

NEW CHARACTERIZATION OF THE NORM OF THE FUNDAMENTAL UNIT OF $\mathbb{Q}(\sqrt{M})$

GEORGES GRAS

ABSTRACT. We give an elementary criterion for the norm of the fundamental unit ε_K of $K = \mathbb{Q}(\sqrt{M})$, M square-free. More precisely, if $\varepsilon_K = a + b\sqrt{M}$, $a, b \in \mathbb{Z}$ or $\frac{1}{2}\mathbb{Z}$, its norm \mathbf{S}_K only depends on $m := \mathbf{gcd}(\frac{a+1}{\mathbf{gcd}(a+1,b)}, M)$ and $m' := \mathbf{gcd}(\frac{a-1}{\mathbf{gcd}(a-1,b)}, M)$ as follows when -1 is a global norm: $\mathbf{S}_K = -1$ if and only if $m = m' = 1$ (resp. $m = m' = 2$) for M odd (resp. even) (Theorems 1.1 or 2.4).

CONTENTS

1. Introduction – Main result	1
2. Characterizations of $\mathbf{N}(\varepsilon_K) = -1$	2
2.1. Class field theory results involving $\mathbf{N}(\varepsilon_K)$	2
2.2. Computation of the non-canonical relations of principality	5
2.3. Main characterization of $\mathbf{N}(\varepsilon_K)$	5
2.4. Computation of \mathbf{S} by means of the \mathbf{gcd} criterion	8
3. Remarks on density questions	9
3.1. Classical approach of the density	9
3.2. Classification by ascending traces of fundamental units	10
3.3. Approximations of the density from the \mathbf{gcd} principle	11
References	16

1. INTRODUCTION – MAIN RESULT

Let $K =: \mathbb{Q}(\sqrt{M})$, $M \in \mathbb{Z}_{\geq 2}$ square-free, be a real quadratic field and let \mathbf{Z}_K be its ring of integers. Recall that M is called the “Kummer radical” of K , contrary to any “radical” $R = Mr^2$ giving the same field K . We will write the elements of \mathbf{Z}_K under the form $\alpha = \frac{1}{2}(u + v\sqrt{M})$, with u, v of same parity. We denote by $\mathbf{T}_{K/\mathbb{Q}} =: \mathbf{T}$ and $\mathbf{N}_{K/\mathbb{Q}} =: \mathbf{N}$, the trace and norm maps in K/\mathbb{Q} , so that $\mathbf{T}(\alpha) = u$ and $\mathbf{N}(\alpha) = \frac{1}{4}(u^2 - Mv^2)$.

We denote by $\varepsilon_K > 1$ the fundamental unit of K and by $\mathbf{S}_K =: \mathbf{S} := \mathbf{N}(\varepsilon_K) \in \{-1, 1\}$ its norm. An obvious necessary condition for $\mathbf{S} = -1$ is to have $-1 \in \mathbf{N}(K^\times)$, equivalent to the fact that any odd prime ramified in K/\mathbb{Q} is congruent to 1 modulo 4.

The starting point of our result is the following observation proved by means of elementary applications of class field theory (see Theorem 2.1 assuming $-1 \in \mathbf{N}(K^\times)$ and Remark 2.2 (iii) in the case $-1 \notin \mathbf{N}(K^\times)$):

Set $M = \prod_{q|M} q$ for the prime divisors q of M and let $\mathfrak{q} \mid q$ be the prime ideal of $K = \mathbb{Q}(\sqrt{M})$ over q . The fundamental unit ε_K of K is of norm -1 if and only if the relation $\prod \mathfrak{q} = (\sqrt{M})$ is the unique non-trivial relation of principality (in the ordinary sense) between the ramified prime ideals of K (that is to say, the \mathfrak{q} 's dividing (\sqrt{M}) and $\mathfrak{q}_2 \mid 2$ if $2 \nmid M$ ramifies, whence if $M \equiv 3 \pmod{4}$).

Of course, when $-1 \notin \mathbf{N}(K^\times)$ and when $2 \nmid M$ ramifies, one can verify the existence of a relation of principality, either of the form $\prod \mathfrak{q}^{e_q}$ (distinct from (1) and (\sqrt{M})) with

Date: May 24, 2023.

2020 Mathematics Subject Classification. Primary 11R11, 11R27, 11R29, 11R37.

Key words and phrases. Real quadratic fields; Fundamental unit; Norm of units; Class field theory; PARI programs.

exponents in $\{0, 1\}$, or else \mathfrak{q}_2 principal (e.g., $M = 3 \times 17$ with \mathfrak{q}_2 principal, the ideals \mathfrak{q}_3 and \mathfrak{q}_{17} being non-principal; for more examples and comments, see Remark 2.2 (iii)).

Then we can state the main result, under the assumption $-1 \in \mathbf{N}(K^\times)$ (see Theorem 2.4 for more details and informations):

Theorem 1.1. *Let $\varepsilon_K = a + b\sqrt{M} > 1$, $a, b \in \mathbb{Z}$ or $\frac{1}{2}\mathbb{Z}$, be the fundamental unit of K . We consider the integers $A + B\sqrt{M}$ and $A' + B'\sqrt{M}$, defined as follows:*

$$\varepsilon_K + 1 = a + 1 + b\sqrt{M} =: g(A + B\sqrt{M}), \quad \text{where } g := \mathbf{gcd}(a + 1, b) \in \mathbb{Z}_{>0},$$

$$\varepsilon_K - 1 = a - 1 + b\sqrt{M} =: g'(A' + B'\sqrt{M}), \quad \text{where } g' := \mathbf{gcd}(a - 1, b) \in \mathbb{Z}_{>0}.$$

Let $m := \mathbf{gcd}(A, M)$ and $m' := \mathbf{gcd}(A', M)$. Then we have:

- (i) If M is odd, ε_K is of norm -1 if and only if $m = m' = 1$.
- (ii) If M is even, ε_K is of norm -1 if and only if $m = m' = 2$.

Let $\mathcal{D}_{\leq \mathbf{X}}$ be the set of discriminants $D \leq \mathbf{X}$ corresponding to quadratic fields K such that $-1 \in \mathbf{N}(K^\times)$ and let $\mathcal{D}_{\leq \mathbf{X}}^-$ the subset of discriminants such that $\mathbf{S} := \mathbf{N}(\varepsilon_K) = -1$,

and put $\Delta_{\text{disc}}^- := \lim_{\mathbf{X} \rightarrow \infty} \frac{\mathcal{D}_{\leq \mathbf{X}}^-}{\mathcal{D}_{\leq \mathbf{X}}}$. Recently, the Stevnhagen conjecture [St, Conjecture 1.4],

for the density $\Delta_{\text{disc}}^- = 0.5805\dots$, has been proved from techniques developed by Koymans–Pagano [KoPa1, KoPa2], in relation with that of Smith [Sm], based on estimations of the 2^k -ranks of the class groups of the K 's, $k \geq 2$. It raises the question of whether our point of view can constitute a way to define another notion of density since it does not seem compatible with the common principle of classification of the fields via their discriminants; this will be discussed in Section 3.

