Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 121 (2006) 30–39
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

The class-number one problem for some real cubic number fields with negative discriminants

Stéphane R. Louboutin

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

Received 1 February 2005; revised 19 September 2005

Available online 3 March 2006

Communicated by D. Zagier

Dedicated to Corinne D.

Abstract

We prove that there are effectively only finitely many real cubic number fields of a given class number with negative discriminants and ring of algebraic integers generated by an algebraic unit. As an example, we then determine all these cubic number fields of class number one. There are 42 of them. As a byproduct of our approach, we obtain a new proof of Nagell's result according to which a real cubic unit $\epsilon > 1$ of negative discriminant is generally the fundamental unit of the cubic order $\mathbf{Z}[\epsilon]$.

MSC: 11R16; 11R29; 11R42

Keywords: Cubic field; Class number; Unit

1. Introduction

Let K be a real quadratic number field of discriminant $d_K > 0$. Let $A_K = \mathbf{Z}[\epsilon]$ be its ring of algebraic integers, where $\epsilon = (u + v\sqrt{d_K})/2 > 1$ is a unit of A_K. This is possible if and only if $v = 1$, hence $d_K = u^2 \pm 4$ for some $u \geqslant 1$. In that case, $\epsilon_K \leqslant \epsilon = (u + \sqrt{d_K})/2 \leqslant \sqrt{d_K + 4}$ and $\mathrm{Reg}_K \ll \log d_K$, where $\epsilon_K > 1$ is the fundamental unit of K and Reg_K its regulator. Hence, according to the Brauer–Siegel theorem which asserts that $\log(h_K \mathrm{Reg}_K)$ is asymptotic to $\frac{1}{2}\log d_K$ as $d_K \to +\infty$, there are only finitely many such real quadratic number fields K of a given class-number h_K. However, to date, no one knows how to make the Brauer–Siegel effective in the

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

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.01.008

Table 1

d_K	$P_K(X)$	d_K	$P_K(X)$
23	$X^3 - X - 1$	367	$X^3 - 7X^2 + 4X - 1$
31	$X^3 - X^2 - 1$	527	$X^3 - 5X^2 - 1$
44	$X^3 - X^2 - X - 1$	671	$X^3 - 11X^2 + 6X - 1$
59	$X^3 - 2X^2 - 1$	695	$X^3 - 8X^2 - 5X - 1$
76	$X^3 - 3X^2 + X - 1$	863	$X^3 - 7X^2 - 4X - 1$
83	$X^3 - 2X^2 - 2X - 1$	959	$X^3 - 6X^2 - X - 1$
87	$X^3 - 2X^2 - X - 1$	983	$X^3 - 7X^2 + 2X - 1$
107	$X^3 - 4X^2 + 2X - 1$	1007	$X^3 - 14X^2 + 7X - 1$
108	$X^3 - 3X^2 - 3X - 1$	1175	$X^3 - 8X^2 + 3X - 1$
135	$X^3 - 3X^2 - 1$	1319	$X^3 - 11X^2 - 6X - 1$
139	$X^3 - 6X^2 + 4X - 1$	1583	$X^3 - 17X^2 - 8X - 1$
140	$X^3 - 5X^2 + 3X - 1$	1871	$X^3 - 8X^2 + X - 1$
175	$X^3 - 3X^2 - 2X - 1$	2039	$X^3 - 9X^2 - 4X - 1$
199	$X^3 - 4X^2 + X - 1$	2759	$X^3 - 12X^2 + 5X - 1$
211	$X^3 - 10X^2 + 6X - 1$	2879	$X^3 - 11X^2 + 4X - 1$
231	$X^3 - 5X^2 - 4X - 1$	3671	$X^3 - 19X^2 + 8X - 1$
247	$X^3 - 4X^2 - 3X - 1$	4511	$X^3 - 16X^2 - 7X - 1$
255	$X^3 - 8X^2 + 5X - 1$	5351	$X^3 - 11X^2 - 1$
268	$X^3 - 13X^2 + 7X - 1$	6719	$X^3 - 27X^2 - 10X - 1$
335	$X^3 - 4X^2 - X - 1$	7871	$X^3 - 21X^2 + 8X - 1$
351	$X^3 - 6X^2 + 3X - 1$	12071	$X^3 + 44X^2 - 13X - 1$

real quadratic case, without assuming a suitable generalized Riemann hypothesis (however, see [Bir1]. See also [Bir1] and [Bir2] for a partial solution to the class number one problem for these two families of real quadratic number fields $M = \mathbf{Q}(\sqrt{m^2 \pm 4})$).

