Class number and class group problems for some non-normal totally real cubic number fields

Stéphane LOUBOUTIN
Institut de Mathématiques de Luminy, UPR 906
163, avenue de Luminy
Case 907
13288 Marseille Cedex 9, FRANCE
loubouti@iml.univ-mrs.fr

November 9, 2000

Abstract

Let $\{K_m\}_{m\geq 4}$ be the family of non-normal totally real cubic number fields associated with the $\mathbf{Q}$-irreducible cubic polynomials $P_m(x) = x^3 - mx^2 - (m+1)x - 1$, $m \geq 4$. We determine all these K_m's with class numbers $h_m \leq 3$: there are 14 such K_m's. Assuming the Generalized Riemann hypothesis for all the real quadratic number fields, we also prove that the exponent e_m of the ideal class groups of these K_m goes to infinity with m and we determine all these K_m's with ideal class groups of exponents $e_m \leq 3$: there are 5 such K_m with ideal class groups of exponent 2, and 6 such K_m with ideal class groups of exponent 3.

[0]1991 Mathematics Subject Classification. Primary 11R16, 11R29, 11R42.
Key words and phrases. cubic field, class number, class group, zeta function.

Contents

1 Introduction

In [Lou4] we tackled some class number and class group problems for some non-normal non-totally real cubic numbers fields, whereas in [Lou6] we tackled some class number and class group problems for some normal totally real cubic numbers fields. Here, we shall tackle some class number and class group problems for non-normal totally real cubic numbers fields, the third and last possible setting for cubic number fields. It is worth pointing out that Section 2 (which provides us with a good explicit lower bound for class numbers of non-normal totally real cubic fields) and Section 3 (which provides us with a rigorous method for computing their class numbers) are of special importance due to their potential usefulness to those willing to deal with (totally real non-normal) cubic fields.

1.1 A family of cubic polynomials

Let $m \geq 4$ be a rational integer and K_m be the totally real cubic number field defined as in [MT, Section 2] by the $\mathbf{Q}$-irreducible cubic polynomial

$$P_m(x) = x^3 - mx^2 - (m+1)x - 1 \quad (m \geq 4)$$

of discriminant

$$d_{P_m} = d_m := m^4 + 2m^3 - 5m^2 - 6m - 23 = (m^2 + m - 3)^2 - 32 > 0.$$

Since d_m is never a perfect square for $m \geq 4$, K_m is always a non-normal totally real cubic field. Notice that K_m is also defined as in [Tho, Prop. (3.6)] by $y^3 P_m((1/y)-1) = y^3-(m+2)y^2+(m+3)y-1$. Let $\rho_m^{(3)} < \rho_m^{(2)} < \rho_m^{(1)} = \rho_m$ be the three distinct real roots of $P_m(x)$ and set $p_m = m^2 + 3m + 3$ and $q_m = 2m^3 + 9m^2 + 9m + 27$. Since $P_m(x) = Q_m(y)/27$ where $y = 3x - m$ and

$$Q_m(X) = X^3 - 3p_m X - q_m,$$

we obtain $d_m = d_{Q_m}/27^2 = (4p_m^3 - q_m^2)/27$,

$$\rho_m^{(i)} = \frac{1}{3}\left(2\sqrt{p_m}\cos\Big(\frac{1}{3}\arctan(\frac{\sqrt{27d_m}}{q_m}) + \frac{2k_i\pi}{3}\Big) + m\right) \tag{1}$$

with $k_1 = 0$, $k_2 = 2$ and $k_3 = 1$, which yields

$$\begin{aligned}
\rho_m^{(1)} &= m + 1 + m^{-2} - 3m^{-3} + 7m^{-4} - 17m^{-5} + 46m^{-6} + O(m^{-7}),\\
\rho_m^{(2)} &= -m^{-1} - m^{-4} - m^{-5} - m^{-6} + O(m^{-7}),\\
\rho_m^{(3)} &= -1 + m^{-1} - m^{-2} + 3m^{-3} - 6m^{-4} + 18m^{-5} - 45m^{-6} + O(m^{-7}).
\end{aligned}$$

We also have the following explicit bounds (valid for $m \geq 4$):

$$\begin{array}{rll} m+1 < & \rho_m^{(1)} & < m+1+m^{-2} \\ -m^{-1}-m^{-3} < & \rho_m^{(2)} & < -m^{-1} \\ -1 < & \rho_m^{(3)} & < -1+m^{-1} \end{array} \tag{2}$$

(look at the signs of the values of P_m evaluated at the three right hand sides and at the three left hand sides of these inequalities).

1.2 The simplest non-normal totally real cubic fields

Lemma 1 *Let K be a cubic number field defined by a $\mathbf{Q}$-irreducible cubic polynomial $Q(Y) = Y^3 - aY - b \in \mathbf{Z}[Y]$. Let $\theta \in K$ be a complex root of $Q(Y)$ and let A_K denote the ring of algebraic integers of K. Hence, $\mathbf{Z}[\theta] \subseteq A_K$. Assume that $p > 3$ is a prime for which there exists some rational integer t satisfying $Q'(t) \equiv 0 \pmod{p}$ and $Q(t) \equiv 0 \pmod{p^2}$. Then, p divides the index $(A_K : \mathbf{Z}[\theta])$. In particular, if there exists some prime $p > 3$ such that p does not divide a but such that p^2 divides the discriminant $d_Q = 4a^3 - 27b^2$ of $Q(Y)$, then p divides the index $(A_K : \mathbf{Z}[\theta])$.*

Proof. $z(t) = (y^2 + ty + t^2 - a)/p$ is a root of the characteristic polynomial $Z^3 - \frac{Q'(t)}{p}Z^2 + \frac{3tQ(t)}{p^2}Z - \frac{(Q(t))^2}{p^3}$ of the linear map $u \mapsto z(t)u$ of the $\mathbf{Q}$-vector space K. Hence, if $Q'(t) \equiv 0 \pmod{p}$ and $Q(t) \equiv 0 \pmod{p^2}$ then $z(t) \in A_K$ and p divides $(A_K : \mathbf{Z}[\theta])$. Let us now prove the second assertion. Since we have assumed that $p > 3$ does not divide a, it suffices to find some integer t such that $4a^2Q'(t) \equiv 0 \pmod{p}$ and $8a^3Q(t) \equiv 0 \pmod{p^2}$. The reader will easily check that any t such that $2at \equiv -3b \pmod{p}$ satisfies these congruences (write $2at = -3b + cp$ for some rational integer c and observe that $4a^2Q'(t) = 3(2at)^2 - 4a^3 \equiv 3(-3b)^2 - 4a^3 \equiv -d_Q \equiv 0 \pmod{p}$ and $8a^3Q'(t) = (2at)^3 - 4a^3(2at) - 8a^3b = (-3b+cp)^3 - 4a^3(-3b+cp) - 8a^3b \equiv 4a^3b - 27b^3 + (27b^2 - 4a^3)cp = bd_Q - cpd_Q \equiv 0 \pmod{p^2}$). •

Lemma 2 *Set $p_m = m^2 + 3m + 3$ and $q_m = 2m^3 + 9m^2 + 9m + 27$. Then,*

$$\gcd(p_m, q_m) = \begin{cases} 1 & \text{if } m \not\equiv 0 \pmod{3} \text{ and } m \not\equiv 3 \pmod{7} \\ 7 & \text{if } m \not\equiv 0 \pmod{3} \text{ and } m \equiv 3 \pmod{7} \\ 3 & \text{if } m \equiv 0 \pmod{3} \text{ and } m \not\equiv 3 \pmod{7} \\ 21 & \text{if } m \equiv 0 \pmod{3} \text{ and } m \equiv 3 \pmod{7} \end{cases}$$

Let $\nu_7(k)$ denote the exponent of 7 in the prime factorization of a positive integer $k \geq 1$. Then, $\nu_7(d_m) \geq 1$ if and only if $m \equiv 3 \pmod 7$. Conversely, assume that $m \equiv 3 \pmod 7$. Then, $\nu_7(d_m) = 2$ if $m \not\equiv 24 \pmod{7^2}$ and $\nu_7(d_m) = 3$ if $m \equiv 24 \pmod{7^2}$.

