MATHEMATICS OF COMPUTATION
Volume 76, Number 257, January 2007, Pages 455–473
S 0025-5718(06)01888-6
Article electronically published on September 11, 2006

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

STÉPHANE R. LOUBOUTIN

Dedicated to Danièle B.

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 $P_m(x) = x^3 - mx^2 - (m+3)x + 1$ and $P_m(x) = x^4 - mx^3 - 6x^2 + mx + 1$. 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 $\mathbf{Q}(\zeta_p)^+$ 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 [Wa1], 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 $\mathbf{Q}(\zeta_p)^+$ of the cyclotomic fields $\mathbf{Q}(\zeta_p)$ of prime conductors p (see [CW, Lemma 2]). However, in accordance

Received by the editor July 8, 2005 and, in revised form, October 14, 2005.
2000 *Mathematics Subject Classification.* Primary 11R16, 11R20, 11R29, 11R42, 11Y40.
Key words and phrases. Real abelian number field, class number, Gauss sums, simplest cubic field, simplest quartic field, simplest quintic field, simplest sextic field.

with Vandiver's conjecture, we found no example of p for which p divides one of these class numbers h_{K_m}.

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 Reg_K be the class number and regulator of K. We have (see [Lan, Chapter XIII] and [Lou4, Section 2]):

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

We let χ_K be any generator of X_K and let σ be a generator of the cyclic Galois group $\mathrm{Gal}(K/\mathbf{Q})$. We developed in [Lou3, Section 4.2], [Lou4, Section 2] and [Lou6, Section 3.3] an efficient method for constructing a generator χ_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 $f_K = \prod_{i=1}^{t} p_i$ is a product of distinct odd primes $p_i \equiv 1 \pmod{q}$ and (ii) that $\chi_K = \prod_{i=1}^{t} \chi_{p_i}$, where each χ_{p_i} is a character of order q modulo p_i. Then, for efficiently computing h_K (when 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 χ be a primitive even Dirichlet character of conductor $f_\chi > 1$ and order $q_\chi > 1$. Set

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

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

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

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

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 $h_K(N) = \frac{1}{\mathrm{Reg}_K} \prod_{1 \neq \chi \in X_K} L'_N(0,\chi)$, 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 numbers fields K of degree q. Then, as $f_K \longrightarrow \infty$ and for*

$$N \geq B(t, f_K, M) := \sqrt{\frac{t f_K}{\pi} \log(M f_K)}, \tag{3}$$

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 [BE82]). 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

problem by using the formula $h_K = |L'(0,\chi_K)|^2/\mathrm{Reg}_K$, by (1), to compute three good enough numerical approximations $|L'_N(0,\chi_K)|^2/\mathrm{Reg}_K$ 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

$$\theta(x,\chi) = \sum_{n\geq 1} \chi(n) e^{-\pi n^2 x/f_\chi} = \frac{W(\chi)}{\sqrt{x}}\theta(\frac{1}{x},\bar{\chi}) \qquad (x>0).$$

Hence, $W(\chi) = \theta(1,\chi)/\overline{\theta(1,\chi)}$, 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, $N\geq B(t,f_\chi,M)$ (see (3)) implies

$$|\theta(1,\chi)-\theta_N(1,\chi)| < \frac{1}{2M^t\sqrt{\pi t}}\frac{f_\chi^{\frac{1}{2}-t}}{\sqrt{\log(Mf_\chi)}}. \tag{4}$$

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 $\theta_N(1,\chi^l)$ to the $\theta(1,\chi^l)$'s for $1\leq l\leq q_\chi$ and $\gcd(l,q_\chi)=1$, provided that $\theta(1,\chi^l)\neq 0$ for $l\leq q_\chi$ and $\gcd(l,q_\chi)=1$. Here, we will simplify the numerical computation of class numbers of simplest fields K by obtaining beforehand explicit formulae 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 8, 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 χ be a primitive, even Dirichlet character of conductor f_χ and order $q>1$ Assume that $\omega(\chi)$ is known and that N is such that $\theta_N(1,\chi)\neq 0$ and $|\theta(1,\chi)-\theta_N(1,\chi)|\leq \epsilon|\theta_N(1,\chi)|/q$ (use (4) to find such a N). Fix W_0 a qth square root of $\omega(\chi)/f_\chi^{q/2}$. Then, $W(\chi)=\zeta_\chi^{k_0}W_0$, where k_0 is the unique integer $k\in\{0,1,\cdots,n-1\}$ such that $|W_N(\chi)-\zeta_\chi^k W_0|<2\epsilon/q$, where $W_N(\chi):=\theta_N(1,\chi)/\overline{\theta_N(1,\chi)}$.*

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], [Sha], [SW] and [SWW].

2. Prerequisites on Gauss sums

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

Lemma 4. *Let $\chi_1,\cdots,\chi_t$ be $t\geq 1$ Dirichlet characters modulo $f_1,\cdots,f_t$. 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 $\chi=\prod_{i=1}^t\chi$, which is therefore a Dirichlet character modulo f of order $q>1$. Then,*

$$\tau(\chi):=\sum_{k=1}^{f}\chi(k)e^{2\pi ik/f}=\epsilon_\chi\prod_{i=1}^{t}\tau(\chi_i) \quad \textit{where } \epsilon_\chi=\prod_{i=1}^{t}\chi_i(f/f_i)$$

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 χ are of the same order q, then

$$\omega(\chi) := (\tau(\chi))^q = \prod_{i=1}^{t} \omega(\chi_i).$$

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

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

Now, let χ be a primitive Dirichlet chraracter of order $q > 1$ and conductor $\Delta > 1$. Let M_χ be the cyclic subfield of $\mathbf{Q}(\zeta_\Delta)$ of conductor Δ associated with χ, i.e., $\mathrm{Gal}(\mathbf{Q}(\zeta_\Delta)/M_\chi) = \ker\chi$. Set

$$\eta(\chi) := \mathrm{Tr}_{\mathbf{Q}(\zeta_\Delta)/M_\chi}(\zeta_\Delta) = \sum_{t\in\ker\chi} \zeta_\Delta^t \in M_\chi. \tag{5}$$

Consider all the characters χ^k, $0 \le k \le q-1$, as defined modulo Δ. Then,

$$\sum_{k=0}^{q-1} \tau(\chi^k) = \sum_{k=0}^{q-1}\sum_{t=1}^{\Delta} \chi^k(a)\zeta_\Delta^t = \sum_{t=1}^{\Delta}\Big(\sum_{k=0}^{q-1}\chi^k(a)\Big)\zeta_\Delta^t = q\sum_{t\in\ker\chi}\zeta_\Delta^t = q\eta(\chi). \tag{6}$$

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

3. Simplest cubic fields

Set $\zeta_3 = (-1+i\sqrt{3})/2$. The units in $\mathbf{Z}[\zeta_3]$ are $\{\pm1, \pm\zeta_3, \pm\zeta_3^2\}$. An algebraic integer $\alpha = a + b\zeta_3 \in \mathbf{Z}[\zeta_3]$ is *primary* if $\alpha \equiv -1 \pmod{3\mathbf{Z}[\zeta_3]}$, i.e., if $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$. The order of the multiplicative group $(\mathbf{Z}[\zeta_3]/3\mathbf{Z}[\zeta_3])^*$ is equal to 6, and the six units in $\mathbf{Z}[\zeta_3]$ 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 $\alpha \in \mathbf{Z}[\zeta_3]$, then exactly one of the six associates of α is primary.

