MATHEMATICS OF COMPUTATION
Volume 69, Number 231, Pages 1229–1244
S 0025-5718(99)01111-4
Article electronically published on March 10, 1999

COMPUTING THE HILBERT CLASS FIELD OF REAL QUADRATIC FIELDS

HENRI COHEN AND XAVIER-FRANÇOIS ROBLOT

ABSTRACT. Using the units appearing in Stark's conjectures on the values of L-functions at $s = 0$, we give a complete algorithm for computing an explicit generator of the Hilbert class field of a real quadratic field.

Let k be a real quadratic field of discriminant d_k, so that $k = \mathbb{Q}(\sqrt{d_k})$, and let ω denote an algebraic integer such that the ring of integers of k is $\mathcal{O}_k := \mathbb{Z} + \omega\mathbb{Z}$. An important invariant of k is its class group Cl_k, which is, by class field theory, associated to an Abelian extension of k, the so-called Hilbert class field, denoted by H_k. This field is characterized as the maximal Abelian extension of k which is unramified at all (finite and infinite) places. Its Galois group is isomorphic to the class group Cl_k; hence the degree $[H_k : k]$ is the class number h_k.

There now exist very satisfactory algorithms to compute the discriminant, the ring of integers and the class group of a number field, and especially of a quadratic field (see [3] and [16]). For the computation of the Hilbert class field, however, there exists an efficient version only for complex quadratic fields, using complex multiplication (see [18]), and a general method for all number fields, using Kummer theory, which is not really satisfactory except when the ground field contains enough roots of unity (see [6], [9] or [15]).

In this paper, we will explore a third way, available for totally real fields, which uses the units appearing in Stark's conjectures [21], the so-called Stark units, to provide an efficient algorithm to compute the Hilbert class field of a real quadratic field. This method relies on the truth of Stark's conjecture (which is not yet proved!), but still we can prove independently of the conjecture that the field obtained is indeed the Hilbert class field and thus forget about the fact that we had to use this conjecture in the first place.

Of course, the possibility of using Stark units for computing Hilbert or ray class fields was known from the beginning, and was one of the motivations for Stark's conjectures. Stark himself gave many examples. It seems, however, that a complete algorithm has not appeared in the literature, and it is the purpose of this paper to give one for the case of real quadratic fields.

In Section 1, we say a few words about how to construct the Hilbert class field of k when the class number is equal to 2. Here, two methods can be used which are very efficient in this case: Kummer theory and genus field theory. In Section 2 we give a special form of Stark's conjectures, namely the Abelian rank one conjecture applied to a particular construction. Section 3 is devoted to the description of the

Received by the editor January 19, 1998 and, in revised form, September 10, 1998.
1991 *Mathematics Subject Classification.* Primary 11R37, 11R42; Secondary 11Y35.

algorithm, and Section 4 to the verification of the result. Section 5 deals with an example.

We end the paper with an Appendix giving a table of Hilbert class fields of real quadratic fields of discriminant less than 2 000.

1. Construction when the class number is equal to 2

We assume in this section that $h_k = 2$. As we already said, in this case there are two powerful methods to compute H_k, and we quote them without proof.

The first uses Kummer theory, which states that when the ground field contains the n-roots of unity, every Abelian extension of exponent dividing n can be obtained by taking n-th roots of elements of the ground field. From this, one easily obtains

Proposition 1.1. *Let k be a real quadratic field of class number 2, let v be a real embedding of k, let η denote the fundamental unit of k such that $v(\eta) > 1$, and let $\mathfrak{A}$ be a non-principal integral ideal of k. Let α be one of the generators of $\mathfrak{A}^2$ chosen so that $v(\alpha) > 0$. Then $H_k = k(\sqrt{\theta})$ for some $\theta \in \{\eta, \alpha, \eta\alpha\}$.*

The second method uses genus field theory, which enables one to construct unramified Abelian extensions of k by taking the compositum of k with Abelian extensions of $\mathbb{Q}$ (see [11]).

Proposition 1.2. *There exists a divisor d of the discriminant d_k with $1 < d < d_k$ and $d \equiv 0, 1 \pmod 4$ such that $H_k = k(\sqrt{d})$.*

Hence the determination of H_k in this case boils down to a finite number of easy tests.

2. A special case of Stark's conjectures

We now assume only that $h_k > 1$. We keep the same notations, we let v be one of the real embeddings of k and we denote by $^-$ the action of the non-trivial element of the Galois group of $k/\mathbb{Q}$. We will identify k with its embedded image $v(k)$ into $\mathbb{R}$. Let K be a quadratic extension of H_k such that K/k is Abelian and v stays real in this extension but $\overline{v}$ becomes complex. We identify K with one of its embedded images in $\mathbb{R}$ (so with one of its images $w(K)$, where w is a place above v).

Let $\mathfrak{f}$ denote the conductor of K/k and G its Galois group. Let $I_k(\mathfrak{f})$ denote the group of fractional ideals coprime with the finite part $\mathfrak{f}_0$ of this conductor, let $P_k(\mathfrak{f})$ denote the group of principal ideals generated by elements multiplicatively congruent to 1 modulo $\mathfrak{f}$, and let $Cl_k(\mathfrak{f}) := I_k(\mathfrak{f})/P_k(\mathfrak{f})$ be the ray class group modulo $\mathfrak{f}$. The Artin map sends any ideal $\mathfrak{A} \in I_k(\mathfrak{f})$ to an element $\sigma_{\mathfrak{A}}$ of the Galois group G, the so-called Artin symbol of $\mathfrak{A}$. For any element $\sigma \in G$ and any complex number s with $\mathrm{Re}(s) > 1$, we can thus define a partial zeta function

$$\zeta_{K/k}(s, \sigma) := \sum_{\sigma_{\mathfrak{A}} = \sigma} \mathcal{N}\mathfrak{A}^{-s},$$

where $\mathfrak{A}$ runs through the integral ideals of $I_k(\mathfrak{f})$ whose Artin symbol is equal to σ. These functions have a meromorphic continuation to the whole complex plane with a simple pole at $s = 1$ and, in our situation, a simple zero at $s = 0$.

Theorem 2.1. *Assume the Abelian rank one Stark conjecture. Then there exists a unit $\varepsilon \in K$ such that*

$$\sigma(\varepsilon) = e^{-2\zeta'_{K/k}(0,\sigma)}$$

for any $\sigma \in G$. *Furthermore, if we set* $\alpha := \varepsilon + \varepsilon^{-1}$, *we have* $H_k = k(\alpha)$ *and* $|\alpha|_w \leq 2$ *for any infinite place* w *of* H_k *which does not divide* v.

We refer to [22] for this conjecture and a more general statement of Stark's conjectures, and to [17] for a proof of this result.

In the next section, we will explain how to compute $\zeta'_{K/k}(0,\sigma)$ for $\sigma \in G$, and how to find the element α as an algebraic number, if it exists.

3. Description of the algorithm

The first task is to find the field K. An easy way is to construct an element $\delta \in \mathcal{O}_k$ such that $\delta > 0$ and $\overline{\delta} < 0$, and to set $K := H_k(\sqrt{\delta})$. Another way is to construct the field K using class field theory. Such a field has conductor $\mathfrak{A}\overline{v}$ for an integral ideal $\mathfrak{A}$ and corresponds *via* class field theory to a subgroup of index 2 of the kernel of the map $Cl_k(\mathfrak{f}) \twoheadrightarrow Cl_k$ where Cl_k is the usual class group. Indeed, the kernel of this map corresponds to the Hilbert class field, and thus its subgroups of index 2 correspond to quadratic extensions of H_k. Hence, we may compute the ray class group modulo $\mathfrak{A}\overline{v}$, where $\mathfrak{A}$ runs through the integral ideals $\mathfrak{A}$, by increasing norm, then compute $\ker(Cl_k(\mathfrak{f}) \twoheadrightarrow Cl_k)$ and check if it contains a subgroup of index 2 whose conductor is $\mathfrak{A}\overline{v}$.