Proof. Recall that $d_m = (4p_m^3 - q_m^2)/27$. The last assertion follows from the previous easier ones once we notice that for $m \equiv 3 \pmod 7$ we have $\nu_7(q_m) \geq 2 \Leftrightarrow m \equiv 24 \pmod{7^2}$. •

Now, we are in a position to prove the main result of this subsection:

Theorem 3 *$\{1, \rho_m, \rho_m^2\}$ is a $\mathbf{Z}$-basis of the ring of algebraic integers A_{K_m} of K_m if and only if either [$m \not\equiv 3 \pmod 7$ and d_m is square-free] or [$m \equiv 3 \pmod 7$, $m \not\equiv 24 \pmod{7^2}$ and $d_m/7^2$ is square-free]. In both cases, K_m is called the mth* **simplest non-normal totally real cubic field**.

Proof. Recall that $\theta_m = 3\rho_m - m$ is a root of $Q_m(Y) = Y^3 - 3p_mY - q_m$ of discriminant $d_{Q_m} = 27^2 d_m$. Notice also that $(A_{K_m} : \mathbf{Z}[\theta_m]) = (A_{K_m} : \mathbf{Z}[\rho_m])$ $(A_K : \mathbf{Z}[\theta_m]) = 3(A_{K_m} : \mathbf{Z}[\rho_m])$, that

$$d_{P_m} = d_m = (A_{K_m} : \mathbf{Z}[\rho_m])^2 d_{K_m} \tag{3}$$

and that neither 2 nor 3 divides $d_m = (m^2 + m - 3)^2 - 32$.

Suppose that $A_{K_m} = \mathbf{Z}[\rho_m]$, hence $(A_{K_m} : \mathbf{Z}[\theta_m]) = 3$. Let p be a prime such that p^2 divides d_m. Then $p > 3$, p^2 divides $d_{Q_m} = 27(4p_m^3 - q_m^2)$ and, according to Lemma 1, p divides $3p_m$. Hence, $p > 3$ divides $\gcd(p_m, q_m)$. According to Lemma 2, we obtain $p = 7$ and $m \equiv 3 \pmod 7$. If we had $m \equiv 24 \pmod{7^2}$, then we would have $Q'_m(0) = -3p_m \equiv 0 \pmod 7$ and $Q_m(0) = -q_m \equiv 0 \pmod{7^2}$ and 7 would divide the index $(A_K : \mathbf{Z}[\theta_m]) = 3$ (Lemma 1), a contradiction. Hence, our conditions are indeed necessary conditions. Conversely, if d_m is square-free then $A_{K_m} = \mathbf{Z}[\rho_m]$ (use (3)). Now assume that $m \equiv 3 \pmod 7$, $m \not\equiv 24 \pmod{7^2}$ and that $d_m/7^2$ is square-free. Then, the index $(A_{K_m} : \mathbf{Z}[\rho_m])$ divides 7. Since $P_m(x+1) = x^3 - (m-3)x^2 - (3m-2)x - (2m+1)$ is 7-Eisenstein, 7 does not divide the index $(A_{K_m} : \mathbf{Z}[\rho_m])$ (see [Nar, Lemma 2.2, page 60]). Therefore, $A_{K_m} = \mathbf{Z}[\rho_m]$ and our conditions are indeed sufficient conditions. •

Remark 4 *Let $N(x)$ be the number of rational integers m in the range $4 \leq m \leq x$ for which $d_m = (m^2 + m - 3)^2 - 32$ is square-free. According to*

[Hoo], *it is reasonable to conjecture that as* $x \to +\infty$ *we have*

$$N(x)/x \to \delta := \prod_{p \geq 2}(1 - \frac{n_p}{p^2}) = \frac{6}{7}\prod_{p>7}(1 - \frac{n_p}{p^2}) = 0.839\cdots$$

where n_p *is the number of solutions modulo* p^2 *of the equation* $(m^2+m-3)^2 \equiv 32 \pmod{p^2}$ *(notice* $n_p = 0$ *if* $p \not\equiv \pm 1 \pmod 8$ *and that* $0 \leq n_p \leq 4$ *for* $p \neq 7$*). However, it seems that nothing in the present literature makes it possible to prove this conjecture, or to prove that there are infinitely many simplest non-normal totally real cubic fields* K_m*.*

1.3 Unit groups

Let $d_m = d_{K_m}$ and Reg_m denote the discriminant and regulator of the mth simplest non-normal totally real cubic field K_m. Since $\rho_m + 1$ is a root of $P_m(x-1) = x^3 - (m+3)x^2 + (m+2)x - 1$, then ρ_m and $\rho_m + 1$ are algebraic units of K_m. Let R_m denote the regulator computed from the subgroup generated by $\{-1, \rho_m, \rho_m + 1\}$. Hence,

$$R_m = \left|\det \begin{pmatrix} \log|\rho_m^{(1)}| & \log(|\rho_m^{(1)} + 1|) \\ \log(|\rho_m^{(2)}|) & \log(|\rho_m^{(2)} + 1|) \end{pmatrix}\right|. \tag{4}$$

The reader will check (by using (2) for m large enough and by using (1) for the remaining small values of m) that we have

$$R_m = \log(1/|\rho_m^{(2)}|)\log(\rho_m^{(1)}) + \log(1/(\rho_m^{(2)} + 1))\log(\rho_m^{(1)}) \leq \log^2(m+1) \tag{5}$$

for $m \geq 4$ (and we do not lose much information, for Reg_m is asymptotic to $\log^2 m$ as m goes to infinity). Now, we are in a position to prove the main result of this subsection:

Theorem 5 *For any simplest non-normal totally real cubic field* K_m*,* $m \geq 4$*, we have* $\mathrm{Reg}_m = R_m$*. (Hence,* $\{-1, \rho_m, \rho_m + 1\}$ *generates the full group of algebraic units of* K_m*.)*

Proof. According to [Cus, Theorem 1] the regulator Reg_K of a totally real cubic field of discriminant d_K satisfies

$$\mathrm{Reg}_K \geq \frac{1}{16}\log^2(d_K/4). \tag{6}$$

Using (5) and (6) we obtain $1 \leq R_m/\mathrm{Reg}_m < 2$ and the desired results (for R_m/Reg_m is a positive rational integer). Notice that our result also follows from [Tho, Proposition (3.6)] according to which the system $\{\rho_m, \rho_m + 1\}$ is a fundamental system of units for the order $\mathbf{Z}[\rho_m]$, $m \geq 4$. •

1.4 Statement of our results

We let h_m and Cl_m denote the class number and ideal class group of the mth simplest non-normal totally real cubic field K_m. We let N_m denote the normal closure of K_m. Hence, N_m is a real dihedral sectic field and we let L_m denote the only (real) quadratic subfield of N_m. It is known that there exists an integer $f_m \geq 1$ such that $d_{K_m} = f_m^2 d_{L_m}$ (in particular, $L_m = \mathbf{Q}(\sqrt{d_{K_m}}) = \mathbf{Q}(\sqrt{d_m})$). According to Theorem 3, we have

$$f_m = \begin{cases} 1 & \text{if } m \not\equiv 3 \pmod 7, \\ 7 & \text{if } m \equiv 3 \pmod 7. \end{cases} \tag{7}$$

Theorem 6 *There are* 14 *simplest non-normal totally real cubic fields* K_m *with class number* $h_m \leq 3$*, namely the ones given in* TABLE 1.

