}^{e(q)})^*$ satisfies $\chi_{\mathcal{Q}}(\epsilon)=N_{k/\mathbf{Q}}(\epsilon)$ for all $\epsilon\in U_k$.*

We let $K_{k,q}$ denote anyone of the p pairwise isomorphic simplest non-normal $2p$-CM-fields $K_{k,\mathcal{Q}}$ as $\mathcal{Q}$ ranges over the p prime ideals of k above q.

3. Lower bounds on relative class numbers

Our aim is to obtain in Theorem 7 lower bounds for relative class numbers of non-normal CM-fields of degree $2p\geqslant 6$ of odd class number whose maximal totally real subfields are cyclic of degree $p\geqslant 3$. We deduce in Corollary 8 that if $h_K^-=1$ then $2p\leqslant 46$, a better upper bound than the one obtained in [Bes, Theorem 2] under the assumption of the Generalized Riemann Hypothesis.

Lemma 5. *Let k be a cyclic number field of prime degree $p\geqslant 3$, let K/k be a quadratic extension with K not normal. Then, $\zeta_K(1-1/4c\log d_K)\leqslant 0$, where $c=(3+2\sqrt{2})/2$.*

Proof. This improves upon [Sta, Lemma 10]. Let $\alpha\in k$ be such that $K=k(\sqrt{\alpha})$. Let α' be any conjugate of α in k such that $K'=k(\sqrt{\alpha'})\neq K$ (this is possible for $K/\mathbf{Q}$ is not normal). Set $K''=k(\sqrt{\alpha\alpha'})$ and $L=k(\sqrt{\alpha},\sqrt{\alpha'})$. Let f, f' and f'' be the norms of the finite parts of the conductors of the quadratic extensions K/k, K'/k and K''/k. Then, $d_K=d_k^2 f$, $d_{K'}=d_k^2 f'$, $d_{K''}=d_k^2 f''$ and $\zeta_L(s)\zeta_k(s)^2=\zeta_K(s)\zeta_{K'}(s)\zeta_{K''}(s)$. Now, f'' divides ff' and K' and K are isomorphic. Hence, $f'=f$, $\zeta_{K'}(s)=\zeta_K(s)$, $d_L=d_Kd_{K'}d_{K''}/d_k^2=d_k^2fd_k^2f'd_k^2f''/d_k^2=d_k^4ff'f''$ divides $d_k^4f^4=(d_K/d_k)^4$, hence divides d_K^4. Since $\zeta_L(s)=(\zeta_K(s)/\zeta_k(s))^2\zeta_{K''}(s)$, any real zero of the entire function $\zeta_K(s)/\zeta_k(s)$ would be a double real zero of $\zeta_L(s)$. It is known that $\zeta_L(s)$ has at most 1 real zero in the range $1-1/c\log d_L\leqslant s<1$ (e.g., see [LLO, Lemma 15]). Hence, $(\zeta_K/\zeta_k)(s)>0$ for $1-1/c\log d_L\leqslant s<1$. In particular,

$$(\zeta_K/\zeta_k)(1-1/4c\log d_K)>0.$$

Since k is a cyclic of odd degree, using the factorization of $\zeta_k(s)$ has a product of Dirichlet L-functions and noticing that $L(s,\chi)L(s,\bar{\chi})=|L(s,\chi)|^2\geqslant 0$ and $\zeta(s)<0$ for $0<s<1$, we obtain that $\zeta_k(s)\leqslant 0$ for $0<s<1$. In particular,

$$\zeta_k(1-1/4c\log d_K)\leqslant 0.$$

The desired result follows. □

Lemma 6. *(See [Lou03, Proposition 4].) Let K be a totally imaginary number field of degree $2n \geqslant 4$. Set $J_n = \int_0^{\pi/2} \sin^{n/2-1}(t)\,dt \leqslant \pi/2$ and $K_n = 2eJ_n/\pi^2$. Assume that $d_K > e^4$. If $\zeta_K(\beta) \leqslant 0$ for some $\beta \in [1-(2/\log d_K), 1)$, then*

$$\mathrm{Res}_{s=1}\big(\zeta_K(s)\big) \geqslant \epsilon_n(\rho_K)\frac{1-\beta}{d_K^{(1-\beta)/2}},$$

where

$$\epsilon_n(\rho) := 1 - K_n\frac{n\log\rho - 1}{n\log\rho - 2}\left(\frac{2\pi^2}{\rho}\right)^{n/2}$$

increases with $\rho > e$, and with n for $\rho \geqslant 2\pi^2$. If $n \geqslant 5$, then $K_n \leqslant 0.48144\ldots$.

Theorem 7. *Let K be a non-normal CM-field of degree $2p$, $p \geqslant 3$ a prime, as in Proposition 3. Hence, $\rho_K = f_k^{1-1/p}\tilde{q}^{1/2p}$, where f_k is the conductor of k. Set $c = (3+2\sqrt{2})/2$ and $C := 4\pi c e^{1/8c} = 38.226\ldots$. Then, $h_K^- \geqslant F_k(\tilde{q})$, where*

$$m \mapsto F_k(m) := \frac{\epsilon_p(f_k^{1-1/p}m^{1/2p})\sqrt{m}}{C\,\mathrm{Res}_{s=1}(\zeta_k(s))\log(f_k^{2p-2}m)}\left(\frac{\sqrt{f_k}}{2\pi}\right)^{p-1} \tag{2}$$

increases with $m > 1$, and $h_K^- \geqslant F(p, f_k, \tilde{q})$, where

$$F(p,f,m) := \frac{\epsilon_p(f^{1-1/p})\sqrt{m}}{C\log(f^{2p-2}m)}\left(\frac{\sqrt{f}}{\pi\log f}\right)^{p-1} \tag{3}$$

increases with $m > 1$ and with $f \geqslant 21$.

Proof. By Lemmas 5 and 6, we obtain

$$\mathrm{Res}_{s=1}\big(\zeta_K(s)\big) \geqslant \frac{\epsilon_p(\rho_K)}{4ce^{1/8c}\log d_K} = \epsilon_p(\rho_K)\frac{\pi}{C\log d_K}. \tag{4}$$

Using (1), we obtain the first lower bound on h_K^-.

Now, if k is a real cyclic field of prime degree $p \geqslant 3$ and conductor f_k, then

$$\mathrm{Res}_{s=1}\big(\zeta_k(s)\big) \leqslant \left(\frac{1}{2}\log f_k\right)^{p-1}$$

(by [Ram, Corollary 1]), and we obtain the second lower bound on h_K^-.