This last idea is probably the best, since heuristics and numerical evidence show that the Stark unit tends to grow exponentially like the square root of the norm of the conductor of K; hence we need to minimize this norm.

Algorithm 3.1. *This algorithm computes a modulus* $\mathfrak{f}$ *and a subgroup* $\mathcal{H}$ *of* $Cl_k(\mathfrak{f})$ *such that* $\mathfrak{f}$ *is the conductor of* $\mathcal{H}$ *and the field* K *corresponding to* $\mathcal{H}$ *by class field theory is a quadratic extension of* H_k *where* v *splits and* $\overline{v}$ *becomes complex. This algorithm uses the tools of* [6].

1. *Set* $n \leftarrow 2$.

2. *Compute the integral ideals* $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$ *of norm* n. *Set* $c \leftarrow 1$.

3. *If* $c > m$ *then set* $n \leftarrow n+1$ *and go back to step* ***2****. Otherwise, set* $\mathfrak{f} \leftarrow \mathfrak{A}_c\overline{v}$. *If* $\mathfrak{f}$ *is a conductor then go to step* ***4****, else set* $c \leftarrow c+1$ *and go to step* ***3****.*

4. *Compute the kernel of* $Cl_k(\mathfrak{f}) \twoheadrightarrow Cl_k$ *and then its subgroups* $\mathcal{H}_1, \ldots, \mathcal{H}_l$ *of index 2. Set* $d \leftarrow 1$.

5. *If* $d > l$ *then set* $c \leftarrow c+1$ *and go back to step* ***3****. If* $\mathfrak{f}$ *is the conductor of* $\mathcal{H}_d$ *then return the result* $(\mathfrak{f}, \mathcal{H}_d)$ *and terminate the algorithm, else set* $d \leftarrow d+1$ *and go to step* ***5****.*

Once the field K is chosen, we need to compute the values $\zeta'_{K/k}(0,\sigma)$. For this purpose, we use Hecke L-functions (see [13] for the more general theory of Artin L-functions). Let χ be a character of $G := Gal(K/k)$. By composition with the Artin map, χ can be considered as being defined on the group $I_k(\mathfrak{f})$. If s denotes a complex number with $\mathrm{Re}(s) > 1$, we define

$$L_{K/k}(s,\chi) := \prod_{\mathfrak{p} \text{ unramified}} (1 - \chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{-1},$$

where $\mathfrak{p}$ runs through the prime ideals of k unramified in K/k. These functions have meromorphic continuations (even holomorphic if χ is non-trivial) to the whole

complex plane and are related to the partial zeta functions by the formula

$$(*) \qquad \zeta_{K/k}(s,\sigma) = \frac{1}{[K:k]} \sum_{\chi \in \widehat{G}} L_{K/k}(s,\chi)\overline{\chi}(\sigma),$$

where the sum is taken over all characters of G.

Let χ be a character of G and let τ denote the non-trivial automorphism of the quadratic extension K/H_k. If $\chi(\tau) = 1$, the functional equation implies that $L'_{K/k}(0,\chi) = 0$; hence χ will not contribute to the value of $\zeta'_{K/k}(0,\sigma)$ in $(*)$. Thus from now on we assume that $\chi(\tau) = -1$. We extend χ to all ideals of k by setting $\chi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is not coprime with the conductor $\mathfrak{f}_\chi$ of χ. To each character χ is associated a canonical L-function defined for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ by

$$L(s,\chi) := \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s})^{-1},$$

where the product is taken over all prime ideals of k.

Lemma 3.2. *Let χ be a character such that $\chi(\tau) = -1$. Then $\mathfrak{f}_\chi = \mathfrak{f}$. In particular, $L_{K/k}(s,\chi) = L(s,\chi)$.*

Proof. Let K_χ be the subfield of K fixed by the kernel of χ. By definition the conductor of K_χ is equal to $\mathfrak{f}_\chi$. It is clear that the conductor of $H_k K_\chi$ is also equal to $\mathfrak{f}_\chi$, and moreover $H_k K_\chi = K$ since K_χ is not included in H_k; thus $\mathfrak{f}_\chi = \mathfrak{f}$. □

We set

$$\Lambda(s,\chi) := C^s \Gamma(s/2)\Gamma\left(\frac{s+1}{2}\right) L(s,\chi),$$

where $C := \pi^{-1}\sqrt{d_k \mathcal{N}\mathfrak{f}}$ and $\Gamma(z)$ is the classical gamma function. This function satisfies the fundamental functional equation

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\overline{\chi}),$$

where $W(\chi)$ is a complex number of modulus equal to 1, called the Artin root number.

Theorem 3.3. *Let $\varkappa > 0$ be a real number. For $n \geq 1$, let*

$$a_n(\chi) := \sum_{\mathcal{N}\mathfrak{A} = n} \chi(\mathfrak{A}),$$

where the sum is taken over all integral ideals of norm n, and let $N := \left\lceil \frac{-C \log \varkappa}{2} \right\rceil$. Define the following two quantities:

$$T(\chi) := \sum_{n=1}^{N} a_n(\overline{\chi}) f_1(C/n),$$

$$S(\chi) := \sum_{n=1}^{N} a_n(\chi) f_2(C/n),$$

with $f_1(x) := \frac{x}{2} e^{-2/x}$ and $f_2(x) := Ei(2/x)$, where $Ei(x) = \int_x^{+\infty} e^{-t} dt/t$ is the exponential integral function. Then

$$L'(0,\chi) = S(\chi) + W(\chi)T(\chi) + \kappa,$$

where the error term κ is smaller than $\varkappa$.

Proof. Letting s tend to 1 in the functional equation gives

$$L'(0,\chi) = \frac{W(\chi)\Lambda(1,\overline{\chi})}{2\sqrt{\pi}}.$$

Then a theorem of Friedman [10] tells us that

$$\Lambda(1,\overline{\chi}) = \sum_{n\geq 1}\left[\overline{a_n(\chi)}f(C/n,1) + \overline{W(\chi)}a_n(\chi)f(C/n,0)\right],$$

where the function f is defined by

$$f(x,s) := \frac{1}{2i\pi}\int_{\sigma-i\infty}^{\sigma+i\infty} x^z \frac{\Gamma(z/2)\Gamma\left(\frac{z+1}{2}\right)}{z-s}\,dz = \frac{2\sqrt{\pi}}{2i\pi}\int_{\sigma-i\infty}^{\sigma+i\infty}\left(\frac{2}{x}\right)^{-z}\frac{\Gamma(z)}{z-s}\,dz$$

for any real number σ such that $\sigma > \mathrm{Re}(s)$. If we differentiate f with respect to the variable x and use the fact that $z/(z-s) = 1 + s/(z-s)$, we obtain

$$xf'(x,s) = \frac{2\sqrt{\pi}}{2i\pi}\int_{\sigma-i\infty}^{\sigma+i\infty}\left(\frac{2}{x}\right)^{-z}\Gamma(z)\,dz + sf(x,s).$$

We solve the differential equation and find that

$$f(x,s) = x^s\int_{1/x}^{+\infty} t^{s-1}F(t)\,dt,$$

where

$$F(t) := \frac{2\sqrt{\pi}}{2i\pi}\int_{\sigma-i\infty}^{\sigma+i\infty}(2t)^{-z}\Gamma(z)\,dz.$$

But the theory of Mellin transforms (see for example [20], Chapter 4) tells us that $F(t) = 2\sqrt{\pi}e^{-2t}$, and thus $f(x,1) = 2\sqrt{\pi}f_1(x)$ and $f(x,0) = 2\sqrt{\pi}f_2(x)$. Finally, we compute the number of terms needed for sufficient accuracy by looking at the asymptotic expansion of the functions f_1 and f_2. □

Thus, we need to compute the following three objects. First, the coefficients $a_n(\chi)$. Second, the functions f_1 and f_2 (there of course exist methods to compute these functions, but here we are interested in efficient methods to compute them for many consecutive values of n). Third, the values of $W(\chi)$.

