J. Aust. Math. Soc. **87** (2009), 129–144
doi:10.1017/S1446788709000081

NONABELIAN NORMAL CM-FIELDS OF DEGREE $2pq$

S.-H. KWON, S. LOUBOUTIN✉ and S.-M. PARK

(Received 17 January 2008; accepted 28 October 2008)

Communicated by I. E. Shparlinski

Abstract

We prove that the relative class number of a nonabelian normal CM-field of degree $2pq$ (where p and q are two distinct odd primes) is always greater than four. Not only does this result solve the class number one problem for the nonabelian normal CM-fields of degree 42, but it has also been used elsewhere to solve the class number one problem for the nonabelian normal CM-fields of degree 84.

2000 *Mathematics subject classification*: primary 11R29; secondary 11R20.

Keywords and phrases: CM-field, relative class number, number field.

1. Introduction

There are only finitely many normal CM-fields N of a given *relative class number* h_N^- (see Odlyzko [Odl]). Their degrees are less than or equal to 266 (see Bessassi [Bes, Theorem 2]), and even to 216 (see Lee and Kwon [LK, Theorem 1]). Those of relative class number one which are Abelian, dihedral, dicyclic or of degree $4p^2$, $p \geq 3$ an odd prime, are known (see Stark [Sta], Louboutin [Lou92], Park and Kwon [PK98], Chang and Kwon [CK98], Yamamura [Yam] and Chang and Kwon [CK00]; Louboutin and Okazaki [LO98], Louboutin, Okazaki and Olivier [LOO], Lefeuvre [Lef], Lefeuvre and Louboutin [LL], Louboutin [Lou99], and Chang and Kwon [CK02]). If $K \subseteq N$ are two CM-fields, then h_K^- divides $4h_N^-$ (see Okazaki [Oka]). Hence, if $h_N^- = 1$ then h_K^- divides four and the determination of all the CM-fields of a given type and of relative class number less than or equal to four is useful for determining the CM-fields of a more complicated type and of relative class number one. Throughout this paper we let $p > q \geq 3$ denote two distinct odd primes. We will prove the following result which not only solves the class number one problem for the nonabelian normal CM-fields of degree 42 but also is used in Park and Kwon [PK07] to solve the class number one problem for the nonabelian normal CM-fields of degree 84.

The research of the first author was supported by a Korea University Grant.

THEOREM 1. *The relative class number of a nonabelian normal CM-field of degree $2pq$ is always greater than four.*

Our strategy for proving Theorem 1 is as follows.

(i) In Section 2, we prove that the nonabelian normal CM-fields of degree $2pq$ are the composita of an imaginary quadratic number field and of a real metacyclic number field of degree pq.
(ii) In Section 3, we use class field theory and modular characters to construct the real metacylic number fields of degree pq. This construction is particularly convenient for computing relative class numbers of nonabelian normal CM-fields of degree $2pq$.
(iii) In Section 4, we explain how to compute efficiently the relative class number of a nonabelian normal CM-field of degree $2pq$.
(iv) In Section 5, we give lower bounds on the relative class numbers of the nonabelian normal CM-field of degree $2pq$.
(v) Finally, in Section 6, we use these results to prove Theorem 1.

Throughout this paper, we use the following notation. Let K be a number field. Then h_K, d_K, A_K, E_K, ω_K, $\zeta_K(s)$ and κ_K denote its class number, the absolute value of its discriminant, its ring of algebraic integers, its group of units, its number of complex roots of unity, its Dedekind zeta function and its residue at its simple pole $s = 1$, respectively. If K is a CM-field, K^+, h_K^- and $Q_K \in \{1, 2\}$ denote its maximal totally real subfield, its relative class number and its Hasse unit index (see Washington [Was, Chapter 4]). We let $\mathfrak{F}_{K/L}$ denote the finite part of the conductor of an abelian extension K/L and set $f_{K/L} = N_{L/\mathbb{Q}}(\mathfrak{F}_{K/L})$. Let $\mathfrak{F}$ be a nonzero integral ideal of a number field L. If $f\mathbb{Z} = \mathfrak{F} \cap \mathbf{Z}$, $f \geq 1$, then Image(E_L) and Image($\mathbb{Z}$) denote the images of E_L and $\{n \in \mathbb{Z} \mid \gcd(n, f) = 1\}$ in the multiplicative group $(A_L/\mathfrak{F})^*$. As a shorthand, we call them the images of E_L and $\mathbb{Z}$ in $(A_L/\mathfrak{F})^*$. This latter image is isomorphic to the multiplicative group $(\mathbb{Z}/f\mathbb{Z})^*$.

2. The nonabelian normal CM-fields of degree $2pq$

Let N_{2pq} be a nonabelian normal CM-field of degree $2pq$ and Galois group G. Since the complex conjugation is in the center $Z(G)$ of G (see Louboutin, Okazaki and Olivier [LOO, Lemma 2]), N_{2pq}^+ is a real normal number field of degree pq. If its Galois group G^+ were Abelian, then it would be cyclic, hence $G/Z(G)$ would also be cyclic and G would be Abelian. This is a contradiction. Therefore, q divides $p-1$, that is, $p \equiv 1 \bmod 2q$, and G^+ is isomorphic to the Frobenius nonabelian group of order pq: $\langle a, b;\, a^p = b^q = 1,\ bab^{-1} = a^s\rangle$, where $s \not\equiv 1 \bmod p$ and $s^q \equiv 1 \bmod p$. A nonabelian normal number field of Galois group isomorphic to a Frobenius group will be referred to as *a metacyclic number field*. Now, let n_p denote the number of p-Sylow subgroups of G. Since $n_p \equiv 1 \bmod p$ and n_p divides $2pq$, it follows that $n_p = 1$ (for $p > 2q$). Hence, N_{2pq} contains an imaginary cyclic subfield $K_{2q} = K_{2q}^+ k_2$

of degree $2q$, where K_{2q}^+ is a real cyclic number field of degree q and k_2 is an imaginary quadratic number field. Hence, we have the following result.

PROPOSITION 2. *Let $p > q \geq 3$ be two distinct odd primes. If N_{2pq} is a nonabelian normal CM-field of degree $2pq$, then $p \equiv 1 \bmod 2q$, N_{2pq}^+ is a real metacyclic number field of degree pq, $N_{2pq} = N_{2pq}^+ k_2$ is a compositum of N_{2pq}^+ and an imaginary quadratic number field k_2 and we have the following lattice of subfields.*

$$\begin{tikzcd}[arrows=dash]
 & N_{2pq} \arrow[dl, "2"'] \arrow[d] \\
N_{2pq}^+ \arrow[d, "p"'] & K_{2q} \arrow[dl, "2"'] \arrow[d] \\
K_{2q}^+ \arrow[d, "q"'] & k_2 \arrow[dl, "2"'] \\
\mathbb{Q} &
\end{tikzcd}$$

N_{2pq}/K_{2q}^+ cyclic of degree $2p$,

$K_{2q}/\mathbb{Q}$ cyclic of degree $2q$,

$N_{2pq}^+/\mathbb{Q}$ metacyclic of degree pq,

K_{2q}^+ and N_{2pq}^+ normal and totally real,

N_{2pq}, K_{2q} and k_2 totally imaginary.

