EFFICIENT COMPUTATION
OF ROOT NUMBERS AND CLASS NUMBERS
OF PARAMETRIZED FAMILIES
OF REAL ABELIAN NUMBER FIELDS

STÉPHANE R. LOUBOUTIN

Abstract. Let \( \{K_m\} \) be a parametrized family of simplest real cyclic cubic, quartic, quintic or sextic number fields of known regulators, e.g., the so-called simplest cubic and quartic fields associated with the polynomials

\[
P_m(x) = x^3 - mx^2 - (m + 3)x + 1 \quad \text{and} \quad P_m(x) = x^4 - mx^3 - 6x^2 + mx + 1.
\]

We give explicit formulas for powers of the Gaussian sums attached to the characters associated with these simplest number fields. We deduce a method for computing the exact values of these Gaussian sums. These values are then used to efficiently compute class numbers of simplest fields. Finally, such class number computations yield many examples of real cyclotomic fields \( \mathbb{Q}(\zeta_p) \) of prime conductors \( p \geq 3 \) and class numbers \( h_p^+ \) greater than or equal to \( p \). However, in accordance with Vandiver’s conjecture, we found no example of \( p \) for which \( p \) divides \( h_p^+ \).

1. Introduction

In Bye, CW, Gra2, Jean, Laz1, Laz2, Lou3, Lou6, Lou7, LP, Sha, SW, SWW, and Wal, various authors dealt with the so-called simplest cubic, quartic, quintic and sextic fields \( K_m \), i.e., the real cyclic cubic, quartic, quintic and sextic number fields associated with the cubic polynomials

\[
P_m(x) = x^3 - mx^2 - (m + 3)x - 1,
\]

the quartic polynomials

\[
P_m(x) = x^4 - mx^3 - 6x^2 + mx + 1,
\]

the quintic polynomials

\[
P_m(x) = x^5 + m^2x^4 - 2(m^3 + 3m^2 + 5m + 5)x^3 + (m^4 + 5m^3 + 11m^2 + 15m + 5)x^2 + (m^3 + 4m^2 + 10m + 10)x + 1,
\]

and the sextic polynomials

\[
P_m(x) = x^6 - 2mx^5 - 5(m + 3)x^4 - 20x^3 + 5mx^2 + 2(m + 3)x + 1.
\]

One nice feature of these families of real cyclic number fields \( K_m \) is that, under some slightly restrictive conditions, not only are their regulators small and their class numbers \( h_{K_m} \) large, but systems of fundamental units of their ring of algebraic integers are known. Hence, they can be used to find real cyclic fields \( K_m \) of prime conductors \( p \) and class numbers \( h_{K_m} \) greater than or equal to \( p \) (see Tables 1, 2, and 3, and [CW, Theorem 2] and [Lou7, Corollary 10]). These class numbers \( h_{K_m} \) divide the class numbers \( h_p^+ \) of the maximal real subfields \( \mathbb{Q}(\zeta_p) \) of the cyclotomic fields \( \mathbb{Q}(\zeta_p) \) of prime conductors \( p \) (see [CW, Lemma 2]). However, in accordance

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
with Vandiver’s conjecture, we found no example of $p$ for which $p$ divides one of these class numbers $h_{K,q}$.

So, let $K$ be a real cyclic number field of degree $q > 1$ associated with a $\mathbf{Q}$-irreducible monic polynomial $P_K(X) = X^q + a_{q-1}X^{q-1} + \cdots + a_0 \in \mathbf{Z}[X]$. Let $X_K$ be the cyclic group (of order $q$) of primitive even Dirichlet characters associated with $K$. Let $h_K$ and $\text{Reg}_K$ be the class number and regulator of $K$. We have (see [Lan Chapter XIII] and [Lou4 Section 2]):

$$h_K \text{Reg}_K = \prod_{1\neq \chi \in X_K} L'(0, \chi).$$  

We let $\chi_K$ be any generator of $X_K$ and let $\sigma$ be a generator of the cyclic Galois group $\text{Gal}(K/\mathbf{Q})$. We developed in [Lou3 Section 4.2], [Lou4 Section 2] and [Lou6 Section 3.3] an efficient method for constructing a generator $\chi_K$ of $X_K$ from the knowledge of $P_K(X)$. This construction is particularly simple in the case that the conductor $f_K$ of $K$ is square-free and all the subfields of $K$ are also of conductor $f_K$, which amounts to asking (i) that $f_K = \prod_{i=1}^l p_i$ is a product of distinct odd primes $p_i \equiv 1 \pmod{q}$ and (ii) that $\chi_K = \prod_{i=1}^l \chi_{p_i}$, where each $\chi_{p_i}$ is a character of order $q$ modulo $p_i$. Then, for efficiently computing $h_K$ (when $\text{Reg}_K$ is known) for $f_K$ large, we use (1) and generalize [WB Section 3] to compute efficiently good enough numerical approximations $L_N'(0, \chi)$ to the $L'(0, \chi)$’s, $1 \neq \chi \in X_K$. Let $\chi$ be a primitive even Dirichlet character of conductor $f_\chi > 1$ and order $q_\chi > 1$. Set

$$\tau(\chi) = \sum_{1 \leq n \leq f_\chi} \chi(n) \exp(2\pi i/n/f_\chi) \quad (\text{Gauss sum}),$$

(2) $$W(\chi) = \tau(\chi)/\sqrt{f_\chi} \quad (\text{root number})$$

(hence, $|W(\chi)| = 1$), and $\omega(\chi) := (\tau(\chi))^q_\chi$. Then (see [Dav Chapter 9], [Lou4 Theorem 12], and [Lou5 (11)])

$$L'(0, \chi) = \frac{1}{2} \sum_{n \geq 1} \chi(n) \int_0^\infty e^{-t} dt + W(\chi) \sqrt{\frac{f_\chi}{\pi}} \sum_{n \geq 1} \frac{\chi(n)}{n} \int_0^\infty e^{-t^2} dt.$$ 

Let $L_N'(0, \chi)$ be the approximation to $L'(0, \chi)$ obtained by disregarding in this formula the indices $n > N$, $N \geq 1$ a positive integer. Then, $L_N'(0, \chi)$ is easy to compute numerically, and setting $h_K(N) = 1/\text{Reg}_K \prod_{1 \neq \chi \in X_K} L'_N(0, \chi)$, we proved:

**Proposition 1** (See [Lou2 Proof of Theorem 7]). Let $q \geq 2$ be a given prime. Fix $t > (q - 1)/2$ and $M > 0$, and let $K$ range over a family of real abelian number fields $K$ of degree $q$. Then, as $f_K \rightarrow \infty$ and for

$$N \geq B(t, f_K, M) := \sqrt{\frac{tf_K}{\pi}} \log(Mf_K),$$

the limit $|h_K - h_K(N)|$ is equal to zero.

From a practical point of view, Proposition 1 is useless if we do not know how to efficiently compute the root numbers $W(\chi)$, $1 \neq \chi \in X_K$. However, there is no known general formula for root numbers (see [BE22]). In the case of simplest cubic fields $K$ of prime conductors $p$, one can use standard formulas on Gauss sums to get a formula for $\omega(\chi_K) = (\tau(\chi_K))^3$. This leaves it unspecified as to which third root of $\omega(\chi_K)/p^{3/2}$ is equal to $W(\chi_K)$. As in [SWW], one can get around this

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
problem by using the formula \( h_K = |L'(0, \chi_K)|^2/\text{Reg}_K \), by (1), to compute three good enough numerical approximations \(|L_N'(0, \chi_K)|^2/\text{Reg}_K \) to \( h_K \) so that only one out of them is close enough to a positive integer to be the numerical approximation to the class number \( h_K \). The main drawbacks of this method are that its complexity is hard to study and that it becomes even more complicated for simplest cubic fields of nonnecessarily prime conductors or for cyclic quintic fields of prime conductors (see [SW] Section 4). In contrast, we recall how one can efficiently compute root numbers. Set

\[
\theta(x, \chi) = \sum_{n \geq 1} \chi(n)e^{-\pi n^2 x f} = \frac{W(\chi)}{\sqrt{x}} \theta\left(\frac{1}{x}, \bar{\chi}\right) \quad (x > 0).
\]

Hence, \( W(\chi) = \theta(1, \chi)/\theta(1, \bar{\chi}) \), provided that \( \theta(1, \chi) \neq 0 \). Also, let \( \theta_N(1, \chi) \) be the approximation to \( \theta(1, \chi) \) obtained by disregarding in this formula the indices \( n > N \), \( N \geq 1 \) a positive integer. Then, \( N \geq B(t, f_X, M) \) (see (2)) implies

\[
|\theta(1, \chi) - \theta_N(1, \chi)| < \frac{f^t}{2M^t \sqrt{\pi t} \log(Mf_X)}.
\]

According to numerical computations, to theoretical results and to a conjecture of ours (see [Lou4] Section 4.4), \( \theta(1, \chi) \neq 0 \) should always hold true. We explained in [Lou4] Section 4.1 how one can compute the exact value of \( \omega(\chi) \) from the numerical computation of good enough approximations \( \theta_N(1, \chi') \) to the \( \theta(1, \chi') \)'s for \( 1 \leq l \leq q_X \) and \( \gcd(l, q_X) = 1 \), provided that \( \theta(1, \chi') \neq 0 \) for \( l \leq q_X \) and \( \gcd(l, q_X) = 1 \). Here, we will simplify the numerical computation of class numbers of simplest fields \( K \) by obtaining beforehand explicit formulæ for the cubic, quartic, quintic and sextic powers \( \omega(\chi_K) \) of the Gauss sums of the primitive cubic, quartic, quintic and sextic Dirichlet characters associated with these simplest cubic, quartic, quintic and sextic fields (see Theorems 3, 10, 14, 17 and 23). Provided that \( \theta(1, \chi) \neq 0 \), it is then easy to deduce the exact value of \( W(\chi) \).

**Proposition 2** (See [Lou4] Lemma 4). Fix \( \epsilon \in (0, 1] \). Let \( \chi \) be a primitive, even Dirichlet character of conductor \( f_X \) and order \( q > 1 \). Assume that \( \omega(\chi) \) is known and that \( N \) is such that \( \theta_N(1, \chi) \neq 0 \) and \( |\theta(1, \chi) - \theta_N(1, \chi)| \leq \epsilon |\theta(1, \chi)|/q \) (use (4) to find such a \( N \)). Fix \( W_0 \) a \( q \)-th square root of \( \omega(\chi)/f_X^{q/2} \). Then, \( W(\chi) = \zeta_{N}^{k_0} W_0 \), where \( k_0 \) is the unique integer \( k \in \{0, 1, \ldots, n-1\} \) such that \( |W_N(\chi) - \zeta_X^{k} W_0| < 2\epsilon/q \), where \( W_N(\chi) := \theta_N(1, \chi)/\theta_N(1, \chi) \).