Lemma 6. *Let $0 \ne \alpha \in \mathbf{Z}[\zeta_3]$ be a nonunit element. Assume that $\alpha \equiv (-1)^t \pmod{3\mathbf{Z}[\zeta_3]}$, where t is the number of irreducible factors of α (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 π_k.*

Proof. For the existence, write $\alpha = u\prod_{k=1}^t \pi_k$ for some unit $u \in \{\pm1, \pm\zeta_3, \pm\zeta_3^2\}$ and some primary irreducibles $\pi_k \equiv -1 \pmod{3\mathbf{Z}[\zeta_3]}$. Since $(-1)^t \equiv \alpha \equiv (-1)^t u \pmod{3\mathbf{Z}[\zeta_3]}$, we obtain $u \equiv 1 \pmod{3\mathbf{Z}[\zeta_3]}$ and $u = 1$. □

Lemma 7 (See [IR, Corollary, page 115])**.** *Let $\pi \equiv -1 \pmod{3\mathbf{Z}[\zeta_3]}$ be a primary irreducible element in $\mathbf{Z}[\zeta_3]$ of norm a rational prime $p \equiv 1 \pmod 3$. For $\alpha \in \mathbf{Z}[\zeta_3]$ coprime with π, 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, δ_m can be written in a unique way as a product $\delta_m = \prod_{k=1}^{t}\pi_k$ of t primary irreducibles elements $\pi_k \in \mathbf{Z}[\zeta_3]$ with $p_k = |\pi_k|^2$. Set $\chi_{\delta_m} = \prod_{k=1}^{t}\chi_{\pi_k}$. Then, χ_{δ_m} is a primitive cubic character modulo Δ_m,

$$\chi_{\delta_m}(2) = \begin{cases} \zeta_3^2 & \text{if } m \equiv 0 \pmod 2, \\ \zeta_3 & \text{if } m \equiv 1 \pmod 2, \end{cases} \tag{7}$$

and

$$\omega(\chi_{\delta_m}) := \tau(\chi_{\delta_m})^3 = \Delta_m\delta_m = \mu(\Delta_m)\left(\frac{m}{3}\right)\frac{2m+3+3i\sqrt{3}}{2}\Delta_m. \tag{8}$$

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

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

(see (5)) is a root of $P_m(x) = x^3-mx^2-(m+3)x-1$. Therefore, $K_m = \mathbf{Q}(\eta(\chi_{\delta_m}))$ is a simplest cubic field of conductor Δ_m and χ_{δ_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

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

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

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

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

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

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

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

and

$$h_{K_m} = |L'(0,\chi_{K_m})|^2/\mathrm{Reg}_{K_m} \geq \Delta_m/(e\log^3\Delta_m).$$

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 $L_m = \mathbf{Q}(\sqrt{\Delta_m})$ and K_m) divides the class number of the

TABLE 1. Least primes $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ with $h_{L_m}h_{K_m} \geq \Delta_m$

m	Δ_m	$\lvert\theta(1,\chi_{K_m})\rvert$	$\frac{2\kappa_m+\epsilon_m}{3}\pi$	h_{L_m}	h_{K_m}	$h_{L_m}h_{K_m}/\Delta_m$
102496	10505737513	$20.268\cdots$	$\pi/3$	891	13152913	$1.115\cdots$
106253	11290018777	$34.364\cdots$	0	2685	6209212	$1.476\cdots$
319760	102247416889	$202.162\cdots$	0	1887	57772549	$1.066\cdots$
554869	307881271777	$88.861\cdots$	$\pi/3$	7983	93739324	$2.430\cdots$
726845	528305834569	$20.938\cdots$	0	13533	176702419	$4.526\cdots$
791021	625716595513	$129.812\cdots$	0	1737	445142272	$1.235\cdots$
796616	634599441313	$357.252\cdots$	0	1155	696739264	$1.268\cdots$
839401	704596557013	$293.373\cdots$	π	1575	554491633	$1.239\cdots$
906437	821630754289	$93.697\cdots$	0	1955	469911916	$1.118\cdots$
1066285	1136966900089	$140.662\cdots$	$\pi/3$	5389	473034223	$2.242\cdots$

real cyclotomic field $\mathbf{Q}^+(\zeta_{\Delta_m})$ (see [CW, Lemma 1]). We list below the least ten m's for which $h_{L_m}h_{K_m} > \Delta_m$.

4. Simplest sextic fields

Using simplest cubic fields we obtain only a few examples of real cyclotomic fields $\mathbf{Q}^+(\zeta_p)$ of prime conductor p and class number greater than or equal to p. To obtain many more examples we will use simplest sextic fields to prove that if $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ is prime and $\Delta_m > 4565$, then the class number of the real cyclotomic field $\mathbf{Q}^+(\zeta_{\Delta_m})$ is greater than or equal to Δ_m (see Remark 11 below). Assume that $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ is square-free, $m \geq 1$, and let K_m and χ_{K_m} be as in Theorem 8. Then, setting $L_m = \mathbf{Q}(\sqrt{\Delta_m})$, the compositum $N_m = L_mK_m$ is a cyclic sextic field of conductor Δ_m and $\chi_{N_m}(n) = \left(\frac{n}{\Delta_m}\right)\chi_{K_m}^2(n)$ 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 $d_m = 6^6\Delta_m^5$.