Conversely, if $p \equiv 1 \bmod 2q$, if N_{2pq}^+ is a real metacyclic number field of degree pq and if k_2 is an imaginary quadratic number field, then their compositum $N_{2pq} = N_{2pq}^+ k_2$ is a nonabelian normal CM-field of degree $2pq$.

Moreover, in that situation $Q_{N_{2pq}} = Q_{K_{2q}} = 1$, $\omega_{N_{2pq}} = \omega_{K_{2q}}$, for K_{2q} is the maximal Abelian subfield of N_{2pq}, $h_{k_2} = h_{k_2}^-$ divides $h_{K_{2q}}^-$, and $h_{K_{2q}}^-$ divides $h_{N_{2pq}}^-$, by Louboutin, Okazaki and Olivier [LOO, Theorem 5]. Hence, if $h_{N_{2pq}}^- \leq 4$, then $h_{K_{2q}}^- \leq 4$. By Park and Kwon [PK97, Theorem 2] and Chang and Kwon [CK98, Theorem 1], there are 89 such K_{2q}, those listed in the first column of Tables 1 and 2.

3. The metacyclic number fields of degree pq

We use class field theory and modular characters to construct the metacyclic fields of degree pq. This construction is particularly convenient for computing relative class numbers of nonabelian normal CM-fields of degree $2pq$. We adopt the notation of Cox [Cox, Ch. 2] and Louboutin, Park and Lefeuvre [LPL, Section 2]. Let $\mathfrak{m}$ be an integral ideal of a real cyclic number field L of prime degree $q \geq 3$ (we will choose $L = K_{2q}^+$). Let $I_L(\mathfrak{m})$ be the group generated by the integral ideals of L prime to $\mathfrak{m}$. Let $P_L(\mathfrak{m})$ be its subgroup generated by the principal ideals (α) with $\alpha \equiv 1 \bmod \mathfrak{m}$. Let $P_{L,\mathbb{Z}}(\mathfrak{m})$ be the subgroup of $I_L(\mathfrak{m})$ generated by the principal ideals (α) such that $\alpha \equiv a \bmod \mathfrak{m}$ for some integer a coprime with $\mathfrak{m}$. The quotient group $Cl_{L,\mathbb{Z}}(\mathfrak{m}) = I_L(\mathfrak{m})/P_{L,\mathbb{Z}}(\mathfrak{m})$ is called the *ring class group* for $\mathfrak{m}$. Recall that if H is a congruence subgroup for $\mathfrak{m}$, that is, if H contains $P_L(\mathfrak{m})$, then there is a unique Abelian extension M/L, all of whose ramified primes divides $\mathfrak{m}$, such that $H = \ker(\Phi_{\mathfrak{m}})$, where $\Phi_{\mathfrak{m}} : I_L(\mathfrak{m}) \longrightarrow \mathrm{Gal}(M/L)$ is the Artin map of M/L (see

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

TABLE 1. The 80 imaginary cyclic sextic fields $K = K_{2q}$ with $q = 3$ and $h_K^- \leq 4$ (see Park and Kwon [PK97, Table 3]), possible p, upper bounds on $C_K(p)$ and possible $\mathfrak{F}_{N_{6p}^+/K^+}$ ($\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ are the prime ideals in K^+ lying above 7 and 13, respectively).

$(f, f_+, m; h_{K^+}, h_K^-)$	r_{tr}	$r_{i,r}$	p	$C_K(p)^{1/3}$	possible $\mathfrak{F}_{N_{6p}^+/K^+}$
(7,7,7;1,1)	7_{tr}		7	29	$(2\cdot 7)$
(9,9,3;1,1)	3_{tr}		•		
(19,19,19;1,1)	19_{tr}		19	12	•
(21,7,3;1,1)		$3_{i,r}$	13	21	•
(28,7,4;1,1)		$2_{i,r}$	7	29	$(2\cdot 7)$, $(2\cdot 11)$
(36,9,4;1,1)		$2_{i,r}$	7	29	•
(39,13,3;1,1)		$3_{i,r}$	13	17	•
(43,43,43;1,1)	43_{tr}		43	18	•
(56,7,8;1,1)		$2_{i,r}$	7	28	$(2\cdot 7)$
(63,9,7;1,1)		$7_{i,r}$	7	29	•
			19	18	•
(63,63,3;3,1)	3_{tr}		•		
(63,63,3;3,1)	3_{tr}		•		
(63,63,7;3,1)	7_{tr}		7	16	•
(67,67,67;1,1)	67_{tr}		67	9	•
(76,19,4;1,1)		$2_{i,r}$	7	18	•
(77,7,11;1,1)		$11_{i,r}$	7	26	$(2\cdot 11)$
			19	17	•
(91,13,7;1,1)		$7_{i,r}$	7	24	•
			19	15	•
(91,91,7;3,1)	7_{tr}		7	15	•
(93,31,3;1,1)		$3_{i,r}$	13	27	•
(104,13,8;1,1)		$2_{i,r}$	7	23	•
(117,117,3;3,1)	3_{tr}		•		
(129,43,3;1,1)		$3_{i,r}$	13	23	•
(133,133,7;3,1)	7_{tr}		7	11	•
(171,171,19;3,1)	19_{tr}		19	12	•
(217,217,7;3,1)	7_{tr}		7	11	$\mathfrak{p}_7^2$
(247,247,19;3,1)	19_{tr}		19	14	•
(35,7,35;1,2)	7_{tr}	$5_{i,r}$	•		
(45,9,15;1,2)	3_{tr}		•		
(52,13,52;1,2)	13_{tr}	$2_{i,r}$	•		
(72,9,24;1,2)	3_{tr}		•		
(91,91,91;3,2)	7_{tr}, 13_{tr}		•		
(91,91,91;3,2)	7_{tr}, 13_{tr}		•		
(105,7,15;1,2)		$3_{i,r}$, $5_{i,r}$	•		
(52,13,4;1,3)		$2_{i,r}$	7	24	•
(57,19,3;1,3)		$3_{i,r}$	13	13	•
(72,9,8;1,3)		$2_{i,r}$	7	28	•
(99,9,11;1,3)		$11_{i,r}$	7	26	•
			19	18	•
(111,37,3;1,3)		$3_{i,r}$	13	8	•

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

TABLE 1. Continued.