We end up with a practically very efficient method for computing class numbers of simplest fields of large conductors. Our method improves upon the ones used in [CW], [Jean], [Shal], [SW] and [SWW].

### 2. Prerequisites on Gauss sums

**Lemma 3.** Let \( \chi \) be a primitive Dirichlet character of conductor \( f_X > 1 \). Then \( |\tau(\chi)| = \sqrt{f_X} \) and \( \tau(\bar{\chi}) = \chi(-1)\tau(\chi) \). If \( \chi \) is quadratic, then \( \tau(\chi) = \sqrt{\chi(-1)/f_X} \).

**Lemma 4.** Let \( \chi_1, \ldots, \chi_t \) be \( t \geq 1 \) Dirichlet characters modulo \( f_1, \ldots, f_t \). Assume that \( \gcd(f_i, f_j) = 1 \) for \( 1 \leq i \neq j \leq t \). Set \( f = \prod_{i=1}^{t} f_i \) and \( \chi = \prod_{i=1}^{t} \chi_i \), which is therefore a Dirichlet character modulo \( f \) of order \( q > 1 \). Then,

\[
\tau(\chi) := \sum_{k=1}^{f} \chi(k)e^{2\pi ik/f} = \epsilon_\chi \prod_{i=1}^{t} \tau(\chi_i) \quad \text{where} \quad \epsilon_\chi = \prod_{i=1}^{t} \chi_i(f/f_i)
\]
and
\[ J(\chi, \chi) := \sum_{k=1}^{f} \chi(k)\chi(1-k) = \prod_{i=1}^{t} J(\chi_i, \chi_i). \]

In particular, if all the \( \chi \) are of the same order \( q \), then
\[ \omega(\chi) := (\tau(\chi))^q = \prod_{i=1}^{t} \omega(\chi_i). \]

**Lemma 5.** Let \( \mu \) denote the Möbius function. Then, \( Tr_{Q(\zeta_f)/Q(\zeta_f)}(\zeta_f) = \mu(f) \).

**Proof.** Apply Lemma 4 with \( \chi = 1_f \) the trivial character modulo \( f \), note that \( \tau(1_f) = Tr_{Q(\zeta_f)/Q(\zeta_f)}(\zeta_f) \), and prove the result in the case that \( f = p^e \) is a power of a prime, in which case the proof is easy. \( \square \)

Now, let \( \chi \) be a primitive Dirichlet character of order \( q > 1 \) and conductor \( \Delta > 1 \). Let \( M_\chi \) be the cyclic subfield of \( Q(\zeta_\Delta) \) of conductor \( \Delta \) associated with \( \chi \), i.e., \( Gal(Q(\zeta_\Delta)/M_\chi) = ker \chi \). Set
\[ \eta(\chi) := \text{Tr}_{Q(\zeta_\Delta)/M_\chi}(\zeta_\Delta) = \sum_{t \in ker \chi} \zeta_\Delta^t \in M_\chi. \]

Consider all the characters \( \chi^k \), \( 0 \leq k \leq q-1 \), as defined modulo \( \Delta \). Then,
\[ \sum_{k=0}^{q-1} \tau(\chi^k) = \sum_{k=0}^{q-1} \sum_{t=1}^{\Delta} \chi^k(a)\zeta_\Delta^t = \sum_{t=1}^{\Delta} \left( \sum_{k=0}^{q-1} \chi^k(a) \right)\zeta_\Delta^t = q \sum_{t \in ker \chi} \zeta_\Delta^t = q\eta(\chi). \]

Moreover, \( \tau(\chi^q-k) = \chi^k(-1)\overline{\tau(\chi^k)} \) for \( 1 \leq k \leq q-1 \) and \( \tau(\chi^0) = \mu(\Delta) \), by Lemma 5. Note finally that \( M_\chi \) is (totally) real if and only if \( \chi \) is even.

### 3. Simplest Cubic Fields

Set \( \zeta_3 = (-1 + i\sqrt{3})/2 \). The units in \( \mathbb{Z}[\zeta_3] \) are \( \{ \pm 1, \pm \zeta_3, \pm \zeta_3^2 \} \). An algebraic integer \( \alpha = a + b\zeta_3 \in \mathbb{Z}[\zeta_3] \) is primary if \( \alpha \equiv -1 \pmod{3\mathbb{Z}[\zeta_3]} \), i.e., if \( a \equiv -1 \pmod{3} \) and \( b \equiv 0 \pmod{3} \). The order of the multiplicative group \( (\mathbb{Z}[\zeta_3]/3\mathbb{Z}[\zeta_3])^* \) is equal to 6, and the six units in \( \mathbb{Z}[\zeta_3] \) form a set of representatives of this group. Therefore, if 3 does not divide the norm \( N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2 \) of \( \alpha \in \mathbb{Z}[\zeta_3] \), then exactly one of the six associates of \( \alpha \) is primary.

**Lemma 6.** Let \( 0 \neq \alpha \in \mathbb{Z}[\zeta_3] \) be a nonunit element. Assume that \( \alpha \equiv (-1)^t \pmod{3\mathbb{Z}[\zeta_3]} \), where \( t \) is the number of irreducible factors of \( \alpha \) (counted with multiplicity). Then, \( \alpha = \prod_{k=1}^{t} \pi_k \) can be written in a unique way as a product of \( t \) primary irreducibles \( \pi_k \).

**Proof.** For the existence, write \( \alpha = u \prod_{k=1}^{t} \pi_k \) for some unit \( u \in \{ \pm 1, \pm \zeta_3, \pm \zeta_3^2 \} \) and some primary irreducibles \( \pi_k \equiv -1 \pmod{3\mathbb{Z}[\zeta_3]} \). Since \( (-1)^t \equiv \alpha \equiv (-1)^tu \pmod{3\mathbb{Z}[\zeta_3]} \), we obtain \( u \equiv 1 \pmod{3\mathbb{Z}[\zeta_3]} \) and \( u = 1 \). \( \square \)

**Lemma 7** (See [IR Corollary, page 115]). Let \( \pi \equiv -1 \pmod{3\mathbb{Z}[\zeta_3]} \) be a primary irreducible element in \( \mathbb{Z}[\zeta_3] \) of norm \( 3 \) a rational prime \( p \equiv 1 \pmod{3} \). For \( \alpha \in \mathbb{Z}[\zeta_3] \) coprime with \( \pi \), let \( \chi_\pi(\alpha) \in \{ 1, \zeta_3, \zeta_3^2 \} \) be the cubic residue symbol defined by \( \alpha^{(p-1)/3} \equiv \chi_\pi(\alpha) \pmod{\pi} \). Then, \( \omega(\chi_\pi) := \tau(\chi_\pi)^3 = p\pi \).
Theorem 8. Assume that $\Delta_m = m^2 + 3m + 9$ is square-free and that $m \geq -1$ (there are infinitely many such $m$’s, by [Lou7, Proposition 2]). Write $\Delta_m = \prod_{k=1}^{t} p_k$ where the $p_k \equiv 1 \pmod{6}$’s are distinct odd primes. Set

$$\delta_m := \mu(\Delta_m) \left( \frac{m}{3} \right) \frac{2m + 3 + 3i\sqrt{3}}{2}.$$ 

Then, $\delta_m$ can be written in a unique way as a product $\delta_m = \prod_{k=1}^{t} \pi_k$ of $t$ primary irreducibles elements $\pi_k \in \mathbb{Z}[\zeta_3]$ with $p_k = |\pi_k|^2$. Set $\chi_{\delta_m} = \prod_{k=1}^{t} \chi_{\pi_k}$. Then, $\chi_{\delta_m}$ is a primitive cubic character modulo $\Delta_m$,

$$\chi_{\delta_m}(2) = \begin{cases} \zeta_3^2 & \text{if } m \equiv 0 \pmod{2}, \\ \zeta_3 & \text{if } m \equiv 1 \pmod{2}, \end{cases}$$ 

and

$$\omega(\chi_{\delta_m}) := \tau(\chi_{\delta_m})^3 = \Delta_m \delta_m = \mu(\Delta_m) \left( \frac{m}{3} \right) \frac{2m + 3 + 3i\sqrt{3}}{2} \Delta_m.$$ 

Moreover (see also [Laz3, Proposition 2.2]),

$$\bar{\eta}_m := \mu(\Delta_m) \left( \frac{m}{3} \right) \eta(\chi_{\delta_m}) + \frac{m - \left( \frac{m}{3} \right)}{3}$$

(see [5]) is a root of $P_m(x) = x^3 - mx^2 - (m+3)x - 1$. Therefore, $K_m = \mathbb{Q}(\eta(\chi_{\delta_m}))$ is a simplest cubic field of conductor $\Delta_m$ and $\chi_{\delta_m}$ is one of the two conjugate characters associated with $K_m$. Hence, me may suppose that $\chi_{K_m} = \chi_{\delta_m}$. Then, setting $\epsilon_m := (1 - \mu(\Delta_m)(\frac{m}{3})) / 2 \in \{0, 1\}$, there exists $k_m \in \{0, 1, 2\}$ such that

$$\arg(W(\chi_{K_m})) = \frac{1}{3} \arctan \left( \frac{3\sqrt{3}}{2m + 3} \right) + \frac{2k_m + \epsilon_m}{3} \pi \pmod{2\pi}.$$ 

Proof. Since $\delta_m \equiv (-1)^t \pmod{3\mathbb{Z}[\zeta_3]}$, the first assertion follows from Lemma 6. By the law of cubic reciprocity (see [12], Theorem 1, page 114), we have

$$\chi_{\delta_m}(2) = \chi_2(\delta_m) \equiv \delta_m \equiv \begin{cases} \zeta_3^2 & \text{if } m \equiv 0 \pmod{2}, \\ \zeta_3 & \text{if } m \equiv 1 \pmod{2}, \end{cases} \pmod{2\mathbb{Z}[\zeta_3]}$$

which implies (7). Using Lemmas 4 and 7 we obtain (8). Finally, let $M_m$ denote the real cyclic cubic field of conductor $\Delta_m$ associated with $\chi_{\delta_m}$. We have $\eta_m := \eta(\chi_{\delta_m}) \in M_m$. Now, $\epsilon(3\bar{\eta}_m - m) = 3\eta_m - \mu(\Delta_m) = \tau + \bar{\tau}$, by Section 2, where $\epsilon = \mu(\Delta_m) \left( \frac{m}{3} \right)$. Using $\tau \bar{\tau} = \Delta_m$ and (8), we obtain $\epsilon(3\bar{\eta}_m - m)^3 = (\tau + \bar{\tau})^3 = \tau^3 + \bar{\tau}^3 + 3\tau \bar{\tau}(\tau + \bar{\tau}) = \epsilon(2m + 3)\Delta_m + 3\epsilon \Delta_m (3\bar{\eta}_m - m)$, by (8). Hence, $\bar{\eta}_m$ is a root of $(3x-m)^3 -(2m+3)\Delta_m -3\Delta_m (3x-m) = 27P_m(x)$, and $\mathbb{Q}(\bar{\eta}_m) = \mathbb{Q}(\eta_m) = M_m$. 