Let N be a real cyclic sextic field. Let U_N and σ 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 $U_N^* = \{\epsilon \in U_N;\ N_{N/L}(\epsilon) \in \{\pm 1\} \text{ and } N_{N/K}(\epsilon) \in \{\pm 1\}\}$ denote the so-called group of *relative units* of N. It is known that there exists some so-called *generating relative unit* $\epsilon_* \in U_N^*$ such that $\{-1, \epsilon_*, \epsilon_*^\sigma\}$ generate U_N^*, and we set

$$\mathrm{Reg}_N^* := (\log|\epsilon_*|)^2 + (\log|\epsilon_*^\sigma|)^2 - (\log|\epsilon_*|)(\log|\epsilon_*^\sigma|) > 0,$$

which does not depend on the generating relative unit. Then, $12\mathrm{Reg}_L\mathrm{Reg}_K\mathrm{Reg}_N^* = Q_N\mathrm{Reg}_N$ for some $Q_N \in \{1,3,4,12\}$ (see [Lou7, Lemma 3]). Now,

$$h_N^* := h_N/(h_Lh_K) = \frac{Q_N}{12\mathrm{Reg}_N^*}|L'(0,\chi_N)|^2 \tag{9}$$

is a positive divisor of h_N, by [CW, Lemma 1], where χ_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 $\Delta_m = m^2+3m+9 \equiv 1 \pmod{12}$ is square-free, and set $a = 4\sqrt{\Delta_m}$. Then,*

$\epsilon_* := -\rho_m(2\rho_m+1)/(\rho_m+2)$ *is a generating relative unit of the simplest sextic field* N_m*,*

$$\epsilon_* = -\sqrt{\frac{4a(a-9)}{9}}\cos\Big(\frac{1}{3}\arctan(\frac{\sqrt{27(a^2-108)}}{2a^2-27a+54})\Big)+1-\frac{a}{3},$$

and

$$\epsilon_*^\sigma = \sqrt{\frac{4a(a+9)}{9}}\cos\Big(\frac{1}{3}\arctan(\frac{\sqrt{27(a^2-108)}}{2a^2+27a+54})+\frac{\pi}{3}\Big)+1+\frac{a}{3}.$$

Theorem 10. *Assume that* $\Delta_m = m^2+3m+9 \equiv 1 \pmod{12}$ *is square-free. Then,*

$$\omega(\chi_{N_m}) := (\tau(\chi_{N_m}))^6 = (-1)^{(\Delta_m-1)/2}\left((2m+3+3i\sqrt{3})/2\right)^4\Delta_m.$$

Hence, setting $\epsilon_m := (1-(-1)^{(\Delta_m-1)/2})/2 \in \{0,1\}$*, there exists* $k_m \in \{0,1,2,3,4,5\}$ *such that*

$$\arg(W(\chi_{N_m})) \equiv \frac{1}{6}\arctan(\frac{3\sqrt{3}}{2m+3})+\frac{2k_m+\epsilon_m}{6}\pi \pmod{2\pi}. \tag{10}$$

Proof. Let χ 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. □

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

5. Simplest quartic fields

Let K be a real cyclic quartic field. Let U_K and σ 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* $\epsilon_* \in U^*_K$ such that $\{-1, \epsilon_*, \epsilon_*^\sigma\}$ generate U^*_K, and we set

$$\mathrm{Reg}^*_K := (\log|\epsilon_*|)^2 + (\log|\epsilon_*^\sigma|)^2 > 0$$

(which does not depend on the generating relative unit). Then, it holds that $2\mathrm{Reg}_L\mathrm{Reg}^*_K = Q_K\mathrm{Reg}_K$ for some $Q_K \in \{1,2\}$ (see [Lou6, Lemma 2]). Since K/L is ramified, h_L divides h_K and

$$h^*_K := h_K/h_L = \frac{Q_K}{2\mathrm{Reg}^*_K}|L'(0,\chi_K)|^2$$

is a positive divisor of h_K.

5.1. **Some quartic Gauss sums.** The units in $\mathbf{Z}[i]$ are $\{\pm 1, \pm i\}$. An algebraic integer $\alpha = a + bi \in \mathbf{Z}[i]$ is *primary* if $\alpha \equiv 1 \pmod{(1+i)^3\mathbf{Z}[i]}$, 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 $(\mathbf{Z}[i]/(1+i)^3\mathbf{Z}[i])^*$ is equal to 4 and the four units in $\mathbf{Z}[i]$ form a set of representatives of this group. Therefore, if 2 does not divide the norm $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$ of $\alpha \in \mathbf{Z}[i]$, then exactly one the four associates of α is primary. If follows that if $0 \neq \alpha \in \mathbf{Z}[i]$ is a nonunit primary element, then α 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 $a \in \mathbf{Z}$ is uniquely determined by $a \equiv (-1)^{(p-1)/4} \pmod 4$. Set $\pi = a + bi \in \mathbf{Z}[i]$ (which is primary). For $\alpha \in \mathbf{Z}[i]$ coprime with π, let $\chi_\pi(\alpha) \in \{\pm 1, \pm i\}$ be the quartic residue symbol defined by $\alpha^{(p-1)/4} \equiv \chi_\pi(\alpha) \pmod \pi$. Then, $\tau(\chi_\pi)^2 = -(-1)^{(p-1)/4}\pi\sqrt{p}$. (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 $\pi_k \in \mathbf{Z}[i]$ such that the $p_k = |\pi_k|^2 \equiv 1 \pmod 4$ are pairwise distinct primes. Set $\Delta_m = |\delta_m|^2 = \prod_{k=1}^t p_k$ and $\chi_{\delta_m} = \prod_{k=1}^t \chi_{\pi_k}$. Then, χ_{δ_m} is a primitive, quartic character modulo Δ_m, $\chi_{\delta_m}(-1) = (-1)^{(\Delta_m - 1)/4}$,*

$$\tau(\chi_{\delta_m})^2 = (-1)^{t+(\Delta_m-1)/4}\delta_m\sqrt{\Delta_m}, \tag{11}$$

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

Proof. According to Lemmas 4 and 12 and using

$$\sum_{k=1}^{t} \frac{p_k - 1}{4} \equiv \frac{\Delta_m - 1}{4} \pmod 2 \tag{12}$$

(by induction on t) and

$$\epsilon_{\chi_{\delta_m}}^2 = \Big(\prod_{i=1}^{t}\prod_{\substack{j=1\\ j\neq i}}^{t} \chi_{\pi_i}(p_j)\Big)^2 = \prod_{i=1}^{t}\prod_{\substack{j=1\\ j\neq i}}^{t} \left(\frac{p_j}{p_i}\right) = \prod_{1\leq i<j\leq t} \left(\frac{p_j}{p_i}\right)\left(\frac{p_i}{p_j}\right) = +1$$