$(f, f_+, m; h_{K^+}, h_K^-)$	r_{tr}	$r_{i,r}$	p	$C_K(p)^{1/3}$	possible $\mathfrak{F}_{N_{6p}^+/K^+}$
(133,133,19;3,3)	19_{tr}		19	15	•
(133,133,19;3,3)	19_{tr}		19	7	•
(133,7,19;1,3)		$19_{i,r}$	19	17	•
			127	14	•
(148,37,4;1,3)		$2_{i,r}$	7	10	•
(152,19,8;1,3)		$2_{i,r}$	7	17	•
(171,171,3;3,3)	3_{tr}		•		
(171,171,3;3,3)	3_{tr}		•		
(244,61,4;1,3)		$2_{i,r}$	7	14	•
(259,259,7;3,3)	7_{tr}		7	5	$\mathfrak{p}_7^2$
(273,91,3;3,3)		$3_{i,r}$	13	15	•
(292,73,4;1,3)		$2_{i,r}$	7	14	(2)
(301,301,7;3,3)	7_{tr}		7	6	•
(301,301,7;3,3)	7_{tr}		7	5	•
(327,109,3;1,3)		$3_{i,r}$	13	13	•
(333,333,3;3,3)	3_{tr}		•		
(341,31,11;1,3)		$11_{i,r}$	7	35	•
			19	23	(11)
(364,91,4;3,3)		$2_{i,r}$	7	12	$(2)\mathfrak{p}_7^2$
(381,127,3;1,3)		$3_{i,r}$	13	15	•
(399,133,3;3,3)		$3_{i,r}$	13	16	•
(469,67,7;1,3)		$7_{i,r}$	7	16	•
			19	11	•
(553,553,7;3,3)	7_{tr}		7	6	•
(657,657,3;9,3)	3_{tr}		•		
(39,13,39;1,4)	13_{tr}		13	17	$(3)\mathfrak{p}_{13}^2$
(56,7,56;1,4)	7_{tr}		7	24	$(2 \cdot 7)$
(84,7,84;1,4)	7_{tr}	$3_{i,r}$	•		
(117,9,39;1,4)	3_{tr}		•		
(117,117,39;3,4)	3_{tr}		•		
(124,31,4;1,4)					
(133,19,7;1,4)					
(155,31,155;1,4)	31_{tr}		31	20	•
(163,163,163;4,4)	163_{tr}		163	4	•
(171,9,19;1,4)					
(172,43,4;1,4)					
(183,61,3;1,4)					
(201,67,3;1,4)					
(209,19,11;1,4)					
(248,31,8;1,4)					
(252,63,4;3,4)					
(259,259,259;3,4)	7_{tr}, 37_{tr}		•		
(473,43,11;1,4)					
(511,73,7;1,4)					
(711,711,3;12,4)	3_{tr}		•		

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

Cox [Cox, Theorem 8.6]). If M is metacyclic of degree pq containing L (we will choose $M = N_{2pq}^{+}$ and $L = K_{2q}^{+}$), then $\mathfrak{F}_{M/L}$ is invariant under the action of $\mathrm{Gal}(L/\mathbb{Q})$ and $\ker \Phi_{\mathfrak{F}_{M/L}}$ is a subgroup of index p of $I_L(\mathfrak{F}_{M/L})$ containing $P_{L,\mathbb{Z}}(\mathfrak{F}_{M/L})$ (see Louboutin, Park and Lefeuvre [LPL, proof of Proposition 1]). Conversely, if $\mathfrak{m}$ is invariant under the action of $\mathrm{Gal}(L/\mathbb{Q})$ and if H is a subgroup of index p of $I_L(\mathfrak{m})$ containing $P_{L,\mathbb{Z}}(\mathfrak{m})$ and invariant under the action of $\mathrm{Gal}(L/\mathbb{Q})$, then its associated field M is a normal, of degree pq and $\mathfrak{F}_{M/L}$ divides $\mathfrak{m}$.

PROPOSITION 3 (See Louboutin, Park and Lefeuvre [LPL, Theorem 2]). *Let $\mathfrak{m}$ be a given ideal of L invariant under the action of $\mathrm{Gal}(L/\mathbb{Q})$. There is a bijective correspondence between the metacyclic number fields M of degree pq containing L with $\mathfrak{F}_{M/L} = \mathfrak{m}$ and the groups of order p generated by the primitive characters χ of order p on the ring class group $Cl_{L,\mathbb{Z}}(\mathfrak{m})$ with $\chi \circ b = \chi^s$.*

PROOF. Let $\mathfrak{I}$ be a nonzero integral ideal of L coprime with the conductor of χ. We have $\Phi_{\mathfrak{m}}(\mathfrak{I}) \in \mathrm{Gal}(M/L)$. Hence,

$$\Phi_{\mathfrak{m}}(b(\mathfrak{I})) = b\Phi_{\mathfrak{m}}(\mathfrak{I})b^{-1} = (\Phi_{\mathfrak{m}}(\mathfrak{I}))^s = \Phi_{\mathfrak{m}}(\mathfrak{I}^s),$$

$b(\mathfrak{I})\mathfrak{I}^{-s} \in \ker \Phi_{\mathfrak{m}}$ and $\chi(b(\mathfrak{I})\mathfrak{I}^{-s}) = +1$. □

Let χ be a character on $Cl_{L,\mathbb{Z}}(\mathfrak{m})$. The *modular character* χ_0 on the multiplicative group $(A_L/\mathfrak{m})^*$ associated with χ is defined by $\chi_0(\alpha) = \chi((\alpha))$, and χ is primitive if and only if χ_0 is primitive. In particular, as in Louboutin, Park and Lefeuvre [LPL, Lemma 3], if $\mathfrak{F}$ is a given ideal of L invariant under the action of $\mathrm{Gal}(L/\mathbb{Q})$ and if there exists a metacyclic number field M of degree pq containing L with $\mathfrak{F}_{M/L} = \mathfrak{F}$, then there exists a primitive modular character χ_0 of order p on $(A_L/\mathfrak{F})^*$ which is trivial on the images of $\mathbb{Z}$ and the group of units E_L of L. Therefore, as in Louboutin, Park and Lefeuvre [LPL, Theorem 6], we obtain the following result.

PROPOSITION 4. *Let f_L denote the conductor of L. For a prime r, set*

$$\Pi_L(r) = \begin{cases} r^{q-1} & \text{if } r \text{ is ramified in } L,\\ (r-1)^{q-1} & \text{if } r \text{ splits in } L,\\ (r^q-1)/(r-1) & \text{if } r \text{ is inert in } L. \end{cases}$$

(1) *If p does not divide f_L, then $\mathfrak{F}_{M/L} = (p^a)\prod_{j=1}^{m}(r_j)$ with $a = 0$ or 2. If p divides f_L, then $\mathfrak{F}_{M/L} = \mathfrak{p}^a\prod_{j=1}^{m}(r_j)$ with $a = 0$ or $2 \le a \le q$, where $(p) = \mathfrak{p}^q$ in L. Here, the r_j are distinct primes not equal to p which satisfy $\Pi_L(r_j) \equiv 0 \bmod p$.*

(2) *Conversely, let $\mathfrak{F}$ be an ideal as in the previous point. Set*

$$f = p^b\prod_{j=1}^{m} r_j \quad \text{with } b = \begin{cases} a & \text{if } p \nmid f_L,\\ 0 & \text{if } p \mid f_L \text{ and } a = 0,\\ 1 & \text{if } p \mid f_L \text{ and } 2 \le a \le q; \end{cases}$$

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

and

$$N_L(\mathfrak{F}) = \begin{cases} p^{q-1}\Pi_L(p) & \text{if } p \nmid f_L \text{ and } a = 2, \\ p^{a-1} & \text{if } p \mid f_L \text{ and } 2 \le a \le q, \\ 1 & \text{if } a = 0. \end{cases}$$

Then $\mathfrak{F} \cap \mathbb{Z} = f\mathbb{Z}$ and $(A_L/\mathfrak{F})^*/(\mathbb{Z}/f\mathbb{Z})^*$ is of order $N_L(\mathfrak{F}) \prod_{j=1}^{s} \Pi_L(r_j)$. Let $n_L(\mathfrak{F})$ be the order of the image of E_L in $(A_L/\mathfrak{F})^*/(\mathbb{Z}/f\mathbb{Z})^*$. If there exists a metacyclic number field M of degree pq containing L with $\mathfrak{F}_{M/L} = \mathfrak{F}$, then p divides the positive integer

$$i_L(\mathfrak{F}) := \frac{N_L(\mathfrak{F})}{n_L(\mathfrak{F})} \prod_{j=1}^{m} \Pi_L(r_j). \tag{1}$$

