

THE EXPONENT THREE CLASS GROUP PROBLEM FOR SOME REAL CYCLIC CUBIC NUMBER FIELDS

STÉPHANE LOUBOUTIN

(Communicated by David E. Rohrlich)

ABSTRACT. We determine all the simplest cubic fields whose ideal class groups have exponent dividing 3, thus generalizing the determination by G. Lettl of all the simplest cubic fields with class number 1 and the determination by D. Byeon of all the simplest cubic fields with class number 3. We prove that there are 23 simplest cubic fields with ideal class groups of exponent 3 (and 8 simplest cubic fields with ideal class groups of exponent 1, i.e. with class number one).

1. INTRODUCTION

Let m be a rational integer and K_m be the cubic field defined by the \mathbf{Q} -irreducible cubic polynomial

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

of discriminant $d_m = f_m^2$ where

$$f_m = m^2 + 3m + 9 > 0.$$

Since K_m is also defined by the cubic polynomial

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

where $m' = -m - 3$, we may and **we will always assume that** $m \geq -1$. Notice that K_m is also defined by

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

as in [Bye]. If ρ_m is any positive real root of $P_m(x)$, then $\rho'_m = -1/(1+\rho_m) \in (-1, 0)$ and $\rho''_m = -1/(1+\rho'_m) = -1 - 1/\rho_m < -1$ are the other roots, so K_m is a (real) cyclic cubic field. Notice that since $P_m(-2) = -2m - 3 < 0 < 1 = P_m(-1) = 1$, $P_m(0) = -1 < 0$ and $P_m(m+1) = -2m - 3 < 0$, then $-2 < \rho''_m < -1 < \rho'_m < 0 \leq m+1 < \rho_m$. Moreover,

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

Received by the editors June 26, 2000.

1991 *Mathematics Subject Classification*. Primary 11R16, 11R29, 11R42.

Key words and phrases. Simplest cubic field, cubic field, class number, class group.

(notice that $P_m(x) = (y^3 - 3f_m y - (2m+3)f_m)/27$ where $y = 3x - m$). According to [Wa, Proposition 1 and Corollary], $\{1, \rho_m, \rho_m^2\}$ is a \mathbf{Z} -basis of the ring of algebraic integers of K_m if and only if either $m \not\equiv 0 \pmod{3}$ and f_m is square-free, or $m \equiv 0, 6 \pmod{9}$ and $f_m/9$ is square-free. In that case, the discriminant d_{K_m} of K_m is equal to d_m , the conductor of K_m is equal to f_m and K_m is called the m th **simplest cubic field**. For most of the $m \geq -1$ the cyclic cubic field defined by $P_m(x)$ is a simplest cubic field:

Proposition 1. *If $N(x)$ is the number of rational integers in the range $-1 \leq m \leq x$ for which K_m is a simplest cubic field, we have as $x \rightarrow \infty$*

$$N(x)/x \rightarrow \frac{8}{9} \prod_{p \equiv 1 \pmod{6}} \left(1 - \frac{2}{p^2}\right) = 0.8309 \dots$$

Proof. Use [Ric] (see the proof of [Lou4, Proposition, page 366]). □

Let Reg_m denote the regulator of the m th simplest cubic field and let R_m denote the regulator computed from the subgroup generated by $\{-1, \rho_m, \rho_m'\}$. Then,

$$(2) \quad R_m = \log^2 \rho_m - (\log \rho_m)(\log(1 + \rho_m)) + \log^2(1 + \rho_m)$$

and using (1) we obtain

$$(3) \quad R_m \leq \frac{1}{4} \log^2 f_m$$

(see [Let, Lemma 1]). We do not lose much information when we use this bound, for Reg_m is asymptotic to $\frac{1}{4} \log^2 f_m$ as m goes to infinity (see [Sh, (14)] or [Let, Lemma 1]). Since the regulator Reg_K of a real cyclic cubic field K of conductor f_K satisfies

