Computation of Relative Class Numbers of Imaginary Abelian Number Fields

Stéphane Louboutin

CONTENTS

We develop an efficient technique for computing relative class numbers of imaginary abelian fields, efficient enough to enable us to easily compute relative class numbers of imaginary cyclic fields of degrees 32 and conductors greater than 10^{13}, or of degrees 4 and conductors greater than 10^{15}. Acccording to our extensive computation, all the 166204 imaginary cyclic quartic fields of prime conductors p less than 10^7 have relative class numbers less than p/2. Our major innovation is a technique for computing numerically root numbers appearing in some functional equations.

1. INTRODUCTION

Let $n \geq 1$ be a given positive integer.

Let $\mathbf{N}$ be an imaginary abelian number field of degree n, hence n is even, and let $\mathbf{N}^+$ be the subfield of $\mathbf{N}$ of degree $n/2$ fixed by the complex conjugation. Then $\mathbf{N}$ is a quadratic extension of $\mathbf{N}^+$ and the class number $h_{\mathbf{N}^+}$ of $\mathbf{N}^+$ divides the class number $h_{\mathbf{N}}$ of $\mathbf{N}$. We call $h_{\mathbf{N}}^- = h_{\mathbf{N}}/h_{\mathbf{N}^+}$ the relative class number of $\mathbf{N}$. Let $f_{\mathbf{N}}$ be the conductor of $\mathbf{N}$. Then $\mathbf{N}$ is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_{f_{\mathbf{N}}})$ and we let $X_{\mathbf{N}}$ denote the group of primitive Dirichlet characters which are trivial on the Galois group of the abelian extension $\mathbb{Q}(\zeta_{f_{\mathbf{N}}})/\mathbf{N}$. For any $\chi \in X_{\mathbf{N}}$ we let f_χ denote its conductor. We let $w_{\mathbf{N}}$ denote the number of roots of unity in $\mathbf{N}$ and $Q_{\mathbf{N}} \in \{1,2\}$ denote the Hasse unit index of $\mathbf{N}$. Finally, we let $X_{\mathbf{N}}^-$ denote the subset of all the $\chi \in X_{\mathbf{N}}$ such that $\chi(-1) = -1$. For each cyclic subgroup X of X_N choose a generator $\psi \in X$, let n_ψ denote the order of ψ, let N_ψ be the norm map from the cyclotomic field $\mathbb{Q}(\zeta_{n_\psi})$ to $\mathbb{Q}$ and finally let Y_N^- denote the set of such odd generators ψ.

Mathematics Subject Classification: Primary, 11R20, 11R29, 11Y40; Secondary, 11M20, 11R42.

Keywords: Imaginary abelian number field, relative class number.

1058-6458/1998 $0.50 per page

The following equality is well known [Washington 1997]:

$$
\begin{aligned}
h_{\mathbf{N}}^- &= Q_{\mathbf{N}} w_{\mathbf{N}} \prod_{\chi \in X_{\mathbf{N}}^-} -\tfrac{1}{2} B_{1,\chi} \\
&= Q_{\mathbf{N}} w_{\mathbf{N}} \prod_{\psi \in Y_{\mathbf{N}}^-} N_\psi\left(-\tfrac{1}{2} B_{1,\psi}\right)
\end{aligned}
\tag{1–1}
$$

with

$$
B_{1,\chi} = \frac{1}{f_\chi} \sum_{x=1}^{f_\chi - 1} x\chi(x) = -\frac{1}{2-\bar{\chi}(2)} S_\chi, \tag{1–2}
$$

where

$$
S_\chi \stackrel{\text{def}}{=} \sum_{1 \le x \le f_\chi/2} \chi(x)
$$

is an algebraic integer. Hence, if χ has order m then S_χ is in $\mathbb{Z}[\zeta_m]$, the ring of algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_m)$. We also note that according to the Brauer-Siegel theorem $\log h_{\mathbf{N}}^-$ is asymptotic to

$$
\tfrac{1}{2} \log\Bigl(\prod_{\chi \in X_{\mathbf{N}}^-} f_\chi \Bigr)
$$

when $f_{\mathbf{N}}$ goes to infinity. In particular, $h_{\mathbf{N}}^-$ is usually a very large integer. Roughly speaking, using (1–1) we have to do $O(f_{\mathbf{N}})$ operations to compute $h_{\mathbf{N}}^-$. In this paper will reduce this amount of required computation down to $O(\sqrt{f_{\mathbf{N}} \log f_{\mathbf{N}}})$ elementary operations. Indeed, we will explain how we can compute the exact values of the integral coordinates of all the $S_\psi \in \mathbb{Z}[\zeta_{n_\psi}]$ which appear in (1–1) and will explain how we can then compute the exact value of $h_{\mathbf{N}}^-$.

However, to make our technique clear, when doing relative class number computation we will assume that $n = 2^r \ge 2$ is a 2-power, that $\mathbf{N}$ is cyclic of degree $n = 2^r$ and of prime conductor p, and that $\mathbf{N}$ is not a cyclotomic field. In that situation, not only are the S_χ algebraic integers, but all the $B_{1,\chi} \in \mathbb{Z}[\zeta_{2^r}]$ are algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$. Moreover $Q_{\mathbf{N}} = 1$, $w_{\mathbf{N}} = 2$ and $Y_{\mathbf{N}}^-$ is reduced to a set with one element.