PROOF. (1) Let M be a metacyclic number field of degree pq containing L with

$$\mathfrak{F}_{M/L} = \prod \mathfrak{R}_j^{e_j},$$

$e_j \ge 1$. According to Kwon and Martinet [KM], $e_j = 1$ if $\mathfrak{R}_j$ does not divide p, $e_j = 2$ if $\mathfrak{R}_j$ divides p but p does not divide f_L, and $2 \le e_j \le q$ if $\mathfrak{R}_j$ divides p and p divides f_L. Moreover, if a prime $r \ne p$ is ramified in the extension M/L, then there exists a primitive character of order p on $(A_L/(r))^*$ which is trivial on the image of $\mathbb{Z}$, hence $|(A_L/(r))^*/\operatorname{Image}(\mathbb{Z})| = \Pi_L(r) \equiv 0 \bmod p$ (see Louboutin, Park and Lefeuvre [LPL, Lemma 5. (1)]).

(2) The second part can be easily proved in a similar way to Louboutin, Park and Lefeuvre [LPL, Theorem 6]. □

We now discuss the primitive modular characters.

PROPOSITION 5. *Let ϕ be a primitive character of order p on $(A_L/\mathfrak{F})^*$ which is trivial on the image of $\mathbb{Z}$. Let σ be a generator of* Gal$(L/\mathbb{Q})$. *Let Z_m denote the additive cyclic group $\mathbb{Z}/m\mathbb{Z}$ of order $m \ge 1$. Let r be a prime.*

(1) *If $\mathfrak{F} = (r) = \mathfrak{r}_1\mathfrak{r}_2 \cdots \mathfrak{r}_q$ splits in L, with $r \equiv 1 \bmod p$, and if $\phi \circ \sigma = \phi^s$ for some s of order $q \bmod p$, then there exists a character ψ of order p on the cyclic group $(A_L/\mathfrak{r}_1)^*$ of order $r-1$ such that for any $\alpha \in A_L$ coprime with (r) we have $\phi(\alpha) = \prod_{j=0}^{q-1} \psi^{s^j}(\sigma^{q-j}(\alpha))$.*

(2) *If $\mathfrak{F} = (r)$ is inert in L, $r^q \equiv 1 \bmod p$ and $r \not\equiv 1 \bmod p$, then any primitive character ϕ of order p on $(A_L/(r))^*$ is trivial on the image of $\mathbb{Z}$ and may be constructed as a character of order p on the cyclic factor group $(A_L/(r))^*/B$ of order p, where B is the subgroup of order $(r^q-1)/p$ of $(A_L/(r))^*$.*

(3) *If $\mathfrak{F} = (p^2)$ and $(p) = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_q$ splits in L and if $\phi \circ \sigma = \phi^s$ for some s of order $q \bmod p$, then there exists a character ψ of order p on the cyclic group $(A_L/\mathfrak{p}_1^2)^*$ of order $p(p-1)$ such that for any $\alpha \in A_L$ coprime with (p) we have $\phi(\alpha) = \prod_{j=0}^{q-1} \psi^{s^j}(\sigma^{q-j}(\alpha))$.*

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

(4) *If $\mathfrak{F}=(p^2)$ and (p) is inert in L, then $(A_L/(p^2))^*$ is isomorphic to $Z_{p^q-1}\times Z_p^q$ and $(A_L/(p^2))^*/\,\mathrm{Image}(\mathbb{Z})$ is isomorphic to $Z_{(p^q-1)/(p-1)}\times Z_p^{q-1}$. Moreover, suppose that $a\in(A_L/(p^2))^*/\,\mathrm{Image}(\mathbb{Z})$ of order $(p^q-1)/(p-1)$ and $b_1,\ldots,b_{q-1}\in(A_L/(p^2))^*/\,\mathrm{Image}(\mathbb{Z})$ of order p are such that $a,b_1,\ldots,b_{q-1}$ generate $(A_L/(p^2))^*/\,\mathrm{Image}(\mathbb{Z})$. Then for any $\alpha\in A_L$ coprime with (p) with $\alpha\equiv a^i b_1^{j_1}\cdots b_{q-1}^{j_{q-1}} \bmod p^2$, we have $\phi(\alpha)=\zeta_p^{k_1j_1+\cdots+k_{q-1}j_{q-1}}$ for some integers $k_1,\ldots,k_{q-1}$.*

(5) *If $\mathfrak{F}=\mathfrak{p}^e$ and $(p)=\mathfrak{p}^q$ is ramified in L, then $(A_L/\mathfrak{p}^e)^*$ with $2\le e\le q$ is isomorphic to $Z_{p-1}\times Z_p^{e-1}$ and $(A_L/\mathfrak{p}^e)^*/\,\mathrm{Image}(\mathbb{Z})$ is isomorphic to Z_p^{e-1}. Then any primitive character of order p on $(A_L/\mathfrak{p}^e)^*$ is trivial on the image of $\mathbb{Z}$. Let $a\in(A_L/\mathfrak{p}^e)^*$ of order $p-1$ and $b_1,\ldots,b_{e-1}\in(A_L/\mathfrak{p}^e)^*$ of order p be such that $a,b_1,\ldots,b_{e-1}$ generate $(A_L/\mathfrak{p}^e)^*$. Then for any $\alpha\in A_L$ coprime with (p) with $\alpha\equiv a^i b_1^{j_1}\cdots b_{e-1}^{j_{e-1}} \bmod p$, we have $\phi(\alpha)=\zeta_p^{k_1j_1+\cdots+k_{e-1}j_{e-1}}$ for some integers $k_1,\ldots,k_{e-1}$.*

PROOF. The proof of (1) is as follows . We may assume that $\mathfrak{r}_j=\sigma^{j-1}(\mathfrak{r}_1)$ for $1\le j\le q$. Let $\phi=\prod_{j=1}^q\psi_j$ be the factorization of ϕ, where ψ_j is a character on $(A_L/\mathfrak{r}_j)^*$. Let $\lambda_1\in A_L$ satisfy $\lambda_1\equiv 1 \bmod \mathfrak{r}_1$ and $\lambda_1\equiv 0 \bmod \mathfrak{r}_j$ for $2\le j\le q$. Set $\lambda_j=\sigma^{j-1}(\lambda_1)$ for $1\le j\le q$. Then $\lambda_j\equiv 1 \bmod \mathfrak{r}_j$, and $\lambda_j\equiv 0 \bmod \mathfrak{r}_{j'}$ for $1\le j'\le q$ and $j'\ne j$. It follows that

$$\begin{aligned}\psi_j(\alpha)&=\phi(\lambda_1+\cdots+\lambda_{j-1}+\lambda_j\alpha+\lambda_{j+1}+\cdots+\lambda_q)\\&=\phi(\sigma^{j-1}(\lambda_1\sigma^{q+1-j}(\alpha)+\lambda_2+\cdots+\lambda_q))\\&=\phi^{s^{j-1}}(\lambda_1\sigma^{q+1-i}(\alpha)+\lambda_2+\cdots+\lambda_q)\\&=\psi_1^{s^{j-1}}(\sigma^{q+1-j}(\alpha))\end{aligned}$$

and

$$\phi(\alpha)=\prod_{j=1}^q\psi_j(\alpha)=\prod_{j=1}^q\psi_1^{s^{j-1}}(\sigma^{q+1-j}(\alpha)),$$

as claimed. The proofs of (2), (4) and (5) are clear. The proof of (3) is similar to that of (1). □