$$(4) \quad \text{Reg}_K \geq \frac{1}{4} \log^2(f_K/2)$$

(see [Cus, Theorem 1]), the bounds (3) and (4) yield $1 \leq R_m/\text{Reg}_m < 2$. Hence, $R_m = \text{Reg}_m$ and $\{-1, \rho_m, \rho_m'\}$ generates the full group of algebraic units of the m th simplest cubic field K_m . Therefore, we have

$$(5) \quad \text{Reg}_m = R_m \leq \frac{1}{4} \log^2 f_m.$$

Let us finally recall that according to the analytic class number formula for algebraic number fields, we have

$$(6) \quad h_m = \frac{f_m}{4\text{Reg}_m} \text{Res}_{s=1}(\zeta_{K_m}).$$

The aim of this paper is to prove the following result which generalizes [Bye].

Theorem 2 (See also [Lou4, Theorem 9]). *There are 31 simplest cyclic cubic fields with ideal class groups Cl_m of exponents 1 or 3, namely the ones given in the following table:*

m	f_m	h_m	Cl_m	m	f_m	h_m	Cl_m
-1	7	1	[1]	22	$559 = 13 \cdot 43$	3	[3]
0	9	1	[1]	24	$657 = 3^2 \cdot 73$	9	[3, 3]
1	13	1	[1]	27	$819 = 3^2 \cdot 7 \cdot 13$	9	[3, 3]
2	19	1	[1]	33	$1197 = 3^2 \cdot 7 \cdot 19$	9	[3, 3]
4	37	1	[1]	34	$1267 = 7 \cdot 181$	9	[3, 3]
6	$63 = 3^2 \cdot 7$	3	[3]	35	$1339 = 13 \cdot 103$	9	[3, 3]
7	79	1	[1]	40	$1729 = 7 \cdot 13 \cdot 19$	9	[3, 3]
8	97	1	[1]	47	$2359 = 7 \cdot 337$	9	[3, 3]
9	$117 = 3^2 \cdot 13$	3	[3]	52	$2869 = 19 \cdot 151$	9	[3, 3]
10	139	1	[1]	53	$2977 = 13 \cdot 229$	9	[3, 3]
13	$217 = 7 \cdot 31$	3	[3]	61	$3913 = 7 \cdot 13 \cdot 43$	27	[3, 3, 3]
14	$247 = 13 \cdot 19$	3	[3]	69	$4977 = 3^2 \cdot 7 \cdot 79$	27	[3, 3, 3]
15	$279 = 3^2 \cdot 31$	3	[3]	78	$6327 = 3^2 \cdot 19 \cdot 37$	27	[3, 3, 3]
18	$387 = 3^2 \cdot 43$	3	[3]	97	$9709 = 7 \cdot 19 \cdot 73$	27	[3, 3, 3]
19	$427 = 7 \cdot 61$	3	[3]	104	$11137 = 7 \cdot 37 \cdot 43$	27	[3, 3, 3]
20	$469 = 7 \cdot 67$	3	[3]				

To prove this result, we first give a lower bound for the class numbers of the simplest cubic fields (see Theorem 4). This lower bound will then enable us to obtain an upper bound on the conductors of the simplest cubic fields whose ideal class groups have exponent 1 or 3 (see Corollary 8). Third, using a necessary condition for the exponent of the ideal class group of a simplest cubic field to divide 3 (see Proposition 9), we will reduce our determination to the computation of the class numbers of only 284 simplest cubic fields. Finally, we will give two methods for computing class numbers of simplest cubic fields, and by computing the class numbers of the latter 284 simplest cubic fields, we will obtain the desired result.

2. LOWER BOUNDS FOR CLASS NUMBERS

Lemma 3. *Let K be a totally real cubic number field of discriminant d_K . Let ζ_K denote the Dedekind zeta function of K . Then $\zeta_K(1 - (2/\log d_K)) \leq 0$ implies*

$$(7) \quad \text{Res}_{s=1}(\zeta_K) \geq \epsilon_K \frac{2}{e \log d_K} \quad \text{with } \epsilon_K = \begin{cases} 0.5 & \text{if } d_K \geq 5 \cdot 10^6, \\ 1 & \text{if } d_K \geq 12 \cdot 10^8. \end{cases}$$