We compute the coefficients $a_n(\chi)$ by using the multiplicative property

$$a_n(\chi) = a_{n/p^m}(\chi)a_{p^m}(\chi),$$

where p^m is the largest power of p that divides n.

Algorithm 3.4. *Let N be an integer and let χ be a character of G such that $\chi(\tau) = -1$. This algorithm computes the coefficients $a_n(\chi)$ for $1 \leq n \leq N$ using the sub-algorithm* ***fill-in****(ϕ,p) which distributes the value of $a_{p^m}(\chi)$ according to the function $\phi : \mathbb{N}\setminus\{0\} \to \mathbb{C}$ (recall that $\chi(\mathfrak{p})$ is set equal to zero whenever the prime ideal $\mathfrak{p}$ divides the conductor of χ).*

1. *For n going from $1 \leq n \leq N$ set $a_n(\chi) \leftarrow 1$ and set $p \leftarrow 1$.*

2. *Set $p \leftarrow$ (least prime $> p$), and if $p > N$ return the coefficients $a_n(\chi)$ for $1 \leq n \leq N$ and terminate the algorithm.*

3a. *If p is inert: for m odd set $\phi(m) = 0$, and for m even, set $\phi(m) = \chi(p)^m$. Execute* ***fill-in****(ϕ,p) and go to step* ***2.***

3b. *If p is ramified: write $p\mathcal{O}_k = \mathfrak{p}^2$ and set $\phi(m) = \chi(\mathfrak{p})^m$. Execute* ***fill-in****(ϕ,p) and go to step* ***2.***

3c. *If p splits: write $p\mathcal{O}_k = \mathfrak{p}\overline{\mathfrak{p}}$. if $\chi(\mathfrak{p}) \neq \chi(\overline{\mathfrak{p}})$, set*

$$\phi(m) = \frac{\chi(\mathfrak{p})^{m+1} - \chi(\overline{\mathfrak{p}})^{m+1}}{\chi(\mathfrak{p}) - \chi(\overline{\mathfrak{p}})},$$

else set

$$\phi(m) = (m+1)\chi(\mathfrak{p})^m.$$

Execute ***fill-in****(ϕ, p) and go to step* ***2.***
Sub-algorithm ***fill-in****(ϕ, p).*

1. *Set $q \leftarrow 1$ and $m \leftarrow 0$.*

2. *Set $q \leftarrow qp$ and $m \leftarrow m+1$. If $q > N$ then terminate the sub-algorithm else set $c \leftarrow q$ and $d \leftarrow 1$.*

3. *If p does not divide d then set $a_c(\chi) = a_c(\chi)\phi(m)$.*

4. *Set $c \leftarrow c+q$ and $d \leftarrow d+1$. If $c < N$ then go to step* ***3****, else go to step* ***2.***

We now need to compute the functions $f_1(C/n)$ and $f_2(C/n)$ for consecutive values of n. For $f_1(C/n) = \frac{C}{2n}e^{-2n/C}$, the algorithm is very simple.

Algorithm 3.5. *Let $A > 0$ be a real number and let $N \geq 1$ be an integer. This algorithm computes the values of $f_1(A/n)$ for $1 \leq n \leq N$.*

1. *Set $V \leftarrow e^{-2/A}, V_1 \leftarrow AV/2, U_1 \leftarrow V_1$ and $n \leftarrow 2$.*

2. *While $n \leq N$, set*

$$U_n \leftarrow U_{n-1} \cdot V,\ V_n \leftarrow \frac{U_n}{n}$$

and $n \leftarrow n+1$.

3. *Return the values V_n for $1 \leq n \leq N$.*

We compute the values of $f_2(C/n) = Ei(2n/C)$ in the same spirit, that is to say by trying to compute the function Ei for only a very few values. For this, we use the following lemma.

Lemma 3.6. *Let $A > 0$ be a positive constant and define $\phi(x) := Ei(xA)$. Then $\phi'(x) = -\frac{1}{x}e^{-xA}$, and more generally for all $m \geq 1$ we have the induction formula*

$$\phi^{(m+1)}(x) = \frac{-1}{x}\left(m\phi^{(m)}(x) + (-A)^m e^{-xA}\right).$$

Proof. The first assertion comes from the definition of the exponential integral function $Ei(x) = \int_x^{+\infty} e^{-t}dt/t$, and the second is easily proved by induction. □

If we have computed $\phi(N)$ we may obtain $\phi(N-1)$ by using Taylor's formula:

$$\phi(N-1) = \phi(N) - \phi'(N) + \frac{1}{2!}\phi''(N) - \frac{1}{3!}\phi^{(3)}(N) + \frac{1}{4!}\phi^{(4)}(N) - ...$$

where the derivatives $\phi^{(m)}(N)$ can be computed by the previous lemma. Moreover, since $(-1)^m\frac{1}{m!}\phi^{(m)}(N)$ is always positive, we need only to sum these terms and stop as soon as the next term becomes smaller than the required precision.

Algorithm 3.7. *Let $A > 0$ be a positive constant and let $N \geq 1$ be an integer. This algorithm computes the values $Ei(nA)$ for $1 \leq n \leq N$ with the precision $\varkappa > 0$.*

1. *Set $F_N \leftarrow Ei(NA)$, $n_{\text{stop}} \leftarrow \lceil 4/A \rceil$ and $n \leftarrow N$. Set also $e_0 \leftarrow e^A$ and $e_1 \leftarrow e^{-NA}$.*

2. *Set $F_{n-1} \leftarrow 0$, $f_0 \leftarrow e_1$, $f_1 \leftarrow -f_0/n$ and $m \leftarrow 1$, $d \leftarrow -1$, $s \leftarrow F_n$.*

3. *If* $|s| > \varkappa$ *then set* $F_{n-1} \leftarrow F_{n-1} + s$, $s \leftarrow df_1$, $f_0 \leftarrow -Af_0$,

$$f_1 \leftarrow -\frac{1}{n}\left(mf_1 + f_0\right),$$

$m \leftarrow m+1$, $d \leftarrow -d/m$ *and go to step* ***3.***

4. *Set* $n \leftarrow n-1$, $e_1 \leftarrow e_1 e_0$. *If* $n > n_{\text{stop}}$ *then go to step* ***2.***

5. *For* $1 \le n \le n_{\text{stop}}$ *compute* $F_n \leftarrow Ei(nA)$ *directly (see below).*

6. *Return the values* F_n *for* $1 \le n \le N$ *and terminate the algorithm.*

For small values of n, we compute the exponential integral by standard means since the Taylor series converges slowly. One can find explicit formulas to compute the function Ei in [3], Proposition 5.6.12.

Note that this type of method for computing Ei and more generally for confluent hypergeometric functions has already been studied in detail, in particular with respect to its numerical stability. See [19, 23, 24].