Now, $P_m(x)$ has only one root $\rho_m > 0$,

$$\rho_m = \frac{1}{3} \left( m + 2\sqrt{\Delta_m} \cos \left( \frac{1}{3} \arctan \left( \frac{\sqrt{27}}{2m + 3} \right) \right) \right),$$

$$\Reg_{K_m} = \log^2 \rho_m - (\log \rho_m)(\log(1 + \rho_m)) + \log^2(1 + \rho_m),$$

and

$$h_{K_m} = |L'(0, \chi_{K_m})|^2 / \Reg_{K_m} \geq \Delta_m / (\epsilon \log^3 \Delta_m).$$

We computed the class numbers of all the $K_m$’s with $-1 \leq m \leq 1066285$ and $\Delta_m = m^2 + 3m + 9 \equiv 1 \pmod{4}$ a prime. In that situation, the product $h_{L_m} h_{K_m}$ (of the class numbers of $L_m = \mathbb{Q}(\sqrt{\Delta_m})$ and $K_m$) divides the class number of the
real cyclotomic field $\mathbb{Q}^+(\zeta_{\Delta_m})$ (see [CW] Lemma 1]). We list below the least ten $m$'s for which $h_{L_m}h_{K_m} > \Delta_m$.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\Delta_m$</th>
<th>$[{1, \chi_{K_m}}]$</th>
<th>$\frac{\Delta_m}{h_{L_m}} \pi$</th>
<th>$h_{L_m}$</th>
<th>$h_{K_m}$</th>
<th>$h_{L_m}h_{K_m}/\Delta_m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>102496</td>
<td>10505737513</td>
<td>20.268 \ldots</td>
<td>$\pi/3$</td>
<td>891</td>
<td>13152913</td>
<td>1.115 \ldots</td>
</tr>
<tr>
<td>100253</td>
<td>11290018777</td>
<td>34.364 \ldots</td>
<td>0</td>
<td>2685</td>
<td>6209212</td>
<td>1.476 \ldots</td>
</tr>
<tr>
<td>319760</td>
<td>102247146889</td>
<td>202.162 \ldots</td>
<td>0</td>
<td>1887</td>
<td>57772549</td>
<td>1.066 \ldots</td>
</tr>
<tr>
<td>554869</td>
<td>30788122777</td>
<td>88.861 \ldots</td>
<td>$\pi/3$</td>
<td>7983</td>
<td>93739324</td>
<td>2.430 \ldots</td>
</tr>
<tr>
<td>726845</td>
<td>528305834569</td>
<td>20.938 \ldots</td>
<td>0</td>
<td>13533</td>
<td>176702419</td>
<td>4.526 \ldots</td>
</tr>
<tr>
<td>791021</td>
<td>62517695513</td>
<td>129.812 \ldots</td>
<td>0</td>
<td>1737</td>
<td>445142272</td>
<td>1.235 \ldots</td>
</tr>
<tr>
<td>796616</td>
<td>63459944113</td>
<td>357.252 \ldots</td>
<td>0</td>
<td>1155</td>
<td>69679264</td>
<td>1.268 \ldots</td>
</tr>
<tr>
<td>839401</td>
<td>70496557013</td>
<td>293.373 \ldots</td>
<td>$\pi$</td>
<td>1575</td>
<td>55491633</td>
<td>1.239 \ldots</td>
</tr>
<tr>
<td>906437</td>
<td>821630754289</td>
<td>93.697 \ldots</td>
<td>0</td>
<td>1955</td>
<td>46991916</td>
<td>1.118 \ldots</td>
</tr>
<tr>
<td>1066285</td>
<td>11369660009089</td>
<td>140.662 \ldots</td>
<td>$\pi/3$</td>
<td>5389</td>
<td>473034223</td>
<td>2.242 \ldots</td>
</tr>
</tbody>
</table>

### 4. Simplest sextic fields

Using simplest cubic fields we obtain only a few examples of real cyclotomic fields $\mathbb{Q}^+(\zeta_p)$ of prime conductor $p$ and class number greater than or equal to $\Delta$. To obtain many more examples we will use simplest sextic fields to prove that if $\Delta = m^2 + 3m + 9 \equiv 1 \pmod{4}$ is prime and $\Delta > 4565$, then the class number of the real cyclotomic field $\mathbb{Q}^+(\zeta_{\Delta})$ is greater than or equal to $\Delta$ (see Remark 11 below). Assume that $\Delta = m^2 + 3m + 9 \equiv 1 \pmod{4}$ is square-free, $m \geq 1$, and let $K_m$ and $\chi_{K_m}$ be as in Theorem 8. Then, setting $L_m = \mathbb{Q}(\sqrt{\Delta_m})$, the compositum $N_m = L_mK_m$ is a cyclic sextic field of conductor $\Delta_m$ and $\chi_{N_m}(n) = \left(\frac{\Delta}{\Delta_m}\right)\chi_{K_m}(n)$ is one of its two conjugate associated sextic characters. Note that $\chi_{N_m}^2 = \chi_{K_m}$.

In [Gra2] M. N. Gras proved that $N_m$ is a simplest sextic field associated with the sextic polynomial

$$P_m(x) = x^6 - 2mx^5 - 5(m+3)x^4 + 20x^3 + 5mx^2 + 2(m+3)x + 1$$

(set $m = (t-6)/4$ in [Gra2] (8))] of discriminant $d_m = 6^6\Delta^5$.

Let $N$ be a real cyclic sextic field. Let $U_N$ and $\sigma$ be its group of algebraic units and a generator of its Galois group. Let $L$ and $K$ denote its real quadratic and real cyclic cubic subfields. Let $U_N' = \{ \epsilon \in U_N; N_{L/K}(\epsilon) \in \{1\} \}$ and $N_{L/K}(\epsilon) \in \{1\}$ denote the so-called group of relative units of $N$. It is known that there exists some so-called generating relative unit $\epsilon_1 \epsilon_2 \in U_N$ such that $\{-1, \epsilon_1, \epsilon_2\}$ generate $U_N'$, and we set

$$\text{Reg}_N^* := (\log |\epsilon_1|)^2 + (\log |\epsilon_2|)^2 - (\log |\epsilon_1|)(\log |\epsilon_2|) > 0,$$

which does not depend on the generating relative unit. Then, $\text{Reg}_{L, K} = Q_N\text{Reg}_{N}$ for some $Q_N \in \{1, 3, 4, 12\}$ (see [Lou7] Lemma 3). Now,

$$h_1^* := h_N/(h_Lh_K) = \frac{Q_N}{12\text{Reg}_N}|L'(0, \chi_N)|^2$$

is a positive divisor of $h_N$, by [CW] Lemma 1], where $\chi_N$ is any one of the two conjugate primitive, even, sextic Dirichlet characters of conductor $f_N$ associated with $N$. For the simplest sextic fields we have:

**Lemma 9** (See [Gra2] Th. 2] and [Lou7] Lemma 6]). Assume that $m > 1$ is such that $\Delta = m^2 + 3m + 9 \equiv 1 \pmod{12}$ is square-free, and let $a = 4\sqrt{\Delta_m}$.
\(\epsilon_s := -\rho_m(2\rho_m + 1)/(\rho_m + 2)\) is a generating relative unit of the simplest sextic field \(N_m\),
\[
\epsilon_s = -\sqrt{\frac{4a(a - 9)}{9}} \cos \left(\frac{1}{3} \arctan \left(\frac{\sqrt{27(a^2 - 108)}}{2a^2 - 27a + 54}\right) + 1 - \frac{a}{3}\right),
\]
and
\[
\epsilon_s^* = \sqrt{\frac{4a(a + 9)}{9}} \cos \left(\frac{1}{3} \arctan \left(\frac{\sqrt{27(a^2 - 108)}}{2a^2 + 27a + 54}\right) + \frac{\pi}{3}\right) + 1 + \frac{a}{3}.
\]

**Theorem 10.** Assume that \(\Delta_m = m^2 + 3m + 9 \equiv 1 \pmod{12}\) is square-free. Then,
\[
\omega(x_{N_m}) := (\tau(x_{N_m}))^6 = (-1)^{(\Delta_m - 1)/2} \left((2m + 3 + 3i\sqrt{3}/2)^4 \Delta_m\right).
\]
Hence, setting \(\epsilon_m := (-1)^{(\Delta_m - 1)/2}/2 \in \{0, 1\}\), there exists \(k_m \in \{0, 1, 2, 3, 4, 5\}\) such that
\[
\arg(W(x_{N_m})) \equiv \frac{1}{6} \arctan \left(\frac{3\sqrt{3}}{2m + 3}\right) + \frac{k_m + \epsilon_m}{6} \pi \pmod{2\pi}.
\]

**Proof.** Let \(\chi\) be a sextic Dirichlet character modulo a prime \(p \equiv 1 \pmod{6}\). Using [BE71] Theorem 3.1 or [Laz4] Lemma 2.1, we have
\[
\omega(\chi) := (\tau(\chi))^6 = \left(\frac{-1}{p}\right) (\omega(\chi)^2)^4/p^3.
\]
Using Lemma 4 and Theorem 8 we obtain the desired result. \(\square\)

**Remark 11.** Since \(Q_{N_m}\) is not that easy to compute, it is much easier to compute \(h_{N_m}^{\ast \ast} := 12h_{N_m}^{\ast}/Q_{N_m} = |L'(0, \chi_K)|^2/\text{Reg}_{K} \in \{h_{N_m}^{\ast}, 3h_{N_m}^{\ast}, 4h_{N_m}^{\ast}, 12h_{N_m}^{\ast}\}\) which divides \(12h_{N_m}^{\ast}\). According to our computation, we have \(h_{K_m}^{\ast}h_{N_m}^{\ast \ast} \geq 12\Delta_m\) for \(4565 < m < 10^5\), which implies \(h_{N_m}/h_{L_m} = h_{K_m}h_{N_m} \geq \Delta_m\), for \(4565 < m < 10^5\), hence for \(m > 4565\) by [Lou7, Theorem 8].