Let χ_0 be a primitive modular character of order p on $(A_L/\mathfrak{F})^*$. We can now construct the primitive characters χ of order p on $Cl_{L,\mathbb{Z}}(\mathfrak{F})$ and of associated modular character equal to χ_0 (see Louboutin, Park and Lefeuvre [LPL, Section 5]). In fact, in all the cases we will have to cope with, the class number $h=h_L$ of $L=K_{2q}^+$ will be relatively prime with p. Let $h^*\in\{1,\ldots,p-1\}$ be such that $hh^*\equiv 1 \bmod p$. For any integral ideal $\mathcal{I}$ of L there exists some $\alpha_{\mathcal{I}}\in A_L$ such that $\mathcal{I}^h=(\alpha_{\mathcal{I}})$, and we obtain

$$\chi(\mathcal{I})=\chi^{hh^*}(\mathcal{I})=\chi^{h^*}(\mathcal{I}^h)=\chi^{h^*}((\alpha_{\mathcal{I}}))=\chi_0^{h^*}(\alpha_{\mathcal{I}}).$$

In the 14 cases for which we will have to compute relative class numbers (see Table 3), we have $q=[L:\mathbb{Q}]=[K_{2q}^+:\mathbb{Q}]=3$ and the groups $(A_L/\mathfrak{F})^*/\langle\mathrm{Image}\ E_L,\ \mathrm{Image}\ \mathbb{Z}\rangle$

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

are cyclic of order p, which makes the required relative class number computations rather easy.

4. Computation of relative class numbers

Set $N = N_{2pq}$, $N^+ = N_{2pq}^+$, $K = K_{2q}$, $K^+ = K_{2q}^+$, and $k = k_2$. Let χ_+ be any one of the $p-1$ primitive Hecke characters of order p associated with the cyclic extension N^+/K^+ of degree p. Let χ_- be the primitive quadratic Hecke character associated with the quadratic extension K/K^+. Then $Q_N = Q_K = 1$, $w_N = w_K$, h_K^- divides h_N^- and

$$h_N^-/h_K^- = \prod_{j=1}^{p-1} 2^{-q} L(0,\, \chi_-\chi_+^j)$$

(use Louboutin [Lou01, (18)]), and $w_N L(0,\, \chi_-\chi_+^j) \in \mathbb{Z}[\zeta_p]$.

Let $\mathfrak{F}_\chi$ be the finite part of the conductor of $\chi = \chi_-\chi_+^j$. Set $f_\chi = N_{K^+/\mathbb{Q}}(\mathfrak{F}_\chi)$ and $A_\chi = \sqrt{d_{K^+} f_\chi/\pi^q}$. Let W_χ be the Artin root number associated to this L-series. Then we have the following absolutely convergent series expansion (see Louboutin [Lou01, Section 3]):

$$L(0,\, \chi) = \frac{A_\chi}{\pi^{q/2}} \left(W_\chi \sum_{n\geq 1} \frac{\overline{a_n(\chi)}}{n} K_{q,1}(n/A_\chi) + \sum_{n\geq 1} \frac{a_n(\chi)}{n} K_{q,2}(n/A_\chi) \right),$$

where $a_n(\chi) = \sum_{N_{K^+/\mathbb{Q}}(I)=n} \chi(I)$ and $0 \leq K_{q,2}(B) \leq K_{q,1}(B) \leq q e^{-B^{2/q}}$ for $B > 0$. We explained in Louboutin [Lou00] and [Lou01] how to use such series expansions to compute the exact value of $L(0,\, \chi) \in \mathbb{Q}(\zeta_p)$, numerical approximations to W_χ being computed by the technique developed in Louboutin [Lou00, Section 5, bottom of p. 388]. It remains to explain how we compute the $a_n(\chi)$. Since $n \mapsto a_n(\chi)$ is multiplicative, we are reduced to computing $a_{r^e}(\chi)$ for $e \geq 1$ and r a prime. Let $\mathfrak{r}$ be a prime ideal in K^+ lying above r. Then $\chi_-(\mathfrak{r}) = \chi_k(r) = (-d_k/r)$. Set $f_N = N_{K^+/\mathbb{Q}}(\mathfrak{F}_{\chi_-\chi_+})$. If $r \mid f_N$, then $a_{r^e}(\chi) = 0$. Otherwise we have the following lemma.

LEMMA 6. *Let r be a prime with* $\gcd(r,\, f_N) = 1$.

(1) *If (r) is inert in K^+, then (r) splits in N^+/K^+, $\chi_+(r) = 1$ and $a_{r^e}(\chi) = 0$ if $e \not\equiv 0 \bmod q$, and $a_{r^e}(\chi) = \chi_k(r)^{e/q}$ otherwise.*

(2) *If $(r) = \mathfrak{r}^q$ is ramified in K^+, then $\mathfrak{r}$ splits in N^+/K^+ and $a_{r^e}(\chi) = \chi_k(r)^e$.*

(3) *If $(r) = \mathfrak{r}\sigma(\mathfrak{r}) \cdots \sigma^{q-1}(\mathfrak{r})$ splits in K^+, then*

$$a_{r^e}(\chi) = \chi_k(r)^e \sum_{a_1+a_2+\cdots+a_q=e} \chi_+(\mathfrak{r})^{a_1+sa_2+\cdots+s^{q-1}a_q}.$$

PROOF. For (3), use $\chi_+ \circ \sigma = \chi_+^s$. □

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

PROPOSITION 7. *Let $K_{(p-1)/q}(p)$ be the subfield of degree $(p-1)/q$ of the cyclotomic field $\mathbb{Q}(\zeta_p)$. Then $L(0, \chi_-\chi_+^j) \in K_{(p-1)/q}(p)$ for $1 \le j \le p-1$, and $h^-_{N_{2pq}}/h^-_{K_{2q}} = (h^-_{N_{2pq}/K_{2q}})^q$ is a perfect qth power, where*

$$h^-_{N_{2pq}/K_{2q}} = N_{K_{(p-1)/q}(p)/\mathbb{Q}}(2^{-q}L(0, \chi_-\chi_+)).$$

Thus, for $q = 3$ and $p = 7$, we have $L(0, \chi_-\chi_+) \in \mathbb{Q}(\sqrt{-7})$ and $h^-_{N_{42}}/h^-_{K_6} = (h^-_{N_{42}/K_6})^3$ is a perfect cube, with $h^-_{N_{42}/K_6} = |2^{-3}L(0, \chi_-\chi_+)|^2$.