Finally, we compute the Artin root number $W(\chi)$. We will essentially follow the method given in [8] with a slightly different computational approach. This method needs to work with the conductor of the character χ, but thanks to lemma 3.2, we know that this conductor is $\mathfrak{f} = \mathfrak{f}_0\overline{v}$ for odd characters.

The following result is a special case of a theorem due to Landau.

Proposition 3.8. *Let* χ *be an odd character of* G. *Choose an element* $\lambda \in \mathfrak{f}_0$ *such that* $\overline{\lambda} > 0$ *and the integral ideal* $\mathfrak{g} = \lambda\mathfrak{f}_0^{-1}$ *is coprime to* $\mathfrak{f}_0$, *and choose an element* $\mu \in \mathfrak{g}$ *such that* $\overline{\mu} > 0$ *and the integral ideal* $\mathfrak{h} = \mu\mathfrak{g}^{-1}$ *is coprime to* $\mathfrak{f}_0$. *Define the Gauss sum*

$$G(\chi) = \chi\left(\sqrt{d_k}\mathfrak{h}\right)\sum_{\beta} e^{2i\pi\,\mathrm{Tr}(\beta\mu/\lambda)},$$

where Tr *denotes the trace of* $k/\mathbb{Q}$ *and* β *runs through a complete residue system of* $(\mathcal{O}_k/\mathfrak{f}_0)^\times$ *such that* $\overline{\beta} > 0$. *Then*

$$W(\chi) = -i\,\frac{G(\chi)}{\sqrt{\mathcal{N}\mathfrak{f}_0}}.$$

This yields the following algorithm.

Algorithm 3.9. *Let* χ *be an odd character of* G. *This algorithm computes the Artin root number* $W(\chi)$ *attached to this character.*

1. *Compute an element* $\lambda \in \mathfrak{f}_0$ *such that* $\overline{\lambda} > 0$ *and* $v_{\mathfrak{p}}(\lambda) = v_{\mathfrak{p}}(\mathfrak{f}_0)$ *for all prime ideals* $\mathfrak{p}$ *dividing* $\mathfrak{f}_0$. *Set* $\mathfrak{g} \leftarrow (\lambda)\mathfrak{f}_0^{-1}$.

2. *Compute two elements* $\mu \in \mathfrak{g}$ *and* $\nu \in \mathfrak{f}_0$ *such that* $\overline{\mu} > 0$ *and* $\mu + \nu = 1$ *(note that* $\mathfrak{g}$ *and* $\mathfrak{f}_0$ *are coprime by construction). Set* $\mathfrak{h} \leftarrow (\mu)\mathfrak{g}^{-1}$.

3. *Let* $\{\alpha_1, \ldots, \alpha_r\}$ *be elements of* $\mathcal{O}_k$, *and let* $d_r \mid d_{r-1} \mid \cdots \mid d_1$ *be positive integers such that* $\overline{\alpha_i} > 0$, *the image* $\widetilde{\alpha_i}$ *of* α_i *modulo* $\mathfrak{f}_0$ *is of order* d_i, *the cardinality of* $(\mathcal{O}_k/\mathfrak{f}_0)^\times$ *is equal to* $d_1 \cdots d_r$, *and*

$$(\mathcal{O}_k/\mathfrak{f}_0)^\times = \prod_{i=1}^{r} \widetilde{\alpha_i}^{(\mathbb{Z}/d_i\mathbb{Z})},$$

(the set $\{\widetilde{\alpha_1}, \ldots, \widetilde{\alpha_r}\}$ *and the matrix whose diagonal entries are the* d_i*'s with zeros elsewhere define a Smith normal form of the finite Abelian group* $(\mathcal{O}_k/\mathfrak{f}_0)^\times$, *see* [6]*).*
Let $G \leftarrow 0$.

4. *For all tuples $(i_1,\dots,i_r)$ such that $0 \le i_1 < d_1,\dots,0 \le i_r < d_r$, compute $\beta \leftarrow \alpha_1^{i_1}\dots\alpha_r^{i_r}$ and let $G \leftarrow G + \chi(\beta)\,e^{2i\pi\mathrm{Tr}(\beta\mu/\lambda)}$.*

5. *Let $W \leftarrow (-i)\,\chi(\mathfrak{h}\sqrt{d_k})\,\frac{G}{\sqrt{\mathcal{N}\mathfrak{f}_0}}$. Output W and terminate the algorithm.*

Using these algorithms and Theorem 3.3, we are now able to compute approximations of $L'_{K/k}(0,\chi)$ for all characters χ. Using formula $(*)$, we then deduce the values $\zeta'_{K/k}(0,\sigma)$ for all σ, and hence approximations of $\sigma(\varepsilon)$ and of the conjugates of α over k (see Theorem 2.1).

Algorithm 3.10. *Let $\mathcal{H}$ be a congruence group of conductor $\mathfrak{f}$ such that the corresponding field K verifies the hypothesis of Section 2, and let $\varkappa > 0$ be a real number. This algorithm computes approximations of the conjugates of α over k with the precision $\varkappa$.*

1. *Let $\chi_1,\dots,\chi_h$ be all the characters of $Gal(K/k)$ such that $\chi_j(\tau) = -1$, where h is the class number of k and τ is the non-trivial automorphism of $Gal(K/H_k)$. Set $C \leftarrow \pi^{-1}\sqrt{d_k\mathcal{N}\mathfrak{f}}$, $N \leftarrow \left\lceil \frac{-C\log\varkappa}{2} \right\rceil$.*

2. *For all j, compute the coefficients $a_n(\chi_j)$ using Algorithm 3.4, and the values $f_1(C/n)$ and $f_2(C/n)$ using Algorithms 3.5 and 3.7 with the precision $\varkappa$.*

3. *Compute the Artin root number $W(\chi_j)$ using Algorithm 3.9, and then deduce the values of $L'(0,\chi_j)$ by the formula of Theorem 3.3, thus of $L'_{K/k}(0,\chi_j)$ by Lemma 3.2.*

4. *Let $\sigma_1,\dots,\sigma_h$ be a system of representatives of the quotient $Gal(K/k)/\langle\tau\rangle$. Compute the values $\zeta'_{K/k}(0,\sigma_j)$ using formula $(*)$ for all j (note that $\zeta'_{K/k}(0,\sigma_j\tau) = -\zeta'_{K/k}(0,\sigma_j)$), and let z_j denote the approximations obtained.*

5. *Set $\widetilde{\alpha}_j \leftarrow e^{-2z_j} + e^{2z_j}$ for all j, return the approximations $\widetilde{\alpha}_j$ of the conjugates of α over k, and terminate the algorithm.*

Once we know the approximations $\widetilde{\alpha}_j$, we compute the polynomial

$$\widetilde{P}(X) := \prod_{j=1}^{h}(X - \widetilde{\alpha}_j) = X^h + \widetilde{\beta}_{h-1}X^{h-1} + \cdots + \widetilde{\beta}_0.$$

If the element α exists, then this polynomial is the approximation of its irreducible polynomial over k, and thus every coefficient $\widetilde{\beta}_j$ should be close to an algebraic integer β_j. Theorem 2.1 also provides a bound for the conjugate of β_j:

$$|\overline{\beta}_j| \le 2^j\binom{h}{j}.$$

We use the following algorithm to recover an integer of k given by an approximation and a bound for its conjugate (recall that $\lfloor x\rfloor$, $\lceil x\rceil$ and $\lfloor x\rceil$ denote respectively the floor, the ceiling and the closest integer to $x \in \mathbb{R}$).