In contrast to the real quadratic case, let $K = \mathbf{Q}(\epsilon) \subseteq \mathbf{R}$ be a real cubic number field with negative discriminant $-d_K < 0$ whose ring of algebraic integers A_K is generated by a unit ϵ, i.e. such that $A_K = \mathbf{Z}[\epsilon]$. This clearly amounts to saying that $A_K = \mathbf{Z}[\epsilon_K]$, where $\epsilon_K > 1$ is the fundamental unit of K. We will prove that the regulators Reg_K of such cubic fields K are $\ll \log d_K$ (see Theorem 2). Using an explicit form of the Brauer–Siegel theorem (see [Lou05]), we will then obtain that the class numbers h_K of such cubic fields K are $\gg d_K^{1/2}/\log^2 d_K$ with explicit constants (Theorem 3) and we will solve the class number one problem for these cubic fields:

Theorem 1. *There are* 42 *non-isomorphic real cubic number fields $K \subseteq \mathbf{R}$ of negative discriminants $-d_K < 0$ which have class-number one and whose rings of algebraic integers are generated by the fundamental unit $\epsilon_K > 1$ of K. Namely, the $K = \mathbf{Q}(\epsilon_K)$ given in Table* 1*, where $\epsilon_K > 1$ is the real root of $P_K(X)$.*

This generalizes [Lou95, Theorem 2], which dealt with the one parameter family of cubic polynomials $P(X) = X^3 + lX - 1$.

2. Lower bounds for class numbers

Let $K = \mathbf{Q}(\epsilon) \subseteq \mathbf{R}$ be a real cubic number field with negative discriminant $-d_K < 0$ whose ring of algebraic integers A_K is generated by a unit ϵ, i.e. such that $A_K = \mathbf{Z}[\epsilon]$. Since $\mathbf{Z}[\epsilon] =$

$\mathbf{Z}[-\epsilon] = \mathbf{Z}[1/\epsilon] = \mathbf{Z}[-1/\epsilon]$, we may assume that $\epsilon > 1$. Then, $A_K = \mathbf{Z}[\epsilon_K]$, where $\epsilon_K > 1$ is the fundamental unit of K. The aim of this section is to obtain an explicit lower bound for the class number h_K of such a K (see Theorem 3 below). To obtain such a lower bound, we need an upper bound on the regulator $\mathrm{Reg}_K = \log \epsilon_K$ of K (see Theorem 2 below). To begin with, we observe that ϵ and ϵ_K are roots of polynomials of type (T) of negative discriminant $-d_K < 0$, where we have defined:

Definition 1. A polynomial of type (T) is a cubic polynomial $P(X) = X^3 - aX^2 + bX - 1 \in \mathbf{Z}[X]$ which is $\mathbf{Q}$-irreducible ($\Leftrightarrow b \neq a$ and $b \neq -a-2$), of negative discriminant $-d_P < 0$, with $d_P = 4(a^3 + b^3) - a^2b^2 - 18ab + 27 > 0$, and whose only real root ϵ_P satisfies $\epsilon_P > 1$ ($\Leftrightarrow P(1) < 0 \Leftrightarrow b \leqslant a - 1$).

Lemma 1. *If* $P(X) = X^3 - aX^2 + bX - 1$ *is of type* (T)*, then* $\epsilon_P - 2 < a < \epsilon_P + 2$, $a \geqslant 0$ *and* $|b| < 1 + 2\sqrt{\epsilon_P} < 1 + 2\sqrt{a+2}$.

Proof. We let $\epsilon_P > 1$, $\epsilon'_P = \alpha + i\beta$ and $\epsilon''_P = \alpha - i\beta = \overline{\epsilon'_P}$ denote the three complex roots of a cubic polynomial $P(X)$ of type (T). Then,

$$\begin{cases} 1 = \epsilon_P\epsilon'_P\epsilon''_P = \epsilon_P(\alpha^2 + \beta^2), \\ b = \epsilon_P\epsilon'_P + \epsilon'_P\epsilon''_P + \epsilon''_P\epsilon_P = 2\alpha\epsilon_P + (\alpha^2 + \beta^2) = 2\alpha\epsilon_P + (1/\epsilon_P), \\ a = \epsilon_P + \epsilon'_P + \epsilon''_P = \epsilon_P + 2\alpha. \end{cases} \tag{1}$$

Using the first equality, we obtain $|\alpha| \leqslant 1/\sqrt{\epsilon_P} < 1$, then $-1 < \epsilon_P - 2 < a = \epsilon_P + 2\alpha < \epsilon_P + 2$. It follows that $|b| < 2\sqrt{\epsilon_P} + 1/\epsilon_P < 2\sqrt{a+2} + 1$. □

Lemma 2. *Let* $P(X)$ *be a cubic polynomial of negative discriminant* $-d_P < 0$*, real root* $\epsilon_P > 1$ *and type* (T)*. It holds that*

$$d_P \leqslant 4\left(\epsilon_P + \epsilon_P^{-1/2}\right)^4/\epsilon_P = 4\left(\epsilon_P^{3/4} + \epsilon_P^{-3/4}\right)^4 \leqslant 64\epsilon_P^3. \tag{2}$$

Moreover, $\epsilon_P \geqslant \epsilon_{P_0} = 1.32471\ldots$*, where* $P_0(X) = X^3 - X - 1$ *is of type* (T) *and negative discriminant* $-d_{P_0} = -23$.