TABLE 1

m	d_m	h_m	m	d_m	h_m
4	257	1	11	$16609 = 17 \cdot 977$	2
5	$697 = 17 \cdot 41$	1	12	$23377 = 97 \cdot 241$	2
6	1489	1	13	32009	3
7	2777	2	14	$42817 = 47 \cdot 911$	3
8	4729	1	15	$56137 = 73 \cdot 769$	2
9	7537	2	17	$91777 = 7^2 \cdot 1873$	3
10	$11417 = 7^2 \cdot 233$	3	18	114889	3

To prove this result, we first use a lower bound for the class numbers h_m of the simplest non-normal totally real cubic fields (see Corollary 11) to obtain the upper bound $m \leq 154$ on the indices m of the simplest non-normal totally real cubic fields K_m whose class numbers are ≤ 3. Finally, we will develop a method for computing class numbers of totally real cubic fields, and by computing the class numbers of the 146 simplest non-normal totally real cubic fields K_m, $4 \leq m \leq 154$, we will obtain the desired result.

Theorem 7 *(Similar to* [Lou4, Theorem 13]*).*

1. *(Similar to* [Lou4, Theorems 3 and 12]*). Under the assumption of the generalized Riemann hypothesis for all the real quadratic fields* L_m*'s, the exponent* e_m *of the ideal class group of* K_m *goes to infinity with* m*. More precisely,* $e_m \gg \log m / \log\log m$ *and* $e_m = 2$ *implies* $m \leq 10^8$ *whereas* $e_m = 3$ *implies* $m \leq 1.3 \cdot 10^{13}$*.*

2. *There are* 11 *simplest non-normal totally real cubic fields* K_m *with ideal class groups* Cl_m *of exponent* $e_m \in \{2, 3\}$ *in the range* $4 \leq$

$m \leq 1.3 \cdot 10^{13}$, namely the ones given in TABLE 2. *Hence, under the assumption of the generalized Riemann hypothesis for all the real quadratic number fields L_m's, these* 11 *fields are the only simplest non-normal totally real cubic fields with ideal class groups of exponent ≤ 3.*

TABLE 2

m	d_m	h_m	Cl_m
7	2777	2	[2]
9	7537	2	[2]
10	$11417 = 7^2 \cdot 233$	3	[3]
11	$16609 = 17 \cdot 977$	2	[2]
12	$23377 = 97 \cdot 241$	2	[2]
13	32009	3	[3]
14	$42817 = 47 \cdot 911$	3	[3]
15	$56137 = 73 \cdot 769$	2	[2]
17	$91777 = 7^2 \cdot 1873$	3	[3]
18	114889	3	[3]
21	$210649 = 313 \cdot 673$	4	[2, 2]
38	$2187409 = 7^2 \cdot 44641$	9	[3, 3]

To prove this result, we will use a necessary condition for the exponent of the ideal class group of K_m to be less than or equal to a given exponent e (see Corollary 13).

2 Lower bounds for class numbers

Let K be a totally real cubic field. Let h_K and ζ_K denote the class number and Dedekind zeta function of K and let $\mathrm{Res}_{s=1}(\zeta_K)$ denote the residue at $s = 1$ of this zeta function. We have

$$h_K = \frac{\sqrt{d_K}}{4\mathrm{Reg}_K}\mathrm{Res}_{s=1}(\zeta_K). \tag{8}$$

To obtain lower bounds for h_K we need lower bounds for $\mathrm{Res}_{s=1}(\zeta_K)$. The key Lemma for obtaining such lower bounds is the following one:

Lemma 8 *(See* [Lou6, proof of Lemma 3]*). Let E be a totally real number field of degree $n > 1$. Set $\lambda_n = n(\gamma + \log(4\pi))/2 - 1 > 0$, where $\gamma = 0.577\cdots$ denotes Euler's constant. Let d_E and ζ_E denote the discriminant and Dedekind zeta function of E. Then, $\frac{1}{2} \leq \log\beta < 1$ and $\zeta_E(\beta) \leq 0$ imply*

$$\mathrm{Res}_{s=1}(\zeta_E) \geq (1-\beta)d_E^{(\beta-1)/2}(1+\lambda_n(1-\beta))(1-\frac{2nd_E^{(1-\beta)/2n}}{d_E^{1/2n}}). \tag{9}$$

Lemma 9

1. *Let K be a totally real non-normal cubic field. Let N denote the normal closure of K. Then, N is a totally real dihedral sextic field. Let L denote the only quadratic subfield of N. Then, L is a real quadratic field and $\zeta_N\zeta^2 = \zeta_K^2\zeta_L$, which yields $d_N = d_K^2 d_L$ and*

$$\mathrm{Res}_{s=1}(\zeta_N) = (\mathrm{Res}_{s=1}(\zeta_K))^2 \mathrm{Res}_{s=1}(\zeta_L). \tag{10}$$

   Moreover, $L = \mathbf{Q}(\sqrt{d_K})$. Hence, $d_K = f^2 d_L$ for some positive rational integer f, d_L divides d_K and d_N divides d_K^3.

2. *Let N be a totally real sextic field. If $\zeta_N(1 - (2/\log d_N)) \leq 0$, then*

$$\mathrm{Res}_{s=1}(\zeta_N) \geq \frac{2\epsilon_N}{e \log d_N} \quad \text{with } \epsilon_N = \begin{cases} 0.25 & \text{if } d_N \geq 6 \cdot 10^{14} \\ 1 & \text{if } d_N \geq 8 \cdot 10^{20} \end{cases} \tag{11}$$

3. *Let N be a totally real number field of degree $n > 1$ and discriminant $d_N \geq (12n/5)^{2n} e^2$. Then, $1 - (2/\log d_N) \leq \beta < 1$ and $\zeta_N(\beta) = 0$ imply*

$$\mathrm{Res}_{s=1}(\zeta_N) \geq \frac{1-\beta}{6e}. \tag{12}$$

4. *(See* [Lou3, Corollaire 5A(a)]*). Set $\kappa = 2 + \gamma - \log(4\pi) = 0.046\cdots$, where $\gamma = 0.577\cdots$ denotes Euler's constant. Let L be a real quadratic field. Then,*

$$\mathrm{Res}_{s=1}(\zeta_L) \leq \frac{1}{2}(\log d_L + \kappa). \tag{13}$$

   Moreover (see [Lou3, Corollaire 7B]*), $\frac{1}{2} \leq \beta < 1$ and $\zeta_L(\beta) = 0$ imply*

$$\mathrm{Res}_{s=1}(\zeta_L) \leq \frac{1-\beta}{8} \log^2 d_L. \tag{14}$$

Proof. Only the second and third points need proofs.
To obtain (11), we choose $E = N$ (for which $n = 6$) and $\beta = 1 - (2/\log d_N)$ in (9). We obtain

$$\mathrm{Res}_{s=1}(\zeta_N) \geq \frac{2g(d_N)}{e \log d_N}$$

where

$$g(x) := (1 + \frac{2\lambda_6}{\log x})(1 - \frac{12e^{1/6}}{x^{1/12}})$$

satisfies $g(x) \geq 0.25$ for $x \geq 6 \cdot 10^{14}$ and $g(x) \geq 1$ for $x \geq 8 \cdot 10^{20}$.
To obtain (12), we choose $E = N$ (for which $n = 6$) in (9). We obtain

$$\mathrm{Res}_{s=1}(\zeta_N) \geq \frac{1-\beta}{e} h(d_N)$$

where $h(x) := 1 - 2ne^{1/n}x^{-1/2n}$ satisfies $h(x) \geq 1/6$ for $x \geq (12n/5)^{2n}e^2$. •

We are now in a position to prove the following roughly speaking 10-fold improvement on [Lou3, Theorem 1]:

Theorem 10 *Let K be a non-normal totally real cubic field. Then*

$$h_K \mathrm{Reg}_K \geq \frac{\epsilon_K \sqrt{d_K}}{2\sqrt{3e}(\log d_K + \kappa)} \quad \textit{with } \epsilon_K = \begin{cases} 0.5 & \textit{if } d_K \geq 11 \cdot 10^6 \\ 1 & \textit{if } d_K \geq 13 \cdot 10^9 \end{cases} \tag{15}$$

where $\kappa = 2 + \gamma - \log(4\pi) = 0.046\cdots$. Notice that $2\sqrt{3e} = 5.711\cdots$.