2. THE METHOD

To begin with, for any odd primitive Dirichlet character χ we will express $B_{1,\chi}$ as the limit of a rapidly absolutely convergent series (see formula (2–3)). So, let χ be an odd primitive Dirichlet character of conductor f and order m. We set

$$
\tau_\chi = \sum_{x=1}^{f-1} \chi(x) e^{2x\pi i/f} \quad \text{and} \quad \varepsilon_\chi = \frac{1}{i\sqrt{f}} \tau_\chi,
$$

$$
g(x,\chi) = \sum_{n \ge 1} n\chi(n) e^{-\pi n^2 x/f} \quad (x > 0) \tag{2–1}
$$

and

$$
F(s,\chi) = \left(\frac{f}{\pi}\right)^{(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) L(s,\chi).
$$

Note also that

$$
\frac{1}{\sqrt{f}} F(0,\chi) = L(0,\chi) = -B_{1,\chi}.
$$

It is known that ε_χ has absolute value equal to one and that

$$
g(1/x,\chi) = \varepsilon_\chi x^{3/2} g(x,\bar{\chi}) = \varepsilon_\chi x^{3/2} \overline{g(x,\chi)}, \tag{2–2}
$$

for $x > 0$. Therefore, for s complex we have

$$
F(s,\chi) = \int_0^\infty g(x,\chi) x^{(s+1)/2} \frac{dx}{x} \quad \text{if } \operatorname{Re}(s) > 1,
$$

and this equals

$$
\int_1^\infty g(x,\chi) x^{(s-1)/2}\, dx + \varepsilon_\chi \int_1^\infty g(x,\bar{\chi}) x^{-s/2}\, dx
$$

for any s, so we get

$$
F(1-s,\chi) = \varepsilon_\chi F(s,\bar{\chi}) \quad \text{for } s \text{ complex},
$$

and we now express $B_{1,\chi} = -L(0,\chi)$ as the limit of a rapidly absolutely convergent series:

$$
B_{1,\chi} = -\frac{\sqrt{f}}{\pi} \Biggl(\varepsilon_\chi \sum_{n \ge 1} \frac{\bar{\chi}(n)}{n} e^{-\pi n^2/f} + \sum_{n \ge 1} \frac{\chi(n)}{n} F(\pi n^2/f) \Biggr), \tag{2–3}
$$

where

$$F(X) = X \int_1^\infty e^{-Xx} \frac{dx}{\sqrt{x}} \leq X \int_1^\infty e^{-Xx} dx = e^{-X}.$$

There are similar results for even primitive Dirichlet characters [Williams and Broere 1976; Schoof and Washington 1988; Seah et al. 1983] and our method developed below could be easily adapted to the numerical computation of class numbers of real abelian number fields (whose regulators are known).

In particular, (2–3) is a rapidly absolutely convergent series which could be used to compute numerical approximations of values of Dirichlet generalized Bernoulli's numbers $B_{1,\chi}$ (see below). But since there is no known general formula for Gauss sums [Berndt and Evans 1981], we should know how to compute ε_χ numerically. To this end, and since τ_χ^m is a product of Jacobi's sums which are algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_m)$, according to the literature bearing on this question, one usually uses known results on Gauss sums to get a formula for $\eta_\chi = \varepsilon_\chi^m$. This leaves it unspecified which m-th root of η_χ is equal to ε_χ. As in [Schoof and Washington 1988, Section 4] and in [Seah et al. 1983], people usually get round this problem by computing, for each of these m possible m-th roots, numerical approximations of L-functions and class numbers. For example, the numerical computation of the class number of a cyclic cubic number field whose regulator is known boils down to the computation of $L(1,\chi)$ for only one Dirichlet L-function for some primitive cubic character χ. In all the cases they considered, it turned out that exactly one out of these $m = 3$ possible choices for $\sqrt[3]{\eta_\chi}$ yielded a value for the class number which was close enough to a positive integer to be the numerical approximation of the class number, thus providing them with the exact value of this sought class number [Seah et al. 1983]. However, if we delt with a cyclic quintic number field, then the numerical computation of its class number would boil down to the computation of $L(1,\chi)$ for only two Dirichlet L-function associated to primitive quintic characters χ. Here, for each of these two L-functions we would have five possible choices for $\sqrt[5]{\eta_\chi}$ and we would end up with twenty five possible values for the class number. It becomes less likely that only one of them is going to be close enough to a positive integer to be the numerical approximation of this sought class number. In fact, for cyclic quintic fields, a slightly different approach was used in [Schoof and Washington 1988], but it also left the authors with twenty possible values for each class number they wanted to compute. Luckily, each time, it turned out that only one of these twenty values was close enough to a positive integer to be the numerical approximation of this sought class number.

Here, we will promote a completely different approach.

Using (2–2) at $s = 1$, we get $\varepsilon_\chi = g(1,\chi)/\overline{g(1,\chi)}$, provided that $g(1,\chi)$ is not equal to zero. We will use (2–2) first to verify that $g(1,\chi) \neq 0$ and then to compute good approximations of all ε_χ's for $\chi \in X_{\mathbf{N}}^-$ (see Theorem 3.1). Second, we will use the rapidly absolutely convergent series (2–3) to obtain good enough approximations of all $B_{1,\chi}$'s to use (1–1) to deduce the exact value of the relative class number of a given $\mathbf{N}$. To begin with, we set

$$B(t,M,f) = \sqrt{\frac{f}{\pi}(t\log(f/\pi) + M)}. \tag{2–4}$$

Throughout this paper we will replace various infinite sums similar to (2–3) by sums up to the least integer greater than or equal to $B(t,M,f)$ where t and M will be be suitably chosen. Note that $n \geq B(t,M,f)$ implies

$$0 \leq F(\pi n^2/f) \leq e^{-\pi n^2/f} \leq (\pi/f)^t e^{-M}.$$

Roughly speaking, we will prove first that we need compute only $B(1,M,f)$ terms in (2–1) to compute ε_χ with an error not exceeding e^{-M} (see Theorem 3.1), second that we need compute only $B(\frac{3}{2}+\varepsilon,M,f)$ terms in (2–3) (where ε_χ is replaced by its just computed approximation) to compute $B_{1,\chi}$ with an error not exceeding e^{-M} (see Theorem 4.2), and third we will show that this enables us to compute the exact value of $B_{1,\chi}$, i.e., to compute the exact values of the the coordinates of the algebraic integer S_χ in the canonical $\mathbb{Z}$-basis of the ring of algebraic integer $\mathbb{Z}[\zeta_m]$ of the cyclotomic field $\mathbb{Q}(\zeta_m)$. Finally, we explain how the knowledge of these coordinates will provide us with the exact value of $h_{\mathbf{N}}^-$. To keep this paper short, when doing actual relative class number computation, we will focus on imaginary cyclic fields of 2-power degrees and prime conductors. In that case all $B_{1,\chi}$ for $\chi \in X_{\mathbf{N}}^-$ are algebraic integers.