Proof. Using $d_P = (|\epsilon_P - \epsilon'_P||\epsilon_P - \epsilon''_P||\epsilon'_P - \epsilon''_P|)^2$ and $1 = \epsilon_P\epsilon'_P\epsilon''_P$, we obtain (2). Since this bound is increasing as a function of $\epsilon_P > 1$, for a given $B > 1$ we can list all the polynomials of type (T) such that $\epsilon_P \leqslant B$. For example, $\epsilon_P \leqslant 1.325$ implies $d_P \leqslant 69$, and $0 \leqslant a \leqslant 3$ and $0 \leqslant |b| \leqslant 3$ (by Lemma 1), and there are only 8 such polynomials $P(X)$ of type (T): $X^3 - X - 1$, $X^3 - X^2 - 1$, $X^3 - X^2 - X - 1$, $X^3 - X^2 - 2X - 1$, $X^3 - 2X^2 + X - 1$, $X^3 - 2X^2 - 1$, $X^3 - 2X^2 - 3X - 1$ and $X^3 - 3X^2 + 2X - 1$. It follows easily that $P(X) = X^3 - X - 1$, for which $d_P = 23$ and $\epsilon_P = 1.32471\ldots$, is the cubic polynomial of type (T) of least root $\epsilon_P > 1$. □

Theorem 2. (Compare with [Lou95, Proposition 5].) *Let* $P(X) = X^3 - aX^2 + bX - 1$ *be a cubic polynomial of type* (T)*. We have*

$$d_P \geqslant \epsilon_P^{3/2}/2. \tag{3}$$

In particular, by Lemma 1*, we have*

$$0 \leqslant a < 2 + (2d_P)^{2/3} \quad \textit{and} \quad |b| < 1 + 2(2d_P)^{1/3}, \tag{4}$$

and there are only finitely many cubic polynomials of type (T) *of a given discriminant.*

Proof. According to Lemma 1, there are only finitely many such polynomials for which $\epsilon_P < 18$ and the result holds true for these polynomials. Hence, we may and we will assume that $\epsilon_P \geqslant 18$. We stick to the notation introduced in (1). In particular, we have

$$d_P = \left(|\epsilon_P - \epsilon'_P||\epsilon_P - \epsilon''_P||\epsilon'_P - \epsilon''_P|\right)^2 \geqslant 4\beta^2\epsilon_P^4\left(1 - \epsilon_P^{-3/2}\right)^4$$

(use the first equality in (1)), and

$$4\beta^2\epsilon_P^4 = \left(4a - b^2\right)\epsilon_P^2 - 2b\epsilon_P + 3$$

(report the value of α, deduced from the second equality in (1), in the first equality in (1), and use $\epsilon_P^3 = a\epsilon_P^2 - b\epsilon_P + 1$).

(i) First, assume that $b \geqslant 0$. Then $4a - b^2 \geqslant 1$. In fact, $4a - b^2 \leqslant 0$ yields a contradiction: Either $b = 0$ leading to $a = b = 0$, or $b > 0$ leading to $0 \leqslant 4\beta^2\epsilon_P^4 = (4a - b^2)\epsilon_P^2 - 2b\epsilon_P + 3 \leqslant -2b\epsilon_P + 3 \leqslant -2\epsilon_P + 3 \leqslant -2 \cdot 18 + 3 < 0$. Further $b\epsilon_P = 2\alpha\epsilon_P^2 + 1 < 2\epsilon_P^{3/2} + 1$, by the first and second equalities in (1). So we obtain

$$d_P \geqslant \left(\epsilon_P^2 - 2\epsilon_P^{3/2} + 1\right)\left(1 - \epsilon_P^{-3/2}\right)^4 \geqslant \epsilon_P^2/2,$$

for $\epsilon_P \geqslant 18$.

(ii) Second, assume that $b < 0$. We set $B = -b$. Since

$$g(B) = d_P = -4B^3 - a^2B^2 + 18aB + 4a^3 + 27$$

is decreasing in the range $B \in [1, +\infty[$ (since $g'' \leqslant 0$ and $g'(1) = -2a^2 + 18a - 12 \leqslant 0$ for $a \geqslant 9$, and notice that $a > \epsilon_P - 2 \geqslant 16$) and since $g(\sqrt{4a+1}) = -a^2 + 2(a-2)\sqrt{4a+1} + 27 < 0$ (since $a > \epsilon_P - 2 \geqslant 16$), we get $4a + 1 > b^2$, i.e. $4a - b^2 \geqslant 0$. Assume first that $4a - b^2 \geqslant 1$. Then,

$$d_P \geqslant \left(\epsilon_P^2 + 2\epsilon_P 3\right)\left(1 - \epsilon_P^{-3/2}\right)^4 \geqslant \epsilon_P^2,$$

for $\epsilon_P \geqslant 5$. Otherwise, we are in the special case $4a = b^2$ and

$$d_P = 4a^{3/2} + 27 > 4(\epsilon_P - 2)^{3/2} + 27 \geqslant 2\epsilon_P^2,$$

for $\epsilon_P \geqslant 2$. We thank the referee for this streamlined version of our original proof of this theorem. □

Remark 1.

(1) If $P(X) = X^3 - 12X^2 - 7X - 1$, then $d_P = 23$, $\epsilon_P = 12.56350\ldots$, $d_P/(\frac{1}{2}\epsilon_P^{3/2}) = 1.03297\ldots.$

(2) When $P(X) = X^3 - M^2X^2 - 2MX - 1$ we have $d_P = 4M^3 + 27$ and $M^2 < \epsilon_P < M^2 + 1$ ($M \geqslant 2$), which imply $d_P \approx 4\epsilon_P^{3/2}$.
(3) Let $B > 0$ be given. Bounds (4) enable us to easily list all the cubic polynomials $P(X)$ of type (T) such that $d_P \leqslant B$.

