MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 323-340

DETERMINATION OF ALL NONQUADRATIC IMAGINARY CYCLIC NUMBER FIELDS OF 2-POWER DEGREES WITH IDEAL CLASS GROUPS OF EXPONENTS ≤ 2

STÉPHANE LOUBOUTIN

ABSTRACT. We determine all nonquadratic imaginary cyclic number fields $\mathbf{K}$ of 2-power degrees with ideal class groups of exponents ≤ 2, i.e., with ideal class groups such that the square of each ideal class is the principal class, i.e., such that the ideal class groups are isomorphic to some $(\mathbf{Z}/2\mathbf{Z})^m$, $m \geq 0$. There are 38 such number fields: 33 of them are quartic ones (see Theorem 13), 4 of them are octic ones (see Theorem 12), and 1 of them has degree 16 (see Theorem 11).

1. INTRODUCTION

It is known (see [9, Corollary 3]) that there are only finitely many imaginary abelian number fields of 2-power degrees with ideal class groups of exponents ≤ 2. Moreover, it was proved in [10] that the conductors of these number fields that are nonquadratic and cyclic over $\mathbf{Q}$ are less than $6 \cdot 10^{11}$. K. Uchida [18] has already determined the imaginary abelian number fields of 2-power degrees with class number one. Here, we will determine the 2-power degrees imaginary cyclic number fields with ideal class groups of exponents ≤ 2 which are not imaginary quadratic number fields. It has long been known (see [3]) that the Brauer-Siegel theorem implies that there are only finitely many imaginary quadratic number fields that have ideal class groups of exponents ≤ 2, that the Siegel-Tatuzawa theorem implies that there are at most 66 such number fields, and that, under the assumption of a suitable generalized Riemann hypothesis, there are exactly 65 such number fields (see [12] and [20]), and the list of the discriminants of these 65 fields is given in Table 5 in [1].

Now, we sketch here our method of proof. Let $\mathbf{K}$ be an imaginary cyclic number field of 2-power degree $[\mathbf{K}:\mathbf{Q}]$. If the ideal class group $\mathrm{Cl}_{\mathbf{K}}$ of $\mathbf{K}$ has exponent ≤ 2, i.e., $\mathrm{Cl}_{\mathbf{K}}$ is an elementary 2-abelian group, i.e., $\mathrm{Cl}_{\mathbf{K}} \cong (\mathbf{Z}/2\mathbf{Z})^m$ for some $m \geq 0$, then the genus group, which is the Galois group of the genus field of $\mathbf{K}$ over $\mathbf{Q}$, is also an elementary 2-abelian group. Thus, by genus theory, we conclude that any Dirichlet character χ associated with $\mathbf{K}$ must be of the form $\chi = \chi_p\chi'$, where χ_p is of p-power conductor for some prime p and order $[\mathbf{K}:\mathbf{Q}]$, and χ' is trivial or quadratic of conductor prime to p. So, for each prime p, we take the family $\mathcal{F}_p$ of imaginary cyclic number fields

Received by the editor March 18, 1993 and, in revised form, July 12, 1993 and October 12, 1993.
1991 *Mathematics Subject Classification*. Primary 11R29, 11R20.

©1995 American Mathematical Society
0025-5718/95 \$1.00 + \$.25 per page

of 2-power degrees such that any Dirichlet character associated with them is of the above form, and consider $\mathbf{K}$ as a field in $\mathscr{F}_p$ for some p. Let $\mathbf{k}$ be the maximal real subfield of $\mathbf{K}$. Since $\mathbf{k}/\mathbf{Q}$ is a 2-extension in which only the prime p ramifies, the narrow class number $h^+(\mathbf{k})$ of $\mathbf{k}$ is odd; hence $h^+(\mathbf{k}) = h(\mathbf{k})$, and we know that the 2-rank of $\mathrm{Cl}_\mathbf{K}$ is $t-1$, where t is the number of primes in $\mathbf{k}$ which are ramified in $\mathbf{K}/\mathbf{k}$. Since $h(\mathbf{k})$ divides $h(\mathbf{K})$, we conclude that $\mathrm{Cl}_\mathbf{K}$ has exponent ≤ 2 if and only if $h(\mathbf{k}) = 1$ and $h^*(\mathbf{K}) = 2^{t-1}$, where $h^*(\mathbf{K})$ denotes the relative class number of $\mathbf{K}$. Now, we separate the case $p = 2$ from the case $p \neq 2$. In each of these two cases we describe $\mathbf{k}$, we explain how to compute t, and thanks to explicit lower bounds for relative class numbers of CM-fields we manage to set upper bounds for the discriminants of the $\mathbf{K}$'s in $\mathscr{F}_p$ such that $h^*(\mathbf{K}) = 2^{t-1}$. Finally, the computation of the relative class numbers of all the $\mathbf{K}$'s in $\mathscr{F}_p$ with discriminants less than this upper bound provides us with our desired determination of all nonquadratic imaginary cyclic number fields of 2-power degrees with ideal class groups of exponents ≤ 2.

2. Notations

By $\mathbf{K}$ we denote a nonquadratic imaginary cyclic number field such that $[\mathbf{K}:\mathbf{Q}] = 2N = 2^n$ with $n \geq 2$. Hence, the maximal real subfield $\mathbf{k}$ of $\mathbf{K}$ is such that $[\mathbf{k}:\mathbf{Q}] = N$. Next, $f_\mathbf{K}$ and $f_\mathbf{k}$ are the conductors of $\mathbf{K}$ and $\mathbf{k}$, $h(\mathbf{K})$ and $h(\mathbf{k})$ are the class numbers of $\mathbf{K}$ and $\mathbf{k}$, and $d(\mathbf{K})$ and $d(\mathbf{k})$ are the discriminants of $\mathbf{K}$ and $\mathbf{k}$. We let χ be any odd primitive Dirichlet character modulo $f_\mathbf{K}$ that generates the cyclic group of order $2N$ of Dirichlet characters associated with $\mathbf{K}$. Moreover, $h^*(\mathbf{K})$ denotes the relative class number of $\mathbf{K}$. Finally, we let $\mathbf{k}_2$ be the real quadratic subfield of $\mathbf{k}$.

3. Imaginary cyclic number fields $\mathbf{K}$ of 2-power degrees such that their genus number fields $\mathbf{H_K}$ have Galois group over $\mathbf{K}$ of exponent ≤ 2

Let $f_\mathbf{K} = \prod q^{n_q}$ be the factorization of $f_\mathbf{K}$. Corresponding to the decomposition $(\mathbf{Z}/f_\mathbf{K}\mathbf{Z})^* = \prod(\mathbf{Z}/q^{n_q}\mathbf{Z})^*$ we may write $\chi = \prod \chi_q$, where χ_q is a nonprincipal primitive character of conductor $f_q = q^{n_q}$. Let $\mathbf{K}_q$ be the cyclic number field associated with χ_q, and let $\mathbf{H_K} = \prod \mathbf{K}_q$ be their compositum. Then $\mathbf{H_K}$ is the genus number field of $\mathbf{K}$, that is to say, $\mathbf{H_K}$ is the maximal abelian number field that is unramified at the finite places over $\mathbf{K}$. As $\mathbf{K}$ is imaginary, then $\mathbf{H_K}/\mathbf{K}$, moreover, is unramified at the infinite places. Hence, from class field theory we get that the Galois group $\mathrm{Gal}(\mathbf{H_K}/\mathbf{K})$ of the extension $\mathbf{H_K}/\mathbf{K}$ is isomorphic to a quotient group of the ideal class group of $\mathbf{K}$. Hence, $\mathrm{Gal}(\mathbf{H_K}/\mathbf{K})$ has exponent ≤ 2 provided that the ideal class group of $\mathbf{K}$ has exponent ≤ 2.

Now we determine this Galois group. First, as χ has order 2^n, each χ_q has order dividing 2^n (say, has order 2^{m_q} with $1 \leq m_q \leq n$), and there exists at least one prime p such that χ_p has order 2^n. We note that this prime p is then totally ramified in $\mathbf{K}/\mathbf{Q}$. We set $\mathbf{M}_p = \prod_{q \neq p} \mathbf{K}_q$. Second, we observe that the only prime integer that ramifies in $\mathbf{K}_q/\mathbf{Q}$ is q. Thus, p does not ramify in $\mathbf{M}_p/\mathbf{Q}$, and we get $\mathbf{M}_p \cap \mathbf{K} = \mathbf{Q}$. Since $\mathbf{H_K} = \mathbf{M}_p\mathbf{K}_p = \mathbf{M}_p\mathbf{K}$, we get that $\mathrm{Gal}(\mathbf{H_K}/\mathbf{K}) = \mathrm{Gal}(\mathbf{M}_p\mathbf{K}/\mathbf{K})$ is isomorphic to $\mathrm{Gal}(\mathbf{M}_p/\mathbf{Q})$. Third, using induction on the number of cyclic number fields $\mathbf{K}_q$ that appear in

$\mathbf{M}_p$, and using ramification arguments, one can easily get that $\mathrm{Gal}(\mathbf{M}_p/\mathbf{Q})$ is isomorphic to $\prod_{q\neq p}\mathrm{Gal}(\mathbf{K}_q/\mathbf{Q})$. Hence, we get that $\mathrm{Gal}(\mathbf{H_K}/\mathbf{K})$ is isomorphic to $\prod_{q\neq p}\mathbf{Z}/2^{m_q}\mathbf{Z}$.