3. A CONJECTURE

In this section, we explain why it is reasonable to conjecture that the complex number $g(1,\chi)$ is never equal to zero.

Theorem 3.1. *Set $g = g(1,\chi)$ and*

$$g_m = g_m(1,\chi) = \sum_{n=1}^{m} n\chi(n)e^{-\pi n^2/f}.$$

Then $m \geq \sqrt{p/2\pi}$ implies $|g - g_m| \leq \frac{f}{2\pi}e^{-\pi m^2/f}$ and

$$|\varepsilon_\chi - g_m/\bar{g}_m| \leq 2\frac{|g-g_m|}{|g_m|} \leq \frac{f}{\pi|g_m|}e^{-\pi m^2/f}. \quad (3\text{–}1)$$

Therefore, $m \geq B(1,M,f)$ and $|g_m| > \frac{1}{2}e^{-M}$ imply $|g-g_m| \leq \frac{1}{2}e^{-M}$, $g \neq 0$, $g_m \neq 0$ and $|\varepsilon_\chi - g_m/\bar{g}_m| \leq e^{-M}/|g_m|$.

Proof. Notice that $x \mapsto xe^{-\pi x^2/f}$ decreases for $x \geq \sqrt{f/2\pi}$. □

Corollary 3.2. 1. *Whenever p is an odd prime let $g_p \geq 2$ denote the least primitive root modulo p and let χ_p be the odd character modulo p defined by $\chi_p(g_p) = \exp(2\pi i/(p-1))$. Hence, the χ_p^k's with $1 \leq k < p$ and k odd are the $(p-1)/2$ odd characters modulo p. Choosing $M = 20$ and letting χ_p^k range over the 773733 odd characters for the 668 odd primes $p \leq 5000$ we get the following table of the ten least values of $|g(1,\chi_p^k)|$ (with $1 \leq k \leq (p-1)/2$ and k odd), according to which we have $g(1,\chi) \neq 0$ for the 773733 odd characters modulo any prime $p \leq 5000$. (Here $\operatorname{ord}(\chi_p^k) = (p-1)/\gcd(p-1,k)$ denotes the order of χ_p^k.)*

p	k	$\operatorname{ord}(\chi_p^k)$	$\lvert g(1,\chi_p^k)\rvert$
2161	725	432	$0.00160\cdots$
3041	535	608	$0.00151\cdots$
2767	285	922	$0.00108\cdots$
1559	775	1558	$0.000830\cdots$
3779	1745	3778	$0.000722\cdots$
1433	273	1432	$0.000618\cdots$
3617	225	3616	$0.000556\cdots$
3061	143	3060	$0.000196\cdots$
3373	615	1124	$0.0000802\cdots$
2803	1337	2802	$0.00000541\cdots$

2. *If χ is an odd primitive quartic character of prime conductor p then $p \equiv 5 \pmod 8$. Conversely, for each prime $p \equiv 5 \pmod 8$ there are two odd quartic characters of conductor p, they are conjugated and we let χ_p be the one well defined by means of $\chi_p(2) = i$. Choosing $M = 20$ and letting χ range over all the 166204 odd primitive quartic characters χ_p of prime conductors p, we get the following table of the ten least values of $|g(1,\chi_p)|$ according to which we have $g(1,\chi_p) \neq 0$ for these 166204 odd quartic characters.*

p	$\lvert g(1,\chi_p)\rvert$
5717	$0.311\cdots$
2537461	$0.271\cdots$
2089037	$0.177\cdots$
114797	$0.153\cdots$
149	$0.143\cdots$

p	$\lvert g(1,\chi_p)\rvert$
907589	$0.121\cdots$
105173	$0.0943\cdots$
2958821	$0.0756\cdots$
7750373	$0.0356\cdots$
3428861	$0.0189\cdots$

According to this Corollary, we put forward the following hypothesis:

Conjecture. For any primitive odd Dirichlet character χ (of conductor f) we have

$$g(1,\chi) = \sum_{n\geq 1} n\chi(n)e^{-\pi n^2/f} \neq 0.$$

Of course, if $x \mapsto g(x,\chi)$ is real valued and $\varepsilon_\chi = -1$ then (2–2) yields $g(1,\chi) = 0$. In particular, for slightly different L-functions, the associated $g(1,\chi)$ can be equal to zero. Indeed, according to [Fröhlich 1972] there exist infinitely many quaternion octic number fields such that the Artin roots number ε_ψ for their irreducible non-abelian characters ψ of degree two of their Galois groups H_8 (the quaternion group of order eight) are equal to -1 (however, since the exact value of ε_ψ is known, we were able in [Louboutin $\geq$ 1998] to develop a technique for computing the values at $s = 1$ of the associated Artin L-functions $s \mapsto L(s,\psi)$, which in turn enabled us to derive an efficient technique for computing relative class numbers of quaternion octic CM-fields).

Finally, we conclude this section with a partial proof of this conjecture:

Theorem 3.3. *Let X_p^- denote the set of odd primitive Dirichlet characters modulo an odd prime p. Set*

$$M_p = \frac{2}{p-1}\sum_{\chi\in X_p^-}|g(1,\chi)|^2$$

(and note that there are $(p-1)/2$ elements in X_p^-). Then M_p is asymptotic to $p^{3/2}/(4\pi\sqrt{2})$ when p goes to infinity. Moreover,

$$|g(1,\chi)| \leq \frac{p}{2\pi} + \sqrt{\frac{p}{2\pi e}}.$$

In particular, for any $c < \pi/(2\sqrt{2})$ there exists p_c such that if $p \geq p_c$ then at least $c\sqrt{p}$ characters in X_p^- satisfy $g(1,\chi) \neq 0$. Therefore, there are infinitely many odd characters χ of prime conductors such that $g(1,\chi) \neq 0$.

