Publ. Math. Debrecen
64/3-4 (2004), 451–461

Class numbers of real cyclotomic fields

By STÉPHANE R. LOUBOUTIN (Marseille)

Abstract. We use simplest sextic fields to produce real cyclotomic fields of class numbers greater than their conductors.

1. Introduction

In 1985, G. Cornell and L. C. Washington used simplest quartic fields (associated with the quartic polynomials $P_m(x) = x^4 - mx^3 - 6x^2 + mx + 1$) to prove that for infinitely many composite n the class number h_n^+ of the maximal real subfield of the cyclotomic field of conductor n satisfies $h_n^+ > n^{3/2-\epsilon}$. Due to the use of the Brauer–Siegel theorem, their lower bound is ineffective. Here, by using simplest sextic fields (associated with the sextic polynomials $P_m(x) = x^6 - 2mx^5 - 5(m+3)x^4 - 20x^3 + 5mx^2 + 2(m+3)x + 1$) we prove that for at least $\gg x^{1/2}$ of the not necessarily composite $n \leq x$ the class numbers h_n^+ of the maximal real subfield of the cyclotomic field of conductor n satisfies $h_n^+ > n^{2-\epsilon}$. Our lower bound being effective and explicit, we can prove that if $n = m^2 + 3m + 9 \equiv 1 \pmod 4$ is square-free (but not necessarily composite), then $h_n^+ > n$ for $m > 24 \cdot 10^6$ (see [Lou5] and the references therein for even more convincing arguments according to which Vandiver's conjecture (i.e., that p never divides h_p^+ for p a prime) is non trivial). More precisely, we will prove:

Mathematics Subject Classification: Primary: 11R18, 11R20, 11R29, 11R42.
Key words and phrases: cyclotomic field, class number, simplest sextic field.

Theorem 1. *Assume that* $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ *is square-free* ($m \geq -1$). *Let* t_m *denote its number of distinct prime factors. Then, the class number of the maximal real subfield* $\mathbf{Q}(\zeta_{\Delta_m})^+$ *of the cyclotomic field of conductor* Δ_m *satisfies*

$$h_{\mathbf{Q}(\zeta_{\Delta_m})^+} \geq \frac{1}{5e}\frac{\Delta_m^2}{3^{t_m}\log^6(4\Delta_m)}. \tag{1}$$

In particular, it holds that $h_{\mathbf{Q}(\zeta_{\Delta_m})^+} > \Delta_m$ *for* $m \geq 24\cdot 10^6$.

2. Simplest cubic fields

In [Bye], [Lou4], [LP], [Sha] and [Wa], various authors dealt with the so called *simplest cubic fields*, the real cyclic cubic number fields associated with the $\mathbf{Q}$-irreducible cubic polynomials

$$P_m(x) = x^3 - mx^2 - (m+3)x - 1$$

of discriminants

$$d_m = \Delta_m^2 \quad \text{where} \quad \Delta_m = m^2+3m+9.$$

$P_m(x)$ has three distinct real roots ϕ_m, ϕ'_m and ϕ''_m that satisfy $\phi''_m < -1 < \phi'_m < 0 < \phi_m$, we have $\phi'_m = \sigma(\phi_m) = -1/(\phi_m+1)$, $\phi''_m = \sigma^2(\phi_m) = -(\phi_m+1)/\phi_m$ and $P_m(x)$ defines a real cyclic cubic field $K_m = \mathbf{Q}(\phi_m)$ and σ is a generator of its Galois group $\mathrm{Gal}(K_m/\mathbf{Q})$. We have

$$\begin{aligned}\phi_m &= \frac{1}{3}\left(2\sqrt{\Delta_m}\cos\left(\frac{1}{3}\arctan\left(\frac{\sqrt{27}}{2m+3}\right)\right)+m\right)\\ &= \sqrt{\Delta_m}-\frac{1}{2}+O\left(\frac{1}{\sqrt{\Delta_m}}\right)\end{aligned} \tag{2}$$

(for the formula, see the proof of Lemma 7, for the asymptotic expansion then use $m = (\sqrt{4\Delta_m - 27}-3)/2$). Since $-x^3P_m(1/x) = P_{-m-3}(x)$, we may assume that $m \geq -1$. Moreover, we will assume that the conductor of K_m is equal to Δ_m, which amounts to asking that (i) $m \not\equiv 0 \pmod 3$ and