Now assume that the Galois group $\mathrm{Gal}(\mathbf{H_K}/\mathbf{K})$ of the abelian extension $\mathbf{H_K}/\mathbf{K}$ has exponent ≤ 2. Then we have $m_q = 1$, $q \neq p$. From this we get the factorization $\chi = \chi_p\chi'$, where χ_p is a primitive Dirichlet character of order 2^n and of conductor f_p a p-power, and χ' is a primitive quadratic character of conductor $f' > 1$ that is prime to p, or χ' is trivial if $f' = 1$. Moreover, $f_{\mathbf{K}} = f_p f'$ and $f_{\mathbf{k}}$, which is the conductor of $\chi^2 = \chi_p^2$, divides f_p. Since χ has order 2^n, any odd power of χ has conductor $f_{\mathbf{K}}$ too and generates the group of Dirichlet characters associated with $\mathbf{K}$.

Definition. For each prime p, let $\mathscr{F}_p$ denote the family of imaginary cyclic number fields $\mathbf{K}$ such that $[\mathbf{K}:\mathbf{Q}] = 2N = 2^n$ for some $n \geq 1$, such that their conductors $f_{\mathbf{K}}$ are factored as $f_{\mathbf{K}} = f_p f'$, where f_p is a p-power and where $f' \geq 1$ is prime to p, and such that any generator χ of the group of Dirichlet characters associated with $\mathbf{K}$ is factored as $\chi = \chi_p\chi'$, where χ_p has conductor f_p and order $2N$ and χ' is quadratic of conductor f' if $f' > 1$, and χ' is trivial if $f' = 1$. Hence, the conductor of the maximal real subfield $\mathbf{k}$ of any number field in $\mathscr{F}_p$ divides f_p, hence is a p-power.

Remark. Let $\mathbf{K}$ be in $\mathscr{F}_p$. Let α_p be in $\mathbf{k}$ such that $\mathbf{K}_p = \mathbf{Q}(\sqrt{\alpha_p})$. Then $\mathbf{K} = \mathbf{Q}(\sqrt{\alpha_p D'})$, where $D' = \chi'(-1)f'$.

Indeed, the result clearly holds if $f' = 1$. Hence, let us assume $f' > 1$. Set $\mathbf{E} = \mathbf{Q}(\sqrt{D'}, \sqrt{\alpha_p})$. Then $\mathbf{E}$ is an abelian number field of degree $4N$ with Galois group $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2N\mathbf{Z}$ and group of Dirichlet characters generated by χ_p and χ'. Hence, $\mathbf{E}$ has exactly three subfields of degrees $2N$, namely, $\mathbf{K}_p$, $\mathbf{k}(\sqrt{D'})$, and $\mathbf{K}$. One can easily check that $\mathbf{M} = \mathbf{Q}(\sqrt{\alpha_p D'})$ is a subfield of $\mathbf{E}$ of degree $2N$ such that $\mathbf{M} \neq \mathbf{K}_p = \mathbf{Q}(\sqrt{\alpha_p})$ (since $\mathbf{M}/\mathbf{Q}$ is ramified above f' which is prime to p) and $\mathbf{M} \neq \mathbf{k}(\sqrt{D'})$ (for otherwise we would have $\sqrt{D'} \in \mathbf{M}$ and $\mathbf{M} = \mathbf{K}_p = \mathbf{Q}(\sqrt{\alpha_p})$). Thus, we get $\mathbf{M} = \mathbf{K}$.

4. Necessary and sufficient conditions for ideal class groups to have exponents ≤ 2, and relative class number formulas

Theorem 1. *Let $\mathbf{K}$ be an imaginary cyclic number field of 2-power degree with ideal class group of exponent ≤ 2. Then $\mathbf{K}$ belongs to $\mathscr{F}_p$ for some prime p.*

Proof. The discussion above shows that an imaginary cyclic number field of 2-power degree belongs to some $\mathscr{F}_p$ if and only if its genus number field $\mathbf{H_K}$ is such that $\mathrm{Gal}(\mathbf{H_K}/\mathbf{K})$ has exponent ≤ 2. □

We would like to show that knowledge of the relative class number of $\mathbf{K}$ enables us to assert whether the ideal class group of $\mathbf{K}$ has exponent ≤ 2.

Lemma (a). (i) *Let $\mathbf{k}$ be the maximal real subfield of a number field $\mathbf{K}$ in any $\mathscr{F}_p$. Then, the narrow class number $h^+(\mathbf{k})$ of $\mathbf{k}$ is odd. Moreover, suppose that $h(\mathbf{K})$ is a 2-power. Then $h(\mathbf{k}) = 1$.*

(ii) *Let $\mathbf{K}$ be a CM-field whose maximal real subfield $\mathbf{k}$ has odd narrow class number. Let t be the number of prime ideals of $\mathbf{K}$ that are ramified in the quadratic extension $\mathbf{K}/\mathbf{k}$. Then the 2-rank of the ideal class group of $\mathbf{K}$ is $t-1$.*

Proof. From [4, Corollary 12.5], and using induction on n, where $[\mathbf{K}:\mathbf{Q}] = 2^n$, we get that $h^+(\mathbf{k})$ is odd. Hence, $h^+(\mathbf{k}) = h(\mathbf{k})$. Since $h(\mathbf{k})$ divides $h(\mathbf{K})$, we get the first assertion. From [4, Lemma 13.7] we get the second. □

Theorem 2. *Let* $\mathbf{K}$ *be an imaginary cyclic number field of* 2*-power degree with maximal real subfield* $\mathbf{k}$. *Then, the ideal class group of* $\mathbf{K}$ *is of exponent* ≤ 2 *if and only if* $\mathbf{k}$ *has prime power conductor and class number one and the relative class number* $h^*(\mathbf{K})$ *of* $\mathbf{K}$ *is equal to* 2^{t-1}, *where* t *is the number of prime ideals of* $\mathbf{k}$ *that are ramified in the quadratic extension* $\mathbf{K}/\mathbf{k}$. *Moreover, the ideal class group of* $\mathbf{K}$ *is then generated by the ideal classes of the* t *prime ideals of* $\mathbf{K}$ *that are ramified in the quadratic extension* $\mathbf{K}/\mathbf{k}$.

Proof. The first part follows from Lemma (a) and Theorem 1. Now, in order to prove the last assertion, it suffices to prove that these t ramified prime ideals $\mathbf{P}_i$, $1 \leq i \leq t$, of $\mathbf{K}$ generate a subgroup of order $\geq 2^{t-1}$ in the ideal class group $H(\mathbf{K})$ of $\mathbf{K}$. Indeed, we have a group homomorphism $\Phi\colon (\mathbf{Z}/2\mathbf{Z})^t \mapsto H(\mathbf{K})$ that sends $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_t)$ to $\Phi(\vec{\varepsilon}) =$ the ideal class of $\mathbf{I}_{\vec{\varepsilon}} = \mathbf{P}_1^{\varepsilon_1} \cdots \mathbf{P}_t^{\varepsilon_t}$. If $\vec{\varepsilon}$ is in the kernel of Φ, then there exists $\alpha \in \mathbf{K}$ such that $\mathbf{I}_{\vec{\varepsilon}} = (\alpha)$. By complex conjugation we get $(\overline{\alpha}) = (\alpha)$, so that there exists a unit η of $\mathbf{K}$ such that $\overline{\alpha} = \eta\alpha$. Now, η is an algebraic integer all of whose conjugates have absolute value 1. Hence, η is a root of unity of $\mathbf{K}$ that is well defined up to multiplication by any element of $\mathbf{E}_{\mathbf{K}}^{\sigma-1}$, where σ denotes complex conjugation. Thus, we have a monomorphism from $\mathrm{Ker}(\Phi)$ to $\mathbf{W}_{\mathbf{K}}/\mathbf{E}_{\mathbf{K}}^{\sigma-1}$, where $\mathbf{W}_{\mathbf{K}}$ denotes the group of roots of unity in $\mathbf{K}$. Since $\mathbf{E}_{\mathbf{K}} = \mathbf{W}_{\mathbf{K}}\mathbf{E}_{\mathbf{k}}$ (Lemma (c) below), we get $\mathbf{E}_{\mathbf{K}}^{\sigma-1} = \mathbf{W}_{\mathbf{K}}^{\sigma-1} = W_{\mathbf{K}}^2$. Hence, $\mathrm{Ker}(\Phi)$ has order ≤ 2 and we get the desired result. □

We will explain in Lemmas (g) and (j) below how to compute this number t of prime ideals of $\mathbf{k}$ that are ramified in the quadratic extension $\mathbf{K}/\mathbf{k}$. Now we explain how one can compute the relative class number of any number field $\mathbf{K}$ in $\mathscr{F}_p$. We remind the reader that the relative class number of an imaginary abelian number field $\mathbf{K}$ is equal to

$$(1)\quad \begin{aligned} h^*(\mathbf{K}) &= Q_{\mathbf{K}} w_{\mathbf{K}} \prod_{\chi \text{ odd}} \left(-\frac{1}{2f_\chi} \sum_{a=1}^{f_\chi - 1} a\chi(a) \right) \\ &= Q_{\mathbf{K}} w_{\mathbf{K}} \prod_{\chi \text{ odd}} \left(\frac{1}{2(2 - \overline{\chi(2)})} \sum_{0<a<f_\chi/2} \chi(a) \right), \end{aligned}$$

with $w_{\mathbf{K}}$ being the number of roots of unity in $\mathbf{K}$, and with $Q_{\mathbf{K}}$ being the unit index defined in Lemma (c) (see [19, Theorem 4.17] and [19, Exercise 4.5].) Now, we have