Finally, we notice that in setting $f = e^x$, we have $x > 3$ for $f \geqslant 21$ and

$$\frac{1}{\log(f^{2p-2}m)}\left(\frac{\sqrt{f}}{\log f}\right)^{p-1} = \frac{1}{(2p-2)x+\log m}\left(\frac{e^{x/2}}{x}\right)^{p-1} =: G(x)$$

satisfies

$$\frac{G'(x)}{G(x)} = \frac{p-1}{2} - \frac{p-1}{x} - \frac{2p-2}{(2p-2)x+\log m} \geqslant \frac{p-1}{2} - \frac{p-1}{3} - \frac{2p-2}{3(2p-2)} = \frac{p-3}{6}$$

and $G'(x) \geqslant 0$. $\square$

Corollary 8. *Let K be a non-normal CM-field of degree $2p$, $p \geqslant 3$ an odd prime, and containing a real cyclic field k of degree p. Assume that $h_K = 1$. Then, $p \leqslant 23$. Moreover, either* (i) *$p = 23$ and $f_k = 47$, or* (ii) *$p = 13$ and $f_k \in \{53, 79\}$, or* (iii) *$p = 11$ and $f_k \in \{23, 67, 121, 331\}$, or* (iv) *$p \leqslant 7$. Finally, since $m \mapsto F_k(m)$ increases with $m > 1$, for a given cyclic number field k of degree $p \geqslant 3$, we can compute an upper bound $\tilde{q}_{max}$ on $\tilde{q}$ when $h_K = 1$ by*

$$\tilde{q}_{max} = \max\bigl\{\tilde{q};\ q \not\equiv 1 \pmod 4 \text{ prime},\ q^{\phi(f_k)/p} \equiv 1 \pmod{f_k} \text{ and } F_k(\tilde{q}) \leqslant 1\bigr\}. \tag{5}$$

Proof. Assume that $h_K = 1$. Then, $h_k = 1$. Hence, p does not divide h_k. Therefore, $f_k = p^2$ or $f_k \equiv 1 \pmod{2p}$ is an odd prime (with $f_k \geqslant 2p + 1$). Conversely, for any such f_k there is only one cyclic real number field of degree p and conductor f_k.

1. First, assume that $p > 23$. Since $f_k \geqslant 2p + 1 > 21$ and $\rho_K \geqslant \rho_k = f_k^{1-1/p} \geqslant \rho_p := (2p + 1)^{1-1/p} \geqslant 2\pi^2$, we obtain $F(p) \leqslant h_K^- = 1$, where

$$F(p) := F(p, 2p + 1, 3) = \epsilon_p(\rho_p)\frac{\sqrt{3}}{C \log(3 \cdot (2p + 1)^{2p-2})}\left(\frac{\sqrt{2p+1}}{\pi \log(2p + 1)}\right)^{p-1},$$

by (3), which implies $p < 197$.

2. Second, for a given prime $p < 197$ we use $F(p, f_k, 3) \leqslant h_K^- = 1$, by (3), to compute an upper bound f_p on f_k when $h_K = 1$. Then, for each possible conductor $f_k = p^2$ or $f_k \equiv 1 \pmod{2p}$ a prime, with $f_k \leqslant f_p$, we compute

$$\mathrm{Res}_{s=1}\bigl(\zeta_k(s)\bigr) = \prod_{l=1}^{(p-1)/2} \frac{1}{f_k}\left|\sum_{a=0}^{\phi(f_k)-1} \exp(2\pi i a l/p) \log\bigl|\sin\bigl(\pi g_k^a/f_k\bigr)\bigr|\right|^2$$

(see [Was, Theorem 4.9]), where g_k is any generator of the cyclic group $(\mathbf{Z}/f_k\mathbf{Z})^*$. Moreover, a prime q splits in k if and only if $q^{\phi(f_k)/p} \equiv 1 \pmod{f_k}$ and we let

$$\tilde{q}_{min} := \min\bigl\{\tilde{q};\ q \not\equiv 1 \pmod 4 \text{ prime and } q^{\phi(f_k)/p} \equiv 1 \pmod{f_k}\bigr\} \tag{6}$$

be the least prime not equal to 1 mod 4 which splits in k. Since $q \geqslant \tilde{q}_{min}$, by (2), we must have $F_k(\tilde{q}_{min}) \leqslant h_K^- = 1$.

If follows that $h_K > 1$ for $p = 17$, $p = 19$, and $23 < p < 197$. The results for $p = 23$, $p = 13$, $p = 11$ and the last assertion also follow. □

4. A special situation

We would like to have a better bound than the one $p \leqslant 23$ obtained in Corollary 8. In fact, if we could dispose of the case $p = 23$, we would have the better bound $p \leqslant 13$ (see Corollary 8). For a given p and a given k, we can use any software for algebraic number theory to decide whether for a given prime $q \not\equiv 1 \pmod 4$ which splits completely in k the odd primitive quadratic character $\chi_{\mathcal{Q}}$ satisfies $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for the $p - 1$ units ϵ of any system of fundamental units of the unit group U_k of k. However, this could be tricky for fields of large degree, i.e. if $p = 23$. The aim of this section is to prove that this can be done much more easily whenever k is the maximal real subfield of the cyclotomic field $\mathbf{Q}(\zeta_{f_k})$, hence for the three cases $(p, f_k) \in \{(5, 11), (11, 23), (23, 47)\}$. That will enable us to obtain in Corollary 10 the bound $p \leqslant 13$, a better result than the bound $p \leqslant 23$ given in Corollary 8.

Proposition 9. *Assume that $p \geqslant 3$ and $l = 2p + 1 \geqslant 7$ are prime. Let ζ_l be any complex primitive lth root of unity. Assume that the relative class number h_l^- of the cyclotomic field $\mathbf{Q}(\zeta_l)$ is odd, which is the case for*

$l \in \{11, 23, 47\}$ (e.g., see [Was, pp. 412–420]). Set $k = \mathbf{Q}(\zeta_l)^+$, of degree $(l-1)/2 = p$. Let $q \not\equiv 1 \pmod 4$ be a prime that splits in k, i.e. assume that $q \equiv -1 \pmod{4l}$ or $q \equiv 1 + 2l \pmod{4l}$. Let $\mathcal{Q}$ be a prime ideal of k above q. Let $\chi_{\mathcal{Q}}$ be the odd quadratic character on the cyclic group $(A_k/\mathcal{Q})^*$ of order $q-1$. Then, $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for all $\epsilon \in U_k$ if and only if $(\frac{n(a)}{q}) = (\frac{a}{l})$ for $2 \leqslant a \leqslant p = (l-1)/2$, where $n(0) = 0$, $n(1) = 1$ and $n(a) = T \cdot n(a-1) - n(a-2)$ for $a \geqslant 2$ (Legendre's symbols), with T any rational integer such that $\zeta_l + \zeta_l^{-1} \equiv T \pmod{\mathcal{Q}}$.