Proof. First, assume that $\zeta_L(1 - (2/\log d_N)) \leq 0$. Then, according to the first point of Lemma 9 we have $\zeta_N(1 - (2/\log d_N)) \leq 0$ and $d_N \leq d_K^3$, and we obtain

$$\begin{aligned} \frac{2\epsilon_N}{3e(\log d_K + \kappa)} \leq \frac{2\epsilon_N}{3e \log d_K} &\leq \frac{2\epsilon_N}{e \log d_N} \\ &\leq \mathrm{Res}_{s=1}(\zeta_N) \quad (\text{by (11)}) \\ &= (\mathrm{Res}_{s=1}(\zeta_K))^2 \mathrm{Res}_{s=1}(\zeta_L) \quad (\text{by (10)}) \\ &\leq \frac{1}{2}(\log d_L + \kappa)(\mathrm{Res}_{s=1}(\zeta_K))^2 \quad (\text{by (13)}) \\ &\leq \frac{1}{2}(\log d_K + \kappa)(\mathrm{Res}_{s=1}(\zeta_K))^2 \end{aligned}$$

and setting $\epsilon_K = \sqrt{\epsilon_N}$, we obtain

$$\mathrm{Res}_{s=1}(\zeta_K) \geq \epsilon_K \frac{2}{\sqrt{3e}(\log d_K + \kappa)}. \tag{16}$$

Second, assume that $\zeta_L(1 - (2/\log d_N)) > 0$. Then, there exists β in the range $1 - (2/\log d_N) \leq \beta < 1$ such that $\zeta_L(\beta) = 0$. According to the first point of Lemma 9, we have $\zeta_N(\beta) = 0 \leq 0$, and we obtain

$$\begin{aligned} \frac{1-\beta}{6e} &\leq \mathrm{Res}_{s=1}(\zeta_N) \quad (\text{for } d_N \geq 6 \cdot 10^{14}, \text{ by (12)}) \\ &= (\mathrm{Res}_{s=1}(\zeta_K))^2 \mathrm{Res}_{s=1}(\zeta_L) \quad (\text{by (10)}) \\ &\leq \frac{1-\beta}{8}(\mathrm{Res}_{s=1}(\zeta_K))^2 \log^2 d_L \quad (\text{by (14)}) \\ &\leq \frac{1-\beta}{8}(\mathrm{Res}_{s=1}(\zeta_K))^2 \log^2 d_K \end{aligned}$$

and

$$\mathrm{Res}_{s=1}(\zeta_K) \geq \frac{2}{\sqrt{3e}\log d_K}. \tag{17}$$

Since (17) is always better than (16), we conclude that (16) is always valid and, using (8), we obtain the desired results (as for the lower bounds for d_K after which $\epsilon_K = \sqrt{\epsilon_N} \geq 0.5$ or $\epsilon_K = \sqrt{\epsilon_N} \geq 1$, they follow from the lower bounds for d_N after which $\epsilon_N \geq 0.25$ or $\epsilon_N \geq 1$ given in (11), once we notice that $d_N = d_K^2 d_L \geq 5d_K^2$ yields $d_N \geq 6 \cdot 10^{14}$ for $d_K \geq 11 \cdot 10^6$ and $d_N \geq 8 \cdot 10^{20}$ for $d_K \geq 13 \cdot 10^9$). •

Corollary 11 *Let h_m denote the class number of the mth simplest non-normal totally real cubic field K_m, $m \geq 4$. Then*

$$h_m \geq \frac{\epsilon_m \sqrt{d_m}}{2\sqrt{3e}(\log(m+1))^2(\log d_m + \kappa)} \quad \textit{with } \epsilon_m = \begin{cases} 0.5 & \textit{if } m \geq 24 \\ 1 & \textit{if } m \geq 76 \end{cases} \tag{18}$$

where $\kappa = 2 + \gamma - \log(4\pi) = 0.046\cdots$. Moreover, if $h_m \leq 3$ then $m \leq 154$.

Proof. According to (11) and Theorem 5, we have $\mathrm{Reg}_{K_m} \leq \log^2(m+1)$. (As for the lower bounds for m after which $\epsilon_m = \epsilon_{K_m} = \sqrt{\epsilon_{N_m}} \geq 0.5$ or $\epsilon_m = \epsilon_{K_m} = \sqrt{\epsilon_{N_m}} \geq 1$, they follow from the lower bounds for d_N after which $\epsilon_N \geq 0.25$ or $\epsilon_N \geq 1$ given in (11), once we notice that $d_{N_m} = d_{K_m}^2 d_{L_m} = d_{K_m}^3 / f_m^2 \geq d_{K_m}^3/7^2 = d_m^3/7^2$ (by (7)) yields $d_{N_m} \geq 6 \cdot 10^{14}$ for $m \geq 24$ and $d_{N_m} \geq 8 \cdot 10^{20}$ for $m \geq 76$.) •

3 Rigorous computation of class numbers

Let K be a cubic number field. Then $(\zeta_K/\zeta)(s) = \sum_{n\geq 1} \phi_n n^{-s}$ is entire, regardless of whether K is a normal or non-normal. Therefore, we can use the analytic class number formula (e.g. (8)) and the rigorous method delineated in [Lou2] to compute the class numbers h_K of cubic fields K of known regulators. From now on we let K denote a totally real cubic number field and we stick to the notation set in [Lou2].

1. Set

$$K_{(2,0,0)}(X) := \frac{X}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} \Gamma^2(s) X^{-2s} \left(\frac{1}{s} + \frac{1}{s - (1/2)} \right) ds$$

(for $X > 0$ and $\alpha > 1$). Using [Lou2, Proposition 1, point (a)], we obtain:

$$\begin{aligned} 0 < K_{(2,0,0)}(X) &\leq 2I_{(2,0,0)}(X) \\ &= 2\int_X^\infty H_{(2,0,0)}(x)dx \\ &= 4\int_X^\infty H_{(0,0,2)}(x)dx \leq 8\int_X^\infty e^{-x}\frac{dx}{x} \leq 8e^{-X}/X. \end{aligned}$$

Setting $A_K = \sqrt{d_K/\pi^2}$, we therefore obtain the following rapidly convergent series expansion

$$\mathrm{Res}_{s=1}(\zeta_K) = \frac{1}{\pi}\sum_{n\geq 1}\frac{\phi_n}{n}K_{(2,0,0)}(n/A_K) \tag{19}$$

(use (5) of [Lou2]). Moreover, arguing as in the proof of [Lou2, Proposition 4], we obtain the rapidly convergent series expansion

$$K_{(2,0,0)}(X) = \pi + a_0(X)X + \sum_{n\geq 1} a_n(X)\frac{X^{2n+1}}{(n!)^2} \tag{20}$$

where

$$a_0(X) := 2\log^2 X + 4(\gamma+1)\log X + \frac{\pi^2}{6} + 2\gamma^2 + 4\gamma - 4,$$

$$a_n(X) := \left(\frac{2}{n} + \frac{2}{n+0.5}\right)\left(\log X + \gamma - \sum_{k=1}^{n}\frac{1}{k}\right) - \left(\frac{1}{n^2} + \frac{1}{(n+0.5)^2}\right)$$

and where $\gamma = 0.577215\cdots$ denotes Euler's constant. Let us now detail how to use (8), (19) and (20) for computing h_K.