Δ_m is squarefree, or (ii) $m \equiv 0,\ 6 \pmod 9$ and $\Delta_m/9$ is squarefree (see [Wa, Proposition 1 and Corollary]). In that situation, $\{-1,\ \phi_m,\ \sigma(\phi_m) = -1/(\phi_m+1)\}$ generate the full group of algebraic units of K_m, the regulator of K_m is

$$\mathrm{Reg}_{K_m} = \log^2 \phi_m - (\log \phi_m)(\log(1+\phi_m)) + \log^2(1+\phi_m), \tag{3}$$

which in using (2) yields

$$\mathrm{Reg}_{K_m} = \frac{1}{4}\log^2 \Delta_m - \frac{\log \Delta_m}{\sqrt{\Delta_m}} + O\left(\frac{\log \Delta_m}{\Delta_m}\right)$$

and proves that

$$\mathrm{Reg}_{K_m} \leq \frac{1}{4}\log^2 \Delta_m \tag{4}$$

for m large enough. By checking numerically that this bound is valid for the remaining m, we obtain that (4) is valid for all $m \geq -1$. Since the regulators of these K_m are small, they should have large class numbers (by Siegel–Brauer's theorem). In fact, we proved (see [Lou4, (12)]):

$$h_{K_m} \geq \frac{\Delta_m}{e \log^3 \Delta_m} \tag{5}$$

(where $e = \exp(1) = 2.71828\ldots$). From now on, to further simplify, we assume that $\Delta_m = m^2+3m+9$ is squarefree. To begin with, we note that there are infinitely many simplest cubic (and sextic) fields:

Proposition 2. *Set*

$$c = \frac{1}{3}\prod_{p\equiv 1 \pmod 3}\left(1-\frac{2}{p^2}\right) = 0.311\ldots$$

Then, $\#\{1 \leq m \leq x;\ m^2+3m+9$ *is squarefree*$\}$ *is asymptotic to* $2cx$, *and* $\#\{1 \leq m \leq x;\ m^2+3m+9 \equiv 1 \pmod 4$ *is squarefree*$\}$ *is asymptotic to* cx.

3. Simplest sextic fields

In [Gra2] M. N. Gras dealt with the so called *simplest sextic fields*, the real cyclic sextic number fields K_m associated with the sextic polynomials

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

(set $m = (t-6)/4$ in [Gra2, (8)]) of discriminants

$$d_m = 6^6\Delta_m^5 \quad \text{where} \quad \Delta_m = m^2+3m+9 \geq 7$$

and roots $\theta_1 = \theta$, $\theta_2 = \sigma(\theta) = (\theta-1)/(\theta+2)$, $\theta_3 = \sigma^2(\theta) = -1/(\theta+1)$ $\theta_4 = \sigma^3(\theta) = -(\theta+2)/(2\theta+1)$, $\theta_5 = \sigma^4(\theta) = -(\theta+1)/\theta$ and $\theta_6 = \sigma^5(\theta) = -(2\theta+1)/(\theta-1)$. Since $x^6P_m(1/x) = P_{-m-3}(x)$, we may assume that $m \geq -1$. Since $P_m(1) = -27 < 0$, $P_m(x)$ has at least one root $\theta > 1$ and, according to the previous formula, for this root θ we have $-2 < \theta_5 < -1 < \theta_4 < -1/2 < \theta_3 < 0 < \theta_2 < 1 < \theta_1$. Hence, $P_m(x)$ has only one root $\rho_m > 1$. Moreover, it is easily seen that

$$\rho_m = 2\sqrt{\Delta_m} - \frac{1}{2} - \frac{19}{8\sqrt{\Delta_m}} + O\left(\frac{1}{\Delta_m}\right). \tag{6}$$

The real quadratic subfield of K_m is $k_2 = \mathbf{Q}(\sqrt{d_m}\,) = \mathbf{Q}(\sqrt{\Delta_m}\,)$. Since $\phi = 1/\theta^{1+\sigma^3} = -(2\theta+1)/(\theta(\theta+2))$ is a root of $x^3 - mx^2 - (m+3)x - 1$, the real cubic subfield of K_m is $k_3 = \mathbf{Q}(\phi)$, and k_3 is a simplest cubic field. From now on, we assume that $m \geq -1$ is such that $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ is squarefree (hence, we must have $m \equiv 0,\ 1 \pmod 4$). In that case, the conductors of k_2, k_3 and K_m are equal to Δ_m.