Lemma (b). *Let* $\mathbf{K}$ *be an imaginary cyclic number field of degree* $2N = 2^n$, $n \geq 1$. *Let* $w_{\mathbf{K}}$ *be the number of roots of unity in* $\mathbf{K}$. *Then,* $w_{\mathbf{K}} = 2$, *except when* $\mathbf{K} = \mathbf{Q}(\zeta_4)$ *(in which case* $w_{\mathbf{K}} = 4$*), or when* $2N+1$ *is prime and* $\mathbf{K} = \mathbf{Q}(\zeta_{2N+1})$ *(in which case* $w_{\mathbf{K}} = 2(2N+1)$*).*

Proof. Let ζ_M be a generator of the cyclic group $\mathbf{W}_{\mathbf{K}}$ (M is even). Assume that we have $M > 2$. Since the imaginary cyclotomic number field $\mathbf{Q}(\zeta_M)$ is included in $\mathbf{K}$, and since the proper subfields of $\mathbf{K}$ are real, we get $\mathbf{K} = \mathbf{Q}(\zeta_M)$. Hence, we have $\varphi(M) = 2^n$. Moreover, since $\mathbf{K}$ is cyclic, we have $M = 4$, or

$M = 2p^k$ for some odd prime p and some $k \geq 1$. Thus, $M = 4$, or $\varphi(M) = (p-1)p^{k-1} = 2^n$, implying $k = 1$ and $M = 2p = 2(2^n + 1) = 2(2N+1)$. □

Lemma (c) (see [7, Satz 24]). *Let* $\mathbf{K}$ *be an imaginary cyclic number field. Let* $\mathbf{k}$ *be the maximal real subfield of* $\mathbf{K}$. *Let* $\mathbf{E_K}$ *be the unit group of* $\mathbf{K}$, *and let* $\mathbf{E_k}$ *be the unit group of* $\mathbf{k}$. *Then,* $Q_{\mathbf{K}} \stackrel{\text{def}}{=} [\mathbf{E_K} : \mathbf{W_K E_k}] = 1$.

From (1) and Lemma (c), we get that if $\mathbf{K} \in \mathscr{F}_p$, then we have the following useful evaluation of the relative class number of $\mathbf{K}$:

$$(2) \qquad h^*(\mathbf{K}) = \frac{w_{\mathbf{K}}}{2^N} \prod_{k=0}^{(N/2)-1} \left| \frac{1}{2 - \chi_p(2^{2k+1})\chi'(2)} \sum_{0<a<f_{\mathbf{K}}/2} \chi_p(a^{2k+1})\chi'(a) \right|^2 .$$

5. The case $p = 2$

We determine the number fields $\mathbf{K}$ with ideal class groups of exponents ≤ 2 that belong to the family $\mathscr{F}_2$.

Theorem 3. *For any 2-power* $2N = 2^n$ $(n \geq 1)$ *and any odd square-free positive integer* f', *there exists exactly one field* $\mathbf{K}$ *in* $\mathscr{F}_2$ *such that* $f_{\mathbf{K}} = 8Nf'$. *Except for the field* $\mathbf{Q}(i)$, *any field in* $\mathscr{F}_2$ *is determined only by* n *and* f'. *Then* $\mathbf{K}$ *and its maximal real subfield* $\mathbf{k}$ *are given explicitly by* $\mathbf{K} = \mathbf{Q}(\alpha_{\mathbf{K}})$ *and* $\mathbf{k} = \mathbf{Q}(\cos(\pi/2N))$ *with*

$$\alpha_{\mathbf{K}} = 2\cos\left(\frac{\pi}{4N}\right)\sqrt{-f'} = \sqrt{-f'\left(2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}\right)}\Bigg\}^{n} .$$

Moreover, $f_{\mathbf{k}} = 4N$, $d(\mathbf{K}) = (16N^2 f')^N/2$, *and* $d(\mathbf{k}) = (2N)^N/2$.

This result readily follows from the following three lemmas:

Lemma (d). *Let* χ_2 *be any primitive Dirichlet character of order* $M = 2^m$, $m \geq 2$, *and of conductor* $f_2 = 2^\alpha$. *Then,* $f_2 = 4M$, *i.e.,* $\alpha = m + 2$.

Proof. $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ and χ_2 is of order M. Hence, $2^{\alpha-2} \geq M$, i.e., $\alpha \geq m+2$. If we had $\alpha \geq m+3$, then $x \equiv 1 \pmod{2^{\alpha-1}}$ would imply $x \equiv 1 \pmod{2^\alpha}$ and $\chi_2(x) = 1$, or would imply $x \equiv 1 + 2^{\alpha-1} \equiv 5^{2^{\alpha-3}} \equiv y^M \pmod{2^\alpha}$ and $\chi_2(x) = 1$ too (with $y = 5^{2^{\alpha-m-3}}$). Hence, χ_2 would not be primitive. □

Lemma (e). *Let* $\mathbf{F} \neq \mathbf{Q}(i)$ *be a cyclic number field of degree* $M = 2^m \geq 2$ *a 2-power and of conductor* $f_{\mathbf{F}}$ *a 2-power too. Then,* $f_{\mathbf{F}} = 4M$ *and* $d(\mathbf{F}) = (2M)^M/2$. *Moreover,* $\mathbf{F} = \mathbf{Q}(\cos(\pi/2M))$ *if* $\mathbf{F}$ *is real, and* $\mathbf{F} = \mathbf{Q}(i\cos(\pi/2M))$ *if* $\mathbf{F}$ *is imaginary.*

Proof. The assertion concerning the discriminant of $\mathbf{F}$ is easily proved inductively on m using the conductor-discriminant formula. □

Lemma (f). *Let* $\mathbf{K} \neq \mathbf{Q}(i)$ *be in* $\mathscr{F}_2$. *Let* χ *be an odd primitive Dirichlet character that generates the cyclic group of Dirichlet characters associated with* $\mathbf{K}$. *Then* $\chi = \chi_2\chi'$, *where* χ_2 *is primitive modulo* $8N$ *and of order* $2N$, *and* χ' *is quadratic and primitive modulo* f' *if* $f' > 1$, *so that* f' *is odd and square-free and* $\chi'(m) = (\frac{m}{f'})$, *and* χ' *is trivial if* $f' = 1$. *Moreover,* $f_{\mathbf{K}} = 8Nf'$ *and*

$f_{\mathbf{K}}$ determines the field $\mathbf{K}$, and we may take for χ_2 the Dirichlet character that is well defined by means of

$$\chi_2(-1) = -\chi'(-1) \quad \textit{and} \quad \chi_2(5) = \exp(2i\pi/(2N)).$$

Hence, from (2) and [6, Lemma 1] which gives $\chi((f_{\mathbf{K}}/2) - a) = \chi(a)$, we have

$$(3) \qquad h^*(\mathbf{K}) = \frac{w_{\mathbf{K}}}{2^N} \prod_{k=0}^{(N/2)-1} \left| \sum_{1 \le a \le 2Nf', \ a \text{ odd}} \chi_2(a^{2k+1}) \left(\frac{a}{f'}\right) \right|^2 .$$

Note that according to Lemma (b) we have $w_{\mathbf{K}} = 2$, except when $\mathbf{K} = \mathbf{Q}(i)$ (in which case $w_{\mathbf{K}} = 4$). If the ideal class group of $\mathbf{K}$ is of exponent ≤ 2, then from Theorem 2 we have $h(\mathbf{K}) = h^*(\mathbf{K}) = 2^{t-1}$, where t is the number of prime ideals of $\mathbf{K}$ that are ramified in $\mathbf{K}/\mathbf{k}$. Now, 2 is totally ramified in $\mathbf{K}/\mathbf{Q}$, so that there is exactly one prime ideal in $\mathbf{K}$ lying above 2 that is ramified in $\mathbf{K}/\mathbf{k}$. If a prime ideal $\mathbf{P}$ of $\mathbf{K}$ lying above an odd prime p is ramified in $\mathbf{K}/\mathbf{k}$, then p divides f'. Since for each odd prime p that divides f' there are at most N prime ideals of $\mathbf{k}$ lying above p, there are at most N prime ideals of $\mathbf{K}$ lying above p that are ramified in $\mathbf{K}/\mathbf{k}$. Hence, we get

$$(4) \qquad t \le 1 + N\omega(f'),$$

where $\omega(f')$ is the number of distinct prime divisors of f'. We now give a computational technique for determining t, so that Theorem 2 provides us with a technique to check whether the ideal class group of $\mathbf{K}$ is of exponent ≤ 2.