PROOF. Since $\chi_+ \circ b = \chi_+^s$ and $\chi_- \circ b = \chi_-$, we have $(\chi_-\chi_+^j) \circ b^l = \chi_-\chi_+^{js^l}$, which implies $a_n(\chi_-\chi_+^j) = a_n(\chi_-\chi_+^{js^l})$ and $L(0, \chi_-\chi_+^j) = L(0, \chi_-\chi_+^{js^l})$, that is, $L(0, \chi_-\chi_+^j) = L(0, \chi_-\chi_+^{j'})$ as soon as $j' = j$ in $(\mathbb{Z}/p\mathbb{Z})^*/\langle s\rangle$. Now, $L(0, \chi_-\chi_+^j) \in \mathbb{Q}(\zeta_p)$, by Siegel–Klingen's Theorem (see Hida [Hid, Corollary 1 p. 57]), and for $\sigma_l \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that $\sigma_l(\zeta_p) = \zeta_p^l$, we have $\sigma_l(a_n(\chi_-\chi_+^j)) = a_n(\chi_-\chi_+^{jl})$, hence $\sigma_l(L(0, \chi_-\chi_+^j)) = L(0, \chi_-\chi_+^{jl})$ and $L(0, \chi_-\chi_+^j) \in K_{(p-1)/q}(p)$, the subfield of $\mathbb{Q}(\zeta_p)$ fixed by $\langle s\rangle$. $\square$

5. Upper bounds on discriminants

We have

$$h_N^- = \frac{Q_N\omega_N}{(2\pi)^{pq}}\sqrt{\frac{d_N}{d_{N^+}}}\frac{\kappa_N}{\kappa_{N^+}} = \frac{\omega_K}{(2\pi)^{pq}}\sqrt{\frac{d_N}{d_{N^+}}}\frac{\kappa_N}{\kappa_{N^+}} \tag{2}$$

(see Washington [Was] and use Proposition 2). Let χ_K be any one of the $q-1$ primitive Dirichlet characters of order $2q$ associated with K. Let $\chi_{N/K}$ be any one of the $p-1$ primitive Hecke characters of order p associated with the cyclic extension N/K of degree p. For $0 < s < 1$, we have

$$\zeta_N(s) = \zeta_K(s)\prod_{j=1}^{p-1} L(s, \chi_{N/K}^j) = \zeta_K(s)\prod_{j=1}^{(p-1)/2} |L(s, \chi_{N/K}^j)|^2$$

and

$$\zeta_K(s) = \zeta_k(s)\prod_{j=1}^{(q-1)/2} |L(s, \chi_K^j)|^2.$$

By Proposition 2, if $h_N^- \le 4$, then $h_k^- \le 4$. Hence, $\zeta_k(s) < 0$ for $0 < s < 1$, by Watkins [Wat1] and [Wat2], which implies $\zeta_N(s) \le 0$ for $0 < s < 1$ and

$$\kappa_N \ge 2/(e \log d_N), \tag{3}$$

provided that $d_N^{1/2pq} \ge 2\pi^2$ (by Louboutin [Lou03, Theorem 1]). By Louboutin [Lou98, Corollary 2 and Theorem 11], for a given K^+ there exists a computable

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

constant μ_{K^+} such that for any N^+ containing K^+ we have

$$\kappa_{N^+} \le \kappa_{K^+}^p (\log(f_{N^+/K^+}) + 4\mu_{K^+})^{p-1}/2^{p-1}, \tag{4}$$

for $d_{N^+}/d_{K^+}^p = f_{N^+/K^+}^{p-1}$. Note that $d_N = d_{K^+}^{2p} f_{N^+/K^+}^{2(p-1)} f_{N/N^+}$ and

$$f_{N/N^+} = f_{K/K^+} \times \gcd(f_{N/K^+}, f_{N^+/K^+})^{p-1} \ge f_{K/K^+}.$$

Using (2), (3) and (4) and noticing that $d_N \mapsto \sqrt{d_N}/\log d_N$ increases with $d_N \ge d_{K^+}^{2p} f_{N^+/K^+}^{2(p-1)} f_{K/K^+} \ge e^2$, we have proved that if $h_N^- \le 4$, then

$$e \ge \frac{2^{p-2}\omega_K \sqrt{d_{K^+}^p f_{N^+/K^+}^{p-1} f_{K/K^+}}}{(2\pi)^{pq}(\log(f_{N^+/K^+}) + 4\mu_{K^+})^{p-1}\kappa_{K^+}^p \log(d_{K^+}^{2p} f_{N^+/K^+}^{2(p-1)} f_{K/K^+})}. \tag{5}$$

6. Proof of Theorem 1

Assume that $h_N^- \le 4$. Then $h_K^- \le 4$. By Park and Kwon [PK97, Theorem 2] and Chang and Kwon [CK98, Theorem 1], there are 89 such K, those listed in the first column of Table 1 (in accordance with the notation in Park and Kwon [PK97] and Chang and Kwon [CK98], we set $f = f_K = f_{K_{2q}}$, $f_+ = f_{K^+} = f_{K_{2q}^+}$ and $m = f_k = f_{k_2}$). We will use Proposition 8 below to exclude 22 of these 89 fields K (those with a • in the fourth column of Table 1) and to show that for 56 of the remaining 67 fields K we know beforehand the possible values of p (see the fourth column of Table 1).

PROPOSITION 8. *Let N be a nonabelian normal CM-field of degree $2pq$, K its subfield of degree $2q$ and k its quadratic subfield. Let r be a prime.*

(1) *If $r = r_{tr} \ne p$ is totally ramified in K, then $\mathfrak{r}$ splits completely in N^+/K^+ and $2^{p-1} \mid h_N^-$, where $\mathfrak{r}^q = rA_{K^+}$.*
(2) *Assume that $r = r_{i,r} \ne p$ is inert in K^+ and ramified in k. Then either (r) splits in N^+/K^+ and $2^{p-1} \mid h_N^-$, or (r) is ramified in N^+/K^+ and $r^q \equiv 1 \bmod p$.*

PROOF. Use Proposition 4 and Louboutin and Okazaki [LO94, Proposition 2]. □

PROPOSITION 9. *Let N be a nonabelian normal CM-field of degree $6p$, K its sextic subfield and k its quadratic subfield. Let r be a prime. Assume that $K \ne \mathbb{Q}(\zeta_7)$ or $p \ne 7$. If r splits in k and if the prime ideals lying above r in K^+ are ramified in N^+/K^+, then $p \mid h_N^-$.*

PROOF. Use Louboutin, Okazaki and Olivier [LOO, Proposition 8]. □

(A) First, assume that some prime r_{tr} is totally ramified in K (there are 46 such K). We must have $p = r_{tr}$, by point (1) of Proposition 8. Hence, at most one prime can be totally ramified in K, which rules out three fields K. We must also have $r_{tr} = p \ge 2q + 1$, which rules out 15 more fields K. Finally, if some other prime

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

TABLE 2. The nine imaginary cyclic fields $K = K_{2q}$ with $q > 3$ and $h_K^- \leq 4$ (see Chang and Kwon [CK98, Table I]).

$(q;\ f,\ f_+, m;\ h_{K^+}, h_K^-)$	r_{tr}	$r_{i,r}$	p	$C_K(p)^{1/q}$
(5;11,11,11;1,1)	11_{tr}		11	9
(5;31,31,31;1,3)	31_{tr}		31	5
(5;33,11,3;1,1)		$3_{i,r}$	11	9
(5;44,11,4;1,1)		$2_{i,r}$	31	8
(5;55,11,55;1,4)	11_{tr}		11	9
(5;75,25,15;1,2)	5_{tr}		•	
(7;43,43,43;1,1)	43_{tr}		43	3
(7;49,49,7;1,1)	7_{tr}		•	
(11;23,23,23;1,3)	23_{tr}		23	3

TABLE 3. For $q = 3$, possible values of p and $\mathfrak{F}_{N_{6p}^+/K^+}$.