3.1. Real cyclic sextic fields. Let K be a real cyclic sextic field. Let f_K, h_K, U_K and σ be its conductor, class number, group of algebraic units and a generator of its Galois group. Let k_2 and k_3 denote its real quadratic and real cyclic cubic subfields. Let f_i, h_{k_i} and U_{k_i} denote their conductors, class numbers and unit groups. Moreover, let $\epsilon_2 > 1$ be the fundamental unit of k_2, and let ϵ_3 and ϵ_3' be any algebraic units of k_3 such that $\{-1, \epsilon_3, \epsilon_3'\}$ generate the full group of algebraic units of k_3. Finally, let $U_K^* = \{\epsilon \in U_K;\ N_{K/k_2}(\epsilon) \in \{\pm 1\} \text{ and } N_{K/k_3}(\epsilon) \in \{\pm 1\}\}$ denote the group of so-called *relative units* of K. If $\pm 1 \neq \epsilon \in U_K^*$, then $\epsilon^\sigma \in U_K^*$ and

$$\operatorname{Reg}(\epsilon_2, \epsilon_3, \epsilon_3', \epsilon, \epsilon^\sigma) = 12 \operatorname{Reg}_{k_2} \operatorname{Reg}_{k_3} \operatorname{Reg}_\epsilon^*$$

where

$$\operatorname{Reg}_\epsilon^* := (\log|\epsilon|)^2 + (\log|\epsilon^\sigma|)^2 - (\log|\epsilon|)(\log|\epsilon^\sigma|) > 0.$$

It is known that there exists some so-called *generating relative unit* $\epsilon_* \in U_K^*$ such that $\{-1, \epsilon_*, \epsilon_*^\sigma\}$ generate U_K^*, and we set

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

(which does not depend on the generating relative unit). With the previous notation, we have:

Lemma 3. *It holds that*

$$\mathrm{Reg}(\epsilon_2, \epsilon_3, \epsilon_3', \epsilon_*, \epsilon_*^\sigma) = 12 \,\mathrm{Reg}_{k_2} \mathrm{Reg}_{k_3} \mathrm{Reg}_K^* = Q_K \,\mathrm{Reg}_K$$

for some $Q_K \in \{1, 3, 4, 12\}$.

PROOF. Noticing (i) that $N_{K/k_2}(N_{K/k_3}(\eta)) = N_{K/k_3}(N_{K/k_2}(\eta)) = N_{K/\mathbf{Q}}(\eta) = \pm 1$ for $\eta \in U_K$, (ii) that $N_{K/k_2}(\eta_3) = N_{k_3/\mathbf{Q}}(\eta_3) = \pm 1$ and $N_{K/k_3}(\eta_3) = \eta_3^2$ for $\eta_3 \in U_{k_3}$, and (iii) that $N_{K/k_3}(\eta_2) = N_{k_2/\mathbf{Q}}(\eta_2) = \pm 1$ and $N_{K/k_2}(\eta_2) = \eta_2^3$ for $\eta_3 \in U_{k_2}$, we obtain that the kernel of

$$U_K \xrightarrow{N_{K/k_2} \times N_{K/k_3}} U_{k_2} \times U_{k_3} \longrightarrow U_{k_2}/_{U_{k_2}^3} \times U_{k_3}/_{\langle -1, U_{k_3}^2 \rangle}$$

is equal to $U_{k_2} U_{k_3} U_K^*$. Hence, the index $Q_K := (U_K : U_{k_2} U_{k_3} U_K^*)$ divides 12. $\square$

Since f_{k_2} and f_{k_3} divide f_K and $d_K = f_{k_2} f_{k_3}^2 f_K^2$ (by the conductor-discriminant formula), we cannot have $d_K = d_{k_2}^3$ $(= f_{k_2}^3)$ nor $d_K = d_{k_3}^2$ $(= f_{k_3}^4)$. Hence, K/k_3 and K/k_2 are ramified, and h_{k_2} and h_{k_3} divide h_K. In fact, we have the better following result (see [CW, Lemma 1]): the product $h_{k_2} h_{k_3}$ divides h_K. We now give explicit lower bounds for the ratio h_K / h_{k_2} (see Theorem 5).