Lemma (g). *We have*

$$t - 1 = \sum_{q|f'} \frac{N}{\lambda(q, N)}, \quad \textit{where } \lambda(q, N) = \operatorname{Min}\{j \ge 1;\ j \textit{ is a 2-power and } q^j \equiv \pm 1 \pmod{4N}\}.$$

Here, q runs over the odd prime divisors of f'.

Proof. The prime $q = 2$ is totally ramified in $\mathbf{K}/\mathbf{Q}$. Now, any odd prime q is not ramified in $\mathbf{k}/\mathbf{Q}$, so that it is ramified in $\mathbf{K}/\mathbf{Q}$ if and only if it divides f'. Then, each prime ideal of $\mathbf{k}$ above q is ramified in $\mathbf{K}/\mathbf{k}$. Hence, $t = 1 + \sum_{q|f'} g_{\mathbf{k}/\mathbf{Q}}(q)$, where $g_{\mathbf{k}/\mathbf{Q}}(q)$ is the number of prime ideals in $\mathbf{k}$ lying above q. Now, we note that $\mathbf{k}$ is associated with the cyclic group generated by the Dirichlet character ψ which is primitive $\bmod 4N$, of order N, and which induces $\chi^2 = \chi_2^2$. Hence, from [19, Theorem 3.7] we get $g_{\mathbf{k}/\mathbf{Q}}(q) = N/\lambda(q, N)$ with $\lambda(q, N) := \operatorname{Min}\{j;\ j \ge 1 \text{ and } \psi^j(q) = 1\}$. Since $\psi^j(q) = \psi(q^j)$, and since $\psi(x) = 1$ if and only if $x \equiv \pm 1 \pmod{4N}$, we get the desired result. We note that since $\psi(q)$ is a root of unity of order dividing N, then $\lambda(q, N)$ is a 2-power. □

Now, using the methods developed in [16], we give a lower bound for the relative class number of $\mathbf{K}$, which will provide us with upper bounds for $[\mathbf{K} : \mathbf{Q}] = 2^n$, $n \ge 2$, and f' whenever $\mathbf{K} \in \mathcal{F}_2$ has an ideal class group of exponent ≤ 2. The following lemma is extracted from the proof of [16, Lemma (ii)].

Lemma (h). *Let* $\mathbf{k} = \mathbf{Q}(\cos(\pi/2N))$ *be the maximal real subfield of the cyclotomic number field* $\mathbf{Q}(\zeta_{4N})$, $2N = 2^n$, $n \geq 2$. *Then, we have* $\mathrm{Res}_1(\zeta_{\mathbf{k}}) \leq (\pi^2/8)^{(N-1)/2}$.

Theorem 4. *Let* $\mathbf{K}$ *be a nonquadratic number field of degree* $2N = 2^n$ *in* $\mathcal{F}_2$, *so that* $f_{\mathbf{K}} = 8Nf'$ *with* f' *odd and square-free and* $d(\mathbf{K}) = (16N^2f')^N/2$. *Then, we have the following lower bound for the relative class number* $h^*(\mathbf{K})$ *of* $\mathbf{K}$:

$$h^*(\mathbf{K}) \geq \frac{1}{10}\left(\frac{16Nf'}{\pi^4}\right)^{N/2}\frac{1}{N\log(16N^2f')}.$$

Hence, $n \geq 6$ *implies that the ideal class group of* $\mathbf{K}$ *is not of exponent* ≤ 2.

Proof. The Dedekind zeta function $\zeta_{\mathbf{k}_2}$ of the real quadratic subfield $\mathbf{k}_2 = \mathbf{Q}(\sqrt{2})$ of $\mathbf{K}$ is negative in $(0, 1)$ (see Lemma (k) below). Moreover, if χ is any character of order $2N$ associated with $\mathbf{K}$, then $\zeta_{\mathbf{K}}/\zeta_{\mathbf{k}_2}$ is the product of the $2N-2$ L-functions $L(s, \chi^k)$, $1 \leq k \leq 2N-1$ and $k \neq N$, associated with $2N-2$ nonquadratic Dirichlet characters which come in conjugate pairs (since $\chi^{2N-k} = \overline{\chi^k}$), so that we have $\zeta_{\mathbf{K}}/\zeta_{\mathbf{k}_2}(s) \geq 0$, $s \in (0, 1)$ (this is the step where we have to assume $2N \geq 4$, i.e., where we have to assume that $\mathbf{K}$ is not an imaginary quadratic number field). Hence, the zeta function $\zeta_{\mathbf{K}}$ of $\mathbf{K}$ is nonpositive on $(0, 1)$. Lemma (h) above and [16, Theorem 2(b)] provide us with the following lower bound, from which we get the desired first result:

$$h^*(\mathbf{K}) \geq \frac{\pi\sqrt{8}}{5e}\exp\left(-\frac{\pi}{2^{3/4}}\right)\left(\frac{16Nf'}{\pi^4}\right)^{N/2}\frac{1}{N\log(16N^2f')}.$$

Now we assume that the ideal class group of $\mathbf{K}$ is of exponent ≤ 2. Then from (4) and Theorem 2 we have $h^*(\mathbf{K}) = h(\mathbf{K}) = 2^{t-1} \leq 2^{N\omega(f')}$, where $\omega(f')$ is the number of prime divisors of f'. Hence, from the above inequality we have

$$\left(\frac{16Nf'}{\pi^4 4^{\omega(f')}}\right)^{N/2} \leq 10N\log(16N^2f').$$

Now, $x \mapsto x^{N/2}/\log(Ax)$ is an increasing function on $[1, +\infty)$ (provided that we have $N \geq 2$ and $A \geq e$), and $f' \geq f_r \stackrel{\text{def}}{=} p_0p_1\cdots p_r$, where $r = \omega(f') \geq 0$ is the number of distinct prime divisors of f' and where $p_0 = 1$, and $(p_i)_{i\geq 1}$ is the increasing sequence of the odd primes (remember that f' is odd and square-free). Hence, we have

$$\left(\frac{16Nf_r}{\pi^4 4^r}\right)^{N/2} \leq 10N\log(16N^2f_r).$$

Moreover,

$$r \mapsto f(r) = \frac{f_r^{N/2}}{2^{Nr}\log(16N^2f_r)}$$

satisfies $f(r+1) \geq f(r)$ if and only if

$$\left(\left(\frac{p_{r+1}}{4}\right)^{N/2} - 1\right)\log(16N^2f_r) \geq \log(p_{r+1}).$$

Hence, we get $f(0) > f(1)$. On the other hand, if $N \geq 4$, then $16N^2f_r \geq 4^4$ and $x \mapsto (x^2-1)\log(4^4) - \log(4x)$ is a positive (and increasing) function on

TABLE 1

n	$N=2^{n-1}$	$\mathrm{Res}_1(\chi_{\mathbf{k}})\leq$	$\omega(f')\leq$	$f'\leq$
2	2	0.624	5	$4\cdot 10^4$
3	4	0.432	4	$2\cdot 10^3$
4	8	0.340	2	23
5	16	0.272	1	3

$[(5/4), +\infty)$. Hence, we get $f(r+1) > f(r)$ for $r \geq 1$. Therefore, $f(r) \geq f(1)$ for $r \geq 0$ if $N \geq 4$. Since $f_1 = 3$, we get

$$\left(\frac{12N}{\pi^4}\right)^{N/2} \leq 10N\log(48N^2) \quad \text{if } N \geq 4.$$

From this, we get $N \leq 16$, i.e., $n \leq 5$. □

Now, by calculating the numerical values of $\mathrm{Res}_1(\zeta_{\mathbf{k}})$ for $2 \leq N = 2^{n-1} \leq 16$, using the finite evaluation

$$|L(1, \chi)| = \frac{1}{\sqrt{f}}\left|\sum_{k=1}^{f-1}\chi(k)\log(\sin(k\pi/f))\right|,$$

which holds whenever χ is a primitive and even Dirichlet character mod f, and by using

$$2^{N\omega(f')} \geq h^*(\mathbf{K}) \geq \frac{4}{e\,\mathrm{Res}_1(\zeta_k)}\left(1 - \frac{\pi(2e^2)^{1/2N}}{2\sqrt{f'}}\right)\left(\frac{2Nf'}{\pi^2}\right)^{N/2}\frac{1}{N\log(16N^2f')}$$

(see [16, Theorem 2(a)]), we get Table 1. (See the proof of Theorem 7 below to see how we get these upper bounds for $\omega(f')$ and how we then get these upper bounds for f'.) From these very reasonable upper bounds for f', from numerical computations based on (3) and Lemma (g), from the necessary and sufficient condition $h(\mathbf{k}) = 1$ and $h^*(\mathbf{K}) = 2^{t-1}$ for the ideal class group of $\mathbf{K}$ to have exponent ≤ 2 (see Theorem 2), and noticing that the class numbers of the maximal real subfields of the cyclotomic number fields $\mathbf{Q}(\zeta_{2N})$ are equal to one for $2N = 4$ and 8, we get

Theorem 5. *There are exactly* 5 *nonquadratic imaginary cyclic number fields in* $\mathscr{F}_2$ *and such that their ideal class groups are of exponents* ≤ 2, *namely, the five* $\mathbf{K} = \mathbf{Q}(\alpha_{\mathbf{K}})$ *given in Table* 2.