Proof. Let K be a totally real number field of degree $n \geq 2$. Assume that $\zeta_K(\beta) \leq 0$ for some β satisfying $\frac{1}{2} \leq \beta < 1$. As in the proof of (6) in [Lou1, Prop A], Hecke’s integral representations of Dedekind zeta functions yields

$$\begin{aligned} \text{Res}_{s=1}(\zeta_K) &\geq \beta(1 - \beta)d_K^{(\beta-1)/2} \int \cdots \int_{\|y\| \geq d_K^{-1}} \exp(-\pi T(y)) \|y\|^{\beta/2} \frac{dy}{y} \\ &= (1 - \beta)d_K^{(\beta-1)/2} \{f_n(\beta) - J_K(\beta)\} \end{aligned}$$

where this multiple integral is over $y = (y_1, \dots, y_n) \in (\mathbf{R}_+^*)^n$, where we have set $\|y\| = \prod_{i=1}^n y_i$ and $T(y) = \sum_{i=1}^n y_i$, where $f_n(s) = s(\pi^{-s/2}\Gamma(s/2))^n$ and where for $s > 0$ we have

$$\begin{aligned} J_K(s) &= s \int \cdots \int_{\|y\| \leq d_K^{-1}} \exp(-\pi T(y)) \|y\|^{s/2} \frac{dy}{y} \\ &= ns \left(\pi^{-s/2}\Gamma(s/2)\right)^{n-1} \int_0^{d_K^{-1/n}} \exp(-\pi y) y^{s/2} \frac{dy}{y} \\ &\quad (\text{for } \{y; \|y\| \leq d_K^{-1}\} \subseteq \{y; \exists i \in \{1, \dots, n\} / y_i \leq d_K^{-1/n}\}) \\ &\leq ns \left(\pi^{-s/2}\Gamma(s/2)\right)^{n-1} \frac{2}{s} d_K^{-s/2n} \\ &\quad (\text{for } \exp(-\pi y) \leq 1) \\ &= 2nf_n(s) \frac{1}{g(s)} d_K^{-s/2n} \end{aligned}$$

with $g(s) = s\pi^{-s/2}\Gamma(s/2)$. Then g is positive and log-convex in the range $s > 0$, hence convex in the range $s > 0$ and $g'(1) = (g'/g)(1) = 1 - (\gamma + \log(4\pi))/2 < 0$ where $\gamma = 0.577 \dots$ denotes Euler's constant. Hence $g'(s) < 0$ for $0 < s < 1$ and $g(s) > g(1) = 1$ for $0 < s < 1$. Therefore, $0 < \beta < 1$ and $\zeta_K(\beta) \leq 0$ implies

$$(8) \quad \text{Res}_{s=1}(\zeta_K) \geq (1 - \beta)d_K^{(\beta-1)/2} (1 - 2nd_K^{-\beta/2n}) f_n(\beta).$$

Set $\beta_K = 1 - (2/\log d_K)$ (to get the factor $(1 - \beta)d_K^{(\beta-1)/2}$ as large as possible) and assume that $\zeta_K(\beta_K) \leq 0$. We obtain

$$(9) \quad \text{Res}_{s=1}(\zeta_K) \geq \frac{2}{e \log d_K} (1 - 2ne^{1/n} d_K^{-1/2n}) f_n(\beta_K).$$

Now, here again $f_n(s)$ is positive and log-convex in the range $s > 0$ and $f'_n(1) = (f'_n/f_n)(1) = -c_n$ with $c_n = n(\gamma + \log(4\pi))/2 - 1 > 0$. Hence, $f_n(\beta_K) \geq f_n(1) + (\beta_K - 1)f'_n(1) = 1 + (2c_n/\log d_K)$. Setting $n = 3$ and

$$(10) \quad \epsilon_K := \left(1 - \frac{6e^{1/3}}{d_K^{1/6}}\right) \left(1 + \frac{2c_3}{\log d_K}\right)$$

we obtain the desired bounds. □

Theorem 4. *Let h_m denote the class number of the m th simplest cubic field K_m , $m \geq -1$. Then*

$$(11) \quad h_m \geq \epsilon_m \frac{f_m}{e \log^3 f_m} \quad \text{with } \epsilon_m = \begin{cases} 0.5 & \text{if } m \geq 44, \\ 1 & \text{if } m \geq 182. \end{cases}$$

Moreover, if $h_m = 1$, then $m \leq 46$, and if $h_m = 3$, then $m \leq 82$.