Algorithm 3.11. *Let $\widetilde{\beta}$ be a real number and let $\varkappa > 0$ and $B > 0$ be two positive real numbers. This algorithm finds, if it exists, a $\beta \in \mathcal{O}_k$ such that $|\widetilde{\beta} - \beta| < \varkappa$ and $|\overline{\beta}| < B$.*

1. *Assume without loss of generality that $\omega > \overline{\omega}$ and set $\Delta \leftarrow \omega - \overline{\omega}$. Set $b \leftarrow \left\lfloor \frac{\widetilde{\beta} - (B+\varkappa)}{\Delta} \right\rfloor$ and $b_{\max} \leftarrow b + 2\left\lceil \frac{B+\varkappa}{\Delta} \right\rceil$.*

2. *If $b > b_{\max}$ then output a message saying that such an integer β does not exist and terminate the algorithm. Otherwise, set $a \leftarrow \left\lfloor \widetilde{\beta} - b\omega \right\rceil$.*

3. *Set $\beta \leftarrow a + b\omega$, if $|\widetilde{\beta} - \beta| < \varkappa$ and $|\overline{\beta}| < B$ then return the element β and terminate the algorithm, else set $b \leftarrow b + 1$ and go to step **2**.*

The correctness of this algorithm follows immediately from the inequalities $-\varkappa < \widetilde{\beta} - a - b\omega < \varkappa$ and $-B < a + b\overline{\omega} < B$, which imply the given inequalities on b and the value of a. Note that it is also possible to use the LLL algorithm for this computation.

We are now able to give the complete algorithm.

Algorithm 3.12. *Let k be a quadratic real number field. Under the hypothesis of Theorem 2.1, this algorithm computes the irreducible polynomial over k of a generating element of H_k.*

1. *Using Algorithm 3.1, find a modulus $\mathfrak{f}$ and a congruence group $\mathcal{H}$ of conductor $\mathfrak{f}$ such that the corresponding field K verifies the hypothesis of Section 2.*

2. *Set $\varkappa \leftarrow 10^{-20} \cdot e^{-\lceil\sqrt{d_k \mathcal{N}\mathfrak{f}}\rceil}$.*

3. *Using Algorithm 3.10, compute approximations $\widetilde{\alpha}_i$ of the conjugates of α over k with precision $\varkappa$. Set*

$$\widetilde{P}(X) \leftarrow \prod_{j=1}^{h} (X - \widetilde{\alpha}_j).$$

4. *Write $P(X) = X^h + \widetilde{\beta}_{h-1}X^{h-1} + ... + \widetilde{\beta}_0$, where $\widetilde{\beta}_j$ are real numbers. For $1 \le j \le h$, using Algorithm 3.11 try to find an algebraic integer β_j such that $|\widetilde{\beta}_j - \beta_j| < \varkappa$ and $|\overline{\beta}_j| \le 2^j \binom{h}{j}$. If it is possible then return the polynomial*

$$X^h + \beta_{h-1}X^{h-1} + ... + \beta_0$$

*and terminate the algorithm. Otherwise, increase the precision by setting for example $\varkappa \leftarrow \varkappa^2$, and go back to step **3**.*

Remark. As we said above, heuristics show that the conjugates of α are mostly of the size of $\exp\left(\sqrt{d_k \mathcal{N}\mathfrak{f}}\right)$; thus the initial precision is chosen so as to obtain twenty additional digits. However, if this is not enough, we double the precision and redo the computations. Note that this is not really an algorithm, since if the conjecture is false it just keeps doubling the precision without stopping.

4. Verification of the result

Let $P(X)$ denote the polynomial given by the above algorithm. Since this algorithm is based on a conjecture, we need to check if a root of this polynomial does generate the Hilbert class field of k.

First, we verify that the polynomial (whose degree is equal to h_k by construction) is irreducible over k. Then let $\widetilde{H}$ be the extension of k generated by any root of $P(X)$. We verify that the extension $\widetilde{H}/k$ is unramified at both finite and infinite places, using the algorithms given in [5].

Once we have proved that the extension $\widetilde{H}/k$ is of degree h_k and unramified, we still have to prove that it is an Abelian extension. In fact, if $h_k = 2$ or 3, this follows from the fact that the extension is unramified. (This is obvious for $h_k = 2$. For $h_k = 3$, assume the extension is not cyclic; then its Galois group is S_3 and k has a quadratic extension which is a subfield of the Galois closure of $\widetilde{H}/k$ and thus unramified. But this is impossible since it implies that 2 divides h_k.) In the general case, we factor the polynomial $P(X)$ in the field $\widetilde{H}$, and it must have

only linear factors if $\widetilde{H}/k$ is Galois. Since every such linear factor corresponds to a k-automorphism of $\widetilde{H}$, we can check if the extension is Abelian by proving that they commute with each other.

However, once we have proved that the extension $\widetilde{H}/k$ is a Galois extension, it is possible to be more efficient for small values of h_k, since there are only a few possibilities for the Galois group $Gal(\widetilde{H}/k)$. Another possibility is to use a result of Bach and Sorenson [1] which gives under GRH an upper bound for the norm of the prime ideals generating the norm group of an Abelian extension. Indeed, this result enables one to write an algorithm which, under GRH, does prove that an extension is Abelian (without having to prove first that it is Galois) and computes at the same time its norm group (see [17] for details).

We now give an algorithm using the first method described above, which does not use GRH.

Algorithm 4.1. *Let $P(X)$ be a polynomial of degree h_k and with coefficients in $\mathcal{O}_k$. This algorithm proves (or disproves) that a root of $P(X)$ generates the Hilbert class field of k.*

1. *Check if $P(X)$ is irreducible over $k[X]$. If this is not the case then output a message saying that P does not generate an extension of degree h_k of k and terminate the algorithm.*

2. *Let θ be a root of P and let $\widetilde{H}$ denote the field $k(\theta)$. Compute the minimal polynomial of θ over $\mathbb{Q}$ and check if $\widetilde{H}$ is totally real using Sturm's algorithm (see* [3]*, Algorithm 4.1.11). If this is not the case then return a message saying that $\widetilde{H}/k$ is ramified at the infinite places and terminate the algorithm.*

3. *Compute the relative discriminant of $\widetilde{H}/k$ using the algorithm given in* [5]*. If it is different from $\mathcal{O}_k$, then output a message saying that $\widetilde{H}/k$ is ramified at the finite places and terminate the algorithm. Otherwise, if $h_k = 2$ or 3 return a message saying that $\widetilde{H} = H_k$ and terminate the algorithm.*

4. *Compute the factorization of $P(X)$ in $\widetilde{H}[X]$. If P does not admit only linear factors then output a message saying that $\widetilde{H}/k$ is not a Galois extension and terminate the algorithm. Otherwise, if $h_k = 4$ or h_k is a prime number return a message saying that $\widetilde{H} = H_k$ and terminate the algorithm.*

5. *Let $X - S_j(Y) \in k[X, Y]$ be such that*

$$P(X) = \prod_{1 \leq j \leq h_k} (X - S_j(\theta))$$

is the factorization of P in $\widetilde{H}[X]$. For all $1 \leq i < j \leq h_k$, check if $S_i(S_j(\theta)) = S_j(S_i(\theta))$. If this is not the case then return a message saying that $\widetilde{H}/k$ is not an Abelian extension and terminate the algorithm, otherwise return a message saying that $\widetilde{H} = H_k$ and terminate the algorithm.

5. An example

The algorithm presented in this paper has been implemented as part of the new version of the PARI/GP [2] package. The `quadhilbert` function uses complex multiplication to compute the Hilbert class field of complex quadratic fields, and the present algorithm for real quadratic fields. The following example was treated using this implementation.