(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,*

$$\delta_m := (-1)^{(m-1)/2}(m + 4i) \equiv 1 \pmod{4\mathbf{Z}[i]}$$

is primary, χ_{δ_m} is a primitive, even, quartic character modulo Δ_m, $\chi_{\delta_m}^2$ is a primitive quadratic character modulo Δ_m, and there exists $\epsilon_m \in \{\pm 1\}$ such that

$$\tau(\chi_{\delta_m}) = \epsilon_m i^{t+(m-1)/2}\Big(\sqrt{(\Delta_m + m\sqrt{\Delta_m})/2} + i\sqrt{(\Delta_m - m\sqrt{\Delta_m})/2}\Big). \tag{13}$$

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

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

is a root of $P_m(x) = x^4 - mx^3 - 6x^2 + mx + 1$. Therefore, $K_m = \mathbf{Q}(\eta(\chi_{\delta_m}))$ is a simplest quartic field of conductor Δ_m and χ_{δ_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

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

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

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

$$\rho_m = \big((m + \sqrt{\Delta_m})/2 + \sqrt{(\Delta_m + m\sqrt{\Delta_m})/2}\big)/2,$$
$$\sigma(\rho_m) = \big((m - \sqrt{\Delta_m})/2 + \sqrt{(\Delta_m - m\sqrt{\Delta_m})/2}\big)/2,$$
$$\mathrm{Reg}^*_{K_m} = \log^2\rho_m + \log^2\sigma(\rho_m),$$

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

$$h^*_{K_m} = h_{K_m}/h_{L_m} = \frac{Q_{K_m}}{2\mathrm{Reg}^*_{K_m}}|L'(0, \chi_{K_m})|^2 \geq \frac{2\Delta_m}{3e(\log\Delta_m + 0.35)^4}.$$

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 [Lou6, Proposition 10] for the determination of Q_{K_m} in the general case.) For the results on the class numbers, see [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, $\epsilon_{L_m}\rho_m^{1-\sigma}$ is a totally positive algebraic unit of K_m. Since the narrow class number $h^+_{K_m}$ of K_m is odd, $\epsilon_{L_m}\rho_m^{1-\sigma}$ is a square in K_m (recall that if K is totally real, then $h^+_K = (U^+_K : U^2_K)h_K$), and $Q_{K_m} = 2$ (by [Gra1, Proposition 1]). □

TABLE 2. Least primes $\Delta_m = m^2 + 16$ with $h_{K_m} \geq \Delta_m$

m	Δ_m	$\lvert\theta(1,\chi_{K_m})\rvert$	ϵ_m	h_{L_m}	$h^*_{K_m}$	h_{K_m}/Δ_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 $\chi^2_{K_m}(q) = (\frac{\Delta_m}{q}) = -1$. Then $\chi_{K_m}(q) \in \{\pm i\}$ and $\chi_{\delta_m}(q) \in \{\pm i\}$. According to the law of bi-quadratic reciprocity (see [IR, Theorem 2, page 123]), we have $\chi_{\delta_m}(q) = \chi_{\delta_m}(-q) = \chi_{-q}(\delta_m) \equiv \delta_m^{(q^2-1)/4} \pmod{q\mathbf{Z}[i]}$, 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 χ_{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 $\mathbf{Q}^+(\zeta_{\Delta_m})$ (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 $\pi_k = A_k + 2iB_k \in \mathbf{Z}[i]$ be primary of prime norms $p_k = A_k^2 + 4B_k^2 \equiv 1 \pmod 4$, $1 \leq k \leq t$. Set $\delta := \prod_{k=1}^d \pi_k = A + 2iB \in \mathbf{Z}[i]$. Then, $\chi_\delta(2) = i^{-B}$. In particular, if K_m is a simplest quartic field and χ_{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 $\chi_{\pi_k}(2) = \chi_{\pi_k}(1+i)\overline{\chi_{\bar\pi_k}(1+i)} = i^{-B_k}$ (by [IR, Exercice 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 $\chi_{K_m}(2) = i^{-\pm 2} = -1$. □

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 $\delta_m = (-1)^{(m+1)/2}(m-2i)$, which is primary, and $\chi_{\Delta_m}(n) = \big(\frac{n}{m(m+2)}\big)\chi_{\delta_m}(n)$. Then, χ_{Δ_m} is a primitive, even, quartic Dirichlet character modulo Δ_m, $\chi^2_{\Delta_m}$ is of conductor d_m, $\chi_{\Delta_m}(2) = i$, and there exists $\epsilon_m \in \{\pm 1\}$ such that*

$$\tau(\chi_{\Delta_m}) = \epsilon_m i^{t+(m^2-1)/8} \sqrt[4]{m(m+2)\Delta_m}\Big(\sqrt{\frac{\sqrt{d_m}+m}{2}} - i\sqrt{\frac{\sqrt{d_m}-m}{2}}\Big). \tag{14}$$

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

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

is a root of $P_m(x) = x^4 - m^2x^3 - (m^3 + 2m^2 + 4m + 2)x^2 - m^2x + 1$. Therefore, $K_m = \mathbf{Q}(\eta(\chi_{\Delta_m}))$ is a cyclic quartic field of conductor Δ_m, and its real quadratic

subfield is $k_m = \mathbf{Q}(\sqrt{d_m})$*, of conductor* d_m*. We may suppose that* $\chi_{K_m} = \chi_{\Delta_m}$ *and there exists* $k_m \in \{0,1\}$ *such that*

$$\arg(W(\chi_{K_m})) = -\arctan(\frac{2}{m+\sqrt{d_m}}) + (t+(m^2-1)/8)\frac{\pi}{4} + k_m\pi \pmod{2\pi}.$$

Proof. By Lemma 16, we have $\chi_{\Delta_m}(2) = \left(\frac{2}{m(m+2)}\right) i^{(-1)^{(m+1)/2}} = i$ (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

$$\tau(\chi_{\Delta_m})^2 = \epsilon(m-2i)\sqrt{m(m+2)\Delta_m}, \tag{15}$$

where

$$\epsilon = (-1)^t\Big(\frac{2}{m}\Big) = \mu(d_m)\Big(\frac{2}{m}\Big)$$

(use Section 2, Corollary 13 and $\left(\frac{m(m+2)}{m^2+4}\right) = -\left(\frac{-2}{m}\right)$), from which (14) follows. Hence χ_{Δ_m} is even and the cyclic quartic field M_m of conductor Δ_m associated with χ_{Δ_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, $\tau(\chi_{\Delta_m}^2) = \tau(1_{m(m+2)}\left(\frac{\bullet}{d_m}\right)) = \epsilon'\sqrt{d_m}$ (use Section 2), where

$$\epsilon' = \mu(m(m+2))\Big(\frac{m(m+2)}{m^2+4}\Big) = -\Big(\frac{-2}{m}\Big)\mu(m(m+2)).$$