Proof. It is clear that $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for all $\epsilon \in U_k$ if and only if this holds true for the all the generators of a subgroup of odd index in U_k. The cyclotomic units of k are defined by

$$\xi_a = \left(\zeta_l^a - \zeta_l^{-a}\right)/\left(\zeta_l - \zeta_l^{-1}\right), \quad 2 \leqslant a \leqslant p = (l-1)/2$$

(they are not exactly the ones defined in [Was, Chapter 8]), -1 and these $p-1$ cyclotomic units generate a subgroup of index $h_l^+ = h_k$ in U_k (see [Was, Theorem 8.2]), and if h_l^- is odd then so is h_l^+ (see [Was, Theorem 10.2]). Notice that h_l^- is much easier to compute than h_l^+. Since $q \equiv 3 \pmod 4$, we have $\chi_{\mathcal{Q}}(-1) = (\frac{-1}{q}) = -1 = (-1)^p = N_{k/\mathbf{Q}}(-1)$. Hence, to complete the proof, it suffices to prove that

$$\chi_{\mathcal{Q}}(\xi_a) = \left(\frac{n(a)}{q}\right) \quad \text{and} \quad N_{k/\mathbf{Q}}(\xi_a) = \left(\frac{a}{l}\right), \quad 2 \leqslant a \leqslant p = (l-1)/2.$$

Since $\xi_a = (\zeta_l + \zeta_l^{-1})\xi_{a-1} - \xi_{a-2}$ for $a \geqslant 2$, where $\xi_0 := 0$ and $\xi_1 := 1$, we have $\xi_a \equiv n(a) \pmod{\mathcal{Q}}$ and $\chi_{\mathcal{Q}}(\xi_a) = \chi_{\mathcal{Q}}(n(a)) = (\frac{n(a)}{q})$. Since $\xi_a \equiv a \pmod{(\zeta_l - 1)}$, we have $N_{k/\mathbf{Q}}(\xi_a) = (\frac{a}{l})$. $\square$

Now, we explain how to compute such a T.

1. Assume that $q \equiv 1 + 2l \pmod{4l}$. Then q splits in $\mathbf{Q}(\zeta_l)$. Let $\tilde{\mathcal{Q}}$ be any prime ideal of $\mathbf{Q}(\zeta_l)$ above the prime q. Let $\mathcal{Q}$ be the prime ideal of k below $\tilde{\mathcal{Q}}$. For any algebraic integer $\alpha \in \mathbf{Q}(\zeta_l)$, there exists $n_\alpha \in \mathbf{Z}$, unique mod q, such that $\alpha \equiv n_\alpha \pmod{\tilde{\mathcal{Q}}}$. As ζ runs over the $l-1$ primitive lth complex roots of unity, n_ζ mod q runs over the $l-1$ elements of order l in the cyclic group $(\mathbf{Z}/q\mathbf{Z})^*$ of order $q-1$ divisible by l. Hence, if we have chosen some integer Z_l mod q of order l in the cyclic group $(\mathbf{Z}/q\mathbf{Z})^*$, we may assume that $\zeta_l \equiv Z_l \pmod{\tilde{\mathcal{Q}}}$, which yields $T = Z_l + Z_l^{-1}$ in $\mathbf{Z}/q\mathbf{Z}$. Finally, to find some $Z_l \in \mathbf{Z}$ of order l in the cyclic group $(\mathbf{Z}/q\mathbf{Z})^*$, we compute $Z_{min} := \min\{Z \geqslant 1;\ Z^{(q-1)/l} \not\equiv 1 \pmod q\}$ and take $Z_l := Z_{min}^{(q-1)/l}$. If we assume the generalized Riemann hypothesis, then $Z_{min} \leqslant 2\log^2 q$ (see [Bach, Theorem 2, p. 372]).

2. Assume that $q \equiv -1 \pmod{4l}$. Then q splits in k and is inert in $L := \mathbf{Q}(\sqrt{-l}) \subseteq \mathbf{Q}(\zeta_l) = kL$, for $(\frac{-l}{q}) = (\frac{q}{l}) = (\frac{-1}{l}) = -1$. Let $\mathcal{Q}$ be any prime ideal of k above the prime q. Then $\mathcal{Q}$ is inert in $\mathbf{Q}(\zeta_l)$. Let $\tilde{\mathcal{Q}}$ be the prime ideal of $\mathbf{Q}(\zeta_l)$ above $\mathcal{Q}$. For any algebraic integer $\alpha \in \mathbf{Q}(\zeta_l)$, there exists $\lambda_\alpha \in \mathbf{Z}[\sqrt{-l}]$, unique mod $q\mathbf{Z}[\sqrt{-l}]$, such that $\alpha \equiv \lambda_\alpha \pmod{\tilde{\mathcal{Q}}}$. As ζ runs over the $l-1$ primitive lth complex roots of unity, λ_ζ runs over the $l-1$ elements of order l in the cyclic group $G := (\mathbf{Z}[\sqrt{-l}]/q\mathbf{Z}[\sqrt{-l}])^*$ of order q^2-1 divisible by l. Hence, if we have chosen some $\Lambda_l \in \mathbf{Z}[\sqrt{-l}]$ of order l in G, we may assume that $\zeta_l \equiv \Lambda_l \pmod{\tilde{\mathcal{Q}}}$, which yields $T = \Lambda_l + \bar{\Lambda}_l$. Indeed, since $\lambda^q \equiv \bar{\lambda} \pmod{q\mathbf{Z}[\sqrt{-l}]}$ for $\lambda \in \mathbf{Z}[\sqrt{-l}]$, and since l divides $q+1$, it follows that $\Lambda_l^{-1} \equiv \Lambda_l^q \equiv \bar{\Lambda}_l \pmod{q\mathbf{Z}[\sqrt{-l}]}$. Finally, to find some $\Lambda_l \in \mathbf{Z}[\sqrt{-l}]$ of order l in G, we find some $\Lambda \in \mathbf{Z}[\sqrt{-l}]$ such that $\Lambda^{(q^2-1)/l} \not\equiv 1 \pmod{q\mathbf{Z}[\sqrt{-l}]}$ and take $\Lambda_l = \Lambda^{(q^2-1)/l}$. We may assume that Z is of the form $Z = z + \sqrt{-l}$ and using $Z^q \equiv \bar{Z} \pmod{q\mathbf{Z}[\sqrt{-l}]}$, we obtain $Z^{(q^2-1)/l} = (Z^{q-1})^{(q+1)/l} \equiv (\bar{Z}/Z)^{(q+1)/l} \pmod{q\mathbf{Z}[\sqrt{-l}]}$. To sum up, we have $T = 2\frac{A^2-lB^2}{A^2+lB^2}$ in $\mathbf{Z}/q\mathbf{Z}$, where $z_{min} \geqslant 1$ is the least positive integer such that $(z+\sqrt{-l})^{(q+1)/l} \equiv A + B\sqrt{-l} \pmod{q\mathbf{Z}[\sqrt{-l}]}$ with $B \not\equiv 0 \pmod q$. These computations are efficiently performed by using the binary expansion of the large exponent $(q+1)/l$.