Proof. Standard orthogonality relations give for the sum $\sum_{\chi\in X_p^-}\chi(a)\bar\chi(b)$ the value

$$\begin{array}{cl} (p-1)/2 & \text{if } b \equiv a \pmod p \text{ and } a \not\equiv 0 \pmod p,\\ -(p-1)/2 & \text{if } b \equiv -a \pmod p \text{ and } a \not\equiv 0 \pmod p,\\ 0 & \text{otherwise.}\end{array}$$

Thus

$$M_p = \sum_{r=1}^{p-1}\sum_{k\geq 0}\sum_{l\geq 0}\Bigl((r+kp)(r+lp)e^{-\pi\frac{(r+kp)^2+(r+lp)^2}{p}} - (r+kp)(p-r+lp)e^{-\pi\frac{(r+kp)^2+(p-r+lp)^2}{p}}\Bigr),$$

from which we easily deduce that M_p is equivalent first to $\sum_{r=1}^{p-1} r^2 e^{-2\pi r^2/p}$, and second to

$$\int_0^\infty r^2 e^{-2\pi r^2/p}\,dr = \frac{p}{4\pi}\int_0^\infty e^{-2\pi r^2/p}\,dr = \frac{p^{3/2}}{4\pi\sqrt{2}}.$$

As for the bound on $|g(1,\chi)|$, we note that $ne^{-\pi n^2/p}$ is less than or equal to $\sqrt{p/(2\pi e)}$ and we use a comparison of series with integrals. □

4. COMPUTATION OF NUMERICAL APPROXIMATIONS OF $B_{1,\chi}$

In this section, we explain how to use (2–3) to compute as good as desired numerical approximations of $B_{1,\chi}$, provided that $g(1,\chi)$ is not equal to zero.

Lemma 4.1. *Let χ be an odd primitive Dirichlet character modulo f.*

1. (See also [Louboutin 1996]). *For any $f \geq 2$ we have*
$$\sum_{n\geq 1}\frac{1}{n}e^{-\pi n^2/f} \leq \tfrac{1}{2}\log f$$
and
$$\sum_{n=1}^{m}\frac{1}{n}F(\pi n^2/f) \leq \int_0^\infty F(\pi t^2/f)\frac{dt}{t} = 1.$$
2. *Set*
$$B_{1,\chi}(m) = -\frac{\sqrt{f}}{\pi}\Bigl(\varepsilon_\chi\sum_{n=1}^{m}\frac{\bar\chi(n)}{n}e^{-\pi n^2/f} + \sum_{n=1}^{m}\frac{\chi(n)}{n}F(\pi n^2/f)\Bigr).$$

We have

$$|B_{1,\chi} - B_{1,\chi}(m)| \leq \frac{f^{3/2}}{\pi^2 m^2}e^{-\pi m^2/f}. \tag{4–1}$$

Therefore, $m \geq B(\frac{1}{2}, M, f)$ *implies*

$$|B_{1,\chi} - B_{1,\chi}(m)| \leq \frac{2e^{-M}}{\sqrt{\pi}(\log(f/\pi) + 2M)}.$$

Proof. Part 2 follows from [Louboutin 1996]. As for (4–1), using $F(X) \leq e^{-X}$, we have

$$\begin{aligned} |B_{1,\chi} - B_{1,\chi}(m)| &\leq 2\frac{\sqrt{f}}{\pi} \sum_{n>m} \frac{1}{n} e^{-\pi n^2/f} \\ &\leq 2\frac{\sqrt{f}}{\pi} \int_m^\infty e^{-\pi x^2/f} \frac{dx}{x} \\ &\leq \frac{2\sqrt{f}}{\pi m^2} \int_m^\infty x e^{-\pi x^2/f} \, dx \\ &= \frac{f^{3/2}}{\pi^2 m^2} e^{-\pi m^2/f}. \end{aligned}$$ □

Theorem 4.2. *Assume* $g_m \neq 0$ *and set*

$$\tilde{B}_{1,\chi}(m) = -\frac{\sqrt{f}}{\pi}\left(\frac{g_m}{\bar{g}_m} \sum_{n=1}^{m} \frac{\bar{\chi}(n)}{n} e^{-\pi n^2/f} + \sum_{n=1}^{m} \frac{\chi(n)}{n} F(\pi n^2/f)\right).$$

Then $m \geq B(t, M, f)$ *implies*

$$|B_{1,\chi} - \tilde{B}_{1,\chi}(m)| \leq \left(\frac{1}{m^2} + \frac{\log f}{2|g_m|}\right) \frac{e^{-M}}{\sqrt{\pi}(f/\pi)^{t-(3/2)}}. \quad (4–2)$$

Therefore, setting

$$t = \frac{3}{2} + \frac{M + \log\log f}{\log(f/\pi)} = \frac{3}{2} + o(1),$$

then $m \geq B(t, M, f)$ *and* $|g_m| \geq \frac{1}{2}e^{-M}$ *imply*

$$|B_{1,\chi} - \tilde{B}_{1,\chi}(m)| \leq 2e^{-M}.$$

Proof. According to (4–1), (3–1) and part 1 of Lemma 4.1, we have

$$\begin{aligned} &|B_{1,\chi} - \tilde{B}_{1,\chi}(m)| \\ &\quad \leq |B_{1,\chi} - B_{1,\chi}(m)| + |B_{1,\chi}(m) - \tilde{B}_{1,\chi}(m)| \\ &\quad \leq \frac{f^{3/2}}{\pi^2 m^2} e^{-\pi m^2/f} + \frac{f^{3/2}}{2\pi^2 |g_m|} (\log f) e^{-\pi m^2/f}. \end{aligned}$$ □

For numerical computation purposes, we note that

$$\begin{aligned} F(X) &= 2\sqrt{X} \int_{\sqrt{X}}^\infty e^{-u^2} \, du \\ &= \sqrt{\pi X} - 2\sum_{n \geq 0} \frac{(-1)^n X^{n+1}}{(2n+1)(n!)}, \end{aligned}$$

a rapidly absolutely convergent series which is useful for numerical computation of $F(X)$ when X is small. Moreover, we have

$$F(X) = \cfrac{Xe^{-X}}{X + \cfrac{1}{2 + \cfrac{2}{X + \cfrac{3}{2 + \cfrac{4}{X + \cfrac{5}{2 + \cdots}}}}}}$$

(see [Wall 1948, pages 356–358]); this is useful for numerical computation of $F(X)$ when X is large.