TABLE 2

$[\mathbf{K}:\mathbf{Q}]$	f'	$f_{\mathbf{K}}$	$\alpha_{\mathbf{K}}$	$h(\mathbf{K})$
4	1	16	$\sqrt{-(2+\sqrt{2})}$	1
4	3	48	$\sqrt{-3(2+\sqrt{2})}$	2
4	5	80	$\sqrt{-5(2+\sqrt{2})}$	2
4	7	112	$\sqrt{-7(2+\sqrt{2})}$	4
8	1	32	$\sqrt{-(2+\sqrt{2+\sqrt{2}})}$	1

6. The case $p \neq 2$

Using the methods developed in [13] and [18], we determine the nonquadratic number fields $\mathbf{K}$ with ideal class groups of exponents ≤ 2 that belong to the families $\mathscr{F}_p$, p any odd prime. In Theorems 11, 12, and 13 we have not only determined these number fields, but we have taken into account the results of the case $p = 2$ in order to state in these three theorems the complete determination of all nonquadratic imaginary cyclic number fields of 2-power degrees with ideal class groups of exponents ≤ 2.

Remark. The real quadratic subfield $\mathbf{k}_2$ of $\mathbf{K} \in \mathscr{F}_p$ is such that $\mathbf{k}_2 = \mathbf{Q}(\sqrt{p})$ with $p \equiv 1 \pmod 4$ an odd prime. Now, thanks to Theorem 1 we know that if $\mathbf{K}$ has ideal class group of exponent ≤ 2, then its maximal real subfield $\mathbf{k}$ has class number one and p is totally ramified in $\mathbf{k}/\mathbf{Q}$. Hence, thanks to [19, Proposition 4.11], we get that $\mathbf{k}_2$ has class number one. This will enable us to get rid of many occurrences of p.

Theorem 6. *For any 2-power $2N = 2^n$ $(n \geq 1)$, any odd prime $p \equiv 1 \pmod{2N}$, and any odd square-free positive integer f', there exists exactly one field $\mathbf{K}$ in $\mathscr{F}_p$ such that $f_{\mathbf{K}} = pf'$. Any field in $\mathscr{F}_p$ is determined only by n and f', and the maximal totally real subfield $\mathbf{k}$ of $\mathbf{K}$ is the cyclic subfield of degree N of the cyclotomic number field $\mathbf{Q}(\zeta_p)$. Moreover, if $f' > 1$, then χ' is the character of the real quadratic number field of conductor f' if $p \equiv 1 + 2N \pmod{4N}$, whereas χ' is the character of the imaginary quadratic number field of conductor f' if $p \equiv 1 \pmod{4N}$. Finally, $f_{\mathbf{k}} = p$, $d(\mathbf{k}) = p^{N-1}$, and $d(\mathbf{K}) = d(\mathbf{k})f_{\mathbf{K}}^N < (p^2 f')^N$.*

This result readily follows from the following lemma, which is similar to Lemma (f).

Lemma (i) (see [13, Lemma 1]). *Let χ_p be a primitive Dirichlet character modulo $f_p = p^k$, $k \geq 1$, of order $2N$ prime to p. Then, we have $k = 1$ and $p \equiv 1 \pmod{2N}$. Moreover, χ_p is even if $p \equiv 1 \pmod{4N}$, and χ_p is odd if $p \equiv 1 + 2N \pmod{4N}$. Hence, if $\mathbf{K}$ with $[\mathbf{K} : \mathbf{Q}] = 2N$ belongs to $\mathscr{F}_p$, then $f_{\mathbf{K}} = pf'$, where $f' \geq 1$ is prime to p, and we may take for χ_p the primitive Dirichlet character modulo p of order $2N$ that is well defined by $\chi_p(g) = \exp(2i\pi/2N)$, where g is a generator of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$.*

Remark. In Lemma (f) the choice of f' modulo 4 determines the parity of χ', hence determines the parity of χ_2. Here, it is the choice of p modulo $4N$ that determines the parity of χ_p, hence determines the parity of χ'.

We note that whenever χ is a Dirichlet character of order $2N = 2^n \geq 4$ such that $\chi(2)$ is a root of unity of order $d_2 \geq 2$ that divides $2N$, then

$$\prod_{k=0}^{N-1}(2 - \chi^{2k+1}(2)) = \left|\prod_{k=0}^{(N/2)-1}(2 - \chi^{2k+1}(2))\right|^2 = (2^{d_2/2} + 1)^{2N/d_2} \stackrel{\text{def}}{=} F_{d_2}.$$

Hence, setting $F_{d_2} = 1$ whenever $d_2 = 1$, and setting $F_{d_2} = 2^N$ whenever $\chi(2) = 0$, then thanks to (2) we get that the relative class number $h^*(\mathbf{K})$ may be computed by means of

$$(5)\qquad h^*(\mathbf{K}) = \frac{w_{\mathbf{K}}}{2^N F_{d_2}} \prod_{k=0}^{(N/2)-1} \left| \sum_{0<a<f_{\mathbf{K}}/2} \chi_p(a^{2k+1})\chi'(a) \right|^2 .$$

Moreover, if the ideal class group of $\mathbf{K}$ has exponent ≤ 2, we have $h^*(\mathbf{K}) = 2^{t-1} \leq 2^{N\omega(f')}$. As in Lemma (g), and noticing that $\chi_p^2(x) = 1$ if and only if $\chi^{(p-1)/N} \equiv 1 \pmod{p}$, we have the following computational technique for evaluating this number t of prime ideals of $\mathbf{k}$ that are ramified in $\mathbf{K}/\mathbf{k}$:

Lemma (j). *We have*

$$t - 1 = \sum_{q|f'} \frac{N}{\lambda(p, q, N)}, \quad \text{where } \lambda(p, q, N) = \mathrm{Min}\,\{j \geq 1 ;\ j \text{ is a 2-power and } q^{j(p-1)/N} \equiv 1 \pmod{p}\}.$$

Here, q runs over the prime divisors of f'.

Theorem 7. *If $\mathbf{K}$ with $2N = [\mathbf{K} : \mathbf{Q}] \geq 8$ belongs to $\mathscr{F}_p$ with $p \equiv 1 \pmod{2N}$ an odd prime, then*

$$(6)\qquad \left(\frac{\sqrt{pf'}}{\pi(\log(p)+2)}\right)^N \leq 9.3N \frac{\log(p^2 f')}{\log(p)+2} h^*(\mathbf{K}).$$

Hence, if the ideal class group of $\mathbf{K}$ has exponent ≤ 2, then we have $N \leq 512$, and if N is given, we can give explicit upper bounds for p and f'. Moreover, if the Dedekind zeta function of the real quadratic subfield $\mathbf{Q}(\sqrt{p})$ of $\mathbf{K}$ does not have any real zero in $(0, 1)$, then

$$(7)\qquad \left(\frac{\sqrt{pf'}}{\pi(\log(p)+2+\gamma-\log(4\pi))}\right)^N \leq 9.3N \frac{\log(p^2 f')}{\log(p)+2+\gamma-\log(4\pi)} h^*(\mathbf{K}),$$

where $\gamma = 0.577215664\ldots$ is Euler's constant.

Proof. The relative class number formula and Lemmas (a), (b), and (i) yield

$$h^*(\mathbf{K}) = \frac{Q_{\mathbf{K}} w_{\mathbf{K}}}{(2\pi)^N} \sqrt{d(\mathbf{K})/d(\mathbf{k})} \prod_{\chi \text{ odd}} L(1, \chi) \geq \frac{2}{(2\pi)^N} f_{\mathbf{K}}^{N/2} \prod_{\chi \text{ odd}} L(1, \chi).$$

On the other hand, whenever $s_0 \geq 1$ is real and χ is an even primitive character $\bmod f \geq 5$, we have

$$|L(s_0, \chi)| \leq \frac{1}{2}\log(f) + 1$$

(see [13, Lemme 4]). Arguing as in the beginning of the proof of Theorem 5, for $2N \geq 4$ we get that the Dedekind zeta function of $\mathbf{K}$ is factored as $\zeta_{\mathbf{K}}(s) = \zeta_{\mathbf{k}}(s) L_1(s)$ with

$$L_1(s) = \prod_{\chi \text{ odd}} L(s, \chi) = \prod_{k=0}^{(N/2)-1} L(s, \chi^{2k+1}) L(s, \overline{\chi^{2k+1}}).$$

Hence, $s \mapsto L_1(s)$ does not have any simple real zero. Thus, in the terminology of [18], $s \mapsto L_1(s)$ does not have any exceptional zero. This is the step where once again we have to exclude quadratic number fields $\mathbf{K}$. Hence, from [18, Proposition 1] we get the following lower bound, from which we get the desired first result:

$$h^*(\mathbf{K}) \geq \frac{f_{\mathbf{K}}^{N/2}}{9.3\pi^N(\log(p)+2)^{N-1}\log(d(\mathbf{K}))} > \frac{(pf')^{N/2}}{9.3N\pi^N(\log(p)+2)^{N-1}\log(p^2f')}.$$

Moreover, whenever χ is a nonprincipal even primitive character $\bmod f$, we have

$$|L(1,\chi)| \leq \frac{1}{2}\log(f) + \frac{2+\gamma-\log(4\pi)}{2}$$

(see [15]). From the factorization

$$\zeta_{\mathbf{K}}(s) = \zeta_{\mathbf{k}_2}(s)\prod_{k=1}^{(N/2)-1} L(s,\chi^k)L(s,\overline{\chi^k})$$

we get that any real simple zero of $\zeta_{\mathbf{K}}$ is a zero of $\zeta_{\mathbf{k}_2}$. Hence, from [18, Proposition 1], if the Dedekind zeta function of the real quadratic subfield $\mathbf{k}_2$ of $\mathbf{k}$ does not have any real zero in $(0,1)$, then we get the following lower bound, from which we get the desired last result:

$$h^*(\mathbf{K}) \geq \frac{f_{\mathbf{K}}^{N/2}}{9.3\pi^N(\log(p)+2+\gamma-\log(4\pi))^{N-1}\log(d(\mathbf{K}))}. \quad \square$$

Let us point out that we have the following sufficient condition for the L-function of the real quadratic subfield $\mathbf{k}_2$ of $\mathbf{k}$ not to have any real zero in $(0,1)$.