5. **Simplest quartic fields**

Let \(K\) be a real cyclic quartic field. Let \(U_K\) and \(\sigma\) be its group of algebraic units and a generator of its Galois group. Let \(L\) denote its real quadratic subfield. Let \(h_L\) be its class number. Finally, let \(U_K^* = \{\epsilon \in U_K; N_K/L(\epsilon) \in \{\pm 1\}\}\) denote the so-called group of relative units of \(K\). There exists some so-called generating relative unit \(\epsilon_s \in U_K^*\) such that \(-1, \epsilon_s, \epsilon_s^2\) generate \(U_K^*\), and we set
\[
\text{Reg}_K^* := (\log |\epsilon_s|)^2 + (\log |\epsilon_s^2|)^2 > 0
\]
(which does not depend on the generating relative unit). Then, it holds that
\[
2\text{Reg}_L \text{Reg}_K = Q_K \text{Reg}_K \text{ for some } Q_K \in \{1, 2\} \pmod{2}\]
(see [Lou7] Lemma 2). Since \(K/L\) is ramified, \(h_L\) divides \(h_K\) and
\[
h_K^* := \frac{Q_K}{2\text{Reg}_K}|L'(0, \chi_K)|^2
\]
is a positive divisor of \(h_K\).
5.1. Some quartic Gauss sums. The units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$. An algebraic integer $\alpha = a + bi \in \mathbb{Z}[i]$ is primary if $\alpha \equiv 1 \pmod{1 + i}$, i.e., if $[a \equiv 1 \pmod{4}$ and $b \equiv 0 \pmod{4}]$ or $[a \equiv -1 \pmod{4}$ and $b \equiv 2 \pmod{4}]$. The order of the multiplicative group $(\mathbb{Z}[i]/(1 + i)^3\mathbb{Z}[i])^*$ is equal to 4 and the four units in $\mathbb{Z}[i]$ form a set of representatives of this group. Therefore, if 2 does not divide the norm $N(\alpha) = a\bar{a} = a^2 + b^2$ of $\alpha \in \mathbb{Z}[i]$, then exactly one of the four associates of $\alpha$ is primary. If follows that if $0 \neq \alpha \in \mathbb{Z}[i]$ is a nonunit primary element, then $\alpha$ can be written in a unique way as a product of primary irreducibles (for the existence, see [IR, Lemma 8 page 121]).

Lemma 12 (See [IR, Theorem 3, page 128]). Let $p = a^2 + b^2 \equiv 1 \pmod{4}$ be a rational prime, where $b$ is even and $a \in \mathbb{Z}$ is uniquely determined by $a \equiv (-1)^{(p-1)/4}$ (mod 4). Set $\pi = a + bi \in \mathbb{Z}[i]$ (which is primary). For $\alpha \in \mathbb{Z}[i]$ coprime with $\pi$, let $\chi_\pi(\alpha) \in \{\pm 1, \pm i\}$ be the quartic residue symbol defined by $\alpha^{(p-1)/4} \equiv \chi_\pi(\alpha)$ (mod $\pi$). Then, $\tau(\chi_\pi) = (-1)^{(p-1)/4}\sqrt{p}$. (An explicit formula for $\tau(\chi_\pi)$ is given in [BE82, Section 4.3], but using it, the numerical determination of $\tau(\chi_\pi)$ would require at least $\gg p$ elementary operations.)

Corollary 13. Let $\delta_m = \prod_{k=1}^{t} \pi_k$ be a product of $t \geq 1$ primary irreducibles $\pi_k \in \mathbb{Z}[i]$ such that the $p_k = \vert \pi_k \vert^2 \equiv 1 \pmod{4}$ are pairwise distinct primes. Set $\Delta_m = \vert \delta_m \vert^2 = \prod_{k=1}^{t} p_k$ and $\chi_{\delta_m} = \prod_{k=1}^{t} \chi_{\pi_k}$. Then, $\chi_{\delta_m}$ is a primitive, quartic character modulo $\Delta_m$, $\chi_{\delta_m}(-1) = (-1)^{(\Delta_m-1)/4}$,

\[ \tau(\chi_{\delta_m})^2 = (-1)^{(\Delta_m-1)/4}\delta_m \sqrt{\Delta_m}, \]

$\chi_{\delta_m}^2$ is a primitive, even quadratic character modulo $\Delta_m$, and $\tau(\chi_{\delta_m}^2) = \sqrt{\Delta_m}$.

Proof. According to Lemmas 9 and 12 and using

\[ \sum_{k=1}^{t} \frac{p_k - 1}{4} = \frac{\Delta_m - 1}{4} \pmod{2}, \]

(by induction on $t$) and

\[ c_{\chi_{\delta_m}} = \left( \prod_{i=1}^{t} \prod_{j=1}^{t} \chi_{\pi_i}(p_j) \right)^2 = \prod_{i=1}^{t} \prod_{j=1}^{t} \left( \frac{p_j}{p_i} \right) = \prod_{1 \leq i < j \leq t} \left( \frac{p_j}{p_i} \right) = +1 \]

(for the $p_i$’s are all equal to 1 modulo 4), we obtain (11). Using (12), we obtain $\chi_{\delta_m}(-1) = \prod_{k=1}^{t} \chi_{\pi_k}(-1) = \prod_{k=1}^{t} (-1)^{(p_k - 1)/4} = (-1)^{(\Delta_m-1)/4}$. 

Theorem 14. Assume that $\Delta_m = m^2 + 16 \equiv 1 \pmod{8}$ is square-free, and that $m \geq 1$ odd (there are infinitely many such $m$’s, by [Lou6, Proposition 7]). Write $\Delta_m = \prod_{k=1}^{t} p_k$ where the $p_k \equiv 1 \pmod{4}$ are distinct odd primes. Then,

\[ \delta_m := (-1)^{(m-1)/2}(m + 4i) \equiv 1 \pmod{4\mathbb{Z}[i]} \]
is primary, \( \chi_{\Delta_m} \) is a primitive, even, quartic character modulo \( \Delta_m \), \( \chi^2_{\Delta_m} \) is a primitive quadratic character modulo \( \Delta_m \), and there exists \( \epsilon_m \in \{ \pm 1 \} \) such that

\[
\tau(\chi_{\Delta_m}) = \epsilon_m e^{\pm i\frac{(m-1)}{2}} \left( \sqrt{(\Delta_m + m\sqrt{\Delta_m})/2} + i\sqrt{(\Delta_m - m\sqrt{\Delta_m})/2} \right).
\]

Moreover, \( Q(\eta(\chi_{\Delta_m})) = Q(\sqrt{(\Delta_m + m\sqrt{\Delta_m})/2}) \) and (see also \cite[Proposition 3.4]{Laz3})

\[
\tilde{\eta}_m := \mu(\Delta_m)(-1)^{(m-1)/2}\eta(\chi_{\Delta_m}) + \frac{m - (-1)^{(m-1)/2}}{4}
\]

is a root of \( P_m(x) = x^4 - m^3x - 3x^2 + mx + 1 \). Therefore, \( K_m = Q(\eta(\chi_{\Delta_m})) \) is a simplest quartic field of conductor \( \Delta_m \) and \( \chi_{\Delta_m} \) is one of the two conjugate characters associated with the simplest quartic field \( K_m \). Hence, we may suppose that \( \chi_{K_m} = \chi_{\Delta_m} \) and there exists \( k_m \in \{ 0, 1 \} \) such that

\[
\arg(W(\chi_{K_m})) = \arctan\left( \frac{4}{m + \sqrt{\Delta_m}} \right) + (t + (m - 1)/2)\frac{\pi}{2} + k_m\pi \pmod{2\pi}.
\]

**Proof.** (13) follows from (11). Since \( \chi_{\Delta_m} \) is even, the cyclic quartic field \( M_m \) of conductor \( \Delta_m \) associated with \( \chi_{\Delta_m} \) is real and \( \eta_m := \eta(\chi_{\Delta_m}) \in M_m \). Now, \( \epsilon(4\tilde{\eta}_m - m - \epsilon\sqrt{\Delta_m}) = 4\eta_m - \mu(\Delta_m) - \sqrt{\Delta_m} = \tau + \tau \), by Section 2 where \( \epsilon := (-1)^{t + (m-1)/2} \). Using \( \tau^2 = \Delta_m \) and (11), we obtain \( (4\tilde{\eta}_m - m - \epsilon\sqrt{\Delta_m})^2 = 2\tau + 2\Delta_m = 2em\sqrt{\Delta_m} + 2\Delta_m \). \( Q(\eta_m) = Q(\tilde{\eta}_m) = Q(\sqrt{(\Delta_m + em\sqrt{\Delta_m})/2}) \subseteq M_m \), and this inclusion is an equality. Finally, \( \tilde{\eta}_m \) satisfies \((4\tilde{\eta}_m - m - \epsilon\sqrt{\Delta_m})^2 = 2em\sqrt{\Delta_m} + 2\Delta_m \). Hence, \( (4\tilde{\eta}_m - m - \epsilon\sqrt{\Delta_m})^2 - \Delta_m = 8\epsilon\sqrt{\Delta_m}\eta_m \) and \( 0 = ((4\tilde{\eta}_m - m - \sqrt{\Delta_m})^2 - 64\Delta_m\tilde{\eta}_m^2 = 256P_m(\tilde{\eta}_m) \).

**5.2. Some numerical computations.** \( P_m(x) \) has only one root \( \rho_m > 1 \),

\[
\rho_m = \left( (m + \sqrt{\Delta_m})/2 + \sqrt{(m + \sqrt{\Delta_m})/2}/2 \right),
\]

\[
\sigma(\rho_m) = \left( (m - \sqrt{\Delta_m})/2 + \sqrt{(m - \sqrt{\Delta_m})/2}/2 \right),
\]

\[
R_{K_m} = \log^2 \rho_m + \log^2 \sigma(\rho_m),
\]

\( L_m = Q(\sqrt{\Delta_m}) \) is the quadratic subfield of the real cyclic quartic field \( K_m \), and

\[
h_{K_m}^2 = h_{K_m}/h_{L_m} = \frac{Q_{K_m}}{2R_{K_m}}|L'(0, \chi_{K_m})|^2 \geq \frac{2\Delta_m}{3e(\log \Delta_m + 0.35)^2}.
\]

**Theorem 15.** Assume that \( m \geq 1 \) and that \( \Delta_m = m^2 + 16 \) is prime. Then, the class numbers and narrow class numbers of \( K_m \) and \( L_m \) are odd, and \( Q_{K_m} = 2 \).