Let k be the real quadratic field generated by $\omega := \sqrt{438}$. We then have $d_k = 1752$, $\mathcal{O}_k = \mathbb{Z} + \mathbb{Z}\omega$, and the class group of k is cyclic of order 4.

The field K can be taken to be the ray class field of k modulo $\mathfrak{p}v$, where $\mathfrak{p}$ is one of the two prime ideals above 11. Note that the extension K/k is cyclic of order 8, so there is no quadratic extension k'/k such that $K = H_k k'$.

If σ denotes a generator of $G := Gal(K/k)$, then $\tau = \sigma^4$. Let ψ be the character of G such that $\psi(\sigma) = \xi_8$, where ξ_8 is a fixed primitive 8-th root of unity. The characters χ such that $\chi(\tau) = -1$ are then ψ, ψ^3, ψ^5 and ψ^7 (note that $\overline{\psi} = \psi^7$, $\overline{\psi^3} = \psi^5$). With the notations of Theorem 3.3, we compute

$$\begin{array}{rcl} S(\psi) & \approx & 1.71552623535657 + 0.744643091777554i, \\ T(\psi) & \approx & 14.1665156497187 + 2.51918530947938i, \\ S(\psi^3) & \approx & 0.842811390359850 + 1.29326746361755i, \\ T(\psi^3) & \approx & 12.8015376467263 - 8.44945647020462i, \end{array}$$

and $S(\psi^7) = \overline{S(\psi)}$, $T(\psi^7) = \overline{T(\psi)}$, $S(\psi^5) = \overline{S(\psi^3)}$, $T(\psi^5) = \overline{T(\psi^3)}$.

For the character ψ, we find that $W(\psi) = e^{2i\pi/8}$ and similarly $W(\psi^3) = -\overline{W(\psi)}$, $W(\psi^5) = \overline{W(\psi^3)} = -W(\psi)$ and $W(\psi^7) = \overline{W(\psi)}$. So we compute the corresponding L-functions, and obtain

$$\begin{array}{rclrcl} \zeta'_{K/k}(0,\sigma) & \approx & 7.25654406363900, & \zeta'_{K/k}(0,\sigma^5) & = & -\zeta'_{K/k}(0,\sigma), \\ \zeta'_{K/k}(0,\sigma^2) & \approx & -0.944193530444349, & \zeta'_{K/k}(0,\sigma^6) & = & -\zeta'_{K/k}(0,\sigma^2), \\ \zeta'_{K/k}(0,\sigma^3) & \approx & 2.94813989197904, & \zeta'_{K/k}(0,\sigma^7) & = & -\zeta'_{K/k}(0,\sigma^3), \\ \zeta'_{K/k}(0,\sigma^4) & \approx & 1.92921444495667, & \zeta'_{K/k}(0,\mathbf{1}) & = & -\zeta'_{K/k}(0,\sigma^4). \end{array}$$

We then compute the values of the conjugates of α over k, and we form its irreducible polynomial

$$X^4 - 2009298.2915480506125X^3 + 839444123.58478759370X^2 - 40221955871.313705629X + 234161017552.69584759$$

which, using Algorithm 3.11, is seen to be very close to the polynomial

$$X^4 + (-48004\sqrt{438} - 1004649)X^3 + (20055096\sqrt{438} + 419722059)X^2 + (-960939696\sqrt{438} - 20110977936)X + (5594323104\sqrt{438} + 117080508780).$$

A relative reduction process gives the following simpler polynomial defining the same field extension:

$$X^4 + 2X^3 + (\sqrt{438} - 25)X^2 + (-\sqrt{438} + 22)X + (-3\sqrt{438} + 63).$$

We now have to check the result: we prove that this polynomial is irreducible over k and that the extension $\widetilde{H}$ that it defines is unramified at both finite and infinite places. Moreover, this polynomial factors completely over $\widetilde{H}$; hence the relative extension $\widetilde{H}/k$ is Galois. Since its degree is equal to 4, this implies that it is Abelian, and since it is unramified this implies that $\widetilde{H}$ is actually the Hilbert class field of k.

Finally, since $k/\mathbb{Q}$ is a cyclic extension, it is possible to find a field L of degree 4 such that $k \cap L = \mathbb{Q}$ and $kL = H_k$ (see [7]). In fact, any subfield L of H_k of degree h_k over $\mathbb{Q}$ and disjoint from k will work. In order to find such a field, one can use the algorithm for subfield computation given in [12], or use the method explained in [4], which gives only some subfields. In our example, we find that such a field is generated by a root of

$$X^4 - 2X^3 - 5X^2 + 6X + 3.$$

Appendix. Tables of Hilbert class fields

For each of the 607 real quadratic field k of discriminant less than 2 000, we give a polynomial defining a field L_k over $\mathbb{Q}$ such that the Hilbert class field of k is the compositum of k and L_k. For the sake of completeness, we recall the list of the 319 fields k with class number equal to 1, for which trivially $L_k = \mathbb{Q}$.

Discriminant of the fields with $h_k = 1$										
5	8	12	13	17	21	24	28	29	33	37
41	44	53	56	57	61	69	73	76	77	88
89	92	93	97	101	109	113	124	129	133	137
141	149	152	157	161	172	173	177	181	184	188
193	197	201	209	213	217	233	236	237	241	248
249	253	268	269	277	281	284	293	301	309	313
317	329	332	337	341	344	349	353	373	376	381
389	393	397	409	412	413	417	421	428	433	437
449	453	457	461	472	489	497	501	508	509	517
521	524	536	537	541	553	556	557	569	573	581
589	593	597	601	604	613	617	632	633	641	649
652	653	661	664	668	669	673	677	681	701	709
713	716	717	721	737	749	753	757	764	769	773
781	789	796	797	809	813	821	824	829	844	849
853	856	857	869	877	881	889	893	908	913	917
921	929	933	937	941	953	956	973	977	989	997
1004	1013	1021	1033	1041	1048	1049	1052	1057	1061	1069
1077	1081	1084	1097	1109	1112	1117	1121	1132	1133	1137
1141	1149	1153	1169	1177	1181	1193	1201	1208	1213	1217
1228	1237	1244	1249	1253	1273	1277	1289	1293	1301	1317
1321	1324	1329	1333	1336	1337	1349	1357	1361	1381	1388
1389	1397	1401	1409	1432	1433	1437	1441	1453	1457	1461
1468	1473	1477	1481	1493	1497	1501	1516	1528	1529	1532
1541	1549	1553	1561	1569	1577	1589	1592	1597	1609	1613
1621	1633	1637	1657	1661	1669	1673	1676	1688	1689	1693
1697	1709	1713	1721	1724	1733	1741	1753	1757	1777	1784
1789	1793	1797	1801	1816	1817	1821	1829	1837	1841	1852
1857	1861	1868	1873	1877	1889	1893	1909	1912	1913	1916
1933	1941	1948	1949	1964	1969	1973	1977	1981	1993	1997

There are 194 fields with class number 2. We give a table for each possible value of the discriminant d_{L_k} of L_k.

First, there are 70 real quadratic fields k of discriminant less than 2 000 with class number 2 and such that $L_k = \mathbb{Q}(\sqrt{5})$.

Discriminant of the fields k such that $h_k = 2$ and $d_{L_k} = 5$									
40	60	65	85	105	120	140	165	185	205
220	265	280	285	305	345	365	380	385	440
460	465	485	545	565	620	645	665	685	705
745	760	805	860	865	885	920	965	1005	1065
1085	1165	1180	1185	1205	1240	1245	1265	1285	1340
1385	1405	1420	1465	1505	1545	1565	1580	1585	1605
1645	1660	1685	1720	1865	1880	1905	1945	1965	1985

There are 34 real quadratic fields k of discriminant less than 2 000 with class number 2 and such that $L_k = \mathbb{Q}(\sqrt{2})$.