Proof. Let χ_m denote any one of the two cubic Dirichlet characters associated with K_m . Since for s real we have $\zeta_{K_m}(s) = \zeta(s)|L(s, \chi_m)|^2$ and since $\zeta(s) < 0$ in the range $0 < s < 1$, we obtain $\zeta_{K_m}(1 - (2/\log d_{K_m})) \leq 0$. Using (5), (6), (7), (10) and $d_{K_m} = f_m^2$, we obtain the desired results. □

Remark 5. According to the computation of the class numbers h_m of all the simplest cubic fields K_m in the range $-1 \leq m \leq 181$ (see Section 4 below), the lower bound

$$(12) \quad h_m \geq \frac{f_m}{e \log^3 f_m}$$

is valid for all the simplest cubic fields K_m , $m \geq -1$.

Remark 6. Our lower bound (12) is better than the one given in [Let] and used in [Let] and [Bye]. Consequently, the bounds on f_m we obtained in Theorem 4 are better than the ones obtained in [Let] and [Bye]. In fact, without our improved lower bound for class numbers it would have been impossible to solve the exponent 3 class group problem for the simplest cubic fields.

Lemma 7. *Let p_i , $1 \leq i \leq t$, denote the distinct prime divisors of the conductor f of a real cyclic cubic number field K . The 3-rank r_3 of the ideal class group of K satisfies $t - 1 \leq r_3 \leq 2(t - 1)$.*

Corollary 8. *If the exponent of the ideal class group of the m th simplest cyclic cubic field K_m , $m \geq -1$, is equal to 3, then $h_m \leq 9^7$, $f_m \leq 2.4 \cdot 10^{11}$, $m \leq 5 \cdot 10^5$ and m must belong to an explicit finite set of 538 positive rational integers less than or equal to 318093.*

Proof. Let t_m denote the number of distinct prime factors of the conductor f_m of the m th simplest cyclic cubic field K_m , and set $p_1 = 7$, $p_2 = 3^2$, $p_3 = 13$, $p_4 = 19$, \dots where for $r \geq 3$ we let p_r denote the $(r - 1)$ th prime $p \equiv 1 \pmod{6}$. Then, $f_m \geq F_{t_m} := \prod_{i=1}^{t_m} p_i$. Assume now that the exponent of the ideal class group of the K_m is equal to 3. Then $h_m \leq 3^{2(t_m-1)}$ (Lemma 7). According to (12) we have $9^{t_m-1} \geq F_{t_m}/(e \log^3 F_{t_m})$ which clearly implies $t_m \leq 8$ and $h_m \leq 3^{2(t_m-1)} \leq 9^7$. Using once again (12) we obtain $f_m \leq 2.4 \cdot 10^{11}$, which implies $-1 \leq m \leq 5 \cdot 10^5$. Finally, there are 415472 simplest cubic fields K_m 's for which $m \leq 5 \cdot 10^5$ and only 538 out of them are such that $9^{t_m-1} \geq f_m/(e \log^3 f_m)$, the largest one being $m = 318093$ for which $f_m = 3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 43 \cdot 61 \cdot 67$ and $t_m = 8$. \square

3. A NECESSARY CONDITION

Now, we will use a necessary condition for the exponent of the ideal class group of K_m to be equal to 3 to get rid of half these 538 previous simplest cubic fields K_m 's: only 284 out of these 538 simplest cubic fields pass this necessary condition of Point 3 of Proposition 9, the largest one being $m = 33648$ for which $f_m = 3^2 \cdot 7 \cdot 31 \cdot 43 \cdot 97 \cdot 139$. To prove Theorem 2 it will only remain to compute the class numbers of these 284 simplest cubic fields (and the structures of the ideal class groups of those whose class numbers are perfect 3-powers). The next section will be devoted to this task.