**Proof.** (See \cite[Lou6]{Laz3} Proposition 10) for the determination of \( Q_{K_m} \) in the general case.) For the results on the class numbers, see \cite[Wa3]{Wa3} proof of Th. 10.4(b)]. Now, the norm of the fundamental unit \( \epsilon_{L_m} > 1 \) of \( L_m \) is equal to \(-1\). Moreover, \( \sigma^3(\rho_m) < -1 < \sigma^2(\rho_m) = 0 < \sigma(\rho_m) < 1 < \rho_m \). Hence, \( \epsilon_{L_m}\rho_m^{-\sigma} \) is a totally positive algebraic unit of \( K_m \). Since the narrow class number \( h_{K_m}^+ \) of \( K_m \) is odd, \( \epsilon_{L_m}\rho_m^{-\sigma} \) is a square in \( K_m \) (recall that if \( K \) is totally real, then \( h_K^+ = (U_K^+ : U_K^2)h_K \)), and \( Q_{K_m} = 2 \) (by \cite[Proposition 1]{Gra1}).
Table 2. Least primes $\Delta_m = m^2 + 16$ with $h_{K_m} \geq \Delta_m$

| $m$    | $\Delta_m$ | $|\Phi(1, \chi_{K_m})|$ | $\epsilon_m$ | $h_{L_m}$ | $h_{K_m}$ | $h_{K_m}/\Delta_m$ |
|--------|-------------|--------------------------|--------------|-----------|-----------|-------------------|
| 524285 | 274874761241| 366.538 \cdots           | +1           | 1911      | 181442581 | 1.261 \cdots      |
| 1680401| 2823747520817| 103.742 \cdots           | -1           | 1537      | 1878644993 | 1.022 \cdots      |

Let $q \equiv 3 \pmod{4}$ be the least positive odd prime such that $\chi_{K_m}^2(q) = \big(q_m^\Delta\big) = -1$. Then $\chi_{K_m}(q) \in \{\pm i\}$ and $\chi_{\delta_m}(q) \in \{\pm i\}$. According to the law of biquadratic reciprocity (see [IR, Theorem 2, page 123]), we have $\chi_{\delta_m}(q) = \chi_{\delta_m}(-q) = \chi_q(-\delta_m) \equiv \delta_m^{(q^2 - 1)/4} \pmod{q\mathbb{Z}[i]}$, which can be efficiently computed by using the binary expansion of $(q^2 - 1)/4$. Hence, by computing $\chi_{K_m}(q)$ and by changing $\chi_{K_m}$ into its conjugate if necessary, we may assume that $\chi_{K_m}(q) = \chi_{\delta_m}(q)$, which implies $\chi_{K_m} = \chi_{\delta_m}$. We used our efficient method to compute the class numbers of all the $K_m$'s with $1 \leq m \leq 1680401$ and $\Delta_m = m^2 + 16$ a prime. In that situation, the class number $h_{K_m} = h_{L_m}h_{K_m}^*$ of $K_m$ divides the class number of the real cyclotomic field $\mathbb{Q}^+(\zeta_{\Delta_m})$ (see [CW] Lemma 2)). We list below the least two $m$'s for which $h_{K_m} > \Delta_m$. Note that G. Cornell and L. C. Washington did not find any such $K_m$ (see [CW bottom of page 268]).

Lemma 16. Let $\pi_k = A_k + 2iB_k \in \mathbb{Z}[i]$ be primary of prime norms $p_k = A_k^2 + 4B_k^2 \equiv 1 \pmod{4}$, $1 \leq k \leq t$. Set $\delta := \prod_{k=1}^t \pi_k = A + 2iB \in \mathbb{Z}[i]$. Then, $\chi_{\delta}(2) = i^{-B}$. In particular, if $K_m$ is a simplest quartic field and $\chi_{K_m}$ is any one of its two associated quartic characters, then $\chi_{K_m}(2) = -1$.

Proof. We have $A_k \equiv 1 + 2B_k \pmod{4}$ and $\chi_{\pi_k}(2) = \chi_{\pi_k}(1 + i)\overline{\chi_{\pi_k}(1 + i)} = i^{-B_k}$ (by [IR] Exercise 37, page 136). It follows that $B \equiv \sum_{k=1}^t B_k \pmod{4}$ and $A \equiv 1 + 2B \pmod{4}$ (by induction on $t$), which implies $\chi_{\delta}(2) = \prod_{k=1}^t \chi_{\pi_k}(2) = i^{-B}$. In particular, we do have $\chi_{K_m}(2) = i^{-2} = -1$. 

5.3. Washington’s cyclic quartic fields. We deal with the family of real cyclic number fields introduced in [Wa2].

Theorem 17. Assume that $\Delta_m := m(m + 2)(m^2 + 4) \equiv 3 \pmod{4}$ is square-free, and that $m \geq 1$ odd. Let $t \geq 1$ denote the number of prime divisors of $d_m := m^2 + 4$. Set $\Delta_m = (-1)^{t(m + 1)/2}(m - 2t)$, which is primary, and $\chi_{\Delta_m}(n) = \big(n^{m(m + 2)}\big)\chi_{\delta_m}(n)$. Then, $\chi_{\Delta_m}$ is a primitive, even, quartic Dirichlet character modulo $\Delta_m$, $\chi_{\Delta_m}^2$ is of conductor $d_m$, $\chi_{\Delta_m}^2(2) = i$, and there exists $\epsilon_m \in \{\pm 1\}$ such that

$$
(14) \quad \tau(\chi_{\Delta_m}) = \epsilon_m t + (m^2 - 1)/2 \sqrt{m(m + 2)\Delta_m}\left(\sqrt{d_m + m} - i\sqrt{d_m - m}\right).
$$

Moreover, $\mathbb{Q}(\eta(\chi_{\Delta_m})) = \mathbb{Q}\left(\sqrt{(\Delta_m \pm \sqrt{m(m + 2)\Delta_m})/2}\right)$ and

$$
\eta_m := \eta_m(\chi_{\Delta_m}) = \frac{m^2 - \mu(\Delta_m) + \left(m + 2\right)\mu(d_m) + \left(-\frac{2}{m}\right)\mu(m(m + 2))\sqrt{d_m}}{4}
$$

is a root of $P_m(x) = x^4 - m^2x^3 - (m^3 + 2m^2 + 4m + 2)x^2 - m^2x + 1$. Therefore, $K_m = \mathbb{Q}(\eta(\chi_{\Delta_m}))$ is a cyclic quartic field of conductor $\Delta_m$, and its real quadratic
subfield is \( k_m = \mathbb{Q}(\sqrt{d_m}) \), of conductor \( d_m \). We may suppose that \( \chi_{K_m} = \chi_{\Delta_m} \) and there exists \( k_m \in \{0, 1\} \) such that
\[
\arg(W(\chi_{K_m})) = -\arctan\left(\frac{2}{m + \sqrt{d_m}}\right) + (t + (m^2 - 1)/8)\frac{\pi}{4} + km\pi \pmod{2\pi}.
\]

Proof. By Lemma \([10]\) we have \( \chi_{\Delta_m}(2) = \left(\frac{-2}{m(m+2)}\right)i^{(m+1)/2} = i \) (check it on the four cases \( m \equiv 1, 3, 5, 7 \pmod{8} \)). By Corollary \([13]\) we have \( \chi_{\Delta_m}(-1) = \left(\frac{-1}{m(m+2)}\right)(-1)^{(d_m-1)/4} = (-1) \times (-1) = +1 \), and
\[
(15) \quad \tau(\chi_{\Delta_m})^2 = \epsilon(m - 2i)\sqrt{m(m + 2)\Delta_m},
\]
where
\[
\epsilon = (-1)^t\left(\frac{2}{m}\right) = \mu(d_m)\left(\frac{2}{m}\right)
\]
(use Section \([2]\) Corollary \([13]\) and \( \left(\frac{m(m+2)}{m+2}\right) = -\left(\frac{-2}{m}\right) \)), from which \([14]\) follows. Hence \( \chi_{\Delta_m} \) is even and the cyclic quartic field \( M_m \) of conductor \( \Delta_m \) associated with \( \chi_{\Delta_m} \) is real. As in the proof of Theorem \([14]\), set \( \tau = \tau(\chi_{\Delta_m}) \) and \( \eta_m := \eta(\chi_{\Delta_m}) \in M_m \). Now, \( \tau(\chi_{\Delta_m}) = \tau(1_{m(m+2)}(\frac{\eta_m}{m})) = \epsilon'\sqrt{d_m} \) (use Section \([2]\)), where
\[
\epsilon' = \mu(m(m + 2))\left(\frac{m(m + 2)}{m^2 + 4}\right) = -\left(\frac{-2}{m}\right)\mu(m(m + 2)).
\]
Hence, \( \eta'_m := 4\eta_m - \mu(\Delta_m) - \epsilon'\sqrt{d_m} = \tau + \tilde{\tau} \), by Section \([2]\). Using \( \tau \tilde{\tau} = \Delta_m \) and \([13]\), we obtain \( \eta'^2_m = 2\Re(\tau^2) + 2\Delta_m = 2em^2(m + 2)\sqrt{d_m} + 2\Delta_m \), \( Q(\eta_m) = Q(\eta'_m) = Q\left(\sqrt{(\Delta_m + em\sqrt{m(m + 2)\Delta_m})/2}\right) \subseteq M_m \), and this inclusion is an equality. Finally, \( \tilde{\eta}_m = (\eta'_m + m^2 + \epsilon(m + 2)\sqrt{d_m})/4 \) satisfies \((4\tilde{\eta}_m - m^2) - \epsilon(m + 2)\sqrt{d_m})^2 = 4\eta'^2_m = 2em^2(m + 2)\Delta_m + 2m^2(m + 2)\sqrt{d_m} \). Hence,
\[
(4\tilde{\eta}_m - m^2) - (m^2 - 4)d_m = 8\epsilon(m + 2)\sqrt{d_m} \tilde{\eta}_m
\]
and\( 0 = ((4\tilde{\eta}_m - m^2) - (m^2 - 4)d_m)^2 - 64(m + 2)^2d_m\tilde{\eta}_m^2 = 256P_m(\tilde{\eta}_m). \)

6. Simplest quintic fields

In \([Jean]\) and \([SW]\), S. Jeannin, R. Schoof and L. C. Washington dealt with the so-called simplest quintic fields, the real cyclic quintic number fields associated with the quintic polynomials
\[
P_m(x) = x^5 + m^2x^4 - 2(m^3 + 3m^2 + 5m + 5)x^3
\]
\[
+ (m^4 + 5m^3 + 11m + 5)x^2 + (m^5 + 4m^2 + 10m + 10)x + 1
\]
of discriminants \( d_m = (m^3 + 5m^2 + 10m + 7)^2\Delta_m^4 \), where \( \Delta_m = m^4 + 5m^3 + 15m^2 + 25m + 25 \). We assume that \( \Delta_m \) is square-free. Then, the conductor of \( K_m \) is equal to \( \Delta_m \) (see \([Jean]\) Th. 1)) and the zeros of \( P_m(X) \) generate the unit group of \( K_m \) (see \([SW]\) Theorem (3.5) and \([Jean]\) Théorème 2)).