Discriminant of the fields k such that $h_k = 2$ and $d_{L_k} = 8$											
104	136	168	232	264	296	424	456	488	552	584	616
712	744	776	808	872	1032	1064	1128	1192	1256	1416	1448
1544	1576	1608	1672	1704	1832	1864	1896	1928	1992		

There are 14 real quadratic fields k of discriminant less than 2 000 with class number 2 and such that $L_k = \mathbb{Q}(\sqrt{3})$.

Discriminant of the fields k such that $h_k = 2$ and $d_{L_k} = 12$						
156	204	348	444	492	636	732
1068	1212	1308	1356	1644	1788	1884

There are 26 real quadratic fields k of discriminant less than 2 000 with class number 2 and such that $L_k = \mathbb{Q}(\sqrt{13})$.

Discriminant of the fields k such that $h_k = 2$ and $d_{L_k} = 13$								
221	273	312	364	377	429	481	533	572
728	741	949	988	1001	1144	1157	1196	1209
1261	1417	1469	1612	1729	1781	1833	1976	

There are 21 real quadratic fields k of discriminant less than 2 000 with class number 2 and such that $L_k = \mathbb{Q}(\sqrt{17})$.

Discriminant of the fields k such that $h_k = 2$ and $d_{L_k} = 17$										
357	408	476	493	561	629	748	952	969	1037	1173
1241	1309	1496	1513	1564	1581	1649	1717	1853	1921	

There remains 29 fields k with class number 2 and such that the discriminant d_{L_k} is larger than 17. We give them in a single table containing first the discriminant of k, and then the discriminant of d_{L_k}, ordered by increasing value of d_{L_k}.

Discriminant and d_{L_k} for the fields k such that $h_k = 2$ and $d_{L_k} > 17$											
609	21	861	21	1113	21	1281	21	1533	21	1869	21
696	24	888	24	984	24	1272	24	1464	24	812	28
1036	28	1148	28	1484	28	957	29	1073	29	1189	29
1276	29	1537	29	1624	29	1653	29	1769	29	1353	33
1749	33	1517	37	1628	37	1961	37	1804	41		

There are 24 real quadratic fields with class number equal to 3 and discriminant less than 2 000. In the following table, we give their discriminants together with a

polynomial defining the field L_k.

Discriminants of the fields K such that $h_K = 3$ and polynomials for L_K			
229	$X^3 - 4X - 1$	257	$X^3 - X^2 - 4X + 3$
316	$X^3 - X^2 - 4X + 2$	321	$X^3 - X^2 - 4X + 1$
469	$X^3 - X^2 - 5X + 4$	473	$X^3 - 5X - 1$
568	$X^3 - X^2 - 6X - 2$	733	$X^3 - X^2 - 7X + 8$
761	$X^3 - X^2 - 6X - 1$	892	$X^3 - X^2 - 8X + 10$
993	$X^3 - X^2 - 6X + 3$	1016	$X^3 - X^2 - 6X + 2$
1101	$X^3 - X^2 - 9X + 12$	1229	$X^3 - X^2 - 7X + 6$
1257	$X^3 - X^2 - 8X + 9$	1304	$X^3 - 11X - 2$
1373	$X^3 - 8X - 5$	1436	$X^3 - 11X - 12$
1489	$X^3 - X^2 - 10X - 7$	1509	$X^3 - X^2 - 7X + 4$
1772	$X^3 - X^2 - 12X + 8$	1901	$X^3 - X^2 - 9X - 4$
1929	$X^3 - X^2 - 10X + 13$	1957	$X^3 - X^2 - 9X + 10$

There are 41 real quadratic fields with class number equal to 4 and discriminant less than 2 000. In the following table, we give their discriminants together with a polynomial defining the field L_k.

Discriminants of the fields K such that $h_K = 4$ and polynomials for L_K			
145	$X^4 - X^3 - 3X^2 + X + 1$	328	$X^4 - 2X^3 - 3X^2 + 2X + 1$
445	$X^4 - X^3 - 5X^2 + 2X + 4$	505	$X^4 - 2X^3 - 4X^2 + 5X + 5$
520	$X^4 - 6X^2 + 4$	680	$X^4 - 6X^2 + 4$
689	$X^4 - X^3 - 5X^2 + X + 1$	777	$X^4 - 2X^3 - 4X^2 + 5X + 1$
780	$X^4 - 2X^3 - 7X^2 + 8X + 1$	793	$X^4 - X^3 - 6X^2 + 8X - 1$
840	$X^4 - 6X^2 + 4$	876	$X^4 - 7X^2 - 6X + 1$
897	$X^4 - 2X^3 - 4X^2 + 5X + 3$	901	$X^4 - 2X^3 - 4X^2 + 5X + 2$
905	$X^4 - X^3 - 7X^2 + 3X + 9$	924	$X^4 - 5X^2 + 1$
1020	$X^4 - 2X^3 - 7X^2 + 8X + 1$	1045	$X^4 - X^3 - 8X^2 + X + 11$
1096	$X^4 - 2X^3 - 5X^2 + 6X + 7$	1105	$X^4 - 9X^2 + 4$
1145	$X^4 - X^3 - 8X^2 + 6X + 11$	1160	$X^4 - 6X^2 + 4$
1164	$X^4 - 2X^3 - 7X^2 + 8X + 4$	1221	$X^4 - X^3 - 10X^2 + X + 1$
1288	$X^4 - 2X^3 - 7X^2 + 8X + 8$	1292	$X^4 - X^3 - 11X^2 + 12X + 8$
1313	$X^4 - X^3 - 8X^2 - 4X + 3$	1320	$X^4 - 6X^2 + 4$
1365	$X^4 - 9X^2 + 4$	1480	$X^4 - 6X^2 + 4$
1560	$X^4 - 9X^2 + 4$	1640	$X^4 - 6X^2 + 4$
1677	$X^4 - X^3 - 7X^2 + 2X + 4$	1736	$X^4 - 2X^3 - 7X^2 + 6X + 9$
1740	$X^4 - 2X^3 - 7X^2 + 8X + 1$	1745	$X^4 - X^3 - 10X^2 + 2X + 19$
1752	$X^4 - 2X^3 - 5X^2 + 6X + 3$	1820	$X^4 - 9X^2 + 4$
1848	$X^4 - 10X^2 + 4$	1885	$X^4 - 9X^2 + 4$
1932	$X^4 - 5X^2 + 1$		

Finally, there are 29 real quadratic fields with class number ranging from 5 to 11 and discriminant less than 2 000. In the following table, we give their discriminants

together with a polynomial defining the field L_k.