Lemma (k) (see [13]). *Let $\chi_{\mathbf{k}_2}$ be the character associated with a real quadratic number field $\mathbf{k}_2$ of conductor $f_{\mathbf{k}_2}$. Set*

$$S_2(n) = \sum_{a=1}^{n}\sum_{b=1}^{a}\chi_{\mathbf{k}_2}(b).$$

If $S_2(n)$ is nonnegative for $1 \leq n \leq f_{\mathbf{k}_2}$, then the Dedekind zeta function of $\mathbf{k}_2$ does not have any real zero in $(0,1)$.

Now, suppose that the ideal class group of $\mathbf{K}$ is of exponent ≤ 2. Using $h^*(\mathbf{K}) \leq 2^{N\omega(f')}$ and (6), we get

$$\left(\frac{\sqrt{pf'}}{2^{\omega(f')}\pi(\log(p)+2)}\right)^N \leq 9.3N\frac{\log(p^2f')}{\log(p)+2}. \tag{8}$$

Now, $x \mapsto x^{N/2}\log(p^2x)$ is an increasing function on $[1,+\infty)$ (provided that we have $N \geq 2$ and $p \geq 3$), and $f' \geq f_r \stackrel{\text{def}}{=} p_0p_1\cdots p_r$, where $r = \omega(f') \geq 0$ is the number of distinct prime divisors of f' and where $p_0 = 1$, $p_1 = 3$, $p_2 = 4$, and $(p_i)_{i\geq 3}$ is the increasing sequence of the odd primes greater than or equal to 5 (remember that 4 divides f' if f' is even). Hence, we have

$$\left(\frac{\sqrt{pf_r}}{2^r\pi(\log(p)+2)}\right)^N \leq 9.3N\frac{\log(p^2f_r)}{\log(p)+2}. \tag{9}$$

Moreover,

$$r \mapsto f(r) = \frac{f_r^{N/2}}{2^{Nr}\log(p^2 f_r)}$$

satisfies $f(r+1) \geq f(r)$ if and only if

$$\left(\left(\frac{p_{r+1}}{4}\right)^{N/2} - 1\right)\log(p^2 f_r) \geq \log(p_{r+1}).$$

Hence, we get $f(0) > f(1) > f(2)$. On the other hand, since we have $N \geq 4$, $\log(p^2 f_r) \geq \log(5^2)$ and $x \mapsto (x^2-1)\log(5^2) - \log(4x)$ is a positive (and increasing) function on $[(5/4), +\infty)$, we get $f(r+1) > f(r)$ for $r \geq 2$. Hence, we have $f(r) \geq f(2)$ for $r \geq 0$. Hence, thanks to (9) and thanks to $f_2 = 12$, we have

$$\left(\frac{\sqrt{3p}}{2\pi(\log(p)+2)}\right)^N \leq 9.3N\frac{\log(12p^2)}{\log(p)+2} < 18.6N. \tag{10}$$

Now, $p \mapsto \sqrt{p}(\log(p)+2)$ is an increasing function, and $p \equiv 1 \pmod{2N}$ implies $p \geq 2N+1$. Hence, from (10) we get

$$\left(\frac{\sqrt{6N+3}}{2\pi(\log(2N+1)+2)}\right)^N < 18.6N, \tag{11}$$

so that we get $N \leq 512$. Moreover, let us fix some N. Since $p \mapsto \sqrt{p}/(\log(p)+2)$ tends to infinity with p, then (10) enables us to put an upper bound for p. Since $r \mapsto f(r)$ tends to infinity with r, then (9) enables us to put an upper bound for $r = \omega(f')$ for each p. Finally, (8) enables us to put an upper bound for f' for each p.

Theorem 8. *Let p be any odd prime. There is no number field* $\mathbf{K}$ *in $\mathcal{F}_p$ with* $[\mathbf{K}:\mathbf{Q}] = 2N$ *such that $N = 512$ or 256 and such that the ideal class group of* $\mathbf{K}$ *has exponent ≤ 2.*

Proof. Suppose that there exists such a number field. Then thanks to the fact that $7681 = 1 + 15 \cdot 512$ is the smallest prime which is congruent to $1 \bmod 512$, we have $p \geq 7681$. However, (10) is not satisfied with $p = 7681$ and $N \in \{256, 512\}$, a contradiction. □

Theorem 9. *Let p be any odd prime. There is no number field* $\mathbf{K}$ *in $\mathcal{F}_p$ with* $[\mathbf{K}:\mathbf{Q}] = 2N$ *such that $N = 128$, 64, or 32 and such that the ideal class group of* $\mathbf{K}$ *has exponent ≤ 2.*

Proof. Suppose that there exists such a number field. The proof is divided into three cases: $N = 128$, 64, and 32.

(i) If $N = 128$, then we have $p \equiv 1 \pmod{256}$, so that we have $p = 257$, $p = 769$, or $p \geq 3329$. Since (10) is not satisfied with $p = 3329$ and since the real quadratic number field $\mathbf{k}_2$ of conductor 257 has class number 3, we get that $N = 128$ implies $p = 769$. Now, with $N = 128$ and $p = 769$ we first note that we have $p \equiv 1 + 2N \pmod{4N}$, so that χ_p is odd and χ' is even, i.e., is associated with the real quadratic number field with discriminant f' if $f' > 1$. Moreover, from (8) we have

$$\left(\frac{\sqrt{769f'}}{2^{\omega(f')}\pi(\log(769)+2)}\right)^{128} \leq 1190.4\frac{\log(769^2 f')}{\log(769)+2}.$$

From this, one can easily get that $f' \in \{1, 12, 60\}$. Now, thanks to Lemma (j) we have Table 3, which provides us with the values t (of the number of prime ideals of $\mathbf{K}$ that are ramified in $\mathbf{K}/\mathbf{Q}$):

TABLE 3

f'	1	12	60
$f_{\mathbf{K}}$	769	9228	46140
t	1	19	21

(We get $\lambda(769, 2, 128) = 64$, $\lambda(769, 3, 128) = 8$, and $\lambda(769, 5, 128) = 64$, where $\lambda(p, q, N)$ is defined in Lemma (j).) Hence, if the ideal class groups of these number fields had exponents ≤ 2, from (6) we would have

$$\left(\frac{\sqrt{769 f'}}{\pi(\log(769)+2)}\right)^{128} \leq 1190.4 \frac{\log(769^2 f')}{\log(769)+2} 2^{t-1},$$

and this is not satisfied for $f' \in \{12, 60\}$. Finally, using Lemma (k), one can easily check that the Dedekind zeta function of the real quadratic subfield $\mathbf{Q}(\sqrt{769})$ does not have any real zero in $(0, 1)$. Now, since (7) is not satisfied with $(p, f') = (769, 1)$, we see that we cannot have $N = 128$, provided that the ideal class group of $\mathbf{K}$ has exponent ≤ 2.

TABLE 4

p \ q	2	3	5	7
641	5	6	5	5
769	5	2	5	6
1153	4	5	6	6

(ii) If $N = 64$, then we have $p \equiv 1 \pmod{128}$, so that we have $p \in \{257, 641, 769, 1153\}$ or $p \geq 1409$. Since (10) is not satisfied with $p = 1409$ and since the real quadratic number field of conductor 257 has class number 3, we get that $N = 64$ implies $p \in \{641, 769, 1153\}$. First, we have Table 4, which provides us with the values $\log_2(\lambda(p, q, N))$ (computed thanks to Lemma (j)). Second, Table 5 provides us with the values t (of the number of prime ideals of $\mathbf{K}$ that are ramified in $\mathbf{K}/\mathbf{Q}$) for each possible pair of

TABLE 5

$(p, \chi_p(-1))$ \ f'	1	3	4	5	12	15	21	60
$(641, -1)$	**1**			3	4		4	6
$(769, +1)$		17	3			19		
$(1153, -1)$					7			

values of p and f' such that (8) is satisfied. (Remember that the primitive quadratic character $\bmod f'$ is of opposite parity to that of χ_p, so that we have $f' \equiv 1 \pmod 4$ or $f' \equiv 8, 12 \pmod{16}$ if $\chi_p(-1) = -1$, whereas we have $f' \equiv 3 \pmod 4$ or $f' \equiv 4, 8 \pmod{16}$ if $\chi_p(-1) = +1$.) Third, there is only one value of $f_{\mathbf{K}} = pf'$ such that (6) is satisfied with $h^*(\mathbf{K}) = 2^{t-1}$, namely, $(p, f') = (641, 1)$. Fourth,

$$h^*(\mathbf{K}) = 3459909927724093303906483733942340 24449 > 2^{t-1}$$

for this number field. Hence, we cannot have $N = 64$, provided that the ideal class group of $\mathbf{K}$ has exponent ≤ 2. We point out that thanks to Lemma (k) one can easily check that the Dedekind zeta function of the real quadratic subfield $\mathbf{Q}(\sqrt{641})$ of $\mathbf{K}$ does not have any real zero in $(0, 1)$. Now, since (7) is not satisfied with $(p, f') = (641, 1)$, we could also get rid of this occurrence without calculating the relative class number $h^*(\mathbf{K})$ of the corresponding number field. Moreover, the referee pointed out to us that we could get rid of this occurrence since the real quartic subfield of $\mathbf{Q}(\zeta_{641})$ has class number five (see [5]).