6.1. Minimal polynomials of Gaussian periods. If \( \gcd(a, f) = 1 \), we let \( \sigma_{a, f} \in \text{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q}) \) be defined by \( \sigma_{a, f}(\zeta_f) = \zeta_f^a \).

Fix \( \chi \) a primitive even Dirichlet character of order \( q \geq 2 \) and conductor \( \Delta > 1 \). All the characters \( \chi^a, a \in \mathbb{Z} \), are considered as characters modulo \( \Delta \).

We assume (i) that \( \Delta \) is square-free, hence \( \Delta = \prod_{i=1}^t p_i \) is a product of \( t \geq 1 \) distinct primes \( p_i \equiv 1 \pmod{q} \), and (ii) that the \( q - 1 \) characters \( \chi^a, 1 \leq a \leq q - 1 \),
are primitive modulo $\Delta$. Then, none of the Gaussian sums $\tau(\chi^a)$, $a \in \mathbb{Z}$, is equal to zero, for $|\tau(\chi^a)| = \sqrt{\Delta}$ if $q$ does not divide $a$ (see [Wa3 Lemma 4.8]) and $\tau(\chi^a) = \mu(\Delta) = (-1)^k$ if $q$ divides $a$ (by Lemma 5). Let $K \subseteq \mathbb{Q}(\zeta_\Delta)$ be the real cyclic number field of degree $q$ and conductor $\Delta$ associated with $\chi$ (see [Wa3 Chapter 3]), i.e., $\text{Gal}(\mathbb{Q}(\zeta_\Delta)/K) = \ker \chi$ as a subgroup of $(\mathbb{Z}/\Delta \mathbb{Z})^* = \text{Gal}(\mathbb{Q}(\zeta_\Delta)/\mathbb{Q})$. For $k \in \mathbb{Z}$, let $k^* \in \mathbb{Z}$ coprime with $\Delta$ be such that $\chi(k^*) = \zeta^{k^*_q}$. Set
\[
\eta_k := \sum_{i=1}^{\Delta} \zeta_{\Delta}^i \in \mathbb{Q}(\zeta_\Delta) \quad (k \in \mathbb{Z}).
\]
Then, $\eta_0 = Tr_{\mathbb{Q}(\zeta_\Delta)/K}(\zeta_\Delta) \in K$.

(16) \[
\sigma_{k^*, \Delta}(\eta_k) = \sum_{i=1}^{\Delta} \zeta_{\Delta}^{ik^*} = \sum_{i=1}^{\Delta} \zeta_{\Delta}^{i+k} = \eta_{i+k},
\]
and $\eta_k = \sigma_{k^*, \Delta}(\eta_0) \in \sigma_{k^*, \Delta}(K) = K$. Now, suppose that $\sum_{i=0}^{q-1} \lambda_i \eta_i = 0$, $\lambda_i \in \mathbb{Q}$. Then, $0 = \sigma_{k^*, \Delta}(\sum_{i=0}^{q-1} \lambda_i \eta_i) = \sum_{i=0}^{q-1} \lambda_i \eta_{i+k}$ for $0 \leq k \leq q-1$, by (16). Since $\det(\eta_{i+k})_{0 \leq i,k \leq q-1} = \prod_{a=0}^{q-1} \tau(\chi^a)$ (by (19)) is not equal to 0, we obtain $\lambda_0 = \cdots = \lambda_{q-1} = 0$. In particular, the $\eta_k$, $0 \leq k \leq q-1$, are $\mathbb{Q}$-linearly independent. Hence, they form a $\mathbb{Q}$-basis of $K$, $K = \mathbb{Q}(\eta_0)$ (see [Lon Theorem 2.11 page 105] for a more general result), and there exists $C = [c_{i,j}]_{0 \leq i,j \leq q-1} \in M_q(\mathbb{Q})$ such that

(17) \[
\eta_0 \eta_i = \sum_{j=0}^{q-1} c_{i,j} \eta_j \quad (0 \leq i \leq q-1).
\]

In particular, $\eta_0$ is an eigenvalue of $C$ and $P(x) := \det(xI_q - C) \in \mathbb{Q}[x]$ is a monic polynomial of degree $q$ such that $P(\eta_0) = 0$, i.e., $P(x)$ is the minimal polynomial of the $\eta_k$‘s. Note that (by (17) and (16)),

(18) \[
\eta_k \eta_{i+k} = \sigma_{k^*, \Delta}(\eta_0 \eta_k) = \sum_{j=0}^{q-1} c_{i,j} \eta_{j+k} \quad (i,k \in \mathbb{Z}).
\]

Remark 18. Let us point out that if $\chi$ is the character of order $q = 6$ and conductor $\Delta = 9$ defined by $\chi(2) = \zeta_6$, then $\tau(\chi^3) = \sum_{a=1}^{9} (\frac{a}{9}) \zeta_6^a = \zeta_9 - \zeta_9^2 + \zeta_9^4 - \zeta_9^5 + \zeta_9^7 - \zeta_9^8 = 0$. Hence, the $\eta_k$, $0 \leq k \leq q-1$, are not $\mathbb{Q}$-linearly independent. Indeed, we have $\eta_0 - \eta_1 - \eta_2 - \eta_3 + \eta_4 - \eta_5 = \zeta_9 - \zeta_9^2 + \zeta_9^4 - \zeta_9^5 + \zeta_9^7 - \zeta_9^8 = 0$.

We now explain how one can practically compute this matrix $C$ (see (20) and Lemma 19 below for the result). Let

(19) \[
\tau(\chi^a) := \sum_{l=1}^{\Delta} \chi^a(l) \zeta_{\Delta}^l = \sum_{k=0}^{q-1} c_{a,k} \eta_k \in K(\zeta_q)
\]
and \( J(\chi^a, \chi^b) \in \mathbb{Q}(\zeta_q) \) denote the Gauss and Jacobi sums associated with the powers of \( \chi \) (considered as not necessarily primitive characters modulo \( \Delta \)). Set

\[
J_{a,b} := \frac{\tau(\chi^a)\tau(\chi^b)}{\tau(\chi^{a+b})}
\]

\[
= \begin{cases} 
J(\chi^a, \chi^b) & \text{if } a, b \text{ and } a + b \not\equiv 0 \pmod{q}, \\
(-1)^t & \text{if } a \equiv 0 \pmod{q}, \\
(-1)^t\Delta & \text{if } a \text{ and } b \not\equiv 0 \pmod{q} \text{ but } a + b \equiv 0 \pmod{q}
\end{cases}
\]

(use Lemma 4 and [IR, Theorem 1, page 93]). We have

\[
J_{a,b}\tau(\chi^{a+b}) = \tau(\chi^a)\tau(\chi^b)
\]

\[
= \sum_{k_1=0}^{q-1} \left\{ \sum_{k_1=0}^{q-1} c_{k_1} \zeta_q^{a+b} \right\} \eta_k \quad \text{(by \((19)\) and \((18)\))}
\]

\[
= \left( \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} c_{i,j} \zeta_q^{-(a+b)j} \right) \sum_{k=0}^{q-1} \zeta_q^{(a+b)k} \eta_k \quad \text{(set } i = k_2 - k_1 \text{ and } j = k - k_1)\]

\[
= \left( \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} c_{i,j} \zeta_q^{-(a+b)j} \right) \tau(\chi^{a+b}) \quad \text{(by \((19)\)),}
\]

which implies (see also [Tha, Proposition 3])

\[
q^{-1} \sum_{i=0}^{q-1} \sum_{j=0}^{q-1} c_{i,j} \zeta_q^{-(a+b)j} = J_{a,b} \quad (0 \leq a, b \leq q - 1),
\]

for \( \tau(\chi^{a+b}) \not\equiv 0 \), from which it follows that

\[
q^2 c_{i,j} = \sum_{a=0}^{q-1} \sum_{b=0}^{q-1} \zeta_q^{-bi+(a+b)j} J_{a,b} \quad (0 \leq i, j \leq q - 1).
\]

\textbf{Lemma 19.} Assume that \( q \) is prime. Set

\[
\delta_{i,j} = \begin{cases} 
1 & \text{if } i \equiv j \pmod{q}, \\
0 & \text{if } i \not\equiv j \pmod{q}.
\end{cases}
\]

Define the coefficients \( d_{i,j} \in \mathbb{Z} \) in a unique way by means of

\[
J_{1,i} := \sum_{j=0}^{q-1} d_{i,j} \zeta_q^j \quad \text{with } \sum_{j=0}^{q-1} d_{i,j} = 0 \quad (0 \leq i \leq q - 1).
\]

For \( 0 \leq m, n \leq q - 1 \), it holds that

\[
qc_{m,n} = (-1)^t \left( \Delta \delta_{m,0} + \delta_{m,n} + \delta_{0,n} - \frac{\Delta + 1}{q} \right) + \sum_{b=1}^{\Delta} d_{b, bm-(1+b)n}.
\]