Lemma 4.

1. *(See* [Lou3, Lemma 6]*.) Let K be a totally real sextic field. Assume that $d_K \geq 8 \cdot 10^{20}$. Then, $\zeta_K(1 - (2/\log d_K)) \leq 0$ implies*

$$\mathrm{Res}_{s=1}(\zeta_K(s)) \geq \frac{2}{e \log d_K}, \tag{7}$$

and $1 - (2/\log d_K) \leq \beta < 1$ and $\zeta_K(\beta) = 0$ imply

$$\mathrm{Res}_{s=1}(\zeta_K(s)) \geq \frac{1 - \beta}{6e}. \tag{8}$$

2. *(See* [Lou2, Corollaire 5A(a) and Corollaire 7B]*.) Let k_2 be a real quadratic field. Set $\kappa_0 = 2 + \gamma - \log(4\pi) = 0.046\ldots$, where $\gamma = 0.577\ldots$ denotes Euler's constant. Then,*

$$\mathrm{Res}_{s=1}(\zeta_{k_2}(s)) \leq \frac{1}{2}(\log f_{k_2} + \kappa_0), \tag{9}$$

and $\frac{1}{2} \leq \beta < 1$ and $\zeta_{k_2}(\beta) = 0$ imply

$$\mathrm{Res}_{s=1}(\zeta_{k_2}(s)) \leq \frac{1-\beta}{8}\log^2 f_{k_2}. \tag{10}$$

Theorem 5. *Set $\kappa_0 = 2 + \gamma - \log(4\pi) = 0.04619\ldots$ Let K be a real cyclic sextic field of conductor f_K and discriminant $d_K = f_{k_2}f_{k_3}^2f_K^2 \geq 8 \cdot 10^{20}$. Then,*

$$h_K/h_{k_2} \geq \frac{Q_K f_{k_3} f_K}{48e\,\mathrm{Reg}_{k_3}\mathrm{Reg}_K^*(\log d_K)(\log f_{k_2} + \kappa_0)}. \tag{11}$$

Proof. We follow the proofs of [Lou1, Theorem 5] and [Lou3, Theorem 7], to which we refer the reader. According to the the conductor-discriminant and analytic class number formulae (see [Lan, Theorem 2 page 259]), it holds that

$$\begin{aligned} h_K/h_{k_2} &= \frac{f_K f_{k_3}}{16\,\mathrm{Reg}_K/\mathrm{Reg}_{k_2}}\frac{\mathrm{Res}_{s=1}(\zeta_K(s))}{\mathrm{Res}_{s=1}(\zeta_{k_2}(s))} \\ &= \frac{Q_K f_K f_{k_3}}{192\,\mathrm{Reg}_{k_3}\mathrm{Reg}_K^*}\frac{\mathrm{Res}_{s=1}(\zeta_K(s))}{\mathrm{Res}_{s=1}(\zeta_{k_2}(s))}. \end{aligned}$$

For $s > 0$ real we have

$$(\zeta_K/\zeta_{k_2})(s) = |L(s,\chi_{k_3})|^2|L(s,\chi_K)|^2 \geq 0.$$

Now, there are two cases to consider.

First, it holds that $\zeta_{k_2}(1-2/\log d_K) \leq 0$. Then $\zeta_K(1-2/\log d_K) \leq 0$, and (7) and (9) yield

$$\frac{\mathrm{Res}_{s=1}(\zeta_K(s))}{\mathrm{Res}_{s=1}(\zeta_{k_2}(s))} \geq \frac{4}{e(\log d_K)(\log f_{k_2} + \kappa_0)}. \tag{12}$$

Second, it holds that $\zeta_{k_2}(1-2/\log d_K) > 0$. Then, there exists β in the range $1-(2/\log d_K) \leq \beta < 0$ such that $\zeta_{k_2}(\beta) = 0$, which implies $\zeta_K(\beta) = 0$, and (8) and (10)

$$\frac{\mathrm{Res}_{s=1}(\zeta_K(s))}{\mathrm{Res}_{s=1}(\zeta_{k_2}(s)} \geq \frac{8}{6e\log^2 f_{k_2}} \geq \frac{4}{3e(\log f_K)(\log f_{k_2}+\kappa_0)}. \tag{13}$$