Proposition 1. (See [Lou05, Corollary 8], and compare with [Lou95, Theorem 1].) *Let K be a non-normal real cubic field of negative discriminant $-d_K \leqslant -79\,507$. Let h_K and $\mathrm{Reg}_K = \log \epsilon_K$ denote the class number and regulator of K, where $\epsilon_K > 1$ is the fundamental unit of K. Set $\lambda = \pi\sqrt{3e} = 8.971\ldots$ and $\mu = (2 + \gamma - \log \pi)/2 = 0.716\ldots$. It holds that*

$$h_K \,\mathrm{Reg}_K \geqslant \frac{\sqrt{d_K}}{\lambda(\log d_K + \mu)}. \tag{5}$$

Theorem 3. *Let K be a non-normal real cubic field of negative discriminant $-d_K \leqslant -79\,507$. Assume that $A_K = \mathbf{Z}[\epsilon_K]$, where $\epsilon_K > 1$ is the fundamental unit of K. Then,*

$$h_K \geqslant \frac{3\sqrt{d_K}}{2\lambda(\log d_K + \mu')^2},$$

where $\lambda = \pi\sqrt{3e} = 8.971\ldots$ and $\mu' = (\mu + \log 2)/2 = 0.70469\ldots$. In particular,

$$d_K \leqslant 64\lambda^2\bigl(\log h_K + O(\log\log h_K)\bigr)^4 h_K^2/9,$$

there are only finitely such K's of a given class number, and $h_K > 1$ for $d_K > 2 \times 10^6$.

Proof. Use (5) and notice that $\mathrm{Reg}_K = \log \epsilon_K \leqslant \frac{2}{3}\log(2d_K)$, by Theorem 2. □

3. When is ϵ_P the fundamental unit of the cubic order $\mathbf{Z}[\epsilon_P]$?

Let ϵ_P be a real cubic algebraic unit of negative discriminant, i.e. ϵ_P is a root of a **Q**-irreducible cubic polynomial $P(X) = X^3 - aX^2 + bX - 1$ whose other two complex roots are not real. The unit group of the cubic order $\mathbf{Z}[\epsilon_P]$ is of rank one and we can ask whether ϵ_P is a generator of this unit group. Since $\mathbf{Z}[\epsilon_P] = \mathbf{Z}[-\epsilon_P] = \mathbf{Z}[1/\epsilon_P] = \mathbf{Z}[-1/\epsilon_P]$, we may assume that $\epsilon_P > 1$, i.e. that $P(X)$ is of type (T). We will give a new proof of the following result due to Nagell:

Theorem 4. (See also [Nag, Satz XXII].) *Let $\epsilon_P > 1$ be the real root of a cubic polynomial $P(X) = X^3 - aX^2 + bX - 1 \in \mathbf{Z}[X]$ of negative discriminant $-d_P < 0$ and type* (T)*, and let $\eta_P > 1$ be the generator greater than 1 of the unit group of the cubic order $\mathbf{Z}[\epsilon_P]$ of negative discriminant $-d_P < 0$. Then, $\epsilon_P = \eta_P$, except in the following cases*:

(1) *$P(X) = X^3 - M^2X^2 - 2MX - 1$, $M \geqslant 1$, in which case $\epsilon_P = \eta_P^2$ where $\eta_P = \epsilon_Q > 1$ is the only real root of $Q(X) = X^3 - MX^2 - 1$ (and $d_P = d_Q = 4M^3 + 27$).*
(2) *$d_P = 23$, $\eta_P = \epsilon_Q > 1$ is the real root of $Q(X) = X^3 - X - 1$ and $\epsilon_P = \eta_P^2$, $\epsilon_P = \eta_P^3$, $\epsilon_P = \eta_P^4$, η_P^5 or η_P^7 are the real roots of $P(X) = X^3 - 2X^2 + X - 1$, $P(X) = X^3 - 3X^2 + 2X - 1$, $P(X) = X^3 - 2X^2 - 3X - 1$, $P(X) = X^3 - 5X^2 + 4X - 1$ or $P(X) = X^3 - 12X^2 - 7X - 1$.*

(3) $d_P = 31$, $\eta_P = \epsilon_Q > 1$ *is the real root of* $Q(X) = X^3 - X^2 - 1$ *and* $\epsilon_P = \eta_P^3$ *or* $\epsilon_P = \eta_P^5$ *are the real roots of* $P(X) = X^3 - 4X^2 + 3X - 1$ *or* $P(X) = X^3 - 6X^2 - 5X - 1$.
(4) $d_P = 44$, $\eta_P = \epsilon_Q > 1$ *is the real root of* $Q(X) = X^3 - X^2 - X - 1$ *and* $\epsilon_P = \eta_P^3$ *is the real root of* $P(X) = X^3 - 7X^2 + 5X - 1$.