Discriminants of the fields K such that $h_K \geq 5$ and polynomials for L_K	
401	$X^5 - X^4 - 5X^3 + 4X^2 + 3X - 1$
577	$X^7 - 2X^6 - 7X^5 + 10X^4 + 13X^3 - 10X^2 - X + 1$
697	$X^6 - 3X^5 - 3X^4 + 11X^3 - X^2 - 5X + 1$
785	$X^6 - X^5 - 8X^4 + 6X^3 + 16X^2 - 10X - 5$
817	$X^5 - X^4 - 6X^3 + 5X^2 + 3X - 1$
904	$X^8 - 2X^7 - 9X^6 + 10X^5 + 22X^4 - 14X^3 - 15X^2 + 2X + 1$
940	$X^6 - 3X^5 - 5X^4 + 14X^3 + 9X^2 - 15X - 5$
985	$X^6 - 3X^5 - 4X^4 + 13X^3 + 3X^2 - 10X + 1$
1009	$X^7 - X^6 - 9X^5 + 2X^4 + 21X^3 + X^2 - 13X - 1$
1093	$X^5 - 8X^3 - 3X^2 + 10X + 4$
1129	$X^9 - 3X^8 - 10X^7 + 38X^6 + 5X^5 - 107X^4 + 58X^3 + 78X^2 - 60X - 1$
1297	$X^{11} - 5X^{10} - 4X^9 + 54X^8 - 53X^7 - 127X^6 + 208X^5 + 69X^4 - 222X^3 + 29X^2 + 56X - 5$
1345	$X^6 - 3X^5 - 8X^4 + 16X^3 + 24X^2 - 5$
1384	$X^6 - 2X^5 - 7X^4 + 14X^3 + 3X^2 - 12X + 4$
1393	$X^5 - X^4 - 7X^3 + 6X^2 + 3X - 1$
1429	$X^5 - X^4 - 13X^3 + 23X^2 + 9X - 23$
1596	$X^8 - 2X^7 - 13X^6 + 16X^5 + 43X^4 - 10X^3 - 34X^2 - 4X + 4$
1601	$X^7 - 2X^6 - 14X^5 + 34X^4 + 4X^3 - 38X^2 + 7X + 1$
1641	$X^5 - X^4 - 10X^3 + X^2 + 21X + 9$
1705	$X^8 - X^7 - 14X^6 + 9X^5 + 62X^4 - 23X^3 - 84X^2 + 20X - 1$
1708	$X^6 - 3X^5 - 8X^4 + 21X^3 - 6X^2 - 5X + 1$
1756	$X^5 - 2X^4 - 10X^3 + 14X^2 + 21X - 16$
1761	$X^7 - 2X^6 - 14X^5 + 14X^4 + 50X^3 - 22X^2 - 51X - 3$
1765	$X^6 - 3X^5 - 6X^4 + 17X^3 + 5X^2 - 14X + 4$
1768	$X^8 - 4X^7 - 6X^6 + 32X^5 - 5X^4 - 48X^3 + 14X^2 + 16X - 4$
1785	$X^8 - 2X^7 - 13X^6 + 17X^5 + 48X^4 - 23X^3 - 33X^2 + 3X + 1$
1897	$X^5 - X^4 - 13X^3 + 8X^2 + 27X + 1$
1937	$X^6 - 10X^4 + 25X^2 - 13$
1996	$X^5 - 9X^3 - 4X^2 + 10X + 4$

These computations were done on a Pentium Pro 200 with 256 Mb of RAM. The total computation time (including class group computations, computations of the generating element, reduction of the result and computation of the field L_k) took about 21 minutes. Note that actually the last two steps (reduction and computation of the field L_k) represented more than 70% of the whole computation time.

All these fields have of course been verified using Algorithm 4.1.

References

1. E. Bach, J. Sorenson, *Explicit Bounds for Primes in Residue Classes*, Math. Comp. **65** (1996), 1717–1735 MR **97a:**11143
2. C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *User Guide to PARI/GP version 2.0.1*, 1997
3. H. Cohen, *A Course in Computational Number Theory*, GTM **138**, Springer-Verlag, 1993 MR **94i:**11105
4. H. Cohen, F. Diaz y Diaz, *A Polynomial Reduction Algorithm*, Sém. Th. Nombres de Bordeaux (Série 2) **3** (1991), 351–360 MR **93a:**11107

5. H. Cohen, F. Diaz y Diaz, M. Olivier, *Algorithmic Techniques for Relative Extensions of Number Fields*, preprint A2X (1997)
6. H. Cohen, F. Diaz y Diaz, M. Olivier, *Computing Ray Class Groups, Conductors and Discriminants*, Math. Comp. **67** (1998), 773–795 MR **98g:**11128
7. G. Cornell, M. Rosen, *A Note on the Splitting of the Hilbert Class Fields*, J. Number Theory **28** (1988), 152–158 MR **89f:**11156
8. D. Dummit, B. Tangedal, *Computing the Leading Term of an Abelian L-function*, ANTS III (Buhler Ed.), Lecture Notes in Computer Sci. **1423** (1998), p.400–411
9. C. Fieker, Computing Class Fields via the Artin Map, preprint, 1997
10. E. Friedman, *Hecke's Integral Formula*, Sém. Th. Nombres de Bordeaux, Exposé No.5 (1987-1988) MR **90i:**11136
11. M. Ishida, *The Genus Fields of Algebraic Number Fields*, LN in Math. **555**, Springer-Verlag, 1976 MR **55:**7990
12. J. Klüners, M. Pohst, *On Computing Subfields*, J. Symbolic Comp. **24** (1997), 385–397 MR **98k:**11161
13. J. Martinet, *Character Theory and Artin L-functions*, *in* Algebraic Number Fields (A. Fröhlich, ed.), Academic Press, London, 1977, 1–87 MR **56:**5502
14. J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992
15. M. Daberkow, M. Pohst, *Computations with Relative Extensions of Number Fields with an Application to the Construction of Hilbert Class Fields*, Proc. ISAAC'95, ACM Press, New-York 1995, 68–76
16. M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, 1989 MR **92b:**11074
17. X.-F. Roblot, *Stark's Conjectures and Hilbert's Twelfth Problem*, preprint; *Algorithmes de Factorisation dans les Extensions Relatives et Applications de la Conjecture de Stark à la Construction des Corps de Classes de Rayon*, Thesis, Université Bordeaux I (1997)
18. R. Schertz, *Problèmes de Construction en Multiplication Complexe*, Sém. Th. Nombres Bordeaux (1992), 239–262 MR **94c:**11051
19. R. Sharma and B. Zohuri, *A General Method for an Accurate Evaluation of Exponential Integrals* $E_1(x)$, $x > 0$, J. Comput. Phys. **25** (1977), 199–204 MR **57:**14339
20. I.N. Sneddon, *The Use of Integral Transforms*, Mc Graw-Hill, New York, 1972
21. H. M. Stark, *Values of L-functions at* $s = 1$. *I. L-functions for quadratic forms*, Advances in Math. **7** (1971), 301–343; *II. Artin L-functions with Rational Characters, ibid.* **17** (1975), 60–92; *III. Totally Real Fields and Hilbert's Twelfth Problem, ibid.* **22** (1976), 64–84; *IV. First Derivatives at* $s = 0$, *ibid.* **35** (1980), 197–235 MR **44:**6620; MR **52:**3082; MR **55:**10427; MR **81f:**10054
22. J.T. Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, Progress in Math. **47**, Birkhaüser, Boston, 1984 MR **86e:**11112
23. R. Terras, *The Determination of Incomplete Gamma Functions through Analytic Integration*, J. Comput. Phys. **31** (1979), 146–151 MR **81d:**65010
24. R. Terras, *Generalized Exponential Operators in the Continuation of the Confluent Hypergeometric Functions*, J. Comput. Phys. **44** (1981), 156–166 MR **82m:**33003

Laboratoire A2X, Université Bordeaux I, 351 cours de la Libération, 33405 Talence Cedex, France

E-mail address: cohen@math.u-bordeaux.fr

Laboratoire A2X, Université Bordeaux I, 351 cours de la Libération, 33405 Talence Cedex, France

Current address: Department of Computer Science, Concordia University, 1455 de Maisonneuve Blvd West, Montreal, Quebec, H3G 1M8

E-mail address: roblot@cs.concordia.ca