3. Hence, we have an easy to implement and fast algorithm to generate the primes q with $q \equiv 1 + 2l \pmod{4l}$ or $q \equiv -1 \pmod{4l}$ for which $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for all the $\epsilon \in U_k$. For example, for

$p = 23$ and $f_k = 47$, we obtain that $q = 1184829391 \approx 10^9$, is the least prime $q \not\equiv 1 \pmod 4$ which splits in k and for which $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for $\epsilon \in U_k$.

Corollary 10. *Let K be a non-normal CM-field of degree $2p$, $p \geqslant 3$ an odd prime, and containing a real cyclic field k of degree p. If $h_K = 1$, then $p \leqslant 13$.*

Proof. For $p = 23$ and $f_k = 47$, we have just seen that $q \geqslant 1184829391$. Hence, $h_K^- \geqslant F_k(\tilde{q}) \geqslant F_k(1184829391) = 278.408\ldots > 1$, with $m \mapsto F_k(m)$ as in (2). □

We point out that we have arrived at this bound $p \leqslant 13$ without using any software dedicated to algebraic number theory. To conclude this section, by using any such software, we further improve this bound $p \leqslant 13$ down to $p \leqslant 11$:

Corollary 11. *Let K be a non-normal CM-field of degree $2p$, $p \geqslant 3$ an odd prime, and containing a real cyclic field k of degree p. If $h_K = 1$, then $p \leqslant 11$. Moreover, if $p = 11$, then $f_k = 23$, $q \leqslant 56128463$ and that are 146 possible q's.*

Proof. By Corollaries 8 and 10, to prove the first assertion we only have to settle the cases $p = 13$ and $f_k \in \{53, 79\}$. If $f_k = 53$, using any software for algebraic number theory we obtain that $q = 940327$ is the least prime $q \not\equiv 1 \pmod 4$ which splits completely in k for which the odd primitive quadratic character $\chi_{\mathcal{Q}}$ satisfies $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for the $p-1$ units ϵ of any system of fundamental units of the unit group U_k of k. Hence, in that case, we have $q \geqslant 940327$, which implies $h_K^- \geqslant F_k(\tilde{q}) \geqslant F_k(940327) = 5.607\ldots > 1$, with $n \mapsto F_k(n)$ as in (2). In the same way, if $f_k = 79$, the least prime q to consider is $q = 936151$, but here again we obtain $h_K^- \geqslant F_k(\tilde{q}) \geqslant F_k(936151) = 57.894\ldots > 1$.

To prove the second assertion, we use Corollary 8 and notice that, in the same way, if $f_k = 67$, $f_k = 121$ or $f_k = 331$, we respectively found that $q = 31259$, $q = 179807$ or $q = 402763$ are the least possible prime to consider. In these three cases we respectively have $h_K^- \geqslant F_k(\tilde{q}) \geqslant F_k(31259) = 2.749\ldots > 1$, $h_K^- \geqslant F_k(\tilde{q}) \geqslant F_k(179807) = 2.526\ldots > 1$ and $h_K^- \geqslant F_k(\tilde{q}) \geqslant F_k(402763) = 15.444\ldots > 1$.

Finally, assume that $p = 11$ and $f_k = 23$. Then $\tilde{q} \leqslant q_{max} = 56128463$ (see (5)), and the computation of the number of q's less than or equal to 56128463 follows from the method developed in this section. □

We point out that we have arrived at this bound $p \leqslant 11$ without doing any relative class number computation. However, to deal with the remaining cases $p \in \{3, 5, 7, 11\}$, we will have to construct a list containing all the possibles K's with $h_K = 1$, and then to compute their relative class numbers (see Section 8). Since computations of relative class numbers are a bit time consuming, (i) in Section 5 we improve upon Theorem 7 to further reduce our list in the cases $p = 3$ and $p = 5$ and (ii) in Section 6 we give a necessary condition for the class number to be equal to one to drastically reduce this list.

5. The case that p is small: $p = 3$ and $p = 5$

For $p = 3$ and $p = 5$, we give a better result than Lemma 5 and obtain better lower bounds on relative class numbers:

Lemma 12. *Let k be a cyclic field of degree p. Let K/k be a quadratic extension, with K not normal. Let N be the normal closure of K. Then, for $d_N > \exp(2(\sqrt{p} - 1))$ it holds that $\zeta_K(1 - (c_{p-1}/\log d_N)) \leqslant 0$, where $c_{p-1} = 2(\sqrt{p} - 1)^2$. Moreover, if K is as in Proposition 3, then $d_N = (d_K \tilde{q}^{p-1})^{2^{p-1}} = (f_k^{2(p-1)} \tilde{q}^p)^{2^{p-1}}$.*