Proof. Suppose that ϵ_P is not the generator greater than 1 of the unit group of the cubic order $\mathbf{Z}[\epsilon_P]$. Let $\eta_P > 1$ be this generator and write $\epsilon_P = \eta_P^n$ with $n \geqslant 2$. Since $\mathbf{Z}[\epsilon_P] = \mathbf{Z}[\eta_P]$ is of discriminant $-d_P$, $\epsilon_P > 1$ and $\eta_P > 1$ are real roots of cubic polynomials of type (T) both of discriminant $-d_P$, and we have

$$1 < \eta_P^{3n/2} = \epsilon_P^{3/2} \leqslant 2d_P \leqslant 8(\eta_P + 1/\sqrt{\eta_P})^4/\eta_P,$$

by (2) and (3), and

$$n < 2 + \frac{\log 4}{\log \eta_P} + \frac{8\log(1 + 1/(\eta_P\sqrt{\eta_P}))}{3\log \eta_P} \tag{6}$$

(which is a decreasing function of $\eta_P > 1$). Hence, $n < 3$, i.e. $n = 2$, for $\eta_P > 5.021$. (And $n \leqslant 11$ in any case, by Lemma 2.) Moreover, $\eta_P \leqslant 5.021$ implies $d_P \leqslant 4(\eta_P + 1/\sqrt{\eta_P})^4/\eta_P < 712$.

Now, if $\eta_P = \epsilon_Q > 1$ is a root of a cubic polynomial $Q(X) = X^3 - aX^2 + bX - 1$ of type (T), then $\epsilon_P = \eta_P^2$ is a root of $P(X) = X^3 - (a^2 - 2b)X^2 + (b^2 - 2a)X - 1$ and $d_P = (ab - 1)^2 d_Q$. Hence, $d_P = d_Q$ if and only if $ab = 0$ or $ab = 2$. Assume first that $ab = 0$. If $b = 0$, then $Q(X) = X^3 - aX^2 - 1$, $P(X) = X^3 - a^2X^2 - 2aX - 1$ and $d_P = d_Q = 4a^3 + 27$. If $a = 0$, then $Q(X) = X^3 + bX - 1$, $P(X) = X^3 + 2bX^2 + b^2X - 1$ and $d_P = d_Q = 4b^3 + 27$. Since $b \leqslant a - 1 = -1$ and $d_Q = 4b^3 + 27 > 0$, we have $b = -1$, $Q(X) = X^3 - X - 1$, $P(X) = X^3 - 2X^2 + X - 1$ and $d_P = d_Q = 23$. Assume now that $ab = 2$. Since $a \geqslant 0$ and $b \leqslant a - 1$, we have $a = 2$, $b = 1$, $Q(X) = X^3 - 2X^2 + X - 1$, $P(X) = X^3 - 2X^2 - 3X - 1$ and $d_P = d_Q = 23$.

Finally, it remains to deal with the case that $d_P < 712$, which implies $0 \leqslant a < 2 + (2 \cdot 712)^{2/3} < 129$, by (4). According to the third point of Remark 1, there are 52 cubic polynomials $P(X)$ of type (T) such that $d_P < 712$. If ϵ_P is not the generator of the unit group of the cubic order $\mathbf{Z}[\epsilon_P]$, then there exist a unit $1 < \eta_P \in \mathbf{Z}[\epsilon_P]$ and $n \geqslant 2$ such that $\epsilon_P = \eta_P^n$, and $\eta_P = \epsilon_Q$ is the real root of a cubic polynomial $Q(X)$ of type (T). Since $\mathbf{Z}[\epsilon_Q] = \mathbf{Z}[\eta_P] \subseteq \mathbf{Z}[\epsilon_P] = \mathbf{Z}[\eta_P^n] = \mathbf{Z}[\epsilon_Q^n] \subseteq \mathbf{Z}[\epsilon_Q]$, we have $\mathbf{Z}[\epsilon_Q] = \mathbf{Z}[\epsilon_P]$ and $d_Q = d_P$. According to Lemma 3 below, we have either $0 \leqslant a_Q < a_P$ or $a_P = a_Q$, $d_P = d_Q = 23$, $P(X) = X^3 - 2X^2 - 3X - 1$ and $Q(X) = X^3 - 2X^2 + X - 1$. Now, Table 2 below lists all the d's less than 712 such that among the 52 cubic polynomials $P(X)$ of negative discriminants $-d_P > -712$ and type (T) there are at least two of them of the same negative discriminant $-d > -712$. From this Table 2, the desired result follows (for all the polynomials in Table 2 fall in one of the four cases considered in this Theorem 4). □

Lemma 3. *Let* $P(X) = X^3 - a_PX^2 + b_PX - 1$ *and* $Q(X) = X^3 - a_QX^2 + b_QX - 1$ *be two cubic polynomials of type* (T). *Then,* $\epsilon_P \geqslant \epsilon_Q^2$ *implies* $a_P > a_Q$, *except in the case that* $Q(X) = X^3 - 2X^2 + X - 1$ *and* $P(X) = X^3 - 2X^2 - 3X - 1$ *where* $\epsilon_P = \epsilon_Q^2$, $a_P = a_Q$ *and* $d_P = d_Q = 23$.