$(f,\ f_+, m;\ h_{K^+}, h_K^-)$	$p = 7$ $C_K(7)^{1/3}$	$p = 13$ $C_K(13)^{1/3}$	$p = 19$ $C_K(19)^{1/3}$	$p \geq 31$ $C_K(p)^{1/3}$	Possible $(\mathfrak{F}_{N_{6p}^+/K^+}, p)$
(124,31,4;1,4)	39	27	23	21	((11), 19)
(133,19,7;1,4)	17	13	12	11	
(171,9,19;1,4)	23	18	17	16	
(172,43,4;1,4)	33	23	20	18	
(183,61,3;1,4)	14	11	10	9	
(201,67,3;1,4)	16	12	11	10	((11), 7)
(209,19,11;1,4)	16	12	11	10	
(248,31,8;1,4)	37	26	23	21	
(252,63,4;3,4)	32	22	20	18	
(473,43,11;1,4)	30	22	20	18	
(511,73,7;1,4)	14	11	10	9	

$r_{i,r}$ is inert in K^+ and ramified in k, then r_{tr} must divide $r_{i,r}^q - 1$, by point (2) of Proposition 8, which rules out three more fields K.

(B) Second, in the case that $(f, f_+, m, h_{K^+}, h_K^-) = (105, 7, 15; 1, 2)$, the primes $r_{i,r} = 3$ and $r_{i,r} = 5$ are both inert in K^+ and ramified in k_2. By point (2) of Proposition 8, p must divide $3^3 - 1$ and $5^3 - 1$, which is a contradiction. Hence, this K is ruled out, and we have ruled out 22 fields K.

(C) Among the 67 (that is, $89 - 22$) remaining K, there are 25 fields K for which some prime r_{tr} is totally ramified in K, in which case $p = r_{tr}$, by point (1) of Proposition 8, and 31 fields K for which some prime $r_{i,r}$ is inert in K^+ and ramified in k, in which case p divides $r_{i,r}^q - 1$, by point (2) of Proposition 8. Hence, for these

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

TABLE 4. The fields $N = N_{6p}$ of degree $6p$ ($\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ are the prime ideals in K^+ lying above 7 and 13, respectively).

$(f, f_+, m; h_{K^+}, h_K^-)$	p	$\mathfrak{F}_{N^+/K^+}$	$2^{-3}L(0, \chi_-\chi_+)$	h_N^-
(7,7,7;1,1)	7	$(2\cdot 7)$	$-(1+\sqrt{-7})/2$	2^3
(28,7,4;1,1)	7	$(2\cdot 7)$	$(1-3\sqrt{-7})/2$	2^{12}
(28,7,4;1,1)	7	$(2\cdot 11)$	$4-2\sqrt{-7}$	$(2^2\cdot 11)^3$
(56,7,8;1,1)	7	$(2\cdot 7)$	$-(5+9\sqrt{-7})/2$	$(2^2\cdot 37)^3$
(77,7,11;1,1)	7	$(2\cdot 11)$	$1+\sqrt{-7}$	2^9
(217,217,7;3,1)	7	$\mathfrak{p}_7^2$	$(1-7\sqrt{-7})/2$	$(2\cdot 43)^3$
(259,259,7;3,3)	7	$\mathfrak{p}_7^2$	$(3-7\sqrt{-7})/2$	$3\cdot(2^3\cdot 11)^3$
(292,73,4;1,3)	7	(2)	$(5-\sqrt{-7})/2$	$3\cdot 2^9$
(341,31,11;1,3)	19	(11)	$\zeta_{19}^2+\zeta_{19}^3+2\zeta_{19}^4+4\zeta_{19}^5$ $+2\zeta_{19}^6+3\zeta_{19}^8+2\zeta_{19}^9+3\zeta_{19}^{12}$ $+\zeta_{19}^{14}+4\zeta_{19}^{16}+4\zeta_{19}^{17}+3\zeta_{19}^{18}$	$3\cdot(11\cdot 1907)^3$
(364,91,4;3,3)	7	$(2)\mathfrak{p}_7^2$	$19-3\sqrt{-7}$	$3\cdot(2^3\cdot 53)^3$
(39,13,39;1,4)	13	$(3)\mathfrak{p}_{13}^2$	$-3\zeta_{13}-\zeta_{13}^2-3\zeta_{13}^3-\zeta_{13}^4$ $-\zeta_{13}^5-\zeta_{13}^6-3\zeta_{13}^7-3\zeta_{13}^8$ $-3\zeta_{13}^9-\zeta_{13}^{10}-3\zeta_{13}^{11}-\zeta_{13}^{12}$	$4\cdot(3\cdot 79)^3$
(56,7,56;1,4)	7	$(2\cdot 7)$	$(25+\sqrt{-7})/2$	$4(2\cdot 79)^3$
(124,31,4;1,4)	19	(11)	$\zeta_{19}-8\zeta_{19}^2-8\zeta_{19}^3-19\zeta_{19}^4$ $+2\zeta_{19}^5-19\zeta_{19}^6+\zeta_{19}^7+2\zeta_{19}^8$ $-19\zeta_{19}^9-9\zeta_{19}^{10}+\zeta_{19}^{11}+2\zeta_{19}^{12}$ $-9\zeta_{19}^{13}-8\zeta_{19}^{14}-9\zeta_{19}^{15}+2\zeta_{19}^{16}$ $+2\zeta_{19}^{17}+2\zeta_{19}^{18}$	$4\cdot(7^2\cdot 11^3\cdot 22963)^3$
(201,67,3;1,4)	7	(11)	$(47+35\sqrt{-7})/2$	$4\cdot(2^3\cdot 337)^3$

$56 = 25 + 31$ fields K, the possible values for p are determined, and compiled in the fourth column of Table 1.

(D) For the remaining 11 (that is, $67 - 56$) fields K (those with an empty fourth column in Tables 1 and 2), we have $q = 3$, and we compute κ_{K^+} and μ_{K^+} and use (5) to obtain an upper bound on p, as compiled in Table 3.

For example, assume that some $N = N_{6p}$ with $h_N^- \le 4$ contains the field $K = K_6$ with $(f, f_+, m; h_{K^+}, h_K^-) = (171, 9, 19; 1, 4)$. Here, $\kappa_{K^+} = 0.377461\cdots$ and

$\mu_{K^+} = 0.303063\cdots$. We claim that $p \le 31$. Indeed, assume that $p > 31$. Then $1 < f_{N^+/K^+} \le 16^3$, by (5), and $f_{N^+/K^+} = r_{N^+/K^+}^3$ is a perfect cube, where $r_{N^+/K^+} > 1$ is square-free and coprime with 2, 3, 5, 7 and 11, by point (1) of Proposition 4 and since $p > 31$ cannot divide either $\Pi_{K^+}(2) = (2^3-1)/(2-1) = 7$, or $\Pi_{K^+}(3) = 3^2$, or $\Pi_{K^+}(5) = (5^3-1)/(5-1) = 31$, or $\Pi_{K^+}(7) = (7^3-1)/(7-1) = 57$, or $\Pi_{K^+}(11) = (11^3-1)/(11-1) = 7\cdot 19$ (we could also use the fact that if $r \in \{5, 7, 11\}$, then r splits in k, hence $r \nmid f_{N^+/K^+}$ by Proposition 9). Thus, $r_{N^+/K^+} = 13$ and we obtain a contradiction. Indeed, $A_{K^+} = \mathbb{Z}[\alpha]$, where $\alpha^3 - 3\alpha - 1 = 0$. Since $\alpha^{61} \equiv 3 \bmod (13)$, it follows that $\alpha \in E_{K^+}$ is of order 61 in the multiplicative group $(A_{K^+}/(13))^*/(\mathbb{Z}/13\mathbb{Z})^*$ of order $\Pi_{K^+}(13) = 3\cdot 61$, and $i_L((13))$ defined in (1) which divides $\Pi_{K^+}(13)/61 = 3$ cannot be divisible by $p \ge 31$.