(iii) If $N = 32$, then we have $p \equiv 1 \pmod{64}$, so that we have

$$p \in \{193, 257, 449, 577, 641, 769, 1153, 1217, 1409, 1601\}$$

or $p \geq 2113$. Since (10) is not satisfied with $p = 2113$ and since the real quadratic number fields of conductors $p \in \{257, 577, 1601\}$ have class numbers greater than or equal to 3, we get that $N = 32$ implies $p \in \{193, 449, 641, 769, 1153, 1217, 1409\}$. Arguing as in points (i) and (ii), we get that there are only three values of $f_{\mathbf{K}} = pf'$ such that (6) is satisfied with $h^*(\mathbf{K}) = 2^{t-1}$, namely, $(p, f') = (193, 1), (449, 1)$, and $(449, 5)$. We have the following values of the relative class numbers of the corresponding number fields: $h^*(\mathbf{K}) = 192026280449$, $h^*(\mathbf{K}) = 500402969557121$, and $h^*(\mathbf{K}) = 2^{32} \cdot 6977 \cdot 12097 \cdot 54415214849$. Since $h^*(\mathbf{K}) > 2^{t-1}$ for these number fields, we cannot have $N = 32$, provided that the ideal class group of $\mathbf{K}$ has exponent ≤ 2. We point out that thanks to Lemma (k) one can easily check that the Dedekind zeta function of the real quadratic subfield $\mathbf{Q}(\sqrt{449})$ of $\mathbf{K}$ does not have any real zero in $(0, 1)$. Now, since (7) is not satisfied with $h^*(\mathbf{K}) = 2^{t-1}$ and $(p, f') = (449, 5)$, we could also get rid of this last occurrence without calculating the relative class numbers $h^*(\mathbf{K})$ of the corresponding number field.

Theorem 9 is thus proved. □

Theorem 10. *For any odd prime p, there is no imaginary cyclic number field $\mathbf{K}$ in $\mathcal{F}_p$ with $[\mathbf{K} : \mathbf{Q}] = 2N = 32$ such that the ideal class group of $\mathbf{K}$ has exponent ≤ 2.*

Proof. Suppose that there exists such a number field. From (10) with $N = 16$ we get $p < 2593$. Now, there are 21 odd primes $p \equiv 1 \pmod{32}$ and $p < 2593$, and there are 17 among them such that the real quadratic number field $\mathbf{k}_2$ of conductor p has class number one, the smallest one being $p = 97$. Now, the left terms of (8) and (9) increase with p and the right terms of (8) and (9) decrease with p for $f' \geq e^4$, i.e., for $f' \geq 55$. Hence, from (9) with $p = 97$ we have $r = \omega(f') \leq 5$, so that (8) with $p = 97$ provides us with

$$\left(\frac{\sqrt{97f'}}{2^5\pi(\log(97)+2)}\right)^{16} \leq 9.3\frac{\log(97^2 f')}{\log(97)+2},$$

TABLE 6

f' \ p	97	193	353	449	673	769	929	1249	1697
1	1		1		1		1	1	1
3		5		2		17			
4		3							
5	2								
7		9							
8	3								
12	5								

TABLE 7

f' \ p	97	193	353	673	769	929
1	1		1	1		1
3		5			17	

hence provides us with $f' \leq 10^4$. Then, there are 14 values of $f_{\mathbf{K}} = pf'$ such that (6) is satisfied with $h^*(\mathbf{K}) = 2^{t-1}$, namely, the ones for which t is given in Table 6. Since relative class number computation yields $h^*(\mathbf{K}) > 2^{t-1}$ for these 14 values of $f_{\mathbf{K}}$, we get the desired result. We point out that $h^*(\mathbf{K}) = 2^{16} \cdot 6977 \cdot 1392481$ for $(p, f') = (769, 3)$. Moreover, thanks to Lemma (k) one can easily check that the Dedekind zeta functions of the real quadratic subfields $\mathbf{Q}(\sqrt{p})$ of $\mathbf{K}$ for $p \in \{97, 193, 353, 449, 673, 769, 929, 1249, 1697\}$ do not have any real zero $(0, 1)$. Now, since (7) is satisfied for only 6 of these 14 occurrences, namely, the ones given in Table 7. We could also get the desired result from the numerical computation of the relative class numbers of these 6 occurrences. □

Theorem 11. *There is exactly one imaginary cyclic number field* $\mathbf{K}$ *in* $\mathcal{F}_{17}$ *with* $[\mathbf{K} : \mathbf{Q}] = 16$ *and such that the ideal class group of* $\mathbf{K}$ *has exponent* ≤ 2, *namely, the cyclotomic number field* $\mathbf{Q}(\zeta_{17})$ *which has class number one. For any other odd prime* p, *there is no such field in* $\mathcal{F}_p$.

Proof. From (10) with $N = 8$ we get $p < 4993$. Moreover, from (9) with $p = 17$ we get $r = \omega(f') \leq 6$, so that (8) with $p = 17$ provides us with $f' \leq 3 \cdot 10^5$. Now, there are 141 values of $f_{\mathbf{K}} = pf'$ such that (6) is satisfied with $p \equiv 1 \pmod{16}$ a prime (we do not require the real quadratic number field $\mathbf{Q}(\sqrt{p})$ to have class number one), and with $h^*(\mathbf{K}) = 2^{t-1}$ (the greatest value of p being $p = 4129$ and the greatest value of $f_{\mathbf{K}}$ being $f_{\mathbf{K}} = 24695$). Since $h^*(\mathbf{K}) > 2^{t-1}$ for all these values of $f_{\mathbf{K}} \neq 17$, we get the desired result. □

Theorem 12. *There are exactly four imaginary cyclic octic number fields with ideal class groups of exponents* ≤ 2. *Namely, the number field*

$$\mathbf{K} = \mathbf{Q}\left(\sqrt{-(2+\sqrt{2+\sqrt{2}})}\right),$$

TABLE 8

$f_{\mathbf{k}}$	f'	$f_{\mathbf{K}}$	$h(\mathbf{K})$
17	3	51	2
17	4	68	4
41	1	41	1

which is such that $h(\mathbf{K}) = 1$, *and the three given in Table* 8.

Proof. From (10) with $N = 4$ we get $p < 14897$. Moreover, from (9) with $p = 17$ we get $r = \omega(f') \leq 7$, so that (8) with $p = 17$ provides us with $f' \leq 3 \cdot 10^6$. Now, there are 1807 values of $f_{\mathbf{K}} = pf'$ such that (6) is satisfied with $p \equiv 1 \pmod 8$ a prime (we do not require the real quadratic number field $\mathbf{Q}(\sqrt{p})$ to have class number one), and with $h^*(\mathbf{K}) = 2^{t-1}$ (the greatest value of p being $p = 13873$ and the greatest value of $f_{\mathbf{K}}$ being $f_{\mathbf{K}} = 691460$). Since $h^*(\mathbf{K}) > 2^{t-1}$ for all these values of $f_{\mathbf{K}}$ but the three given in Table 8, we get the desired result from the fact that $h(\mathbf{k}) = 1$ for the quartic subfields of the cyclotomic number fields $\mathbf{Q}(\zeta_p)$, $p = 17$ or $p = 41$. Indeed, the maximal real subfields $\mathbf{Q}_+(\zeta_p)$ of these two cyclotomic number fields have class number one. Hence, from [19, Theorem 10.4.(a)] we get that any subfield of $\mathbf{Q}_+(\zeta_p)$, $p = 17$ or $p = 41$, has class number one. □

Remarks. The field $\mathbf{K}$ with $f_{\mathbf{K}} = 41$ is the only octic subfield of the cyclic cyclotomic number field $\mathbf{Q}(\zeta_{41})$.