Proposition 9. *Let K_m denote the m th simplest cubic field.*

1. *The least norm Min_{K_m} of the principal non-trivial ideals of K_m is $2m + 3$ (a non-zero integral ideal \mathcal{I} of K_m is called non-trivial if there does not exist any rational integer $n \geq 1$ such that $\mathcal{I} = (n)$).*
2. *Let \mathbf{P} be a split prime ideal of the m th simplest cubic field K_m . Let $p \geq 2$ be such that $\mathbf{P} \cap \mathbf{Z} = p\mathbf{Z}$. If \mathbf{P}^e is principal, then $p^e \geq 2m + 3$.*

3. Assume that the exponent of the ideal class group of K_m divides $e \geq 1$. Then all the primes $p < \sqrt[3]{2m+3}$ which do not divide f_m are inert in K_m , which amounts to asking that the polynomial $P_m(x) = x^3 - mx^2 - (m+3)x - 1$ has no root mod p .
4. (See also [Lou4, Theorems 3 and 12].) Under the assumption of the generalized Riemann hypothesis for all the K_m 's, the exponent e_m of the ideal class group of K_m goes to infinity with m . More precisely, $e_m \gg \log m / \log \log m$.

Proof. Point 1 is nothing but [LP, Theorem 1] rephrased in the notation of [Lou4]. Point 2 follows from Point 1. Point 3 follows from Point 2. Point 4 follows from Point 1 and the proof of [Lou4, Theorem 2]. \square

4. COMPUTATION OF h_m

Since the method delineated in [Sh] for computing h_m is not rigorous (however, using [BW], it could be made rigorous under the assumption of the Riemann hypothesis for the K_m 's) and since the method explained in [Sh] and [Let] applies only to simplest cubic fields of prime conductors, it is worth giving here a rigorous method for computing class numbers of general simplest cubic fields. We will in fact develop two methods for computing such class numbers. The first one is less efficient than the second one. However, it is worth giving for it applies equally well to non-normal totally real cubic fields (and will be used in [Lou6]).

4.1. A general method for computing class numbers of totally real cubic number fields of known regulators. Let K be a totally real 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 cubic field. Therefore, we can use the analytic class number formula (see (6) for the case where K is cyclic) and the method delineated in [Lou2] to compute the class number h of K . Setting $A_K = \sqrt{d_K/\pi^2}$ (notice that $A_{K_m} = f_m/\pi := A_m$ whenever K_m is a simplest cubic field), we obtain the following rapidly convergent series expansion:

$$(13) \quad \text{Res}_{s=1}(\zeta_K) = \frac{1}{\pi} \sum_{n \geq 1} \frac{\phi_n}{n} K_{(2,0,0)}(n/A_K)$$

(use (5) of [Lou2]). Let us now assume that $K = K_m$ is a simplest cubic field. Then, for a given $\lambda > 2$ we can compute the value of h_m by disregarding in (13) the indices $n > \lambda A_m \log A_m$, provided that m is large enough. Finally, since $n \mapsto \phi_n$ is multiplicative we only have to explain how to compute ϕ_{p^k} on prime powers. If p divides f_m then $\phi_{p^k} = 0$. Hence, $\phi_n = 0$ if $\gcd(n, f_m) > 1$. Suppose now that p does not divide f_m . Then

$$\phi_{p^k} = \begin{cases} k+1 & \text{if } p \text{ splits in } K_m \iff P_m(x) \text{ has at least one root mod } p, \\ \epsilon_k & \text{if } p \text{ is inert in } K_m \iff P_m(x) \text{ has no root mod } p, \end{cases}$$

where $\epsilon_k = 1, -1$ or 0 according as $k \equiv 0, 1$ or $2 \pmod{3}$. The main drawback of this method is that we have to test whether the polynomial $P_m(x)$ has a root mod p for all the primes $p \leq \lambda A_m \log A_m$, which is time consuming for large values of f_m . Therefore, this method for computing h_m is efficient only for reasonable values of f_m and could not be used to compute a lot of class numbers of simplest cubic fields with large conductors.