2. Since $n \mapsto \phi_n$ is multiplicative we only have to explain how to compute ϕ_{p^k} on prime powers. We have $\phi_{p^k} = F(p^k) - F(p^{k-1})$ where $F(n)$ is the number of distinct integral ideals of K with norm $n \geq 1$. From now on we also assume that K is not normal, we let L denote the real quadratic subfield of the normal closure of K and recall that there exists an integer $f \geq 1$ such that $d_K = f^2 d_L$. With this notation and letting (a/b) denote Kronecker's symbol, we give in TABLE 3 the values of ϕ_{p^k}.

TABLE 3
First cases: p does not divide d_K

case	(p)	remark	k	$F(p^k)$	ϕ_{p^k}
I	$\mathcal{P}$	$(\frac{d_K}{p}) = +1$	$k \equiv 0 \pmod 3$	1	1
			$k \equiv 1 \pmod 3$	0	-1
			$k \equiv 2 \pmod 3$	0	0
II	$\mathcal{P}_1\mathcal{P}_2$	$(\frac{d_K}{p}) = -1$	$k \equiv 0 \pmod 2$	$(k+2)/2$	1
			$k \equiv 1 \pmod 2$	$(k+1)/2$	0
III	$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$	$(\frac{d_K}{p}) = +1$	any	$(k+1)(k+2)/2$	$k+1$

Next cases: p divides $d_K = f^2 d_L$

case	(p)	remark	k	$F(p^k)$	ϕ_{p^k}
IV	$\mathcal{P}_1^2\mathcal{P}_2$	p does not divide f	any	$k+1$	1
V	$\mathcal{P}^3$	p divides f	any	1	0

In particular, if $(\frac{d_K}{n}) = -1$ then $\phi_n = 0$.

3. According to TABLE 3, for any prime power we have $|\phi_{p^k}| \le k+1 = d(p^k)$, where $d(n)$ denotes the number of positive divisors of $n \ge 1$. Since $n \mapsto d(n)$ and $n \mapsto \phi_n$ are multiplicative, we obtain $|\phi_n| \le d(n)$ for any $n \ge 1$. Set $S_N(n) = \sum_{k=N+1}^{n} = \frac{d(k)}{k^2}$ for $n > N$, and $S_N(N) = 0$. Using $0 < K_{(2,0,0)}(X) \le 8e^{-X}/X$ we obtain

$$\begin{aligned}
R_K(N) &:= \Big|\sum_{n>N} \frac{\phi_n}{n} K_{(2,0,0)}(n/A_K)\Big| \\
&\le 8A_K \sum_{n>N} \frac{d(n)}{n^2} e^{-n/A_K} \\
&= 8A_K \sum_{n>N} (S_N(n) - S_N(n-1)) e^{-n/A_K} \\
&= 8A_K \sum_{n>N} S_N(n)(e^{-n/A_K} - e^{-(n+1)/A_K}) \\
&\le 8A_K S_N(\infty) \sum_{n>N} (e^{-n/A_K} - e^{-(n+1)/A_K}) \\
&= 8A_K S_N(\infty) e^{-(N+1)/A_K}.
\end{aligned}$$

Since

$$S(x) := \sum_{1\le k\le x} \frac{d(k)}{k} \le (\sum_{1\le k\le x} \frac{1}{k})^2 \le \log^2(ex)$$

and since

$$\begin{aligned} S_N(\infty) &= \sum_{n>N} \frac{S(n)-S(n-1)}{n} \\ &\leq \sum_{n>N} \frac{S(n)}{n(n+1)} \\ &\leq \sum_{n>N} \frac{\log^2(en)}{n(n+1)} \\ &\leq \int_N^{\infty} \frac{\log^2(et)}{t^2} dt = \frac{\log^2(eN)+2\log(eN)+2}{N}, \end{aligned}$$

we obtain

$$R_K(N) \leq 8A_K(\log(eN)+2)^2 e^{-N/A_K}/N. \tag{21}$$

Hence, according to (6), (8) and (21), for a given $\lambda > 1$ we can compute the integer h_K by disregarding in (19) the indices $n > \lambda A_K \log A_K$, provided that d_K is large enough.

4. Let p be a given prime satisfying $(\frac{d_K}{p}) = +1$. Assume that the ring of algebraic integers of K is generated by an algebraic integer ρ_K (e.g. assume that K is a simplest non-normal totally real cubic number field), or more generally assume that $K = \mathbf{Q}(\rho_K)$ for some algebraic integer $\rho_K \in K$ such that p does not divide the index $(A_K : \mathbf{Z}[\rho_K])$. Let $P_K(x)$ denote the minimum polynomial over $\mathbf{Q}$ of ρ_K. Then, we are in case I or in case III of TABLE 3 according as $P_K(x)$ does not have or has at least one root modulo p. To compute h_K, we therefore have to test whether the polynomial $P_K(x)$ has at least one root modulo p for all the primes $p \leq \lambda A_K \log A_K$ such that $(d_K/p) = +1$. We will explain in Subsection 3.1 below how to do that in an efficient way which will provide us with a rigorous method for computing class numbers h_K of non-normal totally real cubic fields K of known regulators in $O({d_K}^{0.5+\epsilon})$ elementary operations.

5. Notice finally that $p = 2$ is always inert in any simplest non-normal totally real cubic field K_m. Moreover, for any simplest non-normal totally real cubic field K_m we have $f_m \in \{1, 7\}$ (see (7)).

According to Corollary 11 and to class number computations based on the present method, only 14 simplest non-normal totally real cubic fields K_m have class number $h_m \leq 3$: the 14 ones which appear in TABLE 1, which completes the proof of Theorem 6.

3.1 When does $P_m(x)$ has a root modulo a prime p?

Throughout this subsection, $p > 3$ denotes a prime satisfying $(\frac{d_m}{p}) = +1$. We explain how one can efficiently check whether $P_m(x)$ has at least one root modulo p, i.e., whether we are in Case I or Case III of TABLE 3. To begin with, we notice that it is easier to work with $Q_m(y) = y^3 - 3p_m y - q_m$ of discriminant $27\Delta_m$ with $\Delta_m = 4p_m^3 - q_m^2 = 27d_m$ and that for $p \neq 3$ the polynomial $P_m(x)$ has at least one root modulo p if and only if the polynomial $Q_m(y)$ has at least one root modulo p (see subsection 1.1). Let $\mathbf{F}_p \subseteq \mathbf{F}_{p^2}$ denote the finite fields with p and p^2 elements, respectively. Notice that $Q_m(x)$ has at least one root modulo p if and only if it has at least one root in $\mathbf{F}_{p^2}$. If p divides p_m then $Q_m(y)$ has at least one root modulo p if and only if q_m is a cube in $\mathbf{F}_p$, hence if and only if $q_m^{(p-1)/3} = 1$ in $\mathbf{F}_p$. Now, assume that $p > 3$ does not divide p_m. According to Cardan's formulae (notice that $\mathbf{F}_{p^2}$ always contains the cubic roots of unity), $Q_m(y)$ has at least one root in $\mathbf{F}_{p^2}$ if and only if $(q_m + \sqrt{-\Delta_m})/2$ is a cube in $\mathbf{F}_{p^2}$, hence if and only if $((q_m + \sqrt{-\Delta_m})/2)^{(p^2-1)/3} = 1$ in $\mathbf{F}_{p^2}$. (Notice that since p does not divide p_m and since $((q_m + \sqrt{-\Delta_m})/2)((q_m - \sqrt{-\Delta_m})/2) = (q_m^2 + \Delta_m)/4 = p_m^3$, the fact that $(q_m + \sqrt{-\Delta_m})/2$ is a cube in $\mathbf{F}_{p^2}$ does not depend on the choice of $\sqrt{-\Delta_m}$ in $\mathbf{F}_{p^2}$.) Finally, since $(\frac{d_m}{p}) = +1$, we have $\sqrt{d_m} \in \mathbf{F}_p$. Hence, $\sqrt{-\Delta_m} \in \mathbf{F}_p \Leftrightarrow \sqrt{-3} \in \mathbf{F}_p \Leftrightarrow (\frac{-3}{p}) = +1 \Leftrightarrow p \equiv 1 \pmod 6$ and we obtain:

1. If $p \equiv 1 \pmod 6$, then $\sqrt{-\Delta_m} \in \mathbf{F}_p$ and $((q_m + \sqrt{-\Delta_m})/2)^{(p^2-1)/3} = 1$ in $\mathbf{F}_{p^2}$ if and only if $((q_m + \sqrt{-\Delta_m})/2)^{(p-1)/3} = 1$ in $\mathbf{F}_p$.
2. If $p \equiv 5 \pmod 6$, then $\sqrt{-\Delta_m} \notin \mathbf{F}_p$ and by using the 2-adic development of the exponent $(p^2-1)/3$ we compute in $O(\log p)$ elementary operations in $\mathbf{F}_p$ the coordinates $a \in \mathbf{F}_p$ and $b \in \mathbf{F}_p$ of $(q_m + \sqrt{-\Delta_m})^{(p^2-1)/3} = a + b\sqrt{-\Delta_m}$. We obtain $(q_m + \sqrt{-\Delta_m})^{(p^2-1)/3} = 1$ in $\mathbf{F}_{p^2}$ if and only if $a = 1$ and $b = 0$ in $\mathbf{F}_p$.

4 A necessary condition for class group problems

Theorem 12 *(Similar to* [LP, Th. 1] *and* [Lou4, Prop. 11]*). Assume that $m \geq 60$. Then, for all $\alpha \in \mathbf{Z}[\rho_m]$ either $|N_{K_m/\mathbf{Q}}(\alpha)| \geq 2m - 5$, or α is associated to an integer. (Notice that $N_{K_m/\mathbf{Q}}(1 + 2\rho_m) = -(2m-5)$.)*

Proof. Since $\rho_m^{-1} = \rho_m^2 - m\rho_m - (m+1)$, we deduce that $\{1, \rho_m, \rho_m^{-1}\}$ is a $\mathbf{Z}$-basis of $\mathbf{Z}[\rho_m]$. For $\alpha \in K_m$, let $\alpha = \alpha^{(1)}$, $\alpha' = \alpha^{(2)}$ and $\alpha'' = \alpha^{(3)}$ denote

the conjugates of α and set

$$\Delta(\alpha,\beta,\gamma) := \begin{vmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{vmatrix}.$$

Let $c_1 > 0$ and $c_2 > 0$ be given and let η_1 and η_2 be two given multiplicatively independent units of $\mathbf{Z}[\rho_m]$. According to [LP], for any $\alpha \in \mathbf{Z}[\rho_m]$ there exists η in the group of units generated by η_1 and η_2 such that

$$\begin{aligned} \log c_1 \le \log(|\alpha\eta|) < \log c_1 + |\log|\eta_1|| + |\log|\eta_2||, \\ \log c_2 \le \log(|\alpha'\eta'|) < \log c_2 + |\log|\eta_1'|| + |\log|\eta_2'||. \end{aligned}$$

In particular, in choosing $\eta_1 = \rho_m + 1$ and $\eta_2 = (\rho_m+1)/\rho_m$ (for which $|\eta_1| = \eta_1 = \rho_m + 1 > 1$, $|\eta_2| = \eta_2 = (\rho_m+1)/\rho_m > 1$, $|\eta_1'| = \rho_m' + 1 < 1$ and $|\eta_2'| = -(\rho_m'+1)/\rho_m' > 1$), we obtain that for any $\alpha \in \mathbf{Z}[\rho_m]$ there exists a unit $\eta \in \mathbf{Z}[\rho_m]^*$ such that

$$c_1 \le |\alpha\eta| < c_1(\rho_m+1)^2/\rho_m \ \text{ and } c_2 \le |\alpha'\eta'| < c_2/|\rho_m'|. \tag{22}$$

Now, if $\alpha = a + b\rho_m + c\rho_m^{-1} \in \mathbf{Z}[\rho_m]$ with a, b and c rational, then $b = \Delta(1,\alpha,\rho_m^{-1})/\Delta(1,\rho_m,\rho_m^{-1})$ and $c = \Delta(1,\rho_m,\alpha)/\Delta(1,\rho_m,\rho_m^{-1})$. Set $N = |N_{K_m/\mathbf{Q}}(\alpha)|$ and assume that $N \le 2m-5$. We may assume that α satisfies (22). Noticing that $|\alpha''| = N/|\alpha\alpha'| \le N/(c_1c_2)$ and that $\Delta(1,\rho_m,\rho_m^{-1}) = -\sqrt{d_m}$, we obtain

$$\begin{aligned} |b|\sqrt{d_m} &= |\Delta(1,\alpha,\rho_m^{-1})| \\ &= |\alpha(\rho_m'^{-1} - \rho_m''^{-1}) + \alpha'(\rho_m''^{-1} - \rho_m^{-1}) + \alpha''(\rho_m^{-1} - \rho_m'^{-1})| \\ &= |\alpha\rho_m(\rho_m'' - \rho_m') + \alpha'\rho_m'(\rho_m - \rho_m'') + \alpha''\rho_m''(\rho_m' - \rho_m)| \\ &\le c_1(\rho_m+1)^2|\rho_m'' - \rho_m'| + c_2|\rho_m - \rho_m''| + N|\rho_m''(\rho_m' - \rho_m)|/(c_1c_2) \\ &\le c_1(m+3)^2 + c_2(m+2) + (m+2)(2m-5)/(c_1c_2) \end{aligned}$$

(use $|\rho_m| < m+2$, $|\rho_m''| < 1$, $|\rho_m'' - \rho_m'| < 1$, $|\rho_m - \rho_m''| < m+2$ and $|\rho_m' - \rho_m| < m+2$ for $m \ge 4$, which follow from (2)) and

$$\begin{aligned} |c|\sqrt{d_m} &= |\Delta(1,\rho_m,\alpha)| \\ &= |\alpha(\rho_m'' - \rho_m') + \alpha'(\rho_m - \rho_m'') + \alpha''(\rho_m' - \rho_m)| \\ &\le |\alpha| + (m+2)|\alpha'| + (m+2)|\alpha''| \\ &\le c_1(m+4) + c_2(m+1)(m+2) + (m+2)(2m-5)/(c_1c_2) \end{aligned}$$

which for $c_2 = c_1 = c_0 := 4^{1/3}$ yield $|b| \leq c_0(6m^2+27m+34)/(4\sqrt{d_m})$ and $|c| \leq c_0(6m^2+15m+14)/(4\sqrt{d_m})$, hence yield $|b| < 3$ for $m \geq 15$ and $|c| < 3$ for $m \geq 8$. Now, as in [LP], we could look at the $\alpha = a+b\rho_m+c\rho_m^{-1} \in \mathbf{Z}[\rho_m]$ with a, b and c rational and $|b| \leq 2$ and $|c| \leq 2$. However, we found it easier to choose $c_1 = 15$ and $c_2 = 1/3$ which yield $|b| < 17$ and $|c| < 1$ for $m \geq 60$, hence yield $|b| \leq 16$ and $c = 0$ for $m \geq 60$. Now, we look at the $\alpha = a - b\rho_m \in \mathbf{Z}[\rho_m]$ with a and b rational and $|b| \leq 10$. Since α is a rational integer for $b = 0$ and since $-\alpha$ is associated with α, we may assume that we have $1 \leq b \leq 16$. Now,

$$N_{K_m/\mathbf{Q}}(a - b\rho_m) = b^3 P_m(a/b) = a^3 - ma^2b - (m+1)ab^2 - b^3 := R_b(a),$$

the zeros of $a \mapsto R_b(a)$ are $b\rho_m$, $b\rho'_m$ and $b\rho''_m$, for $2 \leq b \leq 16$ and $m \geq 16$ we have

$$-b < b\rho''_m < -b+1 \leq -1 < b\rho'_m < 0 < b(m+1) < b\rho_m < b(m+1)+1$$

(use (2)), for $b = 1$ and $m \geq 4$ we have

$$-b < b\rho''_m < 0 < b(m+1) < b\rho_m < b(m+1)+1$$

and we may finally assume that $a \notin \{-b, 0, b(m+1)\}$, for otherwise $\alpha = a - b\rho_m$ is associated to the integer b. Hence, for $2 \leq b \leq 16$ and $m \geq 16$ we have

$$\begin{aligned} |N_{K_m/\mathbf{Q}}(a - b\rho_m)| \quad \geq \quad & \min\{-R_b(-b-1), R_b(-b+1), R_b(-1), -R_b(1), \\ & -R_b(b(m+1)-1), R_b(b(m+1)+1)\} \end{aligned}$$

and for $b = 1$ and $m \geq 4$ we have

$$\begin{aligned} |N_{K_m/\mathbf{Q}}(a - b\rho_m)| \quad \geq \quad & \min\{-R_b(-b-1), -R_b(1), \\ & -R_b(b(m+1)-1), R_b(b(m+1)+1)\}. \end{aligned}$$