2. CHARACTERIZATIONS OF $\mathbf{N}(\varepsilon_K) = -1$

In this Section, we give (Theorems 2.1, 2.4) a new characterization of the norm \mathbf{S} of the fundamental unit ε_K of $K = \mathbb{Q}(\sqrt{M})$ when $-1 \in \mathbf{N}(K^\times)$, in particular for the case $\mathbf{S} = -1$ giving the solvability of the norm equation $u^2 - Mv^2 = -4$, $u, v \in \mathbb{Z}_{>0}$.

2.1. Class field theory results involving $\mathbf{N}(\varepsilon_K)$. We will use the classical class field theory context given by the Chevalley–Herbrand formula and by the standard exact sequence defining the group of invariant classes (for simplicity, we refer to our book [Gra1], but any classical reference book may agree). Of course, in the case of quadratic fields, the theory is equivalent to that of quadratic forms and goes back to Gauss and, after that in a number field context, to Kummer, Hilbert, Takagi, Hasse, Chevalley–Herbrand, Fröhlich, Furuta, Ishida, Leopoldt, for particular formulas in the area of genus theory, but we are convinced that the general framework may be used, for instance, in relative quadratic extensions K/k , since the index $(E_k : \mathbf{N}E_K)$ of groups of units, when $E_k \subset \mathbf{N}(K^\times)$, is as mysterious as $(E_{\mathbb{Q}} : \mathbf{N}E_K)$ for $K = \mathbb{Q}(\sqrt{M})$, when $-1 \in \mathbf{N}(K^\times)$ (for some examples in this direction, see [Gra2, Théorème 3.2, Corollaires 3.3, 3.4]).

Theorem 2.1. *Consider Kummer radicals $M = q_1 \cdots q_r$ or $M = 2 \cdot q_2 \cdots q_r$, $r \geq 1$, with odd primes $q_i \equiv 1 \pmod{4}$ ($r = 1$ gives $M = q_1$ or $M = 2$) and let $K = \mathbb{Q}(\sqrt{M})$. If the prime q (odd or not) divides M we denote by \mathfrak{q} the prime ideal of K above q .*

(i) *The fundamental unit ε_K is of norm $\mathbf{S} = -1$ if and only if the relation $\prod_{\mathfrak{q}|M} \mathfrak{q} = (\sqrt{M})$ is the unique relation of principality, distinct from (1), between the ramified prime ideals of K (this relation and the trivial one will be called the canonical relations).*

(ii) *In the case $\mathbf{S} = 1$, the unique non-canonical relation $\mathfrak{m} = \prod_{\mathfrak{q}|m} \mathfrak{q} = (\alpha)$, of support $m \mid M$ distinct from 1 and M , is given by $\varepsilon_K + 1 =: g\alpha$, where the rational integer g is maximal and, similarly, the complementary relation $\mathfrak{n} = \prod_{\mathfrak{q}|n} \mathfrak{q} = (\beta)$, of support $n = \frac{M}{m}$ distinct from 1 and M , is given by $\varepsilon_K - 1 =: g'\beta$ where the rational integer g' is maximal.*

Proof. (i) Let $G := \text{Gal}(K/\mathbb{Q}) =: \langle \sigma \rangle$. The Chevalley–Herbrand formula [Che, pp. 402–405] gives, for the ordinary 2-class group \mathcal{H}_K , $\#\mathcal{H}_K^G = \frac{2^{r-1}}{\langle (-1) : \langle -1 \rangle \cap \mathbf{N}(K^\times) \rangle} = 2^{r-1}$

since $-1 \in \mathbf{N}(K^\times)$ by assumption. Moreover, we have the classical exact sequence:

$$(2.1) \quad 1 \rightarrow \mathcal{H}_K^{\text{ram}} \rightarrow \mathcal{H}_K^G \rightarrow \langle -1 \rangle \cap \mathbf{N}(K^\times) / \langle \mathbf{S} \rangle = \langle -1 \rangle / \langle \mathbf{S} \rangle \rightarrow 1,$$

where $\mathcal{H}_K^{\text{ram}}$ is the subgroup generated by the classes of the ramified prime ideals \mathfrak{q} of K . Indeed, for an invariant class of an ideal \mathfrak{a} , one associates with $(\alpha) := \mathfrak{a}^{1-\sigma}$, $\alpha \in K^\times$, the sign $\mathbf{N}(\alpha) = \pm 1 \in \langle -1 \rangle \cap \mathbf{N}(K^\times) = \langle -1 \rangle$, defined modulo $\langle \mathbf{S} \rangle$ since α is defined modulo $E_K := \langle -1, \varepsilon_K \rangle$.

- **Image.** Since there exists $\beta \in K^\times$ such that $-1 = \mathbf{N}(\beta)$, the ideal (β) , being of norm (1), is of the form $\mathfrak{b}^{1-\sigma}$, giving a pre-image in \mathcal{H}_K^G (surjectivity).

- **Kernel.** If $\mathfrak{a}^{1-\sigma} = (\alpha)$ with $\mathbf{N}(\alpha) = \mathbf{S}$, one may suppose, up to a unit, that $\mathbf{N}(\alpha) = 1$, whence $\alpha = \theta^{1-\sigma}$ (Hilbert's Theorem 90), and $\mathfrak{a}(\theta)^{-1}$ is an invariant ideal, product of a rational ideal by a product of ramified prime ideals of K .

This yields $\#\mathcal{H}_K^{\text{ram}} = \frac{2^{r-1}}{(\langle -1 \rangle : \langle \mathbf{S} \rangle)}$, where we recall that r is the number of ramified prime ideals of K ; let's examine each case for \mathbf{S} :

If $\mathbf{S} = -1$, then $\#\mathcal{H}_K^{\text{ram}} = 2^{r-1}$ and the unique non-trivial relation of principality between the ramified primes is the canonical one, $\prod \mathfrak{q} = (\sqrt{M})$.

If $\mathbf{S} = 1$, then $\#\mathcal{H}_K^{\text{ram}} = 2^{r-2}$, necessarily with $r \geq 2$, and another relation of principality does exist, given by a suitable product $\prod \mathfrak{q}^{e_q} = (\alpha)$, $e_q \in \mathbb{Z}$; since any \mathfrak{q}^2 is principal, one may write the relation under the form $\mathfrak{m} = \prod_{q|m} \mathfrak{q} = (\alpha)$ of support $m \mid M$. For $n = \frac{M}{m}$ we get the non-canonical analogous relation $\mathfrak{n} = \prod_{q|n} \mathfrak{q} = (\beta)$, with $\mathfrak{m}\mathfrak{n} = (\alpha\beta) = (\sqrt{M})$; which proves the first claim.

(ii) From $\mathfrak{m} = (\alpha)$ when $\mathbf{S} = 1$, we get $\alpha^{1-\sigma} = \pm \varepsilon_K^k$, $k \in \mathbb{Z}$; since $\varepsilon_K^2 = \varepsilon_K^{1+\sigma+1-\sigma} = \varepsilon_K^{1-\sigma}$, we may assume that $\mathfrak{m} = (\alpha)$ with $\alpha^{1-\sigma} \in \{\pm 1, \pm \varepsilon_K\}$. If $\alpha^{1-\sigma} = \pm 1$, then $\alpha \in \{1, \sqrt{M}\} \times \mathbb{Q}^\times$ gives the canonical relations (absurd); thus $\alpha^{1-\sigma} = \pm \varepsilon_K$. If for instance $\alpha^{1-\sigma} = 1$, then $(\alpha\sqrt{M})^{1-\sigma} = -1$ and this gives the complementary relation $\mathfrak{n} = (\beta)$ with $\beta^{1-\sigma} = -\varepsilon_K$.