Proof. If $d_N > \exp(2(\sqrt{m+1} - 1))$, then the Dedekind zeta function $\zeta_N(s)$ of a number field N has at most m real zeros in the range $1 - (c_m/\log d_N) \leqslant s < 1$, where $c_m = 2(\sqrt{m+1} - 1)^2$ (see [LLO, Lemma 15]). Write $\mathrm{Gal}(k/\mathbf{Q}) = \langle \sigma \rangle$, $K = k(\sqrt{\alpha})$ and $N = k(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_p})$, where $\alpha_i = \sigma^{i-1}(\alpha)$. The p quadratic extensions $K_i/k = k(\sqrt{\alpha_i})/k$ are pairwise distinct. Indeed, since K is not normal it follows that $\sigma(\alpha)/\alpha \in k \setminus k^2$, which implies $\sigma^i(\alpha)/\alpha \in k \setminus k^2$ for $1 \leqslant i \leqslant p-1$ and $\sigma^i(\alpha)/\sigma^j(\alpha) \in k \setminus k^2$ for $0 \leqslant j < i \leqslant p-1$ (for $\sigma^i(\alpha)/\alpha \in k^2$ implies $\sigma^{ij}(\alpha)/\alpha \in k^2$ (by induction on j) and $\sigma(\alpha)/\alpha \in k^2$ by choosing j such that $ij \equiv 1 \pmod p$). Since the L-function associated with any quadratic extension of k is entire, using the factorization of $\zeta_N(s)/\zeta_k(s)$ has a product of quadratic L-functions, we have $\zeta_N(s) = f(s)\zeta_k(s)\prod_{i=1}^p(\zeta_{K_i}(s)/\zeta_k(s))$ where $f(s)$ is entire. Each K_i being isomorphic to K, we have $\prod_{i=1}^p(\zeta_{K_i}(s)/\zeta_k(s)) = (\zeta_K(s)/\zeta_k(s))^p$. Hence, any real zero of $\zeta_K(s)/\zeta_k(s)$ is a zero of $\zeta_N(s)$ of multiplicity $\geqslant p$, hence is $< 1-(c_{p-1}/\log d_N)$. Therefore,

$$(\zeta_K/\zeta_k)\big(1-(c_{p-1}/\log d_N)\big) > 0.$$

Now, as in the proof of Lemma 5, we have $\zeta_k(s) \leqslant 0$ for $0 < s < 1$. In particular,

$$\zeta_k\big(1-(c_{p-1}/\log d_N)\big) \leqslant 0.$$

The desired result follows. The last assertion follows from the conductor-discriminant formula. □

Instead of Theorem 7, we obtain:

Theorem 13. *Let K be a non-normal CM-field of degree $2p$, $p \geqslant 3$ a prime, as in Proposition 3. Set*

$$C_p := \frac{2^{p-2} \cdot \pi \cdot e^{(\sqrt{p}-1)^2/2^{p-1}}}{(\sqrt{p}-1)^2}.$$

Hence, $C_3 = 13.40546\ldots$ and $C_5 = 18.09783\ldots$. Then, $h_K^- \geqslant G_k(\tilde{q})$, where

$$m \mapsto G_k(m) := \frac{\epsilon_p(f_k^{1-1/p}m^{1/2p})\sqrt{m}}{C_p \operatorname{Res}_{s=1}(\zeta_k(s))\log(f_k^{2p-2}m^p)}\left(\frac{\sqrt{f_k}}{2\pi}\right)^{p-1} \tag{7}$$

increases with $m > 1$.

Proof. Set $\beta = 1-(c_{p-1}/\log d_N)$. Since $c_{p-1} \leqslant 2^{p-1}$ and $d_N \geqslant d_K^{2^{p-1}}$, we have

$$1-(2/\log d_K) \leqslant 1-\big(c_{p-1}/2^{p-1}\log d_K\big) \leqslant 1-(c_{p-1}/\log d_N) = \beta$$

and, instead of (4), we obtain

$$\operatorname{Res}_{s=1}\big(\zeta_K(s)\big) \geqslant \epsilon_p(\rho_K)\frac{2^{p-1}\pi}{C_p \log d_N} = \epsilon_p(\rho_K)\frac{\pi}{C_p\log(f_k^{2(p-1)}\tilde{q}^p)},$$

by using $d_K^{(1-\beta)/2} = \exp(c_{p-1}\frac{\log d_K}{2\log d_N}) \leqslant \exp(c_{p-1}/2^p)$. The result follows. □

6. Necessary conditions for the class number to be equal to one

For some values of p and f_k, say for $(p, f_k) = (5, 11)$, there are many possible simplest non-normal $2p$-CM-fields $K_{k,q}$ with $\tilde{q} \leqslant \tilde{q}_{max}$ (see Table 1). We give a necessary condition for the class number to be equal to one to drastically reduce this list and end up with only few CM-fields $K_{k,q}$ for which we will have to compute their relative class numbers to settle our class number one problem.

Theorem 14. *Let $K = K_{k,q}$ be a simplest non-normal $2p$-CM-field associated with a real cyclic field k of prime degree $p \geqslant 3$ and a prime $q \not\equiv 1 \pmod 4$ which splits completely in k. If $h_K = 1$, then any prime l which splits completely in k and $L = \mathbf{Q}(\sqrt{-q})$ satisfies $l \geqslant \tilde{q}/4^p$.*

Proof. Use [Lou94, Theorem D] and the last assertion of Proposition 3 (see also [Lou97b]). □

For example, if $(p, f_k) = (5, 11)$, then among the 7354 prime numbers $q \leqslant \tilde{q}_{max} = 18536363$ (obtained by the method given in Section 4), only 31 of them satisfy this necessary condition.

7. A table of the finite cases to deal with

Assume that $5 \leqslant p \leqslant 11$ and that $h_K = 1$. By using the method given in the proof of Corollary 8, we can make a list of possible cyclic number fields k such that K^+ must be in this list. For ($p = 3$ or) $p = 5$, not only can we use (5), but we can use it with $G_k(m)$ instead of $F_k(m)$. For example, for $p = 5$ and $f_k = 11$, Theorem 7 yields $\tilde{q}_{max} = 18536363$ (and $N_k(\tilde{q}_{max}) = 7354$ by Section 4), whereas Theorem 13 yields $\tilde{q}_{max} = 34898819$ (and $N_k(\tilde{q}_{max}) = 13313$). However, for $p = 5$ and $f_k = 281$, Theorem 7 yields $\tilde{q}_{max} = 59$, whereas Theorem 13 yields $G_k(\tilde{q}_{min}) = G_k(47) > 1$ and shows that this number field k needs not appear in our list. Hence, for ($p = 3$ or) $p = 5$ we use (5) with $\min(F_k(m), G_k(m))$ instead of $F_k(m)$. We obtained that k is one of the 58 cyclic fields given in Table 1. In fact, since the eight ones of conductors in *bold face letters* have narrow class numbers greater than one, there are only $50 = 58 - 8$ fields k to consider. For $p = 3$ there are too many possible fields k to give them in Table 1, but for $p = 3$ our problem has been solved in [BL1]. In Table 1, for a given p and a given cyclic field k of degree p and conductor f_k, $\tilde{q}_{max}$ as in (5) is an upper bound on $\tilde{q}$ if $h_K^- = 1$, and $N_k(\tilde{q}_{max})$, computed with any software dedicated to number theory, is the number of prime $q \not\equiv 1 \pmod 4$ with $\tilde{q} \leqslant \tilde{q}_{max}$ which split completely in k and for which the odd primitive quadratic character $\chi_{\mathcal{Q}}$ satisfies $\chi_{\mathcal{Q}}(\epsilon) = N_{k/\mathbf{Q}}(\epsilon)$ for the $p - 1$ units ϵ of any system of fundamental units of the unit group U_k of k, i.e., $N_k(\tilde{q}_{max})$ is the number of simplest non-normal $2p$-CM-fields with $\tilde{q} \leqslant \tilde{q}_{max}$. We expect $N_k(\tilde{q}_{max})$ to be asymptotic to

$$\tilde{N}_k(\tilde{q}_{max}) = \frac{1}{p2^p} \frac{\tilde{q}_{max}}{\log \tilde{q}_{max}}.$$