Proof. Assume first that $\epsilon_Q > 2.106$. Then, we do have $a_P \geqslant \epsilon_P - 2/\sqrt{\epsilon_P} \geqslant \epsilon_Q^2 - 2/\epsilon_Q > \epsilon_Q + 2/\sqrt{\epsilon_Q} \geqslant a_Q$. Assume now that $\epsilon_Q \leqslant 2.106$. Then $0 \leqslant a_Q \leqslant 4$, by Lemma 1. According to

Table 2

a_P	$P(X)$	d_P	a_P	$P(X)$	d_P
0	X^3-X-1	23	4	X^3-4X^2-1	283
1	X^3-X^2-2X-1	31	4	X^3-4X^2+3X-1	31
1	X^3-X^2-X-1	44	5	X^3-5X^2-1	527
1	X^3-X^2-1	31	5	X^3-5X^2+4X-1	23
2	X^3-2X^2-3X-1	23	6	X^3-6X^2-5X-1	31
2	X^3-2X^2-1	59	7	X^3-7X^2+5X-1	44
2	X^3-2X^2+X-1	23	9	X^3-9X^2-6X-1	135
3	X^3-3X^2-1	135	12	X^3-12X^2-7X-1	23
3	X^3-3X^2+2X-1	23	16	X^3-16X^2-8X-1	283
4	X^3-4X^2-4X-1	59	25	$X^3-25X^2-10X-1$	527

Table 3

a_Q	$Q(X)$	ϵ_Q	a_Q	$Q(X)$	ϵ_Q
0	X^3-X-1	1.32471...	3	X^3-3X^2+2X-1	2.32471...
1	X^3-X^2-1	1.46557...	3	X^3-3X^2+X-1	2.76929...
1	X^3-X^2-X-1	1.83928...	3	X^3-3X^2-1	3.10380...
1	X^3-X^2-2X-1	2.14789...	3	X^3-3X^2-X-1	3.38297...
2	X^3-2X^2+X-1	1.75487...	3	X^3-3X^2-2X-1	3.62736...
2	X^3-2X^2-1	2.20556...	3	X^3-3X^2-3X-1	3.84732...
2	X^3-2X^2-X-1	2.54681...	4	X^3-4X^2+3X-1	3.14789...
2	X^3-2X^2-2X-1	2.83117...	4	X^3-4X^2+2X-1	3.51154...
2	X^3-2X^2-3X-1	3.07959...	4	X^3-4X^2+X-1	3.80630...
3	X^3-3X^2+2X-1	2.32471...	4	X^3-4X^2-1	4.06064...
3	X^3-3X^2+X-1	2.76929...	4	X^3-4X^2-X-1	4.28762...
3	X^3-3X^2-1	3.10380...	4	X^3-4X^2-2X-1	4.49449...
3	X^3-3X^2-X-1	3.38297...	4	X^3-4X^2-3X-1	4.68577...
3	X^3-3X^2-2X-1	3.62736...	4	X^3-4X^2-4X-1	4.86453...
3	X^3-3X^2-3X-1	3.84732...			

Table 3 which lists the real roots of all the cubic polynomials $Q(X)$ of type (T) with $0 \leqslant a_Q \leqslant 4$, $Q(X)$ is one of the following four polynomials: X^3-X-1, X^3-X^2-1, X^3-X^2-X-1, or X^3-2X^2+X-1. Now, in these four cases, there is no $P(X)$ of type (T) such that $\epsilon_P \geqslant \epsilon_Q^2$ and $0 \leqslant a_P \leqslant a_Q$. Indeed,

(i) If $Q(X)=X^3-X-1$ then $a_Q=0$. Hence, we would have $a_P=0$, $P(X)=X^3-X-1=Q(X)$ and $\epsilon_P=\epsilon_Q<\epsilon_Q^2$.

(ii) If $Q(X)=X^3-X^2-1$ then $a_Q=1$ and $\epsilon_Q^2=1.75487\ldots$. Hence, we would have $0 \leqslant a_P \leqslant 1$, $P(X)$ would be one of the first four polynomials in this table and none of them satisfies $\epsilon_P \geqslant \epsilon_Q^2$.

(iii) Same line of reasoning if $Q(X)=X^3-X^2-X-1$.

(iv) If $Q(X)=X^3-2X^2+X-1$ then $a_Q=2$ and $\epsilon_Q^2=3.07959\ldots$. Hence, we would have $0 \leqslant a_P \leqslant 2$, $P(X)$ would be one of the first nine polynomials in this table and none of them but the last one satisfies $\epsilon_P \geqslant \epsilon_Q^2$. □

4. When is $\mathbf{Z}[\epsilon_P]$ the ring of algebraic integers of the cubic number field $\mathbf{Q}(\epsilon_P)$?

Lemma 4. *Let ϵ_P be a complex root of a $\mathbf{Q}$-irreducible polynomial $P(X) = X^3 - aX^2 + bX - c \in \mathbf{Z}[X]$ of discriminant Δ_P. Let A_K be the ring of algebraic integers of the cubic number field $K = \mathbf{Q}(\epsilon_P)$. Then, $A_K = \mathbf{Z}[\epsilon_P]$ if and only if for all primes $p \geqslant 2$ such that p^2 divides Δ_P we have $P(\alpha) \not\equiv 0 \pmod{p^2}$, where $\alpha \in \mathbf{Z}$ is any rational integer such that $P(\alpha) \equiv P'(\alpha) \equiv 0 \pmod p$.*

Proof. This is a consequence of Dedekind's criterion (see [Coh, Theorem 6.1.4]). See also [DF, Section 17, Theorem I]. □