Since we have $(\varepsilon_K + 1)^{1-\sigma} = \frac{\varepsilon_K + 1}{\varepsilon_K^\sigma + 1} = \frac{\varepsilon_K + 1}{\varepsilon_K^{-1} + 1} = \varepsilon_K$ and similarly $(\varepsilon_K - 1)^{1-\sigma} = -\varepsilon_K$, the quotients $\frac{\varepsilon_K + 1}{\alpha}$ and $\frac{\varepsilon_K - 1}{\beta}$ are invariants under σ , hence are rational numbers; this proves the second claim of the theorem writing $\varepsilon_K + 1 = g\alpha$ and $\varepsilon_K - 1 = g'\beta$ in an obvious manner (g and g' are the maximal rational integer factors of the quadratic integers $\varepsilon_K \pm 1$). \square

Remarks 2.2. (i) If $r = 1$, one finds again the well-known result $\mathbf{S} = -1$ for the prime Kummer radicals $M = q \equiv 1 \pmod{4}$ and for $M = 2$. The properties given by Theorem 2.1, due to the Chevalley–Herbrand formula, come from the “product formula” of Hasse’s norm residue symbols in class field theory [Gra1, Theorem II.3.4.1].

(ii) The theorem is also to be related with that of Trotter [Tro, Theorem, p.198] leading, in another framework, to the study of the equations $mx^2 - ny^2 = \pm 4$, equivalent to the principalities of \mathfrak{m} and \mathfrak{n} , since, for instance, $\mathfrak{m} = (\frac{1}{2}(x + y\sqrt{M}))$ is equivalent to $x^2 - My^2 = \pm 4m$, whence $mx^2 - ny^2 = \pm 4$; then, some *sufficient conditions of solvability* of these equations are given by means of properties of suitable quadratic residues.

Remark 2.3. We intend to give some properties of the case $M = q_1 \cdots q_r$ odd, when one assumes that $-1 \notin \mathbf{N}(K^\times)$ (there exists $q \mid M$ such that $q \equiv 3 \pmod{4}$), then $\mathbf{S} = 1$, the Chevalley–Herbrand formula becomes $\#\mathcal{H}_K^G = \frac{2^{r+\delta-1}}{(\langle -1 \rangle : \langle -1 \rangle \cap \mathbf{N}(K^\times))} = 2^{r+\delta-2}$, where $\delta = 1$ (resp. 0) if $M \equiv 3 \pmod{4}$ (resp. if not) and the exact sequence (2.1) becomes the isomorphism $\mathcal{H}_K^{\text{ram}} \simeq \mathcal{H}_K^G$. Nevertheless, if $M \equiv 1 \pmod{4}$ (thus an even number of primes $q \equiv 3 \pmod{4}$ dividing M), we have $\delta = 0$, so that one obtains the pair of non-canonical relations of principality from the computation of m and n from $\varepsilon_K \pm 1$.

Now, we assume that $M \equiv 3 \pmod{4}$ implying the ramification of 2 with M odd and $\mathbf{S} = 1$. So we have $\delta = 1$, $\#\mathcal{H}_K^{\text{ram}} = 2^{r-1}$ and the existence of a group of relations of principality of order 4 between the $r + 1$ ramified primes, including the canonical ones.

• If $\mathfrak{q}_2 \mid 2$ is principal, this gives the non-canonical relation, and the process using $\varepsilon_K \pm 1$ only gives the canonical relations (1) and (\sqrt{M}) .

• If $\mathfrak{q}_2 \mid 2$ is not principal, this implies the existence of a non-canonical relation of principality, distinct from (1) and (\sqrt{M}) . We intend to show that this relation is not of the form $\mathfrak{q}_2 \cdot \mathfrak{m}$ principal, for \mathfrak{m} distinct from (1) and (\sqrt{M}) . Otherwise, we have:

$$(2.2) \quad \mathfrak{q}_2 \mathfrak{m} = (\alpha) \text{ and } \mathfrak{q}_2 \mathfrak{n} = (\beta), \quad \mathfrak{m}\mathfrak{n} = (\sqrt{M}),$$

whence the existence of units $\varepsilon, \varepsilon'$ such that: $\alpha^2 \varepsilon = 2m$ and $\beta^2 \varepsilon' = 2n$; modulo the squares of units one may choose α and β such that:

$$\alpha^2 = \pm 2m \text{ or } \alpha^2 \varepsilon_K = \pm 2m \quad \text{and} \quad \beta^2 = \pm 2n \text{ or } \beta^2 \varepsilon_K = \pm 2n.$$

The cases $\pm 2m$ and $\pm 2n$ does not hold since the Kummer radical M is unique. So:

$$(2.3) \quad \alpha^2 \varepsilon_K = 2m \quad \text{and} \quad \beta^2 \varepsilon_K = 2n.$$

In the same way, we have, from the principality relations (2.2), $\alpha^{1-\sigma} = \eta$ and $\beta^{1-\sigma} = \eta'$ that we may write (using $\varepsilon_K^2 = \varepsilon_K^{1-\sigma}$ since $\mathbf{S} = \varepsilon_K^{1+\sigma} = 1$):

$$\alpha^{1-\sigma} = \pm 1 \text{ or } \alpha^{1-\sigma} = \pm \varepsilon_K \quad \text{and} \quad \beta^{1-\sigma} = \pm 1 \text{ or } \beta^{1-\sigma} = \pm \varepsilon_K.$$

As above, the cases ± 1 are excluded (e.g., $\alpha^{1-\sigma} = \pm 1$ gives $\alpha \in \mathbb{Q}^\times$ or $\mathbb{Q}^\times \cdot \sqrt{M}$). Thus:

$$(2.4) \quad \alpha^{1-\sigma} = \pm \varepsilon_K \quad \text{and} \quad \beta^{1-\sigma} = \pm \varepsilon_K.$$

From (2.3) one gets the relation $\alpha^2 \beta^2 \varepsilon_K^2 = 2m 2n = 4M$ and then $\alpha \beta \varepsilon_K = \pm 2\sqrt{M}$, giving $(\alpha \beta \varepsilon_K)^{1-\sigma} = -1$. Using relations (2.4), the previous relation leads to:

$$\pm \varepsilon_K \cdot \varepsilon_K \cdot \varepsilon_K^2 = -1 \quad (\text{absurd}).$$

So, when \mathfrak{q}_2 is non-principal, the non-canonical relations are of the form \mathfrak{m} and \mathfrak{n} , given by the usual process. Let's give few examples using Program 2.4:

M	relations	M	relations
3 [3]	1 3 \square q2 principal	51 [3,17]	1 51 [0] q2 principal
6 [2,3]	2 3 \square	55 [5,11]	11 5 [1] q2 non principal
7 [7]	1 7 \square q2 principal	57 [3,19]	3 19 \square D=M
11 [11]	1 11 \square q2 principal	59 [59]	59 1 \square q2 principal
14 [2,7]	7 2 \square	62 [2,31]	2 31 \square
15 [3,5]	3 5 [1] q2 non principal	66 [2,3,11]	33 2 [0]
19 [19]	1 19 \square q2 principal	67 [67]	67 1 \square q2 principal
21 [3,7]	3 7 \square D=M	69 [3,23]	23 3 \square D=M
22 [2,11]	2 11 \square	70 [2,5,7]	14 5 [1] q2 non principal
23 [23]	1 23 \square q2 principal	71 [71]	1 71 \square q2 principal
30 [2,3,5]	5 6 [1] q2 non principal	77 [7,11]	7 11 \square D=M
31 [31]	1 31 \square q2 principal	78 [2,3,13]	26 3 [1] q2 non principal
33 [3,11]	11 3 \square D=M	79 [79]	1 79 [0] q2 principal
35 [5,7]	5 7 [1] q2 non principal	83 [83]	83 1 \square q2 principal
38 [2,19]	2 19 \square	86 [2,43]	43 2 \square
39 [3,13]	13 3 [1] q2 non principal	87 [3,29]	3 29 [1] q2 non principal
42 [2,3,7]	6 7 [1] q2 non principal	91 [7,13]	13 7 [1] q2 non principal
43 [43]	1 43 \square q2 principal	93 [3,31]	31 3 \square D=M
46 [2,23]	2 23 \square	94 [2,47]	2 47 \square
47 [47]	1 47 \square q2 principal	95 [5,19]	5 19 [1] q2 non principal

The mention $D = M$ means that 2 does not ramify, so it does not intervene in the relations; the mention q2 principal is then the unique non-canonical relation and the mention q2 non principal occurs when 2 ramifies but there exists a pair of non-canonical relations $(\mathfrak{m}, \mathfrak{n})$ given in the left column. A box \square means a trivial class group and $[0]$ is equivalent to the principality of \mathfrak{q}_2 when the class group is non-trivial and $[a, b, \dots]$, with not all zero a, b, \dots , gives the components of the class of \mathfrak{q}_2 on the PARI basis of the class group.

The first "non-trivial" example is $M = 51$, where $\varepsilon_{51} = 50 + 7\sqrt{51}$, giving $\varepsilon_{51} + 1 = 51 + 7\sqrt{51}$ ($m = 51$) and $\varepsilon_{51} - 1 = 7(7 + \sqrt{51})$ ($n = 1$), thus the canonical relations.

The case $-1 \notin \mathbf{N}(K^\times)$ being without any mystery regarding the norm \mathbf{S} , we will assume $-1 \in \mathbf{N}(K^\times)$ in the sequel.

2.2. Computation of the non-canonical relations of principality. The following program computes, when $-1 \in \mathbf{N}(K^\times)$ and $\mathbf{S} = 1$, the non-canonical relations of principality between the ramified primes of K to make statistics and notice that any kind of relation seems to occur with the same probability for r fixed.

It uses the arithmetic information given by the PARI instructions $\mathbf{K} = \mathbf{bnfinit}(x^2 - M)$ and $\mathbf{bnfisprincipal}(\mathbf{K}, \mathbf{A})$ testing principalities. When $\mathbf{S} = -1$, the program gives only the trivial list $\mathbf{L} = \text{List}([1, 1, 1, 1])$ corresponding to the canonical relation. The parameter \mathbf{Br} forces $r \geq \mathbf{Br}$. As illustration, let's give examples, for $r = 5$, of the relations of principality $\mathbf{m} = (\alpha)$, $\mathbf{n} = (\beta)$, by means of the exponents $[e_1, \dots, e_r]$ given by the list \mathbf{L} and where the radical M is given via the list of its prime divisors; for instance:

$$\mathbf{M} = [2, 5, 13, 17, 37] \quad \mathbf{L} = \text{List}([0, 1, 0, 1, 1]),$$

means $q_5 \cdot q_{17} \cdot q_{37}$ principal (or $q_2 \cdot q_{13}$ principal).

```
COMPUTATION OF THE RELATIONS OF PRINCIPALITY
{Br=5;for(M=2,10^6,if(core(M)!=M,next);r=omega(M);if(r<Br,next);
i0=1;if(Mod(M,2)==0,i0=2);f=factor(M);ellM=component(f,1);
for(i=i0,r,c=ellM[i];if(Mod(c,4)!=1,next(2)));
L0=List;for(i=1,r,listput(L0,0));P=x^2-M;K=bnfinit(P,1);
print();print("M=",ellM);F=idealfactor(K,M);
for(k=1,2^r-1,B=binary(k);t=#B;L=L0;for(i=1,t,listput(L,B[i],r-t+i));A=1;
for(j=1,r,e=L[j];if(e==0,next);A=idealmul(K,A,component(F,1)[j]));
Q=bnfisprincipal(K,A)[1];if(Q==0,print("L=",L))}}
```

M=[2,5,13,17,37]	L=[0,1,0,1,1]	M=[2,5,13,17,53]	L=[0,0,1,0,1]
M=[2,5,13,29,37]	L=[0,1,1,0,0]	M=[2,5,13,37,41]	L=[0,1,1,0,1]
M=[2,5,13,17,109]	L=[0,1,0,1,1]	M=[2,5,17,37,41]	L=[0,1,0,1,0]
M=[2,5,13,29,73]	L=[0,1,1,0,0]	M=[2,5,13,41,53]	L=[0,0,1,1,1]
M=[2,5,13,37,61]	L=[0,1,1,0,0]	M=[2,5,17,29,61]	L=[0,0,0,1,1]
M=[2,5,13,17,137]	L=[0,1,1,1,0]	M=[2,5,13,17,149]	L=[0,1,0,1,1]
M=[2,5,17,29,73]	L=[0,0,1,0,1]	M=[2,5,13,41,73]	L=[0,1,1,1,0]
M=[2,5,13,29,109]	L=[0,1,0,0,1]	M=[2,5,17,41,61]	L=[0,1,0,0,1]
M=[2,5,13,37,89]	L=[0,0,1,1,1]	M=[2,5,13,17,197]	L=[0,1,0,1,1]
M=[2,5,17,29,89]	L=[0,1,0,1,1]	M=[2,5,29,37,41]	L=[0,1,1,0,1]
M=[2,5,17,29,97]	L=[0,0,1,0,1]	M=[2,5,17,29,109]	L=[0,1,0,1,0]
M=[2,5,17,53,61]	L=[0,1,1,0,1]	M=[2,5,17,37,89]	L=[0,1,0,1,1]
M=[2,5,13,29,149]	L=[0,1,0,0,1]	M=[2,5,13,61,73]	L=[0,1,1,0,0]
M=[2,5,17,37,97]	L=[0,0,1,0,1]	M=[2,5,13,53,89]	L=[0,0,1,1,1]
M=[2,5,17,37,101]	L=[0,1,0,1,0]	M=[2,5,13,17,293]	L=[0,1,0,1,1]
M=[2,5,13,29,173]	L=[0,0,1,0,1]	M=[2,5,29,37,61]	L=[0,0,1,0,1]
M=[2,5,13,37,137]	L=[0,1,1,0,1]	M=[2,5,17,29,137]	L=[0,1,1,1,0]
M=[2,5,17,41,97]	L=[0,0,1,0,1]	M=[2,5,17,37,113]	L=[0,0,1,0,1]
M=[2,5,17,29,149]	L=[0,1,0,1,0]	M=[2,5,13,29,197]	L=[0,0,1,0,1]
M=[2,5,13,61,97]	L=[0,1,1,0,0]	M=[2,5,17,29,157]	L=[0,1,1,1,0]
M=[2,5,13,17,353]	L=[0,1,1,1,0]	M=[2,13,17,29,61]	L=[0,0,0,1,1]
M=[2,5,29,37,73]	L=[0,1,1,0,1]	M=[2,5,17,53,89]	L=[0,0,0,0,1]
M=[2,5,37,41,53]	L=[0,0,1,1,1]	M=[2,5,13,17,373]	L=[0,0,1,0,1]
M=[2,5,13,37,173]	L=[0,0,1,1,0]	M=[2,5,13,73,89]	L=[0,1,1,0,1]
M=[2,5,29,41,73]	L=[0,1,1,1,0]	M=[2,5,13,37,181]	L=[0,1,0,1,0]
M=[2,5,17,29,181]	L=[0,1,0,0,1]	M=[2,5,17,53,101]	L=[0,1,1,0,1]
M=[2,5,13,73,97]	L=[0,0,0,1,1]	M=[2,5,17,61,89]	L=[0,1,0,1,1]
M=[2,5,37,41,61]	L=[0,1,0,1,1]	M=[2,5,17,37,149]	L=[0,1,0,1,0]
M=[2,13,17,41,53]	L=[0,1,0,0,1]	M=[2,5,17,29,197]	L=[0,1,0,0,1]