For some cases, there are many possible values for q. We use Theorem 14 to get rid of most of them, and let $N'_k(\tilde{q}_{max})$ denote the number of $\tilde{q} \leqslant \tilde{q}_{max}$ which satisfy this necessary condition. According to this Table 1, we only have 402 relative class numbers to compute to settle our class number one problem. We will explain in the next section how we performed this relative class number computations. The last two columns of Table 1 give the least such q and the relative class number h_K^- of the CM-field $K_{k,q}$.

8. Computation of relative class numbers

We refer the reader to [Lou97a]. Let K be a CM-field of degree $2n \geqslant 2$. Let k be its maximal totally real subfield, of degree n. Let w_K be the number of roots of unity in K. Let $\chi_{K/k}$ be the quadratic character associated with the quadratic extension K/k. Let $\phi_m = \sum_{N_{k/\mathbf{Q}}(\mathcal{I})=m} \chi_{K/k}(\mathcal{I})$ be the coefficients of the Dirichlet series

$$\zeta_K(s)/\zeta_k(s) = L(s, \chi_{K/k}) = \sum_{m \geqslant 1} \phi_m m^{-s} \quad \big(\Re(s) > 1\big).$$

Set $A_{K/k} = \sqrt{d_K/\pi^n d_k}$. We have

$$h_K^- = \frac{Q_K w_K}{(2\pi)^n} \sqrt{\frac{d_K}{d_k}} \sum_{m \geqslant 1} \frac{\phi_m}{m} K_n(m/A_{K/k}), \tag{8}$$

Table 1

p	f_k	$\tilde{q}_{min}$	$\tilde{q}_{max}$	$N_k(\tilde{q}_{max})$	$N'_k(\tilde{q}_{max})$	q	h_K^-
5	11	23	18536363	7354	31	1451	1
5	25	7	2715007	1226	28	251	3
5	31	67	1812571	867	24	811	3
5	41	3	3557327	1555	24	331	5
5	61	11	76099	53	12	2731	49
5	71	23	10463	8	8	811	25
5	101	107	1483	2	2	971	63
5	131	19	739	0			
5	151	8	810191	416	14	491	1425
5	181	7	1567	1	1	659	149
5	**191**	11	3163				
5	211	31	67	0			
5	241	8	187219	102	13	719	1429
5	251	8	430603	219	18	3947	8315
5	271	23	619	1	1	331	339
5	311	7	331	0			
5	331	23	31	0			
5	431	3	329143	179	14	107	215
5	491	3	251	2	2	179	225
5	571	8	3251	3	2	3019	4775
5	**641**	8	13463				
5	661	3	431	0			
5	761	3	463	1	1	103	2931
5	911	7	2399	3	1	1823	39421
5	971	7	1571	1	1	607	8739
5	1021	3	19	0			
5	1051	3	3	0			
5	1091	3	67	0			
5	1171	3	7	0			
5	1181	8	263	1	1	107	4265
5	1811	7	71	0			
5	1871	3	3	0			
5	**2351**	8	11				
5	2381	7	223	0			
5	2521	3	3	0			
5	3061	8	8	0			
5	3121	8	8	0			
5	3221	3	179	1	1	179	74487
5	3361	7	8	0			
5	3881	3	283	0			
5	4861	7	8	0			
5	**6581**	3	8	0			
5	**8831**	3	3				
5	11251	3	3	0			
7	**29**	59	1769099				
7	43	7	622639	55	37	2887	33
7	49	19	124459	12	12	5879	57
7	71	167	132911	13	8	9803	119
7	**113**	71	227				
7	127	19	359	0			
7	211	19	23	0			
7	281	7	7	0			
7	631	8	983	0			
7	673	8	163	0			
7	757	3	3	0			
7	883	3	3	0			
7	**953**	8	8				
11	23	47	56128463	146	146	137771	7

where $K_n(A)$ is defined for $A > 0$ and satisfies

$$0 \leqslant K_n(A) \leqslant 2n \exp\bigl(-A^{2/n}\bigr). \tag{9}$$

According to (9), this series (8) is absolutely convergent. Moreover, set

$$B(K) \overset{def}{=} A_{K/k}\left(\frac{\lambda}{n} \log A_{K/k}\right)^{n/2}.$$

If $\lambda > 1$ and n are given, then the limit of $|h_K^- - h_K^-(M)|$ as d_K approaches infinity is equal to 0. Here, $h_K^-(M)$ is the approximation of h_K^- obtained by disregarding in (8) the indices $m > M \geqslant B(K)$. In our situation, we have $Q_K = 1$ and $w_K = 2$ (see Proposition 3). We refer the reader to [Lou97a, Propositions 3 and 4] for the computation of numerical approximations to $K_n(A)$ for $A > 0$. Finally, since $m \mapsto \phi_m$ is multiplicative, we only have to explain how to compute ϕ_{l^m} for $l \geqslant 2$ a prime and $m \geqslant 1$:

Proposition 15. *Assume that $K = K_{k,\mathcal{Q}}$. Let $l \geqslant 2$ be a prime.*

1. *Assume that l is ramified in k. Then, $\phi_{l^m} = (-\tilde{q}/l)^m$.*
2. *Assume that l is inert in k. Then, $\phi_{l^m} = (-\tilde{q}/l)^m$ if p divides m, and $\phi_{l^m} = 0$ otherwise.*
3. *Assume that $(l) = \mathcal{L}_1 \cdots \mathcal{L}_p$ splits completely in k. Set $\epsilon_j = \chi_{K/k}(\mathcal{L}_j) \in \{-1, 0 + 1\}$. Let $a_+ \geqslant 0$ be the number of ϵ_j's that are equal to $+1$ and $a_- \geqslant 0$ be the number of ϵ_j's that are equal to -1. Then,*

$$\phi_{l^m} = \begin{cases} (-1)^m \binom{a_- - 1 + m}{a_- - 1} & \text{if } a_+ = 0 \text{ and } a_- \geqslant 1, \\ \binom{a_+ - 1 + m}{a_+ - 1} & \text{if } a_+ \geqslant 1 \text{ and } a_- = 0, \\ \sum_{i+j=m} (-1)^j \binom{a_+ - 1 + i}{a_+ - 1} \binom{a_- - 1 + j}{a_- - 1} & \text{if } a_+ \geqslant 1 \text{ and } a_- \geqslant 1. \end{cases}$$

Proof.