\textbf{Proof.} If \( \gcd(a, q) = 1 \), then

\[
J_{a,ab} = \sum_{k=0}^{q-1} d_{b,k} \zeta_q^{ak}
\]
(if \( b \equiv 0 \pmod{q} \), then \( J_{1,b} = (-1)^t \Delta = J_{a,ab} \), and if \( b \not\equiv 0 \pmod{q} \), then \( J_{a,ab} = J(\chi^a,\chi^{ab}) = \sigma_{a,q}(J(\chi,\chi^b)) = \sigma_{a,q}(J_{1,b}) = \sum_{k=0}^{q-1} db_{k}c_{kq}^{a} \)). Therefore, using (20), we obtain

\[
q^{a}c_{m,n} = \sum_{b=0}^{q-1} \zeta_{b}^{b(n-m)}J_{0,b} + \sum_{a=1}^{q-1} \sum_{b=0}^{q-1} \zeta_{q}^{-bm+(a+b)n}J_{a,b}
\]

\[
= (-1)^t q^{d_{m,n}} + \sum_{a=1}^{q-1} \sum_{b=0}^{q-1} \zeta_{q}^{-abm+(a+b)n}J_{a,ab} \quad \text{(for} \ J_{0,b} = (-1)^t \text{)}
\]

\[
= (-1)^t q^{d_{m,n}} + \sum_{a=1}^{q-1} \sum_{b=0}^{q-1} \sum_{k=0}^{q-1} db_{k}c_{q}^{a(k-bm+(1+b)n)}
\]

\[
= (-1)^t q^{d_{m,n}} - \sum_{b=0}^{q-1} \sum_{k=0}^{q-1} db_{k}c_{q}^{a(k-bm+(1+b)n)}
\]

and

\[
q^{c_{m,n}} = (-1)^t d_{m,n} + \sum_{b=0}^{q-1} db_{b}c_{m,-(1+b)n} \quad (0 \leq m, n \leq q - 1)
\]

(see also [Tha Formula (8)]). Finally, since

\[
d_{0,j} = (-1)^t (q^{d_{0,j}} - 1)/q
\]

(for \( \sum_{j=0}^{q-1} (-1)^t \frac{2^{k_j} - 1}{q} \zeta_{q}^{j} = (-1)^t = J_{1,0} \)) and

\[
d_{q-1,j} = (-1)^t \Delta (q^{d_{0,j}} - 1)/q
\]

(for \( \sum_{j=0}^{q-1} (-1)^t \Delta \frac{2^{k_j} - 1}{q} \zeta_{q}^{j} = (-1)^t \Delta = J_{1,q-1} \)), we obtain the desired result. \( \square \)

**Remark 20.** If \( \chi \) is even, then \( J_{1,q-1-a} = J_{1,a} \) for \( 1 \leq a \leq q - 2 \). Indeed,

\[
\frac{J(\chi,\chi^{q-1-a})}{J(\chi,\chi^{a})} = \frac{\tau(\chi)\tau(\chi^{q-1-a})}{\tau(\chi^{q-a})} = \chi(-1)\left|\frac{\tau(\chi^{1+a})}{\tau(\chi^{a})}\right|^2 = \chi(-1) = 1.
\]

**6.2. Some quintic Gauss sums.**

**Lemma 21.** Assume that \( \Delta_{m} = m^4 + 5m^3 + 15m^2 + 25m + 25 \) is square-free, write \( \Delta_{m} = \prod_{k=1}^{t} p_{k} \) where the \( p_{k} \)'s are distinct odd primes, and set

\[
\delta_{m} := (m + 1)\zeta_{5} + mc_{5}^{2} + (m + 2)c_{5}^{3} + (m + 2)c_{5}^{4} \in \mathbb{Z}[\zeta_{5}].
\]

Then \( N_{\mathbb{Q}(\zeta_{5})/\mathbb{Q}}(\delta_{m}) = \Delta_{m} \). Therefore, \( \delta_{m} = \prod_{k=1}^{t} \mathbb{P}_{k} \) for some distinct prime ideals of \( \mathbb{Z}[\zeta_{5}] \) with \( N_{\mathbb{Q}(\zeta_{5})/\mathbb{Q}}(\mathbb{P}_{k}) = p_{k} \equiv 1 \pmod{5} \). Let \( \chi_{\mathbb{P}_{k}} \) denote the quintic character on the multiplicative group \( \mathbb{Z}[\zeta_{5}]/\mathbb{P}_{k}^{*} \) by letting \( \chi_{\mathbb{P}_{k}}(\alpha) \) be the unique power of \( \zeta_{5} \) congruent to \( \alpha^{(p_{k}-1)/5} \) modulo \( \mathbb{P}_{k} \). Set \( \chi_{\delta_{m}} = \prod_{k=1}^{t} \chi_{\mathbb{P}_{k}} \). Then,

\[
\chi_{\delta_{m}}(2) = \begin{cases} \zeta_{5}^{3} & \text{if} \ m \equiv 0 \pmod{2}, \\ \zeta_{5}^{4} & \text{if} \ m \equiv 1 \pmod{2}. \end{cases}
\]
Moreover,

\[ J_{1,1} = J(\chi_{\delta_m}, \chi_{\delta_m}) = (-1)^t \left( \frac{m}{5} \right) \delta_m \sigma_{3,5}(\delta_m) \]

\[ = (-1)^t \left( \frac{m}{5} \right) \left( \frac{4m^2 + 10m + 5}{5} \delta_5 - \frac{m^2 - 5m - 5}{5} \zeta_5 \right. \]

\[ \quad \left. - \frac{m^2 - 5m - 5}{5} \zeta_5^2 - \frac{m^2 + 5m - 5}{5} \zeta_5^3 - \frac{m^2 + 10m + 20}{5} \zeta_5 \right), \]

\[ J_{1,2} = J(\chi_{\delta_m}, \chi_{\delta_m}^2) = (-1)^t \left( \frac{m}{5} \right) \delta_m \sigma_{2,5}(\delta_m) \]

\[ = (-1)^t \left( \frac{m}{5} \right) \left( \frac{4m^2 + 10m + 5}{5} \delta_5 - \frac{m^2 + 5m - 5}{5} \zeta_5 \right. \]

\[ \quad \left. - \frac{m^2 - 5m - 5}{5} \zeta_5^2 - \frac{m^2 + 10m + 20}{5} \zeta_5 \right), \]

and \( J_{1,3} = J(\chi_{\delta_m}, \chi_{\delta_m}^3) = J(\chi_{\delta_m}, \chi_{\delta_m}) = J_{1,1} \). Then (see also [Leh, Section 5] and [SW (3.4)]),

\[ \tilde{\eta}_m := -(1)^t \left( \frac{m}{5} \right) \eta_m(\chi_{\delta_m}) + \left( \frac{m}{5} \right) - m^2 \]

is a root of \( P_m(x) = x^5 + m^2 x^4 - 2(m^3 + 3m^2 + 5m + 5)x^3 + (m^4 + 5m^3 + 11m^2 + 15m + 5)x^2 + (3m^2 + 4m + 10m + 10)x + 1 \). Therefore, \( K_m = \mathbb{Q}(\eta_m(\chi_{\delta_m})) \) is a simplest quintic field of conductor \( \Delta_m \), and \( \chi_{\delta_m} \) is one of the four conjugate characters associated with the simplest quintic field \( K_m \).

Proof. Using Eisenstein’s reciprocity law (see [IR Th. 1 page 207]), we have

\[ \chi_{\delta_m}(2) = \left( \frac{2}{\delta_m} \right) = \left( \frac{\delta_m}{2} \right) = \delta_m(2^{1-1/5}) = \delta_m^3 \quad (\text{mod } 2). \]

Since \( \delta_m^3 \equiv \zeta_5^3 \quad (\text{mod } 2) \) if \( m \equiv 0 \quad (\text{mod } 2) \) and \( \delta_m^3 \equiv (\zeta_5^2 + \zeta_5^3 + 1)^3 \equiv (-1 - \zeta_5^3) \equiv 1 + \zeta_5 + \zeta_5^2 + 1 \quad (\text{mod } 2) \) if \( m \equiv 1 \quad (\text{mod } 2) \), the desired first result follows.

According to [BEW Th. 2.1.14] and section [2] the principal ideal \( (J(\chi_{\delta_m}, \chi_{\delta_m})) \) of \( \mathbb{Z}[\zeta_5] \) is equal to the principal ideal \( (\delta_m \sigma_{3,5}(\delta_m)) \). Hence, there exists some algebraic unit \( \epsilon \in \mathbb{Z}[\zeta_5] \) such that

\[ J(\chi_{\delta_m}, \chi_{\delta_m}) = (-1)^t \left( \frac{m}{5} \right) \epsilon \delta_m \sigma_{3,5}(\delta_m). \]

Taking absolute values, we obtain \( |\epsilon| = 1 \) and \( \epsilon = \pm \zeta_5^c \) for some \( c \in \mathbb{Z} \) (see [BEW Th. 2.1.13]). Set \( \delta_5 = 1 - \zeta_5 \). Since \( \delta_m \equiv -m \quad (\text{mod } \lambda_5^2) \) (use \( \zeta_5^2 = (1 - \lambda_5)^t \equiv 1 - \lambda_5 \quad (\text{mod } \lambda_5^2) \)), we obtain \( \delta_m \sigma_{3,5}(\delta_m) \equiv m^2 \equiv \left( \frac{m}{5} \right) \quad (\text{mod } m^2 \equiv \left( \frac{m}{5} \right) \quad (\text{mod } 5)) \), and

\[ J(\chi_{\delta_m}, \chi_{\delta_m}) = \pm \zeta_5^c (-1)^t \left( \frac{m}{5} \right) \delta_m \sigma_{3,5}(\delta_m) \equiv \pm (-1)^t \zeta_5^c \equiv \pm (-1)^t (1 - \epsilon \lambda_5) \quad (\text{mod } \lambda_5^2). \]

Since \( J(\chi_{\delta_m}, \chi_{\delta_m}) \equiv (-1)^t \quad (\text{mod } \lambda_5^2) \) (see [BEW 2.1.11] and use Lemma [4]), we obtain that \( c = 0 \), that the sign \( \pm \) in \( \epsilon = \pm \zeta_5^c \) is a sign. The desired formula for \( J_{1,1} \) follows. Applying Remark [20] with \( a = 1 \) to \( \chi = \chi_{\delta_m} \), we have \( J_{1,2} = J_{2,2} = \sigma_{2,5}(J_{1,1}) \) and the desired formula for \( J_{1,2} \). Applying Remark [20] with \( a = 1 \) to \( \chi = \chi_{\delta_m} \), we obtain \( J_{1,3} = J_{1,1} \). Hence, by Lemma [19] \( C = (-1)^t (C_1 + \left( \frac{m}{5} \right) C_2) \).
Then, setting \( \epsilon \) (21) and \( \tau \) (Lemma 22).