Hence, $\eta'_m := 4\eta_m - \mu(\Delta_m) - \epsilon'\sqrt{d_m} = \tau + \bar\tau$, by Section 2. Using $\tau\bar\tau = \Delta_m$ and (15), we obtain $\eta_m'^2 = 2\Re(\tau^2) + 2\Delta_m = 2\epsilon m^2(m+2)\sqrt{d_m} + 2\Delta_m$, $\mathbf{Q}(\eta_m) = \mathbf{Q}(\eta'_m) = \mathbf{Q}\Big(\sqrt{(\Delta_m + \epsilon m\sqrt{m(m+2)\Delta_m})/2}\Big) \subseteq M_m$, and this inclusion is an equality. Finally, $\tilde\eta_m = (\eta'_m + m^2 + \epsilon(m+2)\sqrt{d_m})/4$ satisfies $((4\tilde\eta_m - m^2) - \epsilon(m+2)\sqrt{d_m})^2 = 4\eta_m'^2 = 2m(m+2)d_m + 2\epsilon m^2(m+2)\sqrt{d_m}$. Hence,

$$(4\tilde\eta_m - m^2) - (m^2-4)d_m = 8\epsilon(m+2)\sqrt{d_m}\tilde\eta_m$$

and $0 = ((4\tilde\eta_m - m^2) - (m^2-4)d_m)^2 - 64(m+2)^2 d_m\tilde\eta_m^2 = 256P_m(\tilde\eta_m)$. □

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

$$P_m(x) = x^5 + m^2x^4 - 2(m^3+3m^2+5m+5)x^3 + (m^4+5m^3+11m^2+15m+5)x^2 + (m^3+4m^2+10m+10)x + 1$$

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 Δ_m is square-free. Then, the conductor of K_m is equal to Δ_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 $\sigma_{a,f} \in \mathrm{Gal}(\mathbf{Q}(\zeta_f)/\mathbf{Q})$ be defined by $\sigma_{a,f}(\zeta_f) = \zeta_f^a$.

Fix χ *a primitive even Dirichlet character* of order $q \geq 2$ and conductor $\Delta > 1$. All the characters χ^a, $a \in \mathbf{Z}$, are considered as characters modulo Δ.

We assume (i) that Δ 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 χ^a, $1 \leq a \leq q-1$,

are primitive modulo Δ. Then, none of the Gaussian sums $\tau(\chi^a)$, $a \in \mathbf{Z}$, is equal to zero, for $|\tau(\chi^a)| = \sqrt{\Delta}$ if q does not divide a (see [Wa3, Lemma 4.8]) and $\tau(\chi^a) = \mu(\Delta) = (-1)^t$ if q divides a (by Lemma 5). Let $K \subseteq \mathbf{Q}(\zeta_\Delta)$ be the real cyclic number field of degree q and conductor Δ associated with χ (see [Wa3, Chapter 3]), i.e., $\mathrm{Gal}(\mathbf{Q}(\zeta_\Delta)/K) = \ker\chi$ as a subgroup of $(\mathbf{Z}/\Delta\mathbf{Z})^* = \mathrm{Gal}(\mathbf{Q}(\zeta_\Delta)/\mathbf{Q})$. For $k \in \mathbf{Z}$, let $k^* \in \mathbf{Z}$ coprime with Δ be such that $\chi(k^*) = \zeta_q^k$. Set

$$\eta_k := \sum_{\substack{l=1 \\ \chi(l)=\zeta_q^k}}^{\Delta} \zeta_\Delta^l \in \mathbf{Q}(\zeta_\Delta) \qquad (k \in \mathbf{Z}).$$

Then, $\eta_0 = Tr_{\mathbf{Q}(\zeta_\Delta)/K}(\zeta_\Delta) \in K$,

$$\sigma_{k^*,\Delta}(\eta_i) = \sum_{\substack{l=1 \\ \chi(l)=\zeta_q^i}}^{\Delta} \zeta_\Delta^{lk^*} = \sum_{\substack{l=1 \\ \chi(lk^*)=\zeta_q^{i+k}}}^{\Delta} \zeta_\Delta^{lk^*} = \eta_{i+k}, \tag{16}$$

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

$$C = [c_{i,j}]_{0\le i,j\le q-1} \in M_q(\mathbf{Q})$$

such that

$$\eta_0\eta_i = \sum_{j=0}^{q-1} c_{i,j}\eta_j \qquad (0 \le i \le q-1). \tag{17}$$

In particular, η_0 is an eigenvalue of C and $P(x) := \det(xI_q - C) \in \mathbf{Q}[x]$ is a monic polynomial of degree q such that $P(\eta_0) = 0$, i.e., $P(x)$ is the minimal polynomial of the η_k's. Note that (by (17) and (16)),

$$\eta_k\eta_{i+k} = \sigma_{k^*,\Delta}(\eta_0\eta_i) = \sum_{j=0}^{q-1} c_{i,j}\eta_{j+k} \qquad (i,k \in \mathbf{Z}). \tag{18}$$

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

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

$$\tau(\chi^a) := \sum_{l=1}^{\Delta} \chi^a(l)\zeta_\Delta^l = \sum_{k=0}^{q-1} \zeta_q^{ak}\eta_k \in K(\zeta_q) \tag{19}$$

and $J(\chi^a,\chi^b) \in \mathbf{Q}(\zeta_q)$ denote the Gauss and Jacobi sums associated with the powers of χ (*considered as not necessarily primitive characters modulo* Δ). Set

$$J_{a,b} := \frac{\tau(\chi^a)\tau(\chi^b)}{\tau(\chi^{a+b})} = \begin{cases} J(\chi^a,\chi^b) & \text{if } a,\ b \text{ and } a+b \not\equiv 0 \pmod q, \\ (-1)^t & \text{if } a \text{or } b \equiv 0 \pmod q, \\ (-1)^t\Delta & \text{if } a \text{ and } b \not\equiv 0 \pmod q \text{ but } a+b \equiv 0 \pmod q \end{cases}$$