5. DETERMINATION OF $B_{1,\chi}$

We now explain how our method provides us with an efficient technique for computing relative class numbers of imaginary abelian number fields.

To simplify, we will assume that $\mathbf{N}$ is a non-quadratic imaginary cyclic field of 2-power degree n and prime conductor p. In that case, $\mathbf{N}$ is the maximal subfield of 2-power degree of $\mathbb{Q}(\zeta_p)$, hence p determines $\mathbf{N}$ and n, and we will let $\mathbf{N}_p$ denote the only imaginary cyclic field of conductor p and degree n. We also simplify the notation and set $h_p^- = h_{\mathbf{N}_p}^-$, $w_p = w_{\mathbf{N}_p}$, $Q_p = Q_{\mathbf{N}_p} \in \{1, 2\}$, $X_{n,p} = X_{\mathbf{N}_p}$ and $X_{n,p}^- = X_{\mathbf{N}_p}^-$. Note that according to Brauer-Siegel's theorem $\log h_p^-$ is equivalent to $\frac{n}{4} \log p$ when p goes to infinity. If $\mathbf{N}_p$ is not equal to the cyclotomic field of conductor p, then all $B_{1,\chi}$'s are algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$ and $2^{(n/2)-1}$ times h_p^- is equal to the norm of any of these algebraic integers. We will define a particular generator χ_p of $X_{n,p}$ and will explain how we can compute exact values of the rational integers a_k which are such that

$$B_{1,\chi_p} = \sum_{k=0}^{(n/2)-1} a_k \zeta_n^k.$$

The idea is to compute good approximations of all the $B_{1,\chi}$'s, to express each a_k as a linear combination of these $B_{1,\chi}$ and to use the fact that all the a_k's must be rational integers to deduce their exact values from their good enough numerical approximations. We finally explain how we compute the exact value of h_p^- from these a_k's.

Let $n = 2^r \geq 2$ be a given 2-power.

Let p be an odd prime such that $p \equiv 1 \pmod{n}$. Since the multiplicative group $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, then

$$\mathbf{H} = \{x \in \mathbf{G} : x^{(p-1)/n} = 1\}$$

is its unique subgroup of index n. Let n_p be defined by

$$n_p = \min\{a \geq 1 : a^{(p-1)/2} = \left(\tfrac{a}{p}\right) = -1\},$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. Then n_p has order n in the quotient group $\mathbf{G}/\mathbf{H}$. If χ is a character of order n on $\mathbf{G}$ then χ must be trivial on $\mathbf{H}$ and χ is well determined by the image $\chi(n_p) = \zeta$ which must be some n-th primitive root of unity. For any $x \in \mathbf{G}$ we have $\chi(x) = \zeta^k$ if and only if $\chi(x/n_p^k) = 1$, hence if and only if $x/n_p^k \in \mathbf{H}$, hence if and only if $(x/n_p^k)^{(p-1)/n} = 1$. Setting $m_p = n_p^{(p-1)/n}$ (modulo p) we get the following efficient technique for computing the values of χ:

$$\chi(x) = \zeta^{k_x}$$

where $k_x = \min\{k \in \{0,1,2,\cdots,n-1\} : x^{(p-1)/n} \equiv m_p^k \pmod{p}\}$. Note also that we have $\chi(-1) = \chi(n_p^{(p-1)/2}) = \zeta_n^{(p-1)/2} = (-1)^{(p-1)/n}$, so that χ is odd if and only if $p \equiv 1+n \pmod{2n}$. We shall χ_p denote the character modulo p well defined by

$$\chi_p(n_p) = \zeta_n \stackrel{\text{def}}{=} \exp(2\pi i/n).$$

Proposition 5.1. *Let $\mathbf{N}$ be a non-quadratic imaginary cyclic field of prime conductor p and 2-power degree $[\mathbf{N} : \mathbb{Q}] = n = 2^r \geq 4$. Set $\zeta_n = \exp(2\pi i/n)$.*

1. *We have $p \equiv n+1 \pmod{2n}$ and for any prime $p \equiv n+1 \pmod{2n}$ there exists exactly one imaginary cyclic field of conductor p and degree n, to be denoted by $\mathbf{N}_p$.*
2. *If $p = n+1$ then $\mathbf{N}_p = \mathbb{Q}(\zeta_p)$, $w_p = 2p$ and $Q_p = 1$.*
3. *If $p > n+1$ then $w_p = 2$, $Q_p = 1$, h_p^- is odd* (use [Washington 1997, Theorem 10.4 (b)]),

$$h_p^- \stackrel{\text{def}}{=} h_{\mathbf{N}_p}^- = \frac{2}{2^{n/2}} N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(B_{1,\chi_p}), \qquad (5\text{–}1)$$

and

$$B_{1,\chi_p} = \sum_{k=0}^{(n/2)-1} a_k \zeta_n^k \in \mathbb{Z}[\zeta_n]$$

is an algebraic integer of $\mathbb{Q}(\zeta_n)$ where each

$$a_k = \frac{2}{n}\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{-k} B_{1,\chi_p}) = \frac{2}{n}\sum_{\substack{i=1 \\ i \text{ odd}}}^{n-1} \zeta_n^{-ik} B_{1,\chi_p^i}$$

is a rational integer, which according to part 1 of Lemma 4.1, satisfies

$$|a_k| \leq \max_{\substack{1 \leq i \leq n-1 \\ i \text{ odd}}} |B_{1,\chi_p^i}| \leq \frac{1}{2\pi}\sqrt{p}(\log p + 2)$$

Finally, all these a_k are odd.