\[
C_1 = \frac{1}{25} \begin{pmatrix}
4\Delta + 9 & 4\Delta - 1 & 4\Delta - 1 & 4\Delta - 1 & 4\Delta - 1 \\
-(\Delta - 4) & -(\Delta - 4) & -(\Delta + 1) & -(\Delta + 1) & -(\Delta + 1) \\
-(\Delta - 4) & -(\Delta + 1) & -(\Delta - 4) & -(\Delta + 1) & -(\Delta + 1) \\
-(\Delta - 4) & -(\Delta + 1) & -(\Delta - 4) & -(\Delta + 1) & -(\Delta + 1) \\
-(\Delta - 4) & -(\Delta + 1) & -(\Delta - 4) & -(\Delta + 1) & -(\Delta - 4)
\end{pmatrix}
\]

and

\[
C_2 = \frac{1}{25} \begin{pmatrix}
12m^2 + 30m + 15 & -3m^2 - 5m - 15 & -3m^2 - 5m - 15 & -3m^2 + 20m + 10 & -3m^2 + 20m + 35 \\
-3m^2 - 5m - 15 & 2m^2 + 5m + 15 & 2m^2 + 5m + 15 & 2m^2 + 5m - 10 & 2m^2 + 5m + 35 \\
-3m^2 - 5m - 15 & 2m^2 + 5m + 15 & 2m^2 + 5m + 15 & 2m^2 + 5m - 10 & 2m^2 + 5m + 35 \\
-3m^2 + 20m + 10 & 2m^2 + 5m + 35 & 2m^2 + 5m - 10 & 2m^2 + 5m - 10 & 2m^2 + 5m - 10 \\
-3m^2 + 20m + 10 & 2m^2 + 5m + 35 & 2m^2 + 5m - 10 & 2m^2 + 5m - 10 & 2m^2 + 5m - 10
\end{pmatrix}
\]

Putting everything together, we obtain:

\[
\det \left( x + \frac{m^2}{5} \right) I_5 + \left( \frac{m}{5} \right) C_1 + C_2 = P_m(x).
\]

The proof of the lemma is complete. □

**Lemma 22.** Let \( \chi \) be a primitive quintic Dirichlet character modulo \( f = \prod_{i=1}^{r} p_i \), a product of \( r \geq 1 \) distinct primes equal to 1 modulo 5. Then,

\[
\omega(\chi) := (\tau(\chi))^5 = f \cdot (J(\chi, \chi))^2 \cdot J(\chi^2, \chi^2).
\]

**Proof.** According to Lemma 14 we may assume that \( f = p \equiv 1 \pmod{5} \) is prime. Then, \( \omega(\chi) = pJ(\chi, \chi)J(\chi, \chi^2)J(\chi, \chi^3) \) (see [IR, Proposition 8.3.3] and use \( \chi(-1) = 1 \) for quintic characters) and \( J(\chi, \chi^2)J(\chi, \chi^3) = J(\chi, \chi)J(\chi^2, \chi^2) \) (use [IR, Theorem 1(d), page 93]). The desired result follows. □

Putting everything together, we obtain:

**Theorem 23.** Assume that \( \Delta_m = n^4 + 5m^3 + 15m^2 + 25m + 25 \) is square-free. Choose the quintic character \( \chi_{K_m} \) associated with the simplest quintic field \( K_m \) such that

\[
(21) \quad \chi_{K_m}(2) = \begin{cases} 
\zeta_5^3 & \text{if } m \equiv 0 \pmod{2}, \\
\zeta_5 & \text{if } m \equiv 1 \pmod{2}.
\end{cases}
\]

Then, \( \chi_{K_m} = \chi_5 \) and \( \omega(\chi_{K_m}) := (\tau(\chi_{K_m}))^5 = -\mu(\Delta_m)\left(\frac{m}{5}\right)\Delta_m \Omega_m \), where

\[
\Omega_m = (m^6 + 5m^5 + 5m^4 + 25m^3 + 125m + 125)\zeta_5
\]
\[
+ (m^6 + 5m^5 - 5m^4 - 75m^3 - 175m^2 - 125m)\zeta_5^2
\]
\[
+ (m^6 + 10m^5 + 25m^4 - 100m^2 - 125m)\zeta_5^3
\]
\[
+ (m^6 + 10m^5 + 40m^4 + 75m^3 + 50m^2)\zeta_5^4 \in \mathbb{Z}[\zeta_5].
\]

Hence, setting \( \epsilon_m := (1 + \mu(\Delta_m)\left(\frac{m}{5}\right))/2 \in \{0, 1\} \) and assuming that \( |m| \geq 6 \), there exists \( k_m \in \{0, 1, 2, 3, 4\} \) such that

\[
(22) \quad \arg(W(\chi_{K_m})) = \frac{1}{5} \arg(\Omega_m) + \frac{2k_m + \epsilon_m}{5} \pi \pmod{2\pi}.
\]
Table 3. Simplest quintic fields $K_m$ of prime conductors $\Delta_m < 2 \cdot 10^{10}$

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\Delta_m$</th>
<th>$h_{K_m}$</th>
<th>$m$</th>
<th>$\Delta_m$</th>
<th>$h_{K_m}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>641491</td>
<td>1566401</td>
<td>−237</td>
<td>3089232931</td>
<td>1634411025661</td>
</tr>
<tr>
<td>−61</td>
<td>12765251</td>
<td>66431941</td>
<td>238</td>
<td>3276804731</td>
<td>71 · 46688410201</td>
</tr>
<tr>
<td>66</td>
<td>20479231</td>
<td>61 · 2988151</td>
<td>242</td>
<td>3501489071</td>
<td>2^4 · 299565631061</td>
</tr>
<tr>
<td>73</td>
<td>30425111</td>
<td>11 · 30494041</td>
<td>−249</td>
<td>3767856571</td>
<td>11 · 204883296461</td>
</tr>
<tr>
<td>77</td>
<td>37526591</td>
<td>3233114891</td>
<td>−263</td>
<td>4694424311</td>
<td>11 · 887549864351</td>
</tr>
<tr>
<td>−84</td>
<td>46927381</td>
<td>2068985771</td>
<td>−264</td>
<td>4766572561</td>
<td>11^2 · 2860886261</td>
</tr>
<tr>
<td>−88</td>
<td>56676161</td>
<td>5912208301</td>
<td>268</td>
<td>5256015221</td>
<td>151 · 28085651441</td>
</tr>
<tr>
<td>−99</td>
<td>91352671</td>
<td>3144379001</td>
<td>271</td>
<td>5494201451</td>
<td>6532834598131</td>
</tr>
<tr>
<td>−102</td>
<td>103090711</td>
<td>3626779141</td>
<td>282</td>
<td>6437395351</td>
<td>11 · 1650567867511</td>
</tr>
<tr>
<td>−121</td>
<td>205717691</td>
<td>11420513591</td>
<td>291</td>
<td>7295360131</td>
<td>598840776019</td>
</tr>
<tr>
<td>122</td>
<td>230839031</td>
<td>11 · 5490034301</td>
<td>293</td>
<td>7497114671</td>
<td>11^2 · 88831947341</td>
</tr>
<tr>
<td>128</td>
<td>279170201</td>
<td>24178878281</td>
<td>−303</td>
<td>8291171431</td>
<td>2311 · 11223836111</td>
</tr>
<tr>
<td>129</td>
<td>287909191</td>
<td>32215474121</td>
<td>−312</td>
<td>9325450081</td>
<td>41 · 383458503551</td>
</tr>
<tr>
<td>139</td>
<td>387022451</td>
<td>11 · 3871903571</td>
<td>319</td>
<td>10519144331</td>
<td>13957149210871</td>
</tr>
<tr>
<td>−147</td>
<td>451386751</td>
<td>2^4 · 9707049091</td>
<td>−333</td>
<td>12113395171</td>
<td>151 · 358454263301</td>
</tr>
<tr>
<td>−163</td>
<td>684652511</td>
<td>41 · 19155428231</td>
<td>−339</td>
<td>13013760511</td>
<td>11 · 4393967408821</td>
</tr>
<tr>
<td>162</td>
<td>710402911</td>
<td>2^4 · 26333557751</td>
<td>−362</td>
<td>16937296931</td>
<td>32280558127001</td>
</tr>
<tr>
<td>178</td>
<td>1032554351</td>
<td>320881508831</td>
<td>−363</td>
<td>1725876111</td>
<td>12513395556911</td>
</tr>
<tr>
<td>−187</td>
<td>1190654831</td>
<td>11 · 23562499501</td>
<td>363</td>
<td>17604215731</td>
<td>3^4 · 573154162571</td>
</tr>
</tbody>
</table>

6.3. Some numerical computations. Since

$$P_m(m+1)P_m(m+2) = (m^3 + 5m^2 + 10m + 7)^2 < 0$$

we can use Newton’s method for computing efficiently numerical approximations to a root $\theta_0 \in (m+1, m+2)$ of $P_m(x)$. The four other roots are computed inductively by the transformation

$$\theta_j \mapsto \theta_{j+1} := ((m+2) + m\theta_j - \theta_j^2) / (1 + (m+2)\theta_j),$$

and we finally compute the regulator of $K_m$ by the formula

$$\text{Reg}_{K_m} = \frac{1}{5} \prod_{i=1}^{4} \left( \sum_{j=0}^{4} \zeta_5^{ij} \log |\theta_j| \right) \sim \frac{71}{256} \log^4 \Delta_m$$

(see [SW] Page 550) for the asymptotic) and

$$h_{K_m} = |L'(0, X_{K_m})|^2 |L'(0, X_{K_m}^2)|^2 / \text{Reg}_{K_m} \gg \Delta_m^2 / \log^8 \Delta_m,$$

by [Lou]. We used our efficient method to compute the class numbers of all the simplest quintic fields $K_m$’s with $\Delta_m = m^4 + 5m^3 + 15m^2 + 25m + 25 \leq 2 \cdot 10^{10}$ a prime (see Table 3). In that situation, $h_{K_m}$ divides the class number of the real cyclotomic field $Q^+(\zeta_{\Delta_m})$ (see [CWi] Lemma 2). We list below the least values of $\Delta_m$ for which some prime $q \geq \Delta_m$ (in boldface letters) divides $h_{K_m}$.

7. ACKNOWLEDGMENT

All our class number computations were carried out on a personal microcomputer by using Professor Y. Kida’s UBASIC language which allows fast arbitrary precision calculation on PCs.
References


Institut de Mathématiques de Luminy, UMR 6206, 163, avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France

E-mail address: loubouti@iml.univ-mrs.fr