2.3. Main characterization of $\mathbf{N}(\varepsilon_K)$. Assume that $-1 \in \mathbf{N}(K^\times)$ and let $\mathbf{S} := \mathbf{N}(\varepsilon_K)$.

When $\mathbf{S} = 1$, the non-canonical relation $\mathbf{m} = \prod_{q|m} q = (\alpha)$, of support $m \mid M$ distinct from 1 and M , comes from Theorem 2.1 (ii); it suffices to determine the quadratic integer α , without any rational factor, deduced from $\varepsilon_K + 1$, this giving \mathbf{m} . In the same way $\varepsilon_K - 1$ gives $\mathbf{n} = (\beta)$ of support $n = \frac{M}{m}$ such that $\mathbf{mn} = (\alpha\beta) = (\sqrt{M})$.

Let's give some numerical examples of the process leading to the result:

(i) For $M = 15170 = 2 \cdot 5 \cdot 37 \cdot 41$, $\varepsilon_K = 739 + 6\sqrt{M}$ and:

$$\varepsilon_K + 1 = 740 + 6\sqrt{M} = 2 \times (370 + 3\sqrt{M}),$$

where $2 = \mathbf{gcd}(740, 6)$; then $\mathbf{gcd}(370, M) = 370 = 2 \cdot 5 \cdot 37$, whence the principality of $\mathfrak{m} = \mathfrak{q}_2 \mathfrak{q}_5 \mathfrak{q}_{37}$, which immediately gives the principality of \mathfrak{q}_{41} that can be obtained from:

$$-\varepsilon_K + 1 = -738 - 6\sqrt{M} = -6 \times (123 + \sqrt{M}),$$

for which $\mathbf{gcd}(123, M) = 41$.

(ii) For $M = 141245 = 5 \cdot 13 \cdot 41 \cdot 53$, $\varepsilon_K = 49609 + 132\sqrt{M}$ and:

$$\varepsilon_K + 1 = 49610 + 132\sqrt{M} = 22 \times (2255 + 6\sqrt{M}),$$

where $22 = \mathbf{gcd}(49610, 132)$ and $\mathbf{gcd}(2255, M) = 5 \cdot 41$ giving the principality of $\mathfrak{q}_5 \mathfrak{q}_{41}$, and the principality of $\mathfrak{q}_{13} \mathfrak{q}_{53}$, also obtained from $-\varepsilon_K + 1 = -12 \times (4134 + 11\sqrt{M})$ and $\mathbf{gcd}(4134, M) = 13 \cdot 53$.

(iii) For $M = 999826 = 2 \cdot 41 \cdot 89 \cdot 137$, $\varepsilon_K + 1$ is given by:

$$\begin{aligned} &11109636935777158836160759499956087745610931184259730878643242570969499893 \\ &0608609351188823863817034706422630544237192750927410464023060264033743426 \\ &+111106036003421265074388547121779710827974912909282096975471217501055084 \\ &481117390502436801341332286005566466631729812289759396153149523058885768\sqrt{M} \end{aligned}$$

with the \mathbf{gcd} of the two coefficients equal to:

$$\begin{aligned} &21082286734619551653000708969094423248037542899079230940776043942241398 \\ &= 2 \times 3 \times 43 \times 11210269457991049 \times 7289235104943832975100088612482411236091543240227619, \end{aligned}$$

giving the integer $A + B\sqrt{M} \in \mathbf{Z}_K$ equal to:

$$\begin{aligned} &5269654604181931962753271711433450204598096091653697788648087227648861999187 \\ &+ 5270113123970195868835491287611281655343354587474034791159597224413298316\sqrt{M} \end{aligned}$$

then $\mathbf{gcd}(A, M) = 41 \times 89 \times 137$, giving the principality of:

$$\begin{aligned} \mathfrak{q}_{41} \mathfrak{q}_{89} \mathfrak{q}_{137} = & (5269654604181931962753271711433450204598096091653697788648087227648861999187 \\ & + 5270113123970195868835491287611281655343354587474034791159597224413298316\sqrt{M}) \end{aligned}$$

or simply that of \mathfrak{q}_2 .

Theorem 2.4. *Let $M \geq 2$ be a square-free integer and put $K = \mathbb{Q}(\sqrt{M})$; we assume that $-1 \in \mathbf{N}(K^\times)$. Let $\varepsilon_K = a + b\sqrt{M}$ ($a, b \in \mathbb{Z}$ or $\frac{1}{2}\mathbb{Z}$) be the fundamental unit of K . We consider the following integers $A + B\sqrt{M}$, $A' + B'\sqrt{M} \in \mathbf{Z}_K$, $A, B, A', B' \in \mathbb{Z}$ or $\frac{1}{2}\mathbb{Z}$, where the \mathbf{gcd} function must be understood in \mathbf{Z}_K , giving for instance, $\mathbf{gcd}(\frac{1}{2}U_0, \frac{1}{2}V_0) = \mathbf{gcd}(U_0, V_0)$ for U_0 and V_0 odd; in other words one may see g and g' below as the maximal rational integer factors of the quadratic integers:¹*

$$\begin{aligned} \varepsilon_K + 1 &= a + 1 + b\sqrt{M} =: g(A + B\sqrt{M}), \quad g := \mathbf{gcd}(a + 1, b), \\ \varepsilon_K - 1 &= a - 1 + b\sqrt{M} =: g'(A' + B'\sqrt{M}), \quad g' := \mathbf{gcd}(a - 1, b). \end{aligned}$$

Let $m := \mathbf{gcd}(A, M)$, $n = \frac{M}{m}$, $C = \frac{A}{m}$, $m' := \mathbf{gcd}(A', M)$, $n' = \frac{M}{m'}$, $C' = \frac{A'}{m'}$.