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

$$\begin{aligned} J_{a,b}\tau(\chi^{a+b}) &= \tau(\chi^a)\tau(\chi^b) \\ &= \sum_{k=0}^{q-1}\Big(\sum_{k_1=0}^{q-1}\sum_{k_2=0}^{q-1} c_{k_2-k_1,k-k_1}\zeta_q^{ak_1+bk_2}\Big)\eta_k \ \text{ (by (19) and (18))} \\ &= \Big(\sum_{i=0}^{q-1}\sum_{j=0}^{q-1} c_{i,j}\zeta_q^{bi-(a+b)j}\Big)\sum_{k=0}^{q-1}\zeta_q^{(a+b)k}\eta_k \ \text{ (set } i=k_2-k_1 \text{ and } j=k-k_1) \\ &= \Big(\sum_{i=0}^{q-1}\sum_{j=0}^{q-1} c_{i,j}\zeta_q^{bi-(a+b)j}\Big)\tau(\chi^{a+b}) \ \text{ (by (19))}, \end{aligned}$$

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

$$\sum_{i=0}^{q-1}\sum_{j=0}^{q-1} c_{i,j}\zeta_q^{bi-(a+b)j} = J_{a,b} \qquad (0 \le a,b \le q-1),$$

for $\tau(\chi^{a+b}) \neq 0$, from which it follows that

$$q^2 c_{i,j} = \sum_{a=0}^{q-1}\sum_{b=0}^{q-1}\zeta_q^{-bi+(a+b)j}J_{a,b} \qquad (0 \le i,j \le q-1). \tag{20}$$

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 $d_{i,j} \in \mathbf{Z}$ in a unique way by means of

$$J_{1,i} := \sum_{j=0}^{q-1} d_{i,j}\zeta_q^j \quad \text{with} \quad \sum_{j=0}^{q-1} d_{i,j} = 0 \qquad (0 \le i \le q-1).$$

For $0 \le m,n \le q-1$, it holds that

$$qc_{m,n} = (-1)^t\Big(\Delta\delta_{m,0} + \delta_{m,n} + \delta_{0,n} - \frac{\Delta+1}{q}\Big) + \sum_{b=1}^{q-2} d_{b,bm-(1+b)n}.$$

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 $J_{a,ab} = J(\chi^a, \chi^{ab}) = \sigma_{a,q}(J(\chi, \chi^b)) = \sigma_{a,q}(J_{1,b}) = \sum_{k=0}^{q-1} d_{b,k}\zeta_q^{ak}$). Therefore, using (20), we obtain

$$\begin{aligned} q^2 c_{m,n} &= \sum_{b=0}^{q-1} \zeta_q^{b(n-m)} J_{0,b} + \sum_{a=1}^{q-1}\sum_{b=0}^{q-1} \zeta_q^{-bm+(a+b)n} J_{a,b} \\ &= (-1)^t q\delta_{m,n} + \sum_{a=1}^{q-1}\sum_{b=0}^{q-1} \zeta_q^{-abm+(a+ab)n} J_{a,ab} \quad (\text{for } J_{0,b} = (-1)^t) \\ &= (-1)^t q\delta_{m,n} + \sum_{a=1}^{q-1}\sum_{b=0}^{q-1}\sum_{k=0}^{q-1} d_{b,k}\zeta_q^{a(k-bm+(1+b)n)} \\ &= (-1)^t q\delta_{m,n} - \sum_{b=0}^{q-1}\sum_{k=0}^{q-1} d_{b,k} + \sum_{b=0}^{q-1}\sum_{k=0}^{q-1} d_{b,k}\sum_{a=0}^{q-1} \zeta_q^{a(k-bm+(1+b)n)} \end{aligned}$$

and

$$qc_{m,n} = (-1)^t\delta_{m,n} + \sum_{b=0}^{q-1} d_{b,bm-(1+b)n} \quad (0 \le m, n \le q-1)$$

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

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

(for $\sum_{j=0}^{q-1}(-1)^t\frac{q\delta_{0,j}-1}{q}\zeta_q^j = (-1)^t = J_{1,0}$) and

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

(for $\sum_{j=0}^{q-1}(-1)^t\Delta\frac{q\delta_{0,j}-1}{q}\zeta_q^j = (-1)^t\Delta = J_{1,q-1}$), we obtain the desired result. □

Remark 20. If χ is even, then $J_{1,q-1-a} = J_{1,a}$ for $1 \le a \le q-2$. Indeed,

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

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*

$$\delta_m := (m+1)\zeta_5 + m\zeta_5^2 + (m+2)\zeta_5^3 + (m+2)\zeta_5^4 \in \mathbf{Z}[\zeta_5].$$

Then $N_{\mathbf{Q}(\zeta_5)/\mathbf{Q}}(\delta_m) = \Delta_m$. Therefore, $(\delta_m) = \prod_{k=1}^t \mathcal{P}_k$ for some distinct prime ideals of $\mathbf{Z}[\zeta_5]$ with $N_{\mathbf{Q}(\zeta_5)/\mathbf{Q}}(\mathcal{P}_k) = p_k \equiv 1 \pmod 5$. Let $\chi_{\mathcal{P}_k}$ denote the quintic character on the multiplicative group $(\mathbf{Z}[\zeta_5]/\mathcal{P}_k)^*$ by letting $\chi_{\mathcal{P}_k}(\alpha)$ be the unique power of ζ_5 congruent to $\alpha^{(p_k-1)/5}$ modulo $\mathcal{P}_k$. Set $\chi_{\delta_m} = \prod_{k=1}^t \chi_{\mathcal{P}_k}$. 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,

$$\begin{aligned}J_{1,1} &= J(\chi_{\delta_m},\chi_{\delta_m}) = (-1)^t(\frac{m}{5})\delta_m\sigma_{3,5}(\delta_m)\\ &= (-1)^t(\frac{m}{5})\Big(\frac{4m^2+10m+5}{5} - \frac{m^2-5m-5}{5}\zeta_5\\ &\qquad -\frac{m^2-5}{5}\zeta_5^2 - \frac{m^2+5m-5}{5}\zeta_5^3 - \frac{m^2+10m+20}{5}\zeta_5^4\Big),\\ &\qquad\qquad \vdots\\ J_{1,2} &= J(\chi_{\delta_m},\chi_{\delta_m}^2) = (-1)^t(\frac{m}{5})\delta_m\sigma_{2,5}(\delta_m)\\ &= (-1)^t(\frac{m}{5})\Big(\frac{4m^2+10m+5}{5} - \frac{m^2+5m-5}{5}\zeta_5\\ &\qquad -\frac{m^2-5m-5}{5}\zeta_5^2 - \frac{m^2+10m+20}{5}\zeta_5^3 - \frac{m^2-5}{5}\zeta_5^4\Big),\end{aligned}$$