Proof. If one of these a_k's were even then all of them would be even, $2^{n/2}$ would divide $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(B_{1,\chi_p})$ and h_p^- would be even (use 5–1), a contradiction. □

Now, let $p \equiv 1+n \pmod{2n}$ be given and let us explain how we compute h_p^-, the relative class number of the imaginary abelian field of degree n and conductor p. To begin with, we use Theorem 3.1 to verify that for all the $\chi \in X_{n,p}^-$ we have $g(1,\chi) \neq 0$. We have not yet found any χ such that Theorem 3.1 would not imply $g(1,\chi) \neq 0$. Then we use Theorem 4.2: we let m be the least integer greater than or equal to $B(\frac{3}{2}+\varepsilon, M, f)$ and compute approximations $\tilde{B}_{1,\chi}(m)$ of all $B_{1,\chi}$ for $\chi \in X^-_{n,p}$ (in practice, we choose $M = 15$). Setting

$$\tilde{a}_k = \frac{2}{n}\sum_{\substack{i=1\\ i \text{ odd}}}^{n-1} \zeta_n^{-ik}\tilde{B}_{1,\chi_p^i}(m)$$

we get $|a_k - \tilde{a}_k| < 2e^{-M}$, so that a_k is the nearest integer to $\tilde{a}_k$, and we have computed the exact values of all the a_k's. It is worth noticing that the absolute values of all the $B_{1,\chi_p^i}(m)$ being less than $\frac{\sqrt{p}}{2\pi}(\log f + 2)$, then even for very large values of p we need only work with complex numbers of reasonable absolute values to compute the exact values of the coordinates of B_{1,χ_p}.

It remains to explain how we compute h_p^-. Here of course, we need to work with large precision arithmetic on integers. Setting $S_p(r) = B_{1,\chi_p} \in \mathbb{Z}[\zeta_n]$ and

$$S_p(i) = N_{\mathbb{Q}(\zeta_{2^{i+1}})/\mathbb{Q}(\zeta_{2^i})}(S_p(i+1)) \in \mathbb{Q}(\zeta_{2^i})$$

for $1 \le i \le r-1$, we can write

$$S_p(i) = \sum_{j=0}^{2^{i-1}-1} a_i(j)\zeta_{2^i}^j$$

with

$$\begin{aligned} S_p(i) &= \Bigl(\sum_{j=0}^{2^{i-1}-1} a_i(2j)\zeta_{2^i}^j\Bigr)^2 - \zeta_{2^i}\Bigl(\sum_{j=0}^{2^{i-1}-1} a_i(2j+1)\zeta_{2^i}^j\Bigr)^2 \\ &= \sum_{j=0}^{2^i-1} A_j\zeta_{2^i}^j = \sum_{j=0}^{2^{i-1}-1} a_i(j)\zeta_{2^i}^j, \end{aligned}$$

where $A_0 = (a_i(0))^2$, $A_{2^i-1} = -(a_i(2^i-1))^2$,

$$\begin{aligned} A_j = &\sum_{k=\max(0,j-(2^{i-1}-1))}^{\min(j,2^{i-1}-1)} a_i(2k)a_i(2j-2k) \\ &- \sum_{k=\max(0,j-2^{i-1})}^{\min(j-1,2^{i-1}-1)} a_i(2k+1)a_i(2j-2k-1) \end{aligned}$$

(for $1 \le j \le 2^i - 2$) and $a_{i-1}(j) = A_j - A_{j+2^{i-1}}$ (for $0 \le j \le 2^{i-1}-1$), which enables us to compute the exact value of the positive integer

$$S_p(1) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(B_{1,\chi_p}) = 2^{(n/2)-1}h_p^-.$$

Since we do not have any positive lower bound on the absolute values of the $g(1,\chi)$'s, for we do not even know how to prove they are never equal to zero, we cannot give any proved upper bound on the number of elementary operations our algorithm requires for computing h_p^-. However, in practice, $|g(1,\chi)|$ is never very small so that we may use the bound $B(\frac{3}{2}+\varepsilon, M, f)$ with $M = 15$. We have programmed our formulas in Kida's language Ubasic, which allows fast arbitrary precision calculation on PC's.

For example, let $\mathbf{N}_p$ be the imaginary abelian field of degree 32 and conductor $p = 10^{10}+97$. We get $\min_{\substack{1\le i\le p-1\\ i \text{ odd}}} |g(1,\chi_p^i)| = 456\ 382.26\cdots$, $B_{1,\chi_p} = \sum_{k=0}^{15} a_k\zeta_{32}^k$ with

k	a_k	k	a_k	k	a_k	k	a_k
0	−4809	4	421	8	3991	12	−7377
1	−2705	5	1933	9	2781	13	−7021
2	7729	6	819	10	−13879	14	−4091
3	2979	7	2541	11	−2221	15	537

and $h_p^- = 22391\ 83221\ 41405\ 05711\ 42075\ 03659\ 49593\ 37650\ 55905\ 64162\ 98557\ 82256\ 60609 \approx 2\cdot 10^{64}$.

Now let $\mathbf{N}_p$ be the imaginary abelian field of degree 32 and conductor $p = 10^{13}+609$. We get $\min_{\substack{1\le i\le p-1\\ i \text{ odd}}} |g(1,\chi_p^i)| = 173\ 010\ 991.29\cdots$, $B_{1,\chi_p} = \sum_{k=0}^{15} a_k\zeta_{32}^k$ with

k	a_k	k	a_k	k	a_k	k	a_k
0	−216157	4	−213847	8	−160929	12	152601
1	−211319	5	−264627	9	35681	13	−271679
2	74357	6	−25413	10	309661	14	388853
3	396321	7	−238953	11	−15135	15	537675

and $h_p^- = 10\ 57160\ 41460\ 14284\ 21537\ 30049\ 35283\ 89944\ 64043\ 49937\ 90979\ 09467\ 19576\ 76809\ 23876\ 07191\ 38750\ 25726\ 21601 \approx 10^{91}$.

6. THE IMAGINARY CYCLIC QUARTIC CASE

We now focus on imaginary cyclic quartic fields of prime conductors $p \equiv 5 \pmod 8$, for here we almost have an explicit formula for ε_{χ_p}. Note that $n_p = 2$ and $\mathbf{N}_p = \mathbb{Q}(\sqrt{-(p+b\sqrt{p})})$, where $p = a^2 + b^2$ with $a \geq 1$ odd and b even.