(i) *If M is odd, ε_K is of norm $\mathbf{S} = 1$ if and only if $(m, m') \neq (1, 1)$.*

If M is even, ε_K is of norm $\mathbf{S} = 1$ if and only if, either $m > 2$ or else $m' > 2$.

In other words, the characterization of $\mathbf{S} = -1$ becomes:

If M is odd, ε_K is of norm $\mathbf{S} = -1$ if and only if $m = m' = 1$.

If M is even, ε_K is of norm $\mathbf{S} = -1$ if and only if $m = m' = 2$.

(ii) *If the above conditions giving $\mathbf{S} = 1$ hold, then $\prod_{q|m} \mathfrak{q} = (\alpha)$ and $\prod_{q|n} \mathfrak{q} = (\beta)$, with $\alpha = Cm + B\sqrt{M}$ and $\beta = Bn + C\sqrt{M}$ in \mathbf{Z}_K .*

Proof. We do not consider the particular case $r = 1$ giving $\mathbf{S} = -1$ and $\mathcal{H}_K^G = \mathcal{H}_K^{\text{ram}} = 1$; we prove the characterization of $\mathbf{S} = 1$ of the statement.

• Let's assume $\mathbf{S} = 1$:

Recall, from Theorem 2.1, that since $(\varepsilon_K + 1)^{1-\sigma} = \varepsilon_K$, the ideal $(\varepsilon_K + 1)$ gives, after elimination of its maximal rational factor, the unique non-canonical relation of principality $\mathfrak{m} = (\alpha)$, of support $m \mid M$, $m \neq 1, M$, between the ramified primes.

¹The PARI/GP \mathbf{gcd} function gives instead $\mathbf{gcd}(\frac{1}{2}U_0, \frac{1}{2}V_0) = \frac{1}{2}\mathbf{gcd}(U_0, V_0)$; this gap only occurs when M is odd, in which case this does not matter for the computation of the odd integers m and m' .

Since $(\sqrt{M} \cdot (\varepsilon_K + 1))^{1-\sigma} = -\varepsilon_K$ and $(\varepsilon_K - 1)^{1-\sigma} = -\varepsilon_K$, the ideals $(\sqrt{M} \cdot (\varepsilon_K + 1))$ (leading to $\mathfrak{n} = (\beta)$ of support $n = \frac{M}{m}$) and $(\varepsilon_K - 1)$ (leading to $\mathfrak{m}' = (\alpha')$ of support m') yield the same non-canonical relations of supports n and m' , so that $n = m'$, with m, n distinct from 1, M .

One obtains the suitable condition $m \neq 1$ and $m' = n \neq 1$ when M is odd; if M is even, the integers $m, m' = n$ are of different parity, distinct from 1 and M and such that $mm' = M > 2$; so, if we assume, for instance, $m \leq 2$ (hence $m = 2$), this implies $m' = \frac{M}{m} > 2$.

- Reciprocal. We assume $m \neq 1$ (resp. $m > 2$ or $m' > 2$) if M is odd (resp. even):

In the odd case, $\varepsilon_K \equiv -1 \pmod{\mathfrak{m}}$, \mathfrak{m} of support m , implies $\varepsilon_K^\sigma \equiv -1 \pmod{\mathfrak{m}}$, whence $\mathbf{S} = \varepsilon_K^{1+\sigma} \equiv 1 \pmod{m}$ thus $\mathbf{S} = 1$ since $m \neq 1$ implies $m > 2$ in the odd case.

In the even case, since $m > 2$ or $m' > 2$, the same conclusion holds, using one of the congruence $\varepsilon_K \equiv -1 \pmod{\mathfrak{m}}$ or $\varepsilon_K \equiv 1 \pmod{\mathfrak{m}'}$ (note that in the reciprocal one does not know if $m' = n$).

- The characterization of $\mathbf{S} = -1$ is of course obvious, but the precise statement is crucial for statistical interpretation, especially in the even case:

– In the odd case, one gets $\bar{m} = m' = 1$.

– In the even case, one gets $m \leq 2$ & $m' \leq 2$, but we have $m \neq 1$ and $m' \neq 1$; indeed, let $\varepsilon_K = a + b\sqrt{M}$, $a, b \in \mathbb{Z}$, where $a^2 - Mb^2 = -1$ implies a and b odd (the case of a is obvious, so $a^2 \equiv 1 \pmod{8}$, then b even would imply $1 \equiv -1 \pmod{8}$). Since $\varepsilon_K \equiv 1 \pmod{\mathfrak{q}_2}$ with b odd, necessarily $\varepsilon_K \not\equiv 1 \pmod{2}$ and $(\varepsilon_K + 1) = \mathfrak{q}_2 \mathfrak{a}$, where \mathfrak{a} is an odd ideal and, except for $M = 2$, one gets $\mathfrak{a} \neq 1$, then $(\varepsilon_K^\sigma + 1) = \mathfrak{q}_2 \mathfrak{a}^\sigma$, whence $(\varepsilon_K - 1) = \mathfrak{q}_2 \mathfrak{a}^\sigma$. Then the integers $g = \mathbf{gcd}(a + 1, b)$ and $g' = \mathbf{gcd}(a - 1, b)$ are odd, which gives $A \equiv A' \equiv 0 \pmod{2}$, hence $m = m' = 2$ which is also equivalent to b odd.

- The last claim is immediate since $(A + B\sqrt{M}) = (Cm + B\sqrt{M})$ is invariant by σ , without any rational factor, which leads to $(\sqrt{M}(Cm + B\sqrt{M})) = (Cm\sqrt{M} + BM) = m(B + C\sqrt{M})$ giving rise to $(B + C\sqrt{M})$ without any rational factor. \square

Remark 2.5. (i) In the case M even with $\mathbf{S} = -1$, the ideals $(\varepsilon_K \pm 1)$ do not define invariant classes (except that of \mathfrak{q}_2 in $\mathbb{Q}(\sqrt{2})$ since $(\varepsilon_2 + 1) = (2 + \sqrt{2}) = \sqrt{2} \cdot \varepsilon_2$ and $(\varepsilon_2 - 1) = (\sqrt{2})$; this comes from the fact that it is the unique even case where $\mathcal{H}_K^G = 1$).

But \mathfrak{q}_2 is not principal since there is no non-canonical relation of principality in the case $\mathbf{S} = -1$ (e.g., $M \in \{10, 26, 58, 74, 82, 106, 122, 130, 170\}$).