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)]*),*

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

is a root of $P_m(x) = x^5 + m^2x^4 - 2(m^3+3m^2+5m+5)x^3 + (m^4+5m^3+11m^2+15m+5)x^2 + (m^3+4m^2+10m+10)x + 1$. *Therefore,* $K_m = \mathbf{Q}(\eta_m(\chi_{\delta_m}))$ *is a simplest quintic field of conductor* Δ_m*, and* χ_{δ_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

$$\chi_{\delta_m}(2) = \left(\frac{2}{\delta_m}\right)_5 = \left(\frac{\delta_m}{2}\right)_5 \equiv \delta_m^{(2^4-1)/5} \equiv \delta_m^3 \pmod{(2)}.$$

Since $\delta_m^3 \equiv \zeta_5^3 \pmod{(2)}$ if $m \equiv 0 \pmod 2$ and $\delta_m^3 \equiv (\zeta_5^2+\zeta_5^3+\zeta_5^4)^3 \equiv (-1-\zeta_5)^3 \equiv 1+\zeta_5+\zeta_5^2+\zeta_5^3 \equiv \zeta_5^4 \pmod{(2)}$ if $m \equiv 1 \pmod 2$, 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 $\mathbf{Z}[\zeta_5]$ is equal to the principal ideal $(\delta_m\sigma_{3,5}(\delta_m))$. Hence, there exists some algebraic unit $\epsilon \in \mathbf{Z}[\zeta_5]$ such that

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

Taking absolute values, we obtain $|\epsilon| = 1$ and $\epsilon = \pm\zeta_5^c$ for some $c \in \mathbf{Z}$ (see [BEW, Th. 2.1.13]). Set $\lambda_5 = 1-\zeta_5$. Since $\delta_m \equiv -m \pmod{\lambda_5^2}$ (use $\zeta_5^l = (1-\lambda_5)^l \equiv 1-l\lambda_5 \pmod{\lambda_5^2}$), we obtain $\delta_m\sigma_{3,5}(\delta_m) \equiv m^2 \equiv (\frac{m}{5}) \pmod{\lambda_5^2}$ (for $m^2 \equiv (\frac{m}{5}) \pmod 5$), and

$$J(\chi_{\delta_m},\chi_{\delta_m}) = \pm\zeta_5^c(-1)^t(\frac{m}{5})\delta_m\sigma_{3,5}(\delta_m) \equiv \pm(-1)^t\zeta_5^c \equiv \pm(-1)^t(1-c\lambda_5) \pmod{\lambda_5^2}.$$

Since $J(\chi_{\delta_m},\chi_{\delta_m}) \equiv (-1)^t \pmod{\lambda_5^2}$ (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 $\chi = \chi_{\delta_m}^2$, 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, $C = (-1)^t(C_1 + (\frac{m}{5})C_2)$

with

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

and

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

It follows that $\eta(\chi_{\delta_m})$ is a root of $\det(xI_5 - C)$ and that $\tilde{\eta}_m$ is a root of

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

The proof of the lemma is complete. □

Lemma 22. *Let χ 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 4, 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 $\Delta_m = m^4 + 5m^3 + 15m^2 + 25m + 25$ is square-free. Choose the quintic character χ_{K_m} associated with the simplest quintic field K_m such that*

$$\chi_{K_m}(2) = \begin{cases} \zeta_5^3 & \text{if } m \equiv 0 \pmod 2, \\ \zeta_5^4 & \text{if } m \equiv 1 \pmod 2. \end{cases} \tag{21}$$

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

$$\begin{aligned} \Omega_m \;=\; & (m^6+5m^5+5m^4+25m^2+125m+125)\zeta_5 \\ & +(m^6+5m^5-5m^4-75m^3-175m^2-125m)\zeta_5^2 \\ & +(m^6+10m^5+25m^4-100m^2-125m)\zeta_5^3 \\ & +(m^6+10m^5+40m^4+75m^3+50m^2)\zeta_5^4 \in \mathbf{Z}[\zeta_5]. \end{aligned}$$

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

$$\arg(W(\chi_{K_m})) \equiv \frac{1}{5}\arg(\Omega_m) + \frac{2k_m+\epsilon_m}{5}\pi \pmod{2\pi}. \tag{22}$$

TABLE 3. Simplest quintic fields K_m of prime conductors $\Delta_m < 2 \cdot 10^{10}$

m	Δ_m	h_{K_m}	m	Δ_m	h_{K_m}
27	641491	**1566401**	−237	3089232931	**1634411025661**
−61	12765251	**66431941**	238	3276804731	$71 \cdot$ **46688410201**
66	20479231	$61 \cdot$ **2988151**	242	3501489071	$2^4 \cdot$ **299565631061**
73	30425111	$11 \cdot$ **30494041**	−249	3767856571	$11 \cdot$ **204883296461**
77	37526591	**3233114891**	−263	4694424311	$11 \cdot$ **887549864351**
−84	46927381	**2068985771**	−264	4766572561	$11^2 \cdot$ **2860886261**
−88	56676161	**5912208301**	268	5256015221	$151 \cdot$ **28085651441**
−99	91352671	**3144379001**	271	5494201451	**6532834598131**
−102	103090711	**3626779141**	282	6437395351	$11 \cdot$ **1650567867511**
−121	205717691	**11420513591**	291	7295360131	**5988407760191**
122	230839031	$11 \cdot$ **5490034301**	293	7497114671	$11^2 \cdot$ **88831947341**
128	279170201	**24178878281**	−303	8291171431	$2311 \cdot$ **11223836111**
129	287909191	**32215474121**	−312	9325450081	$41 \cdot$ **383458530551**
139	387022451	$11 \cdot$ **3871903571**	319	10519144331	**13957149210871**
−147	451386751	$2^4 \cdot$ **9707049091**	−333	12113395171	$151 \cdot$ **358454263301**
−163	684652511	$41 \cdot$ **19155428231**	−339	13013760511	$11 \cdot$ **4393967408821**
162	710402911	$2^4 \cdot$ **26333557751**	−362	16937296931	**32280558127001**
178	1032554351	**320881058831**	−363	17125876111	**125133985556911**
−187	1190654831	$11 \cdot$ **23562499501**	363	17604215731	$3^4 \cdot$ **573154162571**