Theorem 5. *Let ϵ_P be a complex root of $P(X) = X^3 - aX^2 + bX - 1 \in \mathbf{Z}[X]$. Assume that $P(X)$ is $\mathbf{Q}$-irreducible ($\Leftrightarrow b \neq a$ and $b \neq -a-2$). Let A_K be the ring of algebraic integers of the cubic number field $K = \mathbf{Q}(\epsilon_P)$. Then, $A_K = \mathbf{Z}[\epsilon_P]$ if and only if the four following conditions are satisfied*:

(1) *if $a \equiv b \equiv 1 \pmod 2$, then $a \not\equiv b \pmod 4$*;
(2) *if $a \equiv b \equiv 0 \pmod 3$, then $a \not\equiv b \pmod 9$*;
(3) *if $a \equiv b \equiv -1 \pmod 3$, then $a + b \not\equiv -2 \pmod 9$*;
(4) *if $p > 3$ is prime and p^2 divides d_P, then $3b \equiv a^2 \pmod p$ but $2a^3 - 9ab + 27 \not\equiv 0 \pmod{p^2}$.*

Proof. First, 2^2 divides d_P if and only if $a \equiv b \equiv 1 \pmod 2$, in which case we may take $\alpha = 1$ for which $P(\alpha) = -a + b$.

Second, 3^2 divides d_P if and only if $a \equiv b \equiv 0 \pmod 3$, in which case we may take $\alpha = 1$ for which $P(\alpha) = -a + b$, or $a \equiv b \equiv -1 \pmod 3$, in which case we may take $\alpha = -1$ for which $P(\alpha) = -a - b - 2$.

Third, we assume that $p > 3$ and p^2 divides d_P. Since

$$9P(X) = (3X - a)P'(X) + 2\big(3b - a^2\big)X + ab - 9,$$

$P(\alpha) \equiv P'(\alpha) \equiv 0 \pmod p$ implies $2(a^2 - 3b)\alpha \equiv ab - 9 \pmod p$. If we had $3b \not\equiv a^2 \pmod p$, using $2^3(a^2 - 3b)^3 P((ab - 9)/(2(a^2 - 3b^2))) = (2a^3 - 9ab + 27)d_P$, we would obtain $P(\alpha) \equiv 0 \pmod{p^2}$. Hence, $3b \equiv a^2 \pmod p$. Since p divides

$$27\Delta_P = -4\big(27a^3 + (3b)^3\big) + 3a^2(3b)^2 + 162a(3b) - 729 \equiv -\big(a^3 - 27\big)^3 \pmod p,$$

we have $a^3 \equiv 27 \pmod p$, $27P(X) \equiv (3X - a)^3 \pmod p$ and $3\alpha \equiv a \pmod p$. Since $Q'(a) = -3a^2 + 9b \equiv 0 \pmod p$, where $Q(X) = 27P(X/3) = X^3 - 3aX^2 + 9bX - 1$, we obtain $27P(\alpha) = Q(3\alpha) \equiv Q(a) = -2a^3 + 9ab - 27 \not\equiv 0 \pmod{p^2}$. □

5. Proof of Theorem 1

To complete the proof of Theorem 1, it remains to generate all such fields K with $d_K \leqslant 2 \times 10^6$ (by Theorem 3) and then to compute their class numbers. To complete this task, we first generate all the cubic polynomials $P(X) = X^3 - aX^2 + bX - 1$ of type (T) with $d_P \leqslant 2 \times 10^6$. We first observe that according to (4) we have $0 \leqslant a < 2 + (2d_P)^{2/3} < 25\,201$, and for any given such a, Lemma 1 gives a small upper bound on $|b|$. Now, for a given such $P(X)$ of real root $\epsilon_P > 1$, we use Theorem 5 to determine whether $\mathbf{Z}[\epsilon_P]$ is the ring of algebraic integers of the

Table 4

a	b	d_P	a	b	d_P	a	b	d_P	a	b	d_P
0	−1	**23**	4	3	**31**	7	5	**44**	11	−6	1319
1	0	**31**	4	2	107	7	4	367	12	5	2759
1	−1	**44**	4	1	199	7	2	983	12	−7	**23**
1	−2	**31**	4	−1	335	7	−4	863	13	7	268
2	1	**23**	4	−3	247	8	5	255	14	7	1007
2	0	**59**	4	−4	**59**	8	3	1175	16	−7	4511
2	−1	87	5	4	**23**	8	1	1871	17	−8	1583
2	−2	83	5	3	140	8	−5	695	19	8	3671
2	−3	**23**	5	0	**527**	9	−4	2039	21	8	7871
3	2	**23**	5	−4	231	9	−6	**135**	25	−10	**527**
3	1	76	6	4	139	10	6	211	27	−10	6719
3	0	**135**	6	3	351	11	6	671	44	13	12 071
3	−2	175	6	−1	959	11	4	2879	121	−22	**5351**
3	−3	108	6	−5	**31**	11	0	**5351**			