To get illustrations for M even, $\mathbf{S} = -1$, the following program computes the class group of K (in $\text{HK} = \text{K.clgp}$), then (in R) the components of the (non-trivial) class of \mathfrak{q}_2 :

```
{forstep(M=2,10^6,2,if(core(M)!=M,next);K=bnfinit(x^2-M,1);
S=norm(K.fu[1]);if(S=1,next);q2=component(idealfactor(K,2),1)[1];
R=bnfisprincipal(K,q2)[1];print("M=",M," R=",R," HK=",K.clgp)}}
```

M=10	R=[1]	HK=[2, [2]]	M=199810	R=[0, 0, 1, 1]	HK=[128, [16, 2, 2, 2]]
M=82	R=[2]	HK=[4, [4]]	M=519514	R=[32, 1]	HK=[128, [64, 2]]
M=130	R=[0, 1]	HK=[4, [2, 2]]	M=613090	R=[32, 0, 1]	HK=[256, [64, 2, 2]]
M=226	R=[4]	HK=[8, [8]]	M=690562	R=[16, 2]	HK=[128, [32, 4]]
M=442	R=[0, 1]	HK=[8, [4, 2]]	M=700570	R=[8, 1, 0, 1]	HK=[128, [16, 2, 2, 2]]
M=2210	R=[1, 1, 1]	HK=[8, [2, 2, 2]]	M=720802	R=[16, 0]	HK=[128, [32, 4]]
M=3026	R=[2, 2]	HK=[16, [4, 4]]	M=776866	R=[16, 0, 0]	HK=[128, [32, 2, 2]]

But we have the cases M even and $\mathbf{S} = 1$ (e.g., $M \in \{34, 146, 178, 194, 386, 410, 466, 482, 514, 562\}$), where relations \mathfrak{q}_2 principal are more frequent when r is small (e.g., $M \in \{34, 146, 178, 194, 386, 466, 482\}$; for $M = 410$, the relation is given by $m = 41, n = 10$).

(ii) Consider the field $L = K(\sqrt{2})$ for M even, $M =: 2M'$; the extension L/K is unramified since $\mathbb{Q}(\sqrt{M'})/\mathbb{Q}$ is not ramified at 2. The extension of \mathfrak{q}_2 in L becomes the principal ideal $(\sqrt{2})$ whatever the decomposition of 2 in $\mathbb{Q}(\sqrt{M'})/\mathbb{Q}$. Meanwhile, if 2 is inert in this extension (i.e., $M' \equiv 5 \pmod{8}$), \mathfrak{q}_2 can not be principal in K , otherwise, if $\mathfrak{q}_2 = (\alpha)$, then, in L , $\alpha = \eta\sqrt{2}$, where η is a unit of L , and by unicity of radicals (up to K^\times) this is absurd and the class of \mathfrak{q}_2 capitulates in L .

So either $m = 2$ & $m' = 2$, with \mathfrak{q}_2 non-principal and $\mathbf{S} = -1$ (e.g., $M \in \{10, 26, 58, 74, 82, 106, 122\}$ showing that reciprocal does not hold since 2 may split in $\mathbb{Q}(\sqrt{M'})/\mathbb{Q}$,

as for $M = 82$), or else $m = 2$ & $m' > 2$, giving the principality of q_2 and $\mathbf{S} = 1$ (e.g., all the previous cases $M \in \{34, 146, 178, 194, 386, 466, 482\}$).

2.4. Computation of \mathbf{S} by means of the gcd criterion. The following PARI/GP program computes (if any) the non-canonical relation of principality \mathbf{m} distinct from (1), (\sqrt{M}) between the ramified primes, *only by means of the previous result on the coefficients of the fundamental unit* (Theorem 2.4), and deduces the norm S without calculating it; when there are no non-canonical relations (whence $\mathbf{S} = -1$), the corresponding data is empty. One has only to give the bound BD of the discriminants D whose odd prime divisors are congruent to 1 modulo 4. The counters CD , Cm , Cp , C22 , enumerate the sets \mathcal{D} , \mathcal{D}^- , \mathcal{D}^+ and the set \mathcal{D}_{22}^- of cases where $m = m' = 2$ (equivalent to M even and $\mathbf{S} = -1$), respectively; for short we do not write the cases where $m = 1$, giving $\mathbf{S} = -1$ ($M \in \{5, 13, 17, 29, 37, \dots\}$):

```

MAIN PROGRAM COMPUTING S VIA THE RELATIONS OF PRINCIPALITY
{BD=10^7;CD=0;Cm=0;Cp=0;C22=0;for(D=5,BD,v=valuation(D,2);if(v!=0 & v!=3,next);
i0=1;M=D;if(v=3,M=D/4;i0=2);if(core(M)!=M,next);if(Mod(M,4)==3,next);
r=omega(M);f=factor(M);ellM=component(f,1);for(i=i0,r,ell=ellM[i];
if(Mod(ell,4)==3,next(2));CD=CD+1;res=lift(Mod(M,2));e=quadunit(D);
Y=component(e,3)/(res+1);X=component(e,2)+res*Y;g=gcd(X+1,Y);m=gcd((X+1)/g,M);
if(m==1,S=-1;print("D=",D," M=",M," relations: ",",",",",",",",", S=",S);Cm=Cm+1);
if(m>2,S=1;print("D=",D," M=",M," relations: ",m,",",M/m,", S=",S);Cp=Cp+1);
if(m==2,gp=gcd(X-1,Y);mp=gcd((X-1)/gp,M);
if(mp>2,S=1;print("D=",D," M=",M," relations: ",m,",",mp,", S=",S);Cp=Cp+1);
if(mp==2,S=-1;print("D=",D," M=",M," relations: ",",",",",",",",", S=",S,",",", m=mp=2");
Cm=Cm+1;C22=C22+1));
print("CD=",CD," Cm=",Cm," Cp=",Cp," C22=",C22);
print("Cm/CD=",Cm/CD+0.0," Cp/CD=",Cp/CD+0.0);
print("C22/CD=",C22/CD+0.0," C22/Cm=",C22/Cm+0.0)}

```

```

D=8 M=2      relations:  , , S=-1, m=mp=2
D=40 M=10   relations:  , , S=-1, m=mp=2
D=104 M=26  relations:  , , S=-1, m=mp=2
D=136 M=34  relations:  2,17, S=1
D=205 M=205 relations:  5,41, S=1
D=221 M=221 relations:  17,13, S=1
D=232 M=58  relations:  , , S=-1, m=mp=2
D=296 M=74  relations:  , , S=-1, m=mp=2
D=305 M=305 relations:  5,61, S=1
D=328 M=82  relations:  , , S=-1, m=mp=2
D=377 M=377 relations:  13,29, S=1
D=424 M=106 relations:  , , S=-1, m=mp=2
D=488 M=122 relations:  , , S=-1, m=mp=2
D=505 M=505 relations:  5,101, S=1
D=520 M=130 relations:  , , S=-1, m=mp=2
D=545 M=545 relations:  109,5, S=1
D=584 M=146 relations:  73,2, S=1
D=680 M=170 relations:  , , S=-1, m=mp=2
D=689 M=689 relations:  53,13, S=1
D=712 M=178 relations:  89,2, S=1
D=745 M=745 relations:  149,5, S=1
D=776 M=194 relations:  2,97, S=1
D=793 M=793 relations:  13,61, S=1
D=808 M=202 relations:  , , S=-1, m=mp=2
D=872 M=218 relations:  , , S=-1, m=mp=2
D=904 M=226 relations:  , , S=-1, m=mp=2
D=905 M=905 relations:  181,5, S=1
D=1096 M=274 relations:  , , S=-1, m=mp=2
D=1160 M=290 relations:  , , S=-1, m=mp=2
D=1192 M=298 relations:  , , S=-1, m=mp=2
D=1205 M=1205 relations:  5,241, S=1
D=1256 M=314 relations:  , , S=-1, m=mp=2
D=1345 M=1345 relations:  269,5, S=1
D=1384 M=346 relations:  , , S=-1, m=mp=2
D=1405 M=1405 relations:  5,281, S=1
D=1448 M=362 relations:  , , S=-1, m=mp=2
D=1469 M=1469 relations:  13,113, S=1
D=1480 M=370 relations:  , , S=-1, m=mp=2
D=1513 M=1513 relations:  17,89, S=1