We deduce the desired result from the fact that
$R_b(b(m+1)+1) = b^2m^2 + (3b^2+2b)m - b^3 + 2b^2 + 3b + 1$,
$-R_b(b(m+1)-1) = b^2m^2 + (3b^2-2b)m + b^3 + 2b^2 - 3b + 1$,
$-R_b(1) = (b^2+b)m + (b^3+b^2-1)$,
and $-R_b(-b-1) = (b^2+b)m + b^3 + 2b^2 + 3b + 1$ are all greater than $2m-5$ in the range $m \geq 60 > 16 \geq b \geq 1$, and from the fact that
$R_b(-1) = (b^2-b)m - b^3 + b^2 - 1$
and $R_b(-b+1) = (b^2-b)m - b^3 + 2b^2 - 3b + 1$ are all greater than or equal to $2m-5$ in the range $m \geq 60 > 16 \geq b \geq 2$. •

Corollary 13 *Let e_m denote the exponent of the ideal class group of the mth simplest non-normal totally real cubic field K_m, $m \geq 60$.*

1. *If $p < (2m-5)^{1/e_m}$ is a prime for which we are not in case I of* TABLE 3, Section 3, *then we are in case V of* TABLE 3, Section 3. *In other words, if $P_m(x)$ has at least one root modulo p for some prime p satisfying $2 \leq p < (2m-5)^{1/e_m}$, then $p = 7$ and $m \equiv 3 \pmod 7$.*

2. *Let L_m denote the real quadratic subfield of the normal closure N_m of K_m. We have $(\frac{d_{L_m}}{p}) = +1$ for all the primes p satisfying $2 \leq p < (2m-5)^{1/e_m}$.*

Proof. Let $p \geq 2$ be a prime less than $(2m-5)^{1/e_m}$.

1. Since we are not in case I, there is some prime ideal $\mathcal{P}$ of norm p above p. Assume that we are not in case V. Then, there exists another prime ideal above p and by using the uniqueness of the prime ideal factorization of an ideal, we obtain that the principal ideal $\mathcal{P}^{e_m} = (\alpha)$ is generated by an algebraic integer α of K_m which is not associated to an integer. Therefore, $p^{e_m} = N_{K_m/\mathbf{Q}}(\mathcal{P}^{e_m}) = |N_{K_m/\mathbf{Q}}(\alpha)| \geq 2m-5$ (Theorem 12). A contradiction. Therefore, we are in Case V, hence p divides f_m, and according to (7) we obtain the desired result.

2. If we are in case I then $(\frac{d_{K_m}}{p}) = +1$. Since $d_{K_m} = f_m^2 d_{L_m}$ we do have $(\frac{d_{L_m}}{p}) = +1$. If we are not in case I, then $p = 7$ and $m \equiv 3 \pmod 7$. Write $m = 3 + 7\lambda$. Then $d_m/7^2 = ((m^2+m-3)^2 - 32)/7^2 \equiv (2\lambda+1)^2 \pmod 7$. Since $m \not\equiv 24 \pmod{49}$, we have $2\lambda + 1 \not\equiv 0 \pmod 7$. Since $d_{K_m} = d_m = f_m^2 d_{L_m}$ we have $d_{L_m} = d_m/7^2$ and $(\frac{d_{L_m}}{p}) = (\frac{d_m/7^2}{7}) = (\frac{(2\lambda+1)^2}{7}) = +1$. •

5 A sieving algorithm

Let $2 = p_1 < p_2 < \cdots < p_m < \cdots$ be the increasing sequence of primes. For each prime $p \geq 2$, let $f_p \geq 1$ be a positive rational integer and let $\mathcal{P}_p(m)$ be a property defined for all $m \geq m_0$ and whose truth value depends only on m modulo f_p. We also assume that for each prime p there exists some $m \geq m_0$ such that $\mathcal{P}_p(m)$ is false. For each integer $k \geq 1$ we then set

$$Min_k = \min\{m \geq m_0;\ \text{all the } \mathcal{P}_{p_i}(m) \text{ are false for } 1 \leq i \leq k\}.$$

We describe an easy to implement algorithm which for a given $k_1 \geq 1$ of reasonable size computes inductively the Min_k for $1 \leq k \leq k_1$.

Suppose that, for some $k < k_1$, we have already computed the n_k classes $m_k(j)$, $1 \leq j \leq n_k$, of m modulo $\pi_k = \prod_{i=1}^{k} f_{p_i}$ such that all the $\mathcal{P}_{p_i}(m)$ are false for $1 \leq i \leq k$ if and only if there exists $j \in \{1, 2, \cdots, n_k\}$ such that $m \equiv m_k(j) \pmod{\pi_k}$. We assume that $m_0 \leq m_k(1) < m_k(2) < \cdots < m_k(f_k)$. Hence, $Min_k = m_k(1)$. Let us explain how to compute n_{k+1} and the $m_{k+1}(j)$, $1 \leq j \leq n_{k+1}$. We set

$$E_k = \{m_k(j) + \lambda \pi_k;\ 1 \leq j \leq n_k,\ 0 \leq \lambda \leq p_{k+1} - 1\},$$

we let m range over the $p_{k+1} n_k$ elements of E_k and keep track only of those $m \in E_k$ for which $\mathcal{P}_{p_{k+1}}(m)$ is false (since the $\mathcal{P}_i(m)$ depends on m modulo f_i only, for any $m \in E_k$ all the $\mathcal{P}_{p_i}(m)$ are false for $1 \leq i \leq k$). In practice, n_k goes to infinity with k very fast (roughly speaking, we may expect each $\mathcal{P}_i(m)$ to be false for $f_i/2$ of the f_i classes modulo f_i. Hence, we may expect n_k to be round $\pi_k/2^k$). Therefore, depending on how much space we are able to allocate to the storage of the $m_k(j)$, we must stop our computation at some small index k_0. To compute inductively the Min_{k+1} for $k_0 \leq k < k_1$, we then use the naïve algorithm which consists to let $m \geq Min_k$ range only modulo the n_{k_0} classes modulo π_{k_0} defined by the set E_{k_0} and we check whether all the $\mathcal{P}_i(m)$, $k_0 < i \leq k+1$ are false. This is roughly speaking f_{k_0}/n_{k_0} times faster than sieving all the integers m, and we might expect f_{k_0}/n_{k_0} to be round 2^{k_0}. Of course, we first fill in a table $Test(m, i) = \mathcal{P}_{p_i}(m \bmod f_i)$ for $0 \leq m \leq f_i - 1$ and $1 \leq i \leq k_1$.