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

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

and we finally compute the regulator of K_m by the formula

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

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

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

by [Lou1]. We used our efficient method to compute the class numbers of all the simplest quintic fields K_m's with $\Delta_m = m^4+5m^3+15m^2+25m+25 \le 2\cdot 10^{10}$ a prime (see Table 3). In that situation, h_{K_m} divides the class number of the real cyclotomic field $\mathbf{Q}^+(\zeta_{\Delta_m})$ (see [CW, Lemma 2]). We list below the least values of Δ_m for which some prime $q \ge \Delta_m$ (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

[BE71] B. C. Berndt and R. J. Evans. Sums of Jacobi, Gauss, and Jacobsthal. *J. Number Theory* **11** (1979), 349–398. MR0544263 (81j:10054)

[BE82] ———, The determination of Gauss sums. *Bull. Amer. Math. Soc.* **5** (2) (1981), 107–129. Corrigendum in **7** (2) (1982), 441. MR0621882 (82h:10051); MR0663795 (83i:10049)

[BEW] B. C. Berndt, R. J. Evans and K. S. Williams. *Gauss and Jacobi sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998. MR1625181 (99d:11092)

[Bye] D. Byeon. Class number 3 problem for the simplest cubic fields. *Proc. Amer. Math. Soc.* **128** (2000), 1319–1323. MR1664337 (2000j:11158)

[CW] G. Cornell and L. C. Washington. Class numbers of cyclotomic fields. *J. Number Theory* **21** (1985), 260–274. MR0814005 (87d:11079)

[Dav] H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, Grad. Texts Math., **74**, Third Edition, 2000. MR1790423 (2001f:11001)

[Gra1] M. N. Gras. Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de **Q**. Publ. Math. Besancon, 1977/78, fasc. 2, pp1–26&1–53.

[Gra2] ———, Special units in real cyclic sextic fields. *Math. Comp.* **48** (1988), 543–556. MR0866107 (88m:11092)

[IR] K. Ireland and M. Rosen. *A classical introduction to modern number theory. Second edition.* Graduate Texts in Mathematics, **84**, Springer-Verlag, New York, 1990. MR1070716 (92e:11001)

[Jean] S. Jeannin. Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer. J. Théor. Nombres Bordeaux **8** (1996), no. 1, 75–92. MR1399947 (97k:11154)

[Lan] S. Lang. *Algebraic Number Theory. Second edition.* Graduate Texts in Mathematics, **110**. Springer-Verlag, New York, 1994. MR1282723 (95f:11085)

[Laz1] A. J. Lazarus. Class numbers of simplest quartic fields. *Number theory (Banff, AB, 1988), 313–323, Walter de Gruyter, Berlin*, 1990. MR1106670 (92d:11119)

[Laz2] ———, On the class number and unit index of simplest quartic fields. *Nagoya Math. J.* **121** (1991), 1–13. MR1096465 (92a:11129)

[Laz3] ———, Gaussian periods and units in certain cyclic fields. *Proc. Amer. Math. Soc.* **115** (1992), 961–968. MR1093600 (92j:11118)

[Laz4] ———, The sextic period polynomial. *Bull. Austral. Math. Soc.* **49** (1994), 293–304. MR1265365 (95e:11118)

[Leh] E. Lehmer. Connection between Gaussian periods and cyclic fields. *Math. Comp.* **50** (1988), 535–541. MR0929551 (89h:11067a)

[Lon] Robert L. Long. *Algebraic Number Theory.* Monographs and Textbooks in Pure and Applied Mathematics, Vol. **41**. Marcel Decker, Inc., New York–Basel, 1977. MR0469888 (57:9668)

[Lou1] S. Louboutin. Minoration au point 1 des fonctions L et détermination des corps sextiques abéliens totalement imaginaires principaux. *Acta Arith.* **62** (1992), 109–124. MR1183984 (93h:11100)

[Lou2] ———, Computation of relative class numbers of CM-fields by using Hecke L-functions. *Math. Comp.* **69** (2000), 371–393. MR1648395 (2000i:11172)

[Lou3] ———, The exponent three class group problem for some real cyclic cubic number fields. *Proc. Amer. Math. Soc.* **130** (2002), 353–361. MR1862112 (2002h:11106)

[Lou4] ———, Efficient computation of class numbers of real abelian number fields. *Lect. Notes in Comp. Sci.* **2369** (2002), 134–147. MR2041079 (2005d:11182)

[Lou5] ———, Computation of class numbers of quadratic number fields. *Math. Comp.* **71** (2002), 1735–1743. MR1933052 (2003i:11163)

[Lou6] ———, The simplest quartic fields with ideal class groups of exponents less than or equal to 2. *J. Math. Soc. Japan* **56** (2004), 717–727. MR2071669 (2005e:11137)

[Lou7] ———, Class numbers of real cyclotomic fields. *Publ. Math. Debrecen* **64** (2004), 451–461. MR2058916 (2005b:11172)

[LP] F. Lemmermeyer and A. Pethö. Simplest cubic fields. *Manuscripta Math.* **88** (1995), 53–58. MR1348789 (96g:11131)

[Sha] D. Shanks. The simplest cubic fields. *Math. Comp.* **28** (1974), 1137–1152. MR0352049 (50:4537)

[Sta] H. M. Stark. Dirichlet's class-number formula revisited. *Contemp. Math.* **143** (1993), 571–577. MR1210543 (94a:11133)

[SW] R. Schoof and L. C. Washington. Quintic polynomials and real cyclotomic fields with large class numbers. *Math. Comp.* **50** (1988), 543–556. MR0929552 (89h:11067b)

[SWW] E. Seah, L. C. Washington and H. C. Williams. The calculation of a large cubic class number with an application to real cyclotomic fields. *Math. Comp.* **41** (1983), 303–305. MR0701641 (84m:12008)

[Tha] F. Thaine. Families of irreducible polynomials of Gaussian periods and matrices of cyclotomic numbers. *Math. Comp.* **69** (2000), 1653–1666. MR1653998 (2001a:11179)

[Wa1] L. C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.* **48** (1987), 371–384. MR0866122 (88a:11107)

[Wa2] ———, A family of cyclic quartic fields arising from modular curves. *Math. Comp.* **57** (1991), no. 196, 763–775. MR1094964 (92a:11120)

[Wa3] ———, *Introduction to Cyclotomic Fields. Second edition.* Graduate Texts in Mathematics, **83**, Springer-Verlag, 1997. MR1421575 (97h:11130)

[WB] H. C. Williams and J. Broere. A computational technique for evaluating $L(1, \chi)$ and the class number of a real quadratic field. *Math. Comp.* **30** (1976), 887-893. MR0414522 (54:2623)

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