Proposition 6.1. *Let $p = a^2 + b^2 \equiv 1 \pmod 4$ be prime and set*

$$\alpha_p = \sqrt{\frac{p + a\sqrt{p}}{2}} + i\frac{b}{|b|}\sqrt{\frac{p - a\sqrt{p}}{2}}.$$

1. *For $\alpha \in \mathbb{Z}[i]$ coprime with $\pi = a + ib$ let the quartic residue symbol $[\frac{\alpha}{\pi}] \in \{\pm 1, \pm i\}$ be defined by $\alpha^{(p-1)/4} \equiv [\frac{\alpha}{\pi}] \pmod \pi$. We have*

$$\left[\frac{2}{\pi}\right] = (-1)^{(p-1)/4} i^{-ab/2}.$$

2. *Let $p = a^2 + b^2 \equiv 5 \pmod 8$ be prime, where $a \equiv -1 \pmod 4$ and $b \equiv 2 \pmod 4$ are rational integers. Hence, $ab \equiv 2 \pmod 4$. Choose the sign of b so that*

$$i = \chi_p(2) = \left[\frac{2}{\pi}\right] = -i^{-ab/2},$$

i.e., so that $ab \equiv 2 \pmod 8$. Then, for some $\varepsilon_p = \pm 1$, we have $\tau_{\chi_p} = \varepsilon_p \alpha_p$.

Proof. We may assume that a is odd. We let $(\frac{\alpha}{\beta})$ denote quadratic residue symbols. We have

$$\left[\frac{2}{\pi}\right] = \left[\frac{-i(1+i)^2}{\pi}\right] = \left[\frac{-i}{\pi}\right]\left(\frac{1+i}{\pi}\right) = (-1)^{(p-1)/4} i^{((a^2+b^2)-1)/4}\left(\frac{1+i}{\pi}\right)$$

(for $[\frac{i}{\pi}] = i^{(p-1)/4}$), and $a(1+i) \equiv a + b \pmod \pi$ yields

$$\begin{aligned}\left(\frac{1+i}{\pi}\right) &= \left(\frac{a(a+b)}{p}\right) \\ &= \left(\frac{|a||a+b|}{p}\right) = \left(\frac{p}{|a|}\right)\left(\frac{p}{|a+b|}\right) \\ &= \left(\frac{p}{|a+b|}\right) = \left(\frac{2a^2}{|a+b|}\right) = \left(\frac{2}{|a+b|}\right) \\ &= i^{-((a+b)^2-1)/4}.\end{aligned}$$

If the sign of b is chosen as required, then according to part 1 we have $\chi_p = (/\pi)_4$ where $\pi = a + ib$ and the desired result follows from [Ireland and Rosen 1990, Lemma 6 on page 121 and Proposition 9.10.1] which yield $\tau_{\chi_p}^2 = \pi\sqrt{p}$. Note also that according to [Berndt and Evans 1981] there is no known efficient technique for computing numerically this sign ε_p. □

Once we have proved, using Theorem 3.1, that $g(1, \chi_p) \neq 0$, and once we have computed good approximations of ε_{χ_p}, we can deduce the exact values of $\pm 1 = \varepsilon_p = \tau_{\chi_p}/\alpha_p = i\sqrt{p}\varepsilon_{\chi_p}/\alpha_p$ and $\tau_{\chi_p} = \varepsilon_p \alpha_p$. Then, according to Lemma 4.1 and since $B_{1,\chi_p} = x + yi$ is in $\mathbb{Z}[i]$, we need compute only $B(\frac{1}{2}, M, f)$ terms to determine the exact value of B_{1,χ_p} and we end up with an exact value for $L(1, \chi_p)$. For example, with $p = 10^{10} + 61 = 88795^2 + (-45994)^2$ we found $\varepsilon_p = +1$, $B_{1,\chi_p} = 12099 + 20507i$, $h_p^- = \frac{1}{2}|B_{1,\bar{\chi}_p}|^2 = 283\ 461\ 425 = 5^2 \cdot 13 \cdot 872169$ and

$$\begin{aligned}L(1, \chi_p) &= -\frac{\pi}{\sqrt{p}}\varepsilon_{\chi_p} B_{1,\bar{\chi}_p} = i\pi\overline{B_{1,\chi_p}/\tau_{\chi_p}} \\ &= \pi\frac{20507 + 12099i}{\sqrt{\frac{p + 88795\sqrt{p}}{2}} + i\sqrt{\frac{p - 88795\sqrt{p}}{2}}}. \\ &= 0.715907801\cdots - 0.216809690\cdots i\end{aligned}$$

Note that we could not have computed τ_{χ_p} or B_{1,χ_p} easily by simply using their definition, for this p is much too large. Here are two more examples:

1. If $p = 10^{14} + 133 = 9919967^2 + 1262638^2$ then $\varepsilon_p = -1$, $B_{1,\chi_p} = 145937 - 3209401i$ and $h_p^- = 5\ 160\ 776\ 193\ 385$.

2. If $p = 10^{15} + 37 = 17936879^2 + (-26043586)^2$ then $\varepsilon_p = -1$, $B_{1,\chi_p} = -9475929 + 163987i$ and $h_p^- = 44\ 910\ 061\ 074\ 605$.

Proposition 6.2. *There are* 166204 *primes* $p \equiv 5 \pmod 8$ *less than or equal to* 10^7. *For* 82204 *out of them we have* $\varepsilon_p = +1$ *while for the* 84000 *remaining ones we have* $\varepsilon_p = -1$.