Since the right hand side of (12) is always less than or equal to the right hand side of (13) (for $f_{k_2}f_{k_3} \geq \mathrm{lcm}(f_{k_2}, f_{k_3}) = f_K$ yields $d_K = f_{k_2}f_{k_3}^2 f_K^2 \geq f_K^3$), the lower bound (12) is always valid and the desired result follows. □

3.2. Simplest sextic fields.

Lemma 6 (See [Gra2, Theorem 2])**.** *Assume that* $m > 1$ *is such that* $\Delta_m = m^2+3m+9$ *is squarefree (hence,* $m \geq 4$ *and* $\Delta_m \geq 37$*), and set* $a = 4\sqrt{\Delta_m}$*. Then,*

$$\epsilon_* := \rho_m^{1-\sigma^3} = -\rho_m(2\rho_m+1)/(\rho_m+2)$$

is a generating relative unit of the simplest sextic field K_m*,*

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

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

and

$$\mathrm{Reg}_{K_m}^* = \mathrm{Reg}_{\epsilon_*}^* = \log^2 a - 30\frac{\log a}{a^2} + O\left(\frac{\log a}{a^3}\right)$$

is asymptotic to $\frac{1}{4}\log^2\Delta_m$ *and satisfies* $\mathrm{Reg}_{K_m}^* \leq \frac{1}{4}\log^2(16\Delta_m)$*. Therefore, by* (3)*, it holds that*

$$\mathrm{Reg}_{k_3}\mathrm{Reg}_{K_m}^* \leq \frac{1}{16}\log^4(4\Delta_m). \tag{14}$$

Proof. Since ϵ_* and ϵ_*^σ are roots of $(x-1)^6 - 16\Delta_m(x^2+x)^2$ (see [Gra2, Section 4]) and since $\rho_m > 1$ yields $\epsilon_* = -\rho_m(2\rho_m+1)/(\rho_m+2) < -1 < \epsilon_*^\sigma = -(\rho_m(\rho_m-1))/((\rho_m+1)(\rho_m+2)) < 0$, it follows that ϵ_* is a root of $(x-1)^3+a(x^2+x)$ whereas ϵ_*^σ is a root of $(x-1)^3-a(x^2+x)$, both of discriminant $a^2(a^2-108)$. Now, in the range $a>\sqrt{108}$ the roots of these cubic polynomials depend continuously on a, and $\rho_m=\frac{1}{2}a-\frac{1}{2}-\frac{19}{2}a^{-1}+O(a^{-2})$ (by (6)) yields $\epsilon_*=-a+4+7a^{-1}+O(a^{-2})$ and $\epsilon_*^\sigma=-1+8a^{-1}+O(a^{-2})$. Hence, the following lemma provides us with the desired result. $\square$

Lemma 7. *Assume that $a>\sqrt{108}$ and $a\neq(27+\sqrt{297})/4$. Then, the three real roots of the cubic polynomial $(x-1)^3+a(x^2+x)\in\mathbf{R}[x]$ of discriminant $a^2(a^2-108)>0$ are*

$$\rho=-\sqrt{\frac{4a(a-9)}{9}}\cos\left(\frac{1}{3}\arctan\left(\frac{\sqrt{27(a^2-108)}}{|2a^2-27a+54|}\right)+\frac{2k\pi}{3}\right)+1-\frac{a}{3}$$

$$=\begin{cases}-a+4+7a^{-1}+O(a^{-2}) & \text{for } k=0\\ a^{-1}+O(a^{-2}) & \text{for } k=1\\ -1-8a^{-1}+O(a^{-2}) & \text{for } k=2,\end{cases}$$

and the three real roots of the cubic polynomial $(x-1)^3-a(x^2+x)\in\mathbf{R}[x]$ of discriminant $a^2(a^2-108)>0$ are

$$\rho'=\sqrt{\frac{4a(a+9)}{9}}\cos\left(\frac{1}{3}\arctan\left(\frac{\sqrt{27(a^2-108)}}{2a^2+27a+54}\right)+\frac{2k\pi}{3}\right)+1+\frac{a}{3}$$

$$=\begin{cases}a+4-7a^{-1}+O(a^{-2}) & \text{for } k=0\\ v-1+8a^{-1}+O(a^{-2}) & \text{for } k=1\\ -a^{-1}+O(a^{-2}) & \text{for } k=2.\end{cases}$$