1. We have $(l) = \mathcal{L}^p$, $\mathcal{L}^m$ is the only ideal of norm l^m and $\phi_{l^m} = \chi_{K/k}(\mathcal{L})^m = \chi_{K/k}(\mathcal{L})^{mp} = \chi_{K/k}((l))^m = \chi_0(l)^m = (-\tilde{q}/l)^m$.
2. We have $(l) = \mathcal{L}$ and $\chi_{K/k}(\mathcal{L}) = \chi_{K/k}((l)) = \chi_0(l) = (-\tilde{q}/l)$. There exists an ideal $\mathcal{I}$ of norm l^m if and only if p divides m, in which case $\mathcal{I} = (l)^{m/p}$ is the only such ideal, and $\phi_{l^m} = \chi_{K/k}(\mathcal{L}^{m/p}) = \chi_{K/k}(\mathcal{L}^{m/p})^p = \chi_{K/k}((l))^m = (-\tilde{q}/l)^m$.
3. Notice that $\epsilon_1 \cdots \epsilon_p = \chi_{K/k}((l)) = \chi_0(l) = (-\tilde{q}/l)$. Here,

$$\phi_{l^m} = \sum_{\substack{a_1 + \cdots + a_p = i \\ a_j \geqslant 0}} \epsilon_1^{a_1} \cdots \epsilon_p^{a_p}$$

is the coefficient of x^m in the power series expansion of $\frac{1}{(1-x)^{a_+}(1+x)^{a_-}}$. $\square$

9. The determination

Theorem 16. *There is no non-normal CM-field of class number one and whose maximal totally real subfield is cyclic of degree $p > 5$ a prime.*

Table 2

f_k	q	$P_k(X)$	d_K	$\rho_K = d_K^{1/6}$
7	167	$X^3 - 18X^2 + 101X - 167$	$7^4 \cdot 167$	8.587...
7	239	$X^3 - 19X^2 + 118X - 239$	$7^4 \cdot 239$	9.115...
7	251	$X^3 - 22X^2 + 145X - 251$	$7^4 \cdot 251$	9.190...
7	379	$X^3 - 26X^2 + 181X - 379$	$7^4 \cdot 379$	9.844...
7	491	$X^3 - 26X^2 + 209X - 491$	$7^4 \cdot 491$	10.278...
7	547	$X^3 - 27X^2 + 222X - 547$	$7^4 \cdot 547$	10.464...
7	1051	$X^3 - 34X^2 + 341X - 1051$	$7^4 \cdot 1051$	10.668...
9	71	$X^3 - 30X^2 + 117X - 71$	$9^4 \cdot 71$	8.804...
9	199	$X^3 - 39X^2 + 318X - 199$	$9^4 \cdot 199$	10.454...
9	379	$X^3 - 30X^2 + 237X - 379$	$9^4 \cdot 379$	11.639...
9	523	$X^3 - 57X^2 + 507X - 523$	$9^4 \cdot 523$	12.281...
9	739	$X^3 - 33X^2 + 315X - 739$	$9^4 \cdot 739$	13.009...
13	47	$X^3 - 15X^2 + 62X - 47$	$13^4 \cdot 47$	10.502...
13	79	$X^3 - 14X^2 + 61X - 79$	$13^4 \cdot 79$	11.452...
19	31	$X^3 - 11X^2 + 34X - 31$	$19^4 \cdot 31$	12.620...
19	83	$X^3 - 18X^2 + 89X - 83$	$19^4 \cdot 83$	14.871...
31	2	$X^3 - 12X^2 + 17X - 2$	$31^4 \cdot 2^3$	13.955...
37	11	$X^3 - 10X^2 + 21X - 11$	$37^4 \cdot 11$	16.558...
61	3	$X^3 - 15X^2 + 14X - 3$	$61^4 \cdot 3$	18.609...

Table 3

f_k	q	$P_k(X)$	d_K	$\rho_K = d_K^{1/10}$
11	1451	$X^5 - 43X^4 + 612X^3 - 3325X^2 + 5195X - 1451$	$11^8 \cdot 1451$	14.102...
11	1583	$X^5 - 28X^4 + 296X^3 - 1431X^2 + 2942X - 1583$	$11^8 \cdot 1583$	14.225...
11	1783	$X^5 - 34X^4 + 337X^3 - 1416X^2 + 2632X - 1783$	$11^8 \cdot 1783$	14.395...
11	1871	$X^5 - 45X^4 + 623X^3 - 2824X^2 + 4469X - 1871$	$11^8 \cdot 1871$	14.465...
11	2971	$X^5 - 45X^4 + 711X^3 - 4496X^2 + 8869X - 2971$	$11^8 \cdot 2971$	15.149...

Theorem 17. *(See [BL1].) There are* 19 *non-isomorphic non-normal CM-fields of degree* 6, *of class number one and whose maximal totally real subfields are cyclic cubic fields*: *the* 19 *simplest non-normal sextic CM-fields* $K = K_{k,q}$ *given in Table* 2. *Here, k is defined as the splitting field of* $P_k(X) = X^3 - aX^2 + bX - q \in \mathbf{Z}[X]$ *which is the minimal polynomial of an algebraic element* $\alpha_q \in k$ *of norm q such that* $K_{k,q} = k(\sqrt{-\alpha_q})$. *Therefore,* $K_{k,q}$ *is generated by any one of the complex roots of* $P_{K_{k,q}}(X) = -P_k(-X^2) = X^6 + aX^4 + bX^2 + q$.

Theorem 18. *There are* 5 *non-isomorphic non-normal CM-fields of degree* 10, *of class number one and whose maximal totally real subfields are cyclic quintic fields*: *the* 5 *simplest non-normal CM-fields* $K = K_{k,q}$ *of degree* 10 *given in Table* 3. *Here, k is defined as the splitting field of* $P_k(X) = X^5 - aX^4 + bX^3 - cX^2 + dX - q \in \mathbf{Z}[X]$ *which is the minimal polynomial of an algebraic element* $\alpha_q \in k$ *of norm q such that* $K_{k,q} = k(\sqrt{-\alpha_q})$. *Therefore,* $K_{k,q}$ *is generated by any one of the complex roots of* $P_{K_{k,q}}(X) = -P_k(-X^2) = X^{10} + aX^8 + bX^6 + cX^4 + dX^2 + q$.