4.2. A more efficient method for computing class numbers of simplest cubic fields. Suppose we knew how to compute the values taken on by χ_m , any one of the two conjugate primitive cubic characters associated with the cyclic cubic field K_m . According to (6) and the explicit formula for $L(1, \chi)$ for even primitive Dirichlet characters, we have

$$(14) \quad h_m = \frac{1}{\text{Reg}_m} \left| \sum_{\substack{1 \leq k \leq f_m/2 \\ \gcd(k, f_m) = 1}} \chi_m(k) \log \sin\left(\frac{k\pi}{f_m}\right) \right|^2,$$

which provides us with a simple and rather fast technique for computing h_m (which however requires $O(f_m^{1+\epsilon}) = O(A_m^{1+\epsilon})$ elementary operations to compute h_m). So, let us explain how one can efficiently determine such a χ_m . Fix ζ_3 a complex third root of unity. For a given prime $p \equiv 1 \pmod{6}$ we set $g_p = \min\{g \geq 1; g^{(p-1)/3} \not\equiv 1 \pmod{p}\}$, $G_p = g_p^{(p-1)/3} \pmod{p}$ and let χ_p be the cubic character mod p defined (for $\gcd(x, p) = 1$) by $\chi_p(x) = 1, \zeta_3$ or ζ_3^2 according as $x^{(p-1)/3} \equiv 1, G_p$ or $G_p^2 \pmod{p}$. Also we let χ_9 denote the primitive cubic character mod 9 defined (for $\gcd(x, 9) = 1$) by the following table:

$x \pmod{9}$	1	2	4	5	7	8
$\chi(x)$	1	ζ_3	ζ_3^2	ζ_3^2	ζ_3	1

Write $f_m = \prod_{i=1}^t p_i$, where the p_i are pairwise distinct, with $p_1 = 9$ or $p_1 \equiv 1 \pmod{6}$ a prime, and with each $p_i \equiv 1 \pmod{6}$ a prime for $2 \leq i \leq t$. To each $n \in \{0, 1, \dots, 2^{t-1} - 1\}$ we associate its 2-adic development $n = \sum_{i=2}^t (a_i - 1)2^{i-2}$, $a_i \in \{1, 2\}$, and the primitive mod f_m cubic character

$$\phi_n = \chi_{p_1} \prod_{i=2}^t \chi_{p_i}^{a_i}$$

(where the χ_{p_i} are as above). For a given simplest cubic field K_m of conductor $f_m = \prod_{i=1}^t p_i$ there exists a unique $n \in \{0, 1, \dots, 2^{t-1} - 1\}$ such that the primitive cubic character ϕ_n is one of the two conjugate primitive cubic characters χ_m associated with K_m . The following algorithm provides us with an efficient technique for determining this unique n :

1. $n := 0, n' := 2^{t-1} - 1$.
2. If $n = n'$, then goto step 9.
3. $p := 2$.
4. While p does not split in K_m do $p := \text{next prime}$
(we use the fact that a prime p which does not divide f_m splits in K_m if and only if $P_m(x)$ has at least one root mod p).
5. If $\phi_n(p) \neq 1$, then $\{n := n + 1; \text{goto step 2}\}$.
6. If $\phi_{n'}(p) \neq 1$, then $\{n' := n' - 1; \text{goto step 2}\}$.
7. $p := \text{next prime}$.
8. Goto step 4
9. Return(n).

Practically, this algorithm is fast, for we only have to use Step 4 for small primes p . In fact, assume the Generalized Riemann Hypothesis. Then, for any distinct Dirichlet characters χ and χ' mod f there exists some prime $p \leq 3 \log^2 f$ which does not divide f such that $\chi(p) \neq \chi'(p)$ (apply [Ba, Theorem 3] with $G = \ker(\chi\chi'^{-1})$). Hence, under the assumption of the GRH the primes p which crop up in our algorithm satisfy $p \leq 3 \log^2 f_m$.

According to computations based on this method, only 46 out of the previously considered 284 simplest cubic fields have class numbers of the form $h_m = 3^e$, $e \geq 0$: the 31 ones which appear in Theorem 2 and the 15 following ones $m \in \{110, 144, 153, 173, 178, 222, 258, 288, 385, 447, 477, 659, 664, 690, 2674\}$. Finally, using any software for algebraic number fields (as Pari or KASH) to compute the structure of the ideal class groups of these 46 simplest cubic fields, we complete the proof of Theorem 2.