Proof. The roots of a cubic polynomial x^3-px-q, with $p\geq 0$ and $q\neq 0$ and of discriminant $d=4p^3-27q^2>0$, are

$$2\,\mathrm{sgn}\,(q)\sqrt{\frac{p}{3}}\cos\left(\frac{1}{3}\arctan\left(\sqrt{\frac{d}{27q^2}}\right)+\frac{2k\pi}{3}\right),\quad 0\leq k\leq 2,$$

where $\mathrm{sgn}\,(q)=+1$ for $q>0$ and $\mathrm{sgn}(q)=-1$ for $q<0$. $\square$

Theorem 8. *Assume that* $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ *is square-free* $(m \geq -1)$. *Let* h_{k_2} *denote the class number of the real quadratic subfield* k_2 *of the simplest sextic field* K_m. *Then,*

$$h_{K_m}/h_{k_2} \geq \frac{\Delta_m^2}{15e\log^6(4\Delta_m)}. \tag{15}$$

In particular, for $m \geq 10^5$ *it holds that* $h_{K_m} > \Delta_m$.

Proof. If $\Delta_m \leq 2 \cdot 10^4$ then

$$h_{K_m}/h_{k_2} \geq h_{k_3} \geq \frac{\Delta_m}{e\log^3\Delta_m} \geq \frac{\Delta_m^2}{15e\log^6(4\Delta_m)},$$

by (5), and (15) holds true (recall that the cubic subfield k_3 of the simplest sextic field K_m is the simplest cubic field of conductor Δ_m and that the product $h_{k_2}h_{k_3}$ divides h_{K_m}). If $\Delta_m \geq 2\cdot 10^4$ then $d_{K_m} = \Delta_m^5 > 8\cdot 10^{20}$ and (15) holds true, by (11) and (14). $\square$

4. Proof of Theorem 1

For proving (1), we use the following Lemma and then apply (15):

Lemma 9. *Assume that* $\Delta_m = m^2+3m+9 \equiv 1 \pmod 4$ *is squarefree* ($m \geq -1$) *and let the notation be as in Theorem 8. Then,* $h_{\mathbf{Q}(\zeta_{\Delta_m})^+} \geq 3^{1-t_m}h_{K_m}/h_{k_2}$.

Proof. We argue as in [CW, page 269]. Let H_m and G_m^+ denote the Hilbert class field and the maximal real subfield of the narrow genus field of the simplest sextic field K_m of conductor Δ_m. Hence, $G_m^+ = H_m \cap \mathbf{Q}(\zeta_{\Delta_m})^+$. Let G_3 denote the genus field of k_3 and let G_2^+ denote the maximal real subfield of the narrow genus field of k_2. Then, G_3 is real, $(G_3 : k_3) = 3^{t_m-1}$ (for the conductor of k_3 is equal to Δ_m), $G_m^+ = G_3G_2^+$ and

$$(G_m^+ : K_m) = (G_3 : k_3)(G_2^+ : k_2) = 3^{t_m-1}(G_2^+ : k_2)$$

divides $3^{t_m-1}h_2$.

Now, since

$$\begin{aligned}(H_m\mathbf{Q}(\zeta_{\Delta_m})^+ : \mathbf{Q}(\zeta_{\Delta_m})^+) &= (H_m : H_m \cap \mathbf{Q}(\zeta_{\Delta_m})^+)\\ &= (H_m : G_m^+)\\ &= \frac{(H_m : K_m)}{(G_m^+ : K_m)} = \frac{h_{K_m}}{(G_m^+ : K_m)} \geq \frac{h_{K_m}}{3^{t_m-1}h_2}\end{aligned}$$

divides the class number of $\mathbf{Q}(\zeta_{\Delta_m})^+$, the proof of the lemma is complete. $\square$