If $f_{\mathbf{k}} = 17$, then $\mathbf{k}$ is the only quartic subfield of the cyclic cyclotomic number field $\mathbf{Q}(\zeta_{17})$. Hence, $\mathbf{k} = \mathbf{Q}(\sqrt{17 + 4\sqrt{17}})$. Indeed, if $\alpha = \sqrt{17 + 4\sqrt{17}}$, then $\mathbf{Q}(\alpha)/\mathbf{Q}$ is a real normal quartic number field, hence an abelian quartic number field, so that we only have to show that $\mathbf{Q}(\alpha)$ is included in some $\mathbf{Q}(\zeta_{17^n})$, $n \geq 1$. In order to get this result, it is sufficient to show that the discriminant of the number field $\mathbf{Q}(\alpha)$ is a power of 17. But this follows from the fact that $\beta = \frac{1+\sqrt{\alpha}}{2}$ and $\gamma = \frac{1+\sqrt{17}}{2}$ are algebraic integers of $\mathbf{Q}(\alpha)$ such that

$$d(1, \beta, \gamma, \beta\gamma) = \frac{1}{16^2} d(1, \alpha, \sqrt{17}, \alpha\sqrt{17}) = \frac{1}{16^4} d(1, \alpha, \alpha^2, \alpha^3) = 17^3.$$

Moreover, set

$$\alpha_{\mathbf{k}} = \sqrt{17}(3 + \sqrt{17}) + (1 - \sqrt{17})\alpha.$$

Since $34 + 2\sqrt{17} = (-3 + \sqrt{17})^2(17 + 4\sqrt{17})$, then thanks to [17, p. 173] we have

$$\cos(2\pi/17) = \frac{1}{16}\{(-1 + \sqrt{17}) + (5 - \sqrt{17})\alpha + 2\sqrt{\alpha_{\mathbf{k}}}\}.$$

Hence,

$$\mathbf{Q}(\cos(2\pi/17)) = \mathbf{Q}(\sqrt{\alpha_{\mathbf{k}}})$$

and the number fields of conductors 51 and 68 given in Theorem 12 are $\mathbf{Q}(\sqrt{-3\alpha_{\mathbf{k}}})$ and $\mathbf{Q}(\sqrt{-4\alpha_{\mathbf{k}}}) = \mathbf{Q}(\sqrt{-\alpha_{\mathbf{k}}})$.

The cyclic quartic case. In [13, 14] we recently succeeded in proving that there are exactly 33 imaginary cyclic quartic number fields with ideal class groups of exponents ≤ 2. Hence, we will not consider the cyclic quartic case in our numerical computations. Indeed, using the methods developed here, it would require a great amount of numerical computation in order to get the imaginary cyclic quartic number fields with ideal class groups of exponents ≤ 2. Hence, we simply remind the reader of our following results.

Theorem 13 (see [13, 14]). *There are exactly* 33 *imaginary cyclic quartic number fields with ideal class groups of exponents* ≤ 2. *Namely, the ones with class numbers* h *and conductors* f *given as follows*:

$h=1$	$\mathbf{Q}\left(\sqrt{-(5+2\sqrt{5})}\right)$	$f=5$
	$\mathbf{Q}\left(\sqrt{-(13+2\sqrt{13})}\right)$	$f=13$
	$\mathbf{Q}\left(\sqrt{-(2+\sqrt{2})}\right)$	$f=16$
	$\mathbf{Q}\left(\sqrt{-(29+2\sqrt{29})}\right)$	$f=29$
	$\mathbf{Q}\left(\sqrt{-(37+6\sqrt{37})}\right)$	$f=37$
	$\mathbf{Q}\left(\sqrt{-(53+2\sqrt{53})}\right)$	$f=53$
	$\mathbf{Q}\left(\sqrt{-(61+6\sqrt{61})}\right)$	$f=61$
$h=2$	$\mathbf{Q}\left(\sqrt{-(5+\sqrt{5})}\right)$	$f=40$
	$\mathbf{Q}\left(\sqrt{-3(2+\sqrt{2})}\right)$	$f=48$
	$\mathbf{Q}\left(\sqrt{-13(5+2\sqrt{5})}\right)$	$f=65$
	$\mathbf{Q}\left(\sqrt{-5(13+2\sqrt{13})}\right)$	$f=65$
	$\mathbf{Q}\left(\sqrt{-5(2+\sqrt{2})}\right)$	$f=80$
	$\mathbf{Q}\left(\sqrt{-17(5+2\sqrt{5})}\right)$	$f=85$
	$\mathbf{Q}\left(\sqrt{-(13+3\sqrt{13})}\right)$	$f=104$
	$\mathbf{Q}\left(\sqrt{-7(17+4\sqrt{17})}\right)$	$f=119$
$h=4$	$\mathbf{Q}\left(\sqrt{-3(5+2\sqrt{5})}\right)$	$f=60$
	$\mathbf{Q}\left(\sqrt{-(17+4\sqrt{17})}\right)$	$f=68$
	$\mathbf{Q}\left(\sqrt{-21(5+2\sqrt{5})}\right)$	$f=105$
	$\mathbf{Q}\left(\sqrt{-7(2+\sqrt{2})}\right)$	$f=112$
	$\mathbf{Q}\left(\sqrt{-3(5+\sqrt{5})}\right)$	$f=120$
	$\mathbf{Q}\left(\sqrt{-(17+\sqrt{17})}\right)$	$f=136$
	$\mathbf{Q}\left(\sqrt{-7(5+2\sqrt{5})}\right)$	$f=140$
	$\mathbf{Q}\left(\sqrt{-29(5+2\sqrt{5})}\right)$	$f=145$
	$\mathbf{Q}\left(\sqrt{-5(29+2\sqrt{29})}\right)$	$f=145$
	$\mathbf{Q}\left(\sqrt{-(41+4\sqrt{41})}\right)$	$f=164$
	$\mathbf{Q}\left(\sqrt{-3(73+8\sqrt{73})}\right)$	$f=219$
	$\mathbf{Q}\left(\sqrt{-17(13+2\sqrt{13})}\right)$	$f=221$
	$\mathbf{Q}\left(\sqrt{-15(17+4\sqrt{17})}\right)$	$f=255$
$h=8$	$\mathbf{Q}\left(\sqrt{-3(13+2\sqrt{13})}\right)$	$f=156$
	$\mathbf{Q}\left(\sqrt{-33(5+2\sqrt{5})}\right)$	$f=165$
	$\mathbf{Q}\left(\sqrt{-11(5+2\sqrt{5})}\right)$	$f=220$
	$\mathbf{Q}\left(\sqrt{-21(13+2\sqrt{13})}\right)$	$f=273$
	$\mathbf{Q}\left(\sqrt{-57(5+2\sqrt{5})}\right)$	$f=285$

BIBLIOGRAPHY

1. Z. I. Borevitch and I. R. Chafarevitch, *Number Theory*, Academic Press, New York and London, 1966.
2. D. A. Buell, H. C. Williams, and K. S. Williams, *On the imaginary bicyclic fields with class number* 2, Math. Comp. **31** (1977), 1034–1042.
3. S. Chowla, *An extension of Heilbronn's class number theorem*, Quart. J. Math. **5** (1934), 304–307.
4. P. E. Conner and J. Hurrelbrink, *Class number parity*, Ser. in Pure Math., Vol. 8, World Scientific, Singapore, 1988.
5. M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré* 4 *de* **Q**, Publ. Math. Univ. Besançon, 1977–78.

6. K. Hardy, R. H. Hudson, D. Richman, and K. S. Williams, *Determination of all imaginary cyclotomic quartic fields with class number* 2, Trans. Amer. Math. Soc. **311** (1989), 1–55.
7. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
8. K. Horie, *On the class number of cyclotomic fields*, Manuscripta Math. **65** (1989), 465–477.
9. K. Horie and M. Horie, *CM fields and exponents of their ideal class groups*, Acta Arith. **55** (1990), 157–170.
10. ——, *On the exponents of ideal class groups of CM-fields*, Lecture Notes in Math., vol. 1434, Springer-Verlag, Berlin and New York, 1990, pp. 143–148.
11. K. Horie, *On the exponent of the ideal class group of cyclotomic fields*, Proc. Amer. Math. Soc. **119** (1993), 1049–1052.
12. S. Louboutin, *Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratiques imaginaires. Application*, C. R. Acad. Sci. Paris Sér. I Math. **310** (1990), 795–800.
13. ——, *Détermination des corps quartiques cycliques totalement imaginaires à groupe des classes d'idéaux d'exposant* ≤ 2, Manuscripta Math. **77** (1992), 385–404.
14. ——, *Détermination des corps quartiques cycliques totalement imaginaires à groupe des classes d'idéaux d'exposant* ≤ 2, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), 251–254.
15. ——, *Majorations explicites de* $|L(1, \chi)|$, C. R. Acad. Sci. Paris Sér. I Math. **316** (1993), 11–14.
16. ——, *Lower bounds for relative class numbers of CM-fields*, Proc. Amer. Math. Soc. **120** (1994), 425–434.
17. I. Stewart, *Galois theory*, 2nd ed., Chapman and Hall, London, 1989, Chapter 17.
18. K. Uchida, *Imaginary abelian number fields of degree* 2^m *with class number one*, Proc. Internat. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields (Kataka, Japan), Nagoya Univ., Nagoya, 1986, pp. 151–170.
19. L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., vol. 83, Springer-Verlag, Berlin and New York, 1982.
20. P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124.
21. K. Yamamura, *The determination of the imaginary abelian number fields with class number one*, Math. Comp. **62** (1994), 899–921.

Département de Mathématiques, Université de Caen, U.F.R, Sciences, Esplanade de la Paix, 14032 Caen Cedex, France

E-mail address: `louboutiQuniv-caen.fr`