In our situation (see Point 1 of Corollary 13), we let $\mathcal{P}_2(m)$ be false for any $m \geq 4$, we define $\mathcal{P}_7(m)$ to be true if and only if [$m \not\equiv 3 \pmod{7}$ and $P_m(x)$ has at least one root modulo p], we define $\mathcal{P}_p$ for $p \neq 2, 7$ to be true if and only if $P_m(x)$ has at least one root modulo p. Hence, $f_2 = 1$ and $f_p = p$ for all the primes $p \geq 3$. With that choice for the $\mathcal{P}_p$'s, $m > (p_k^{e_m} + 5)/2$ implies $(2m-5)^{1/e_m} > p_k$, hence implies $m \geq Min_k$ (use Point 1 of Corollary 13), i.e.,

$$m > (p_k^{e_m} + 5)/2 \text{ implies } m \geq Min_k. \tag{23}$$

We chose $k_0 = 8$, $k_1 = 32$ and computed TABLE 4 (notice that $f_{k_0}/n_{k_0} = 1052.266\cdots$. (See also [LPW] and [GMW] for other examples of similar Tables). Now, assume that $e_m \in \{2, 3\}$. According to (23) and TABLE 4, $m \geq 25329 = (p_{12}^3 + 5)/2$ implies $m \geq Min_{12} = 120933$, hence implies $m > 113943 = (p_{18}^3 + 5)/3$, hence implies $m \geq Min_{18} = 31104036$, hence implies $m > 29431937 = (p_{72}^3 + 5)/2$, hence implies $m \geq Min_{72} \geq Min_{29} >$

$1.3 \cdot 10^{13}$. To sum up,

$$e_m \in \{2,3\} \text{ and } m \geq 25329 \text{ imply } m > 1.3 \cdot 10^{13}.$$

TABLE 4

k	p_k	π_k	n_k	Min_k	k	p_k	Min_k
1	2	1	1	4	17	59	31104036
2	3	3	2	5	18	61	31104036
3	5	15	4	6	19	67	157973558
4	7	105	8	8	20	71	502966203
5	11	1155	32	26	21	73	502966203
6	13	15015	192	26	22	79	731476488
7	17	255255	768	411	23	83	731476488
$k_0 = 8$	19	4849845	4608	1338	24	89	731476488
9	23			1338	25	97	34782715941
10	29			1338	26	101	224438601896
11	31			6021	27	103	859096423843
12	37			120993	28	107	2360271004106
13	41			120993	29	109	15237756589091
14	43			976221	30	113	15445624974333
15	47			2806203	31	127	15445624974333
16	53			3402656	32	1	19226470646643

Remark 14 *We could have chosen the slightly more complicated property $\mathcal{P}_7(m)$ to be true if and only if [[$m \not\equiv 3 \pmod 7$ or $m \equiv 24 \pmod{49}$] and $P_m(x)$ has at least one root modulo p], in which case we would have had $f_7 = 49$.*

6 The exponent 2 or 3 class group problems

Let us finally prove Theorem 7. We will use:

Theorem 15 *(See* [Ba, Theorem 2]*). Let L be real quadratic number field of discriminant d_L. Under the assumption of the Generalized Riemann hypothesis for L, if $(\frac{d_L}{p}) = +1$ for all primes $p < x$ then $x < 2\log^2 d_L$.*

1. Point 1 of Theorem 7 follows from Point 2 of Corollary 13 and Theorem 15 according to which (use $d_{L_m} \leq d_{K_m} = d_m$) we have:

$$e_m > \log(2m-5)/\log(2\log^2 d_{L_m}) \geq \log(2m-5)/\log(2\log^2 d_m)$$

(under the assumption of the Generalized Riemann Hypothesis for all the L_m's).

2. Let us now prove Point 2 of Theorem 7. According to the end of the previous section, $e_m \in \{2,3\}$ and $m \leq 1.3 \cdot 10^{13}$ imply $m \leq 25328$. Now, there are only 199 values of $m \leq 25328$ for which either $4 \leq m < 60$, or $m \geq 60$ and the necessary conditions of the first point of Corollary 13 are satisfied. Only 195 out of these 199 possible values of m are such that K_m is a simplest non-normal totally real cubic field, the largest one is $m = 23378$ (for the four excluded values $m \in \{156, 281, 453, 1898\}$ we have $m \not\equiv 3 \pmod 7$ and d_m is not square-free). For only 14 out of these 195 values of m is h_m either a perfect 2-power greater than 2 (namely, for $m \in \{21, 23, 26, 27, 37, 40, 44, 54, 57\}$) or a perfect 3-power greater than 3 (namely, for $m \in \{22, 38, 41, 52, 158\}$). By computing the class group structures of the 14 associated K_m's (by using Pari), we obtained TABLE 5 and therefore get the desired result.

TABLE 5

m	d_m	h_m	Cl_m
21	$210649 = 313 \cdot 673$	4	[2, 2]
22	$252977 = 17 \cdot 23 \cdot 647$	9	[9]
23	$301369 = 23 \cdot 13103$	4	[4]
26	$488569 = 127 \cdot 3847$	4	[4]
27	5666977	8	[8]
37	$1968377 = 431 \cdot 4567$	16	[16]
38	$2187409 = 7^2 \cdot 44641$	9	[3, 3]
40	2679737	16	[16]
41	$2954929 = 359 \cdot 8231$	9	[9]
44	3908497	16	[16]
52	$7578977 = 7^2 \cdot 137 \cdot 1129$	27	[9, 3]
54	8803057	16	[16]
57	$10909777 = 73 \cdot 199 \cdot 751$	16	[16]
158	$630964129 = 17 \cdot 23 \cdot 41 \cdot 39359$	81	[81]

7 Acknowledgement

It is a great pleasure for us to thank R. Okazaki who introduced us to this family of cubic fields K_m and suggested the lower bound $2m - 5$ in Proposition 12. All our class number computations were carried out on a personal microcomputer by using Pr. Y. Kida's UBASIC language.

References

[Ba] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.* **55** (1990), 355-380. MR **91m**:11096.

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

[Cus] T. W. Cusik. Lower bounds for regulators. *Lectures Notes in Math.* **1068** (1984), 63-73. MR **85k**:11052.

[GMW] A. Granville, R. A. Mollin and H. C. Williams. An upper bound on the least inert prime. *Canad. J. Math.* **52** (2000), 369-380. MR **?**:?.

[Hoo] C. Hooley. On the power free values of polynomials. *Mathematika* **14** (1967), 21-26. MR **35**# 5405.

[Lou1] S. Louboutin. Lower bounds for relative class numbers of CM-fields. *Proc. Amer. Math. Soc.* **120** (1994), 425-434. MR **94d**:11089.

[Lou2] S. Louboutin. Calcul du nombre de classes des corps de nombres. *Pacific J. Math.* **171** (1995), 455-467. MR **97a**:11176.

[Lou3] S. Louboutin. Class number problems for cubic number fields. *Nagoya Math. J.* **138** (1995), 199-208. MR **96f**:11145.

[Lou4] S. Louboutin. Class-group problems for cubic number fields. *Japan. J. Math.* **23** (1997), 365-378. MR **99a**:11124.

[Lou5] S. Louboutin. Majorations explicites du résidu au point 1 des fonctions zêta des corps de nombres. *J. Math. Soc. Japan* **50** (1998), 57-69. MR **99a**:11131.

[Lou6] S. Louboutin. The exponent three class group problem for some real cyclic cubic number fields. *Proc. Amer. Math. Soc.*, to appear.

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

[LPW] R. F. Lukes, C. D. Patterson and H. C. Williams. Some results on pseudosquares. *Math. Comp.* **65** (1996), 361-372. MR **96e**:11010.

[MT] M. Mignotte and N. Tzanakis. On a family of cubics. *J. Number Theory* **39** (1991), 41-49. MR **92h**:11021.

[Nar] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Second edition, Springer-Verlag, Berlin 1990. MR **91h**:11107.

[Tho] E. Thomas. Fundamental units for orders in certain cubic number fields. *J. reine Angew. Math.* **310** (1979), 33-55. MR **81b**:12009.

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