Theorem 6.3. *For any prime* $p \equiv 5 \pmod 8$ *let* h_p^- *denote the relative class number of the imaginary cyclic quartic fields of conductor* p. *Then*

1. *For the* 64 *primes* $p \equiv 5 \pmod 8$ *less than* 1621 *we have* $h_p^- \le p/5$, *but* $h_{1621}^- = 333$.
2. *For the* 814 *primes* $p \equiv 5 \pmod 8$ *less than* 29989 *we have* $h_p^- \le p/4$, *but* $h_{29989}^- = 8325$.
3. *For the* 11878 *primes* $p \equiv 5 \pmod 8$ *less than* 578029 *we have* $h_p^- \le p/3$, *but* $h_{578029}^- = 198725$.
4. *For the* 109542 *primes* $p \equiv 5 \pmod 8$ *such that* $p < 6389629$ *we have* $h_p^- \le 2p/5$, *but* $h_{6389629}^- = 2765413$.

We have not been able to find the smallest prime $p \equiv 5 \pmod 8$ such that $h_p^- \ge p/2$. Nevertheless, we note that there are 77 primes $p \equiv 5 \pmod 8$ less than 1679516029 such that $\chi_p(q) = +1$ for the first nine odd primes $q \in \{3, 5, 7, 11, 13, 17, 19, 23, 29\}$. They all have relative class numbers h_p^- less than $p/2$, but $h_{1679516029}^- = 904595821 > p/2$. It can be proved that for any $c > 0$ there are infinitely many primes $p \equiv 5 \pmod 8$ such that $h_p^- \ge cp$.

7. AN APPLICATION OF SUCH EXTENSIVE COMPUTATIONS

To conclude this paper, we finally give one possible use of our efficient technique for doing extensive computations of relative class numbers of imaginary cyclic fields of 2-power degrees and (large) prime conductors: they are useful when dealing with Catalan's equation $x^p - y^q = 1$ (here x and y denote relative integers, and p and q denote positive integers (we may assume that p and q are prime)). This equation has only finitely many solutions [Tijdeman 1976]. But to date, it is not proved that its only solutions are the trivial ones. However, in using the following Theorem, bounds on relative class numbers and extensive relative class number computation, various authors [Mignotte and Roy 1997; Steiner 1998] have lately proved that if Catalan's equation has a non-trivial solution (x, y, p, q) then $\min(p, q)$ must be large.

Theorem 7.1 [Schwarz 1995]. *Let* $p \ne q$ *be odd prime numbers and let* $\mathbf{N}_p$ *denote the imaginary subfield of* 2*-power degree of the cyclotomic field* $\mathbb{Q}(\zeta_p)$. *Then Catalan's equation* $x^p - y^q = 1$ *has no non-trivial integral solution if* $p^{q-1} \not\equiv 1 \pmod{q^2}$ *and* q *does not divide* h_p^-.

Let us sketch how they use this Theorem. First, assume $p \equiv 3 \pmod 4$ and $p < q$. Then $\mathbf{N}_p = \mathbb{Q}(\sqrt{-p})$ is an imaginary quadratic field and we always have $h_p^- < p$. Therefore, if Catalan's equation $x^p - y^q = 1$ has a non-trivial integral solution then $p^{q-1} \equiv 1 \pmod{q^2}$. Now, assume $p \equiv 5 \pmod 8$ and $p < q$. Then $\mathbf{N}_p$ is the imaginary cyclic quartic field of conductor p and we do not always have $h_p^- < p$. However, according to our computation, if $p < 10^7$ and if Catalan's equation $x^p - y^q = 1$ has a non-trivial integral solution, then $p^{q-1} \equiv 1 \pmod{q^2}$. We refer the reader to [Mignotte and Roy 1997] for a lesser trivial and more comprehensive exposition of the usefulness of such relative class number considerations to prove that Catalan's equation often has no non-trivial solution. We also refer the reader to [Steiner 1998].

REFERENCES

[Berndt and Evans 1981] B. C. Berndt and R. J. Evans, "The determination of Gauss sums", *Bull. Amer. Math. Soc.* (*N.S.*) **5**:2 (1981), 107–129. Corrigendum im **7**:2 (1982), 441.

[Fröhlich 1972] A. Fröhlich, "Artin root numbers and normal integral bases for quaternion fields", *Invent. Math.* **17** (1972), 143–166.

[Ireland and Rosen 1990] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second ed., Graduate Texts in Mathematics, Springer, New York, 1990.

[Louboutin 1996] S. Louboutin, “Majorations explicites de $|L(1,\chi)|$, II”, *C. R. Acad. Sci. Paris Sér. I Math.* **323**:5 (1996), 443–446.

[Louboutin $\geq$ 1998] S. Louboutin,

“Computation of relative class numbers of CM-fields by using Hecke L-functions” *Math. Comp.*. to appear.

[Mignotte and Roy 1997] M. Mignotte and Y. Roy, “Minorations pour l'équation de Catalan”, *C. R. Acad. Sci. Paris Sér. I Math.* **324**:4 (1997), 377–380.

[Schoof and Washington 1988] R. Schoof and L. C. Washington, “Quintic polynomials and real cyclotomic fields with large class numbers”, *Math. Comp.* **50**:182 (1988), 543–556.

[Schwarz 1995] W. Schwarz, “A note on Catalan's equation”, *Acta Arith.* **72**:3 (1995), 277–279.

[Seah et al. 1983] E. Seah, L. C. Washington, and H. C. Williams, “The calculation of a large cubic class number with an application to real cyclotomic fields”, *Math. Comp.* **41**:163 (1983), 303–305.

[Steiner 1998] R. Steiner, “Class number bounds and Catalan's equation”, *Math. Comp.* **67**:223 (1998), 1317–1322.

[Tijdeman 1976] R. Tijdeman, “On the equation of Catalan”, *Acta Arith.* **29**:2 (1976), 197–209.

[Wall 1948] H. S. Wall, *Analytic theory of continued fractions*, Van Nostrand, New York, 1948.

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997.

[Williams and Broere 1976] H. C. Williams and J. Broere, “A computational technique for evaluating $L(1,\chi)$ and the class number of a real quadratic field”, *Math. Comp.* **30**:136 (1976), 887–893.

Stéphane Louboutin, Université de Caen, UFR Sciences, Département de Mathématiques, 14032 Caen, France, loubouti@math.unicaen.fr

Received June 23, 1997; accepted in revised form February 12, 1998