Let us now prove the last assertion of Theorem 1. If $t_m \geq 10$ then $\Delta_m \geq P_{t_m}$ and

$$\frac{1}{5e}\frac{\Delta_m}{3^{t_m}\log^6(4\Delta_m)} \geq \frac{1}{5e}\frac{P_{t_m}}{3^{t_m}\log^6(4P_{t_m})} := u_{t_m} \geq u_{10} > 1,$$

where P_t denotes the product of the least t primes $p \equiv 1 \pmod 6$ (for p divides Δ_m implies $p \equiv 1 \pmod 6$ and $x/\log^6(4x)$ increases with x for

$x \geq e^6/4$ and u_t increases with t for $t \geq 3$). Finally, if $t_m \leq 9$ and $m \geq 24 \cdot 10^6$, then

$$\frac{1}{5e}\frac{\Delta_m}{3^{t_m}\log^6(4\Delta_m)} \geq \frac{1}{5e}\frac{\Delta_m}{3^9\log^6(4\Delta_m)} > 1,$$

which completes the proof of the last assertion of Theorem 1.

Corollary 10. *Let $c = 0.311\ldots$ be as in Proposition 2. Let $\epsilon > 0$ be given. For at least $(c + o(1))x^{1/2}$ positive odd squarefree integers $n \leq x$ (where this $o(1)$ is effective) it holds that the class number h_n^+ of the maximal real subfield $\mathbf{Q}(\zeta_n)^+$ of the cyclotomic field $\mathbf{Q}(\zeta_n)$ of conductor n satisfies $h_n^+ > n^{2-\epsilon}$.*

PROOF. Let n range over the squarefree integers of the form $n = \Delta_m := m^2 + 3m + 9 \equiv 1 \pmod 4$, $m \geq -1$. The number of such $n \leq x$ is asymptotic to $c\sqrt{x}$, by Proposition 2. The well known upper bound $t = \omega(n) \ll (\log n)/\log\log n$ implies $3^n = n^{o(1)}$, and we use (1) to obtain the desired result. $\square$

This result is better than the non-effective one given in [CW, Theorem 2] according to which $h_n^+ > n^{3/2-\epsilon}$ for infinitely many composite n.

References

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

[CW] G. CORNELL and L. C. WASHINGTON, Class numbers of cyclotomic fields, *J. Number Theory* **21** (1985), 260–274.

[Gra1] M. N. GRAS, Familles d'unités dans les extensions cycliques réelles de degré 6 de **Q**, *Publ. Math. Besancon* (1984/1985–1985/86).

[Gra2] M. N. GRAS, Special units in real cyclic sextic fields, *Math. Comp.* **48** (1988), 543–556.

[Lan] S. LANG, Algebraic Number Theory. Second edn., *Graduate Texts in Mathematics* **110**, *Springer-Verlag, New York*, 1994.

[Lou1] S. LOUBOUTIN, CM-fields with cyclic ideal class groups of 2-power orders, *J. Number Theory* **67** (1997), 1–10.

[Lou2] S. LOUBOUTIN, Majorations explicites du résidu au point 1 des fonctions zêta des corps de nombres, *J. Math. Soc. Japan* **50** (1998), 57–69.

[Lou3] S. LOUBOUTIN, Class number and class group problems for some non-normal totally real cubic number fields, *Manuscripta Math.* **106** (2001), 411–427.

[Lou4] S. Louboutin, The exponent three class group problem for some real cyclic cubic number fields, *Proc. Amer. Math. Soc.* **130** (2002), 353–361.

[Lou5] S. Louboutin, Efficient computation of class numbers of real abelian number fields, *Lect. Notes in Comp. Sci.* **2369** (2002), 134–147.

[LP] F. Lemmermeyer and A. Pethő, Simplest cubic fields, *Manuscripta Math.* **88** (1995), 53–58.

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

[Wa] L. C. Washington, Class numbers of the simplest cubic fields, *Math. Comp.* **48** (1987), 371–384.

STÉPHANE R. LOUBOUTIN
INSTITUT DE MATHÉMATIQUES DE LUMINY
UPR 9016, 163, AVENUE DE LUMINY, CASE 907
13288 MARSEILLE CEDEX 9
FRANCE

E-mail: louboutí@iml.univ-mrs.fr

(Received March 28, 2003; revised June 6, 2003)