10. Conclusion

Let $K = k(\sqrt{-\alpha})$ be a non-normal CM-field of degree 2, $p \geqslant 3$ a prime, whose maximal totally real subfield k of degree p is cyclic. Here α is a totally positive element of k. Let σ be a generator of the Galois group $\mathrm{Gal}(k/\mathbf{Q})$. Let $\alpha' \in \{\sigma^l(\alpha);\ 1 \leqslant l \leqslant p-1\}$ be any conjugate of α in k such that $K' = k(\sqrt{-\alpha'}) \neq K$ (this is possible for $K/\mathbf{Q}$ is not normal). Set $L = k(\sqrt{-\alpha}, \sqrt{-\alpha'})$. Then L is a CM-field of degree $4p$ and of maximal totally real subfield $L^+ = k(\sqrt{\alpha\alpha'})$. According to [LO98, Proposition 2(b)], we have

$$h_L^- = \frac{Q_L}{2}\left(h_K^-/Q_K\right)^2,$$

and if h_K^- is odd, then $Q_K = 1$ (see also Proposition 3), $Q_L = 2$, $h_L^- = (h_K^-)^2$ and h_L is odd. In particular, if $h_K^- = 1$ then $h_L^- = 1$. Hence, we can construct many non-normal non-isomorphic CM-fields L of degree 12 or 20, of relative class number one and of odd class number. Therefore, nothing prevents some of them to be of class number one. Since $h_L^- = 1$ we have $h_L = h_{L^+}$. Since L^+ is only of degree 6 or 10, using any software dedicated to algebraic number theory, we can compute h_{L^+}. In our situation, for a given K there are $(p-1)/2$ non-isomorphic CM-fields L, the $L := k(\sqrt{-\alpha}, \sqrt{-\sigma^l(\alpha)})$ with $1 \leqslant l \leqslant (p-1)/2$, hence 1 of them for $p = 3$, and 2 of them for $p = 5$. Hence, we can construct 19 non-isomorphic non-normal CM-fields L of degree 12, of relative class number one and of odd class number, and $10 = 2 \times 5$ non-isomorphic non-normal CM-fields L of degree 20, of relative class number one and of odd class number. We found that all these $29 = 19 + 10$ non-normal CM-fields L have class number one, i.e. that $h_{L^+} = 1$ for these $29 = 19 + 10$ non-normal CM-fields L.

References

[Bach] E. Bach, Explicit bounds for primality testing and related problems, Math. Comp. 55 (1990) 355–380.

[Bes] S. Bessassi, Bounds for the degrees of CM-fields of class number one, Acta Arith. 106 (2003) 213–245.

[BL1] G. Boutteaux, S. Louboutin, The class number one problem for some non-normal sextic CM-fields, in: Proceedings of the China–Japan Number Theory Conference and the RIMS Analytic Number Theory Conference, Kluwer Academic Publishers, 2002, pp. 27–37.

[BL2] G. Boutteaux, S. Louboutin, The class number one problem for some non-normal sextic CM-fields. Part 2, Acta Math. Inform. Univ. Ostrav. 10 (2002) 3–23.

[CH] P.E. Conner, J. Hurrelbrink, Class Number Parity, Ser. Pure Math., vol. 8, World Scientific, Singapore, 1988, xi, 234 p.

[He] E. Hecke, Lectures on the Theory of Algebraic Numbers, Grad. Texts in Math., vol. 77, Springer-Verlag, New York, 1981, Translated from the German by George U. Brauer, Jay R. Goldman, R. Kotzen.

[LK] G.-N. Lee, S.-H. Kwon, CM-fields with relative class number one, Math. Comp. 75 (2006) 997–1013.

[LLO] F. Lemmermeyer, S. Louboutin, R. Okazaki, The class number one problem for some non-abelian normal CM-fields of degree 24, J. Theor. Nombres Bordeaux 11 (1999) 387–406.

[LO94] S. Louboutin, R. Okazaki, 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.

[LO98] S. Louboutin, R. Okazaki, The class number one problem for some non-abelian normal CM-fields of 2-power degrees, Proc. Lond. Math. Soc. 76 (1998) 523–548.

[Lou94] S. Louboutin, On the class number one problem for non-normal quartic CM-fields, Tohoku Math. J. 46 (1994) 1–12.

[Lou96] S. Louboutin, Determination of all quaternion octic CM-fields with class number 2, J. Lond. Math. Soc. 54 (1996) 227–238.

[Lou97a] S. Louboutin, Computation of relative class numbers of CM-fields, Math. Comp. 66 (1997) 1185–1194.

[Lou97b] S. Louboutin, Powerful necessary conditions for class-number problems, Math. Nachr. 183 (1997) 173–184.

[Lou03] S. Louboutin, Explicit lower bounds for residues at $s = 1$ of Dedekind zeta functions and relative class numbers of CM-fields, Trans. Amer. Math. Soc. 355 (2003) 3079–3098.

[Lou08] S. Louboutin, Some explicit upper bounds for residues of zeta functions of number fields taking into account the behavior of the prime 2, Manuscripta Math. 125 (2008) 43–67.

[LYK] S. Louboutin, H.-S. Yang, S.-H. Kwon, The non-normal quartic CM-fields and the dihedral octic CM-fields with ideal class groups of exponent $\leqslant 2$, Math. Slovaca 54 (2004) 535–574.

[Neu] J. Neukirch, Algebraic Number Theory, Grundlehren Math. Wiss., vol. 322, Springer-Verlag, Berlin, 1999.

[PK] S.-M. Park, S.-H. Kwon, Class number one problem for normal CM-fields, J. Number Theory 125 (2007) 59–84.

[Ram] O. Ramaré, Approximate formulae for $L(1, \chi)$, Acta Arith. 100 (2001) 245–256.

[Sta] H.M. Stark, Some effective cases of the Brauer–Siegel Theorem, Invent. Math. 23 (1974) 135–152.

[Was] L.C. Washington, Introduction to Cyclotomic Fields, Second edition, Grad. Texts in Math., vol. 83, Springer-Verlag, New York, 1997.

[Yam] K. Yamamura, The determination of the imaginary abelian number fields with class-number one, Math. Comp. 62 (1994) 899–921.