Remark 10. For very large values of m , we could use the technique delineated in [Lou5] to compute efficiently h_m in only (conjecturally) $O(f_m^{0.5+\epsilon}) = O(A_m^{0.5+\epsilon})$ elementary operations.

5. THE EXPONENT 2 CLASS GROUP PROBLEM

Theorem 10 (see also [Lou4, Theorem 13]). 1. *Assume that the exponent of the ideal class group of a simplest cubic field K_m is equal to 2. Then f_m is a prime equal to 1 mod 6 and $p^{(f_m-1)/3} \not\equiv 1 \pmod{f_m}$ for all the primes p such that $p^2 < 2m + 3$.*

2. *There are only 5 simplest cubic fields K_m with ideal class groups of exponent 2 for $-1 \leq m \leq 10^{10}$, namely the K_m 's with $m \in \{11, 17, 23, 25, 29\}$ (and these five fields K_m have class number 4).*
3. *Under the assumption of the generalized Riemann hypothesis for all the K_m 's, there are exactly 5 simplest cubic fields K_m with ideal class groups of exponent 2, namely the ones given in the previous point.*

Proof. 1. This point follows from Lemma 7 and Point 3 of Proposition 9.

2. There are only 39 values of $m \leq 10^{10}$ for which the condition of this first point is satisfied. The largest one is $m = 1814$. For only 7 out of these 39 values of m is $h_m = 2^r \geq 2$ a perfect 2-power, namely $m \in \{11, 17, 23, 25, 29, 64, 143\}$. By computing the class group structures of the 7 associated K_m 's, we get the desired result (the structure of the ideal class group of K_{64} is $[4, 4]$ and that of K_{143} is $[4, 4, 2, 2]$).
3. Under the assumption of the generalized Riemann hypothesis there exists some prime $p \leq (8 \log f_m + 7.5)^2$ such that $\chi_m(p) = +1$ (use [BS, Theorem 5.1]). Hence, according to Point 3 of Proposition 9, if the exponent of the ideal class group of K_m is equal to 2, then $(8 \log f_m + 7.5)^4 \geq 2m + 3$, which implies $m \leq 10^{10}$. \square

REFERENCES

- [Ba] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.* **55** (1990), 355-380. MR **91m**:11096
- [BS] E. Bach and J. Sorenson. Explicit bounds for primes in residue classes. *Math. Comp.* **65** (1996), 1717-1735. MR **97a**:11143
- [BW] J. Buchmann, J. and H. C. Williams. On the computation of the class number of an algebraic number field. *Math. Comp.* **53** (1989), 679-688. MR **90a**:11128
- [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. Cusick. Lower bounds for regulators. *Lectures Notes in Math.* **1068** (1984), 63-73. MR **85k**:11052
- [Let] G. Lettl. A lower bound for the class number of certain cubic number fields. *Math. Comp.* **46** (1986), 659-666. MR **87e**:11123

- [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. Computation of relative class numbers of imaginary abelian number fields. *Experimental Math.* **7** (1998), 293-303. MR **2000c**:11207
- [Lou6] S. Louboutin. Class number and class group problems for some non-normal totally real cubic number fields. In preparation.
- [LP] F. Lemmermeyer and A. Pethö. Simplest cubic fields. *Manuscripta Math.* **88** (1995), 53-58. MR **96g**:11131
- [Ric] C. Ricci. Ricerche arithmetiche sui polinomi. *Rend. Circ. Mat. Palermo* **57** (1933), 433-475.
- [Sh] D. Shanks. The simplest cubic fields. *Math. Comp.* **28** (1974), 1137-1152. MR **50**:4537
- [Wa] L. C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.* **48** (1987), 371-384. MR **88a**:11107

INSTITUT DE MATHÉMATIQUES DE LUMINY, UPR 906, 163, AVENUE DE LUMINY, CASE 907,
13288 MARSEILLE CEDEX 9, FRANCE

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