(E) Fix K and p. Using (5), we compute $C_K(p)$ such that if $h_N^- \le 4$ then $f_{N^+/K^+} < C_K(p)$, as compiled in the fifth column in Tables 1, 2 and 3. Using Proposition 4, we find all the possible conductors $\mathfrak{F}_{N^+/K^+}$ with $1 < f_{N^+/K^+} < C_K(p)$ (since no prime $p > 3$ divides h_{K^+} when $h_K^- \le 4$, we cannot have $f_{N^+/K^+} = 1$). For $q > 3$, there is no possible such $\mathfrak{F}_{N^+/K^+}$. Using Proposition 5 and proceeding as in point (D), we find all the possible modular characters on a given $(A_L/\mathfrak{F}_{N^+/K^+})^*$, then all the possible primitive characters on $Cl_{K^+,\mathbb{Z}}(\mathfrak{F}_{N^+/K^+})$ of a given modular character. Finally, we compute h_N^- for the associated CM-fields N. For $q = 3$, we end up with 14 CM-fields N for which we must compute h_N^-. We used the series expansions for $K_{3,1}(B)$ and $K_{3,2}(B)$ given in Louboutin [Lou00, Theorem 17]. Our computational results are summarized in Table 4, which proves Theorem 1. The computations were carried out by using the PARI and KANT softwares (see [BBBCO] and [DFKPRSW]).

References

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, PARI-GP version 2.1.5, http://pari.math.u-bordeaux.fr.

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

[CK98] K.-Y. Chang and S.-H. Kwon, ‘Class number problem for imaginary cyclic number fields’, *J. Number Theory* **73** (1998), 318–338.

[CK00] ———, ‘Class numbers of imaginary abelian fields’, *Proc. Amer. Math. Soc.* **128** (2000), 2517–2528.

[CK02] ———, ‘The nonabelian CM-fields of degree 36 with class number one’, *Acta Arith.* **101** (2002), 53–61.

[Cox] D. A. Cox, ‘Primes of the form $x^2 + ny^2$’, in: *Fermat, Class Field Theory, and Complex Multiplication* (John Wiley & Sons, New York, 1989).

[DFKPRSW] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, ‘KANT V_4’, *J. Symbolic Comput.* **24** (1997), 267–283.

[Hid] H. Hida, *Elementary Theory of L-Functions and Eisenstein Series*, London Mathematical Society, Student Texts, 26 (Cambridge University Press, Cambridge, 1993).

[KM] S.-H. Kwon and J. Martinet, ‘Sur les corps résolubles de degré premier’, *J. Reine. Angew. Math.* **375** (1987), 12–23.

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

[Lef] Y. Lefeuvre, ‘Corps diédraux à multiplication complexe principaux’, *Ann. Inst. Fourier* **50** (2000), 67–103.

[LL] Y. Lefeuvre and S. Louboutin, ‘The class number one problem for the dihedral CM-fields’, in: *Algebraic Number Theory and Diophantine Analysis (Graz, 1998)* (de Gruyter, Berlin, 2000), pp. 249–275.

[Lou92] S. Louboutin, ‘Minoration au point 1 des fonctions L et détermination des corps sextiques abéliens totalement imaginaires principaux’, *Acta Arith.* **62** (1992), 109–124.

[Lou98] ———, ‘Upper Bounds on $|L(1, \chi)|$ and applications’, *Canad. J. Math.* **50** (1998), 794–815.

[Lou99] ———, ‘The class number one problem for the dihedral and dicyclic CM-fields’, *Colloq. Math.* **80** (1999), 259–265.

[Lou00] ———, ‘Computation of relative class numbers of CM-fields by using Hecke L-functions’, *Math. Comp.* **69** (2000), 371–393.

[Lou01] ———, ‘Computation of $L(0, \chi)$ and of relative class numbers of CM-fields’, *Nagoya Math. J.* **161** (2001), 171–191.

[Lou03] ———, ‘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.

[LO94] S. Louboutin and R. Okazaki, ‘Determination of all nonnormal quartic CM-fields and of all nonabelian normal octic CM-fields with class number one’, *Acta Arith.* **67** (1994), 47–62.

[LO98] ———, ‘The class number one problem for some nonabelian normal CM-fields of 2-power degrees’, *Proc. London Math. Soc.* **76** (1998), 523–548.

[LOO] S. Louboutin, R. Okazaki and M. Olivier, ‘The class number one problem for some nonabelian normal CM-fields’, *Trans. Amer. Math. Soc.* **349** (1997), 3657–3678.

[LPL] S. Louboutin, Y.-H. Park and Y. Lefeuvre, ‘Construction of the real dihedral number fields of degree $2p$. Applications’, *Acta Arith.* **89** (1999), 201–215.

[Odl] A. Odlyzko, ‘Some analytic estimates of class number and discriminants’, *Invent. Math.* **29** (1975), 275–286.

[Oka] R. Okazaki, ‘Inclusion of CM-fields and divisibility of relative class numbers’, *Acta Arith.* **92** (2000), 319–338.

[PK97] Y.-H. Park and S.-H. Kwon, ‘Determination of all imaginary abelian sextic number fields with class number ≤ 11’, *Acta Arith.* **82** (1997), 27–43.

[PK98] ———, ‘Determination of all nonquadratic imaginary cyclic number fields of 2-power degree with class number ≤ 20’, *Acta Arith.* **83** (1998), 211–223.

[PK07] S.-M. Park and S.-H. Kwon, ‘Class number one problem for normal CM-fields’, *J. Number Theory* **125** (2007), 59–84.

[Sta] H. Stark, ‘A complete determination of all complex quadratic fields of class number one’, *Michigan Mathematics J.* **14** (1967), 1–27.

[Was] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edn, Graduate Texts in Mathematics, 83 (Springer, Berlin, 1997).

[Wat1] M. Watkins, ‘Real zeros of real odd Dirichlet L-functions’, *Math. Comp.* **73** (2004), 415–423.

[Wat2] ———, ‘Class numbers of imaginary quadratic fields’, *Math. Comp.* **73** (2004), 907–938.

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

S.-H. KWON, Department of Mathematics Education, Korea University, 136-701, Seoul, Korea
e-mail: sounhikwon@korea.ac.kr

https://doi.org/10.1017/S1446788709000081 Published online by Cambridge University Press

S. LOUBOUTIN, Institut de Mathématiques de Luminy, UMR 6206, 163 avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France
e-mail: loubouti@iml.univ-mrs.fr

S.-M. PARK, Department of Mathematics, Korea University, 136-701, Seoul, Korea
e-mail: smpark@korea.ac.kr