real cubic field $K = \mathbf{Q}(\epsilon_P)$. If so, we can finally easily compute its class number h_K (by using the method explained in [BLW,BWB], [Lou95, Section 3] and [Lou01, Section 3]), and get rid of the polynomials $P(X)$ for which $h_K > 1$. As a result of our computation, Table 4 provides all the cubic polynomials of type (T) such that (i) $d_P \leqslant 2 \times 10^6$ (there are 2972 of them), (ii) $\mathbf{Z}[\epsilon_P]$ is the ring of algebraic integers of the real cubic field $K_P = \mathbf{Q}(\epsilon_P)$ (there are 2214 of them) and (iii) the class number of K_P is equal to one (there are 55 of them). The discriminants which appear at least twice are in bold face letters. However, according to Theorem 4, any two fields in Table 4 with the same discriminant are equal. This observation completes the proof of Theorem 1. Notice however that $P(X) = X^3 - 9X^2 - X - 1$ and $Q(X) = X^3 - 15X^2 - 7X - 1$ both have type (T) and discriminant $-d_P = -d_Q = -3020$, but whereas $K_P = \mathbf{Q}(\epsilon_P)$ and $K_Q = \mathbf{Q}(\epsilon_Q)$ are both of discriminant -3020 and class number 3, they are not isomorphic (since $A_{K_P} = \mathbf{Z}[\epsilon_P]$ and $A_{K_Q} = \mathbf{Z}[\epsilon_Q]$ and since $P(X)$ is irreducible modulo $p = 11$ whereas $Q(X) = (X+2)(X+6)(X+10)$ modulo 11, it follows that the prime $p = 11$ remains inert in K_P but splits completely in K_Q). We also refer the reader to [Ger, Theorem 2] which proves that for a given $\Delta < 0$ there is generally at most one cubic field $K \subset \mathbf{R}$ of negative discriminant $-d_K = \Delta$ and class number h_K not divisible by 3.

The referee communicated to us a PARI-GP program for doing these computations. Both computations yielded the same results.

6. Conclusion

Say that a quartic polynomial $P(X)$ is of type (T) if it is of the form $P(X) = X^4 - aX^3 + bX - cX + 1 \in \mathbf{Z}[X]$, is $\mathbf{Q}$-irreducible, has no real root, which implies $d_P > 0$, and if the associated quartic number field K_P is not a cyclotomic field. Notice that the unit rank of K_P is equal to 1. Let α_1, $\bar{\alpha}_1$, α_2 and $\bar{\alpha}_2$ be its four complex roots. Since K_P is not one of the three quartic cyclotomic fields $\mathbf{Q}(\zeta_n)$ with $n \in \{8, 10, 12\}$, at least one out the four complex roots of $P(X)$ has absolute value not equal to one (see [Was97, Lemma 1.6]). Hence, we may assume that $|\alpha_1| > 1$, which implies $|\alpha_2| < 1$. From now on, we let $\epsilon_P (= \alpha_1$ or $\bar{\alpha}_1)$ be any one of the two conjugate complex roots of $P(X)$ of absolute value greater than one. Is that true that, as in Theorem 2, there exist $c_1 > 0$ and $c_2 > 0$ such that for any quartic polynomial $P(X)$ of type (T) we have

$$d_P \geqslant c_1|\epsilon_P|^{c_2}?$$

In that case, using [Lou05] it should be possible to prove, as in Theorem 3, that if K is ranges over the non-cyclotomic totally complex quartic fields such that their rings of algebraic integers are of the form $A_K = \mathbf{Z}[\epsilon_K]$, where ϵ_K with $|\epsilon_K| > 1$ is the fundamental unit of K, then its class number h_K goes explicitly to infinity with d_K.

References

[BLW] P. Barrucand, J. Loxton, H.C. Williams, Some explicit upper bounds on the class number and regulator of a cubic field with negative discriminant, Pacific J. Math. 128 (1987) 209–222.

[BWB] P. Barrucand, H.C. Williams, L. Naniuk, A computational technique for determining the class number of a pure cubic field, Math. Comp. 30 (1976) 312–323.

[Bir1] A. Biró, Yokoi's conjecture, Acta Arith. 106 (2003) 85–104.

[Bir2] A. Biró, Chowla's conjecture, Acta Arith. 107 (2003) 179–194.

[Coh] H. Cohen, A Course in Computational Algebraic Number Theory, fourth printing, Grad. Texts in Math., vol. 138, Springer-Verlag, Berlin, 2000.

[DF] B.N. Delone, D.K. Faddeev, The Theory of Irrationalities of the Third Degree, Transl. Math. Monogr., vol. 10, Amer. Math. Soc., Providence, RI, 1964.

[Ger] F. Gerth III, Cubic fields whose class numbers are not divisible by 3, Illinois J. Math. 20 (1976) 486–493.

[Lou95] S. Louboutin, Class number problems for cubic number fields, Nagoya Math. J. 138 (1995) 199–208.

[Lou01] S. Louboutin, Class number and class group problems for some non-normal totally real cubic number fields, Manuscripta Math. 106 (2001) 411–427.

[Lou05] S. Louboutin, On the Brauer–Siegel theorem, J. London Math. Soc. (2) 72 (2005) 40–52.

[Nag] T. Nagell, Zur Theorie der kubishen Irrationlitaten, Acta Math. 55 (1930) 33–65.

[Was97] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Grad. Texts in Math., vol. 83, Springer-Verlag, Berlin, 1997.