```


D=1517 M=1517 relations: 41,37, S=1
 D=1537 M=1537 relations: 29,53, S=1
 D=1544 M=386 relations: 2,193, S=1
 D=1576 M=394 relations: , , S=-1, m=mp=2
 D=1640 M=410 relations: 41,10, S=1
 D=1717 M=1717 relations: 17,101, S=1
 D=1768 M=442 relations: , , S=-1, m=mp=2
 D=1832 M=458 relations: , , S=-1, m=mp=2
 D=1864 M=466 relations: 233,2, S=1
 D=1885 M=1885 relations: 29,65, S=1
 D=1928 M=482 relations: 2,241, S=1
 D=1945 M=1945 relations: 389,5, S=1
 D=1961 M=1961 relations: 37,53, S=1
 (...)
 D=9999592 M=2499898 relations: , , S=-1, m=mp=2
 D=9999617 M=9999617 relations: 21881,457, S=1
 D=9999665 M=9999665 relations: 153841,65, S=1
 D=9999688 M=2499922 relations: , , S=-1, m=mp=2
 D=9999709 M=9999709 relations: 113,88493, S=1
 D=9999784 M=2499946 relations: 353,7082, S=1
 D=9999797 M=9999797 relations: 34129,293, S=1
 D=9999821 M=9999821 relations: 1381,7241, S=1
 D=9999845 M=9999845 relations: 1999969,5, S=1
 D=9999944 M=2499986 relations: 73529,34, S=1
 D=9999953 M=9999953 relations: 270269,37, S=1
 D=9999977 M=9999977 relations: 277,36101, S=1
 BD=10⁷:
 CD=866200 Cm=691947 Cp=174253 C22=70295
 Cm/CD =0.79883052 Cp/CD =0.20116947
 C22/CD=0.08115331 C22/Cm=0.10159015

3. REMARKS ON DENSITY QUESTIONS

A classical principle in number theory is to examine some deep invariants (as class groups, units, etc.) of families of fields (assuming, in general, that some parameters are fixed, as for instance, the Galois group, the signature, etc.), classified regarding the discriminants. The analytic reason is that the order of magnitude of $\frac{h_K \cdot R_K}{\sqrt{D_K}}$ is controlled by suitable ζ -functions and then, if the discriminant D_K increase in the family, the class number h_K and/or the regulator R_K increase or, at least, have a larger complexity. This case represents the reality quite well in a global context, but it can be questioned for p -adic framework or non semi-simple Galois setting. We intend to give some remarks in this direction about the norm of $\mathbf{S} = \mathbf{N}(\varepsilon_K)$ linked significantly to the 2-class group.

3.1. Classical approach of the density. We will describe the case of $\mathbf{S} = -1$, using the following definitions:

Definitions 3.1. (i) Denote by \mathcal{M} (resp. \mathcal{D}) the set of all Kummer radicals (resp. of all Discriminants), such that $-1 \in \mathbf{N}(K^\times)$. We have, from a result of Rieger [Rie]:

$$\#\mathcal{M}_{\leq \mathbf{X}} \approx \frac{3}{2\pi} \prod_{p \equiv 1 \pmod{4}} \left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}} \frac{\mathbf{X}}{\sqrt{\log(\mathbf{X})}} \approx \frac{0.464592... \mathbf{X}}{\sqrt{\log(\mathbf{X})}}, \quad \#\mathcal{D}_{\leq \mathbf{X}} \approx \frac{3}{4} \#\mathcal{M}_{\leq \mathbf{X}}.$$

(ii) Denote by $\mathcal{M}^- \subset \mathcal{M}$ (resp. $\mathcal{D}^- \subset \mathcal{D}$) the subset of all Kummer radicals (resp. of all Discriminants), such that $\mathbf{S} := \mathbf{N}(\varepsilon_K) = -1$ and put:

$$\Delta_{\text{disc}}^- := \lim_{\mathbf{X} \rightarrow \infty} \frac{\mathcal{M}_{\leq \mathbf{X}}^-}{\mathcal{M}_{\leq \mathbf{X}}} = \lim_{\mathbf{X} \rightarrow \infty} \frac{\mathcal{D}_{\leq \mathbf{X}}^-}{\mathcal{D}_{\leq \mathbf{X}}}.$$

Many heuristics have given Δ_{disc}^- around 0.5 or 0.6. Our characterization would give a density around $\frac{3}{2} \cdot \left(\frac{6}{\pi^2}\right)^2 \approx 0.554363041753...$, but without a precise classification by means of ascending discriminants or of number of ramified primes, a context using structure of the 2-class group, whence quadratic symbols, Rédei's matrices, Furuta symbols [Fu], etc. These classical principles consist in using the filtration of the 2-class group following, e.g., the theoretical algorithm described in whole generality in [Gra3], with the

fixed point formulas generalizing that of Chevalley–Herbrand (say for the quadratic case):

$$\#(\mathcal{H}_K^{i+1}/\mathcal{H}_K^i) = \frac{2^{r-1}}{(\Lambda_K^i : \Lambda_K^i \cap \mathbf{N}(K^\times))}, \quad i \geq 0,$$

where $\mathcal{H}_K^i = \text{Ker}(1 - \sigma)^i$, the Λ_K^i 's, with $\Lambda_K^i \subseteq \Lambda_K^{i+1}$ for all i , defining a sequence of suitable subgroups of \mathbb{Q}^\times ; more precisely, $\Lambda_K^0 = \langle -1 \rangle$, $\Lambda_K^1 = \langle -1, q_1, \dots, q_r \rangle$, the next Λ_K^{i+1} 's introducing “random” numbers $b = \mathbf{N}(b)$ from identities of the form $\mathbf{a} = (y)b^{1-\sigma}$, when $x \in \Lambda_K^i$ is such that $(x) = \mathbf{N}(a) = \mathbf{N}(y)$, $cl(a) \in \mathcal{H}_K^i$, $y \in K^\times$.

Then the index $(\Lambda_K^i : \Lambda_K^i \cap \mathbf{N}(K^\times))$ being nothing else than $\#\rho_K^i(\Lambda_K^i)$, where ρ_K^i is the r -uple of Hasse’s norm residue symbols giving rise to generalized “Rédei matrices of quadratic residue symbols”, or more simply, random maps $\mathbb{F}_2^{r_i} \rightarrow \mathbb{F}_2^{r-1}$ (product formula of the symbols), $r_i = \dim_{\mathbb{F}_2}(\Lambda_K^i/(\Lambda_K^i)^2)$.

Similar viewpoints are linking the norm of ε_K to the structure of the 2-class group in the restricted sense (see many practical examples in [Gra2]).

This proportion of \mathcal{D}^- inside \mathcal{D} ([St, § 1, p. 122], [BoSt, (1.3), p. 1328]), was conjectured by Stevenhagen to be:

$$P = 1 - \prod_{k \geq 0} \left(1 - \frac{1}{2^{1+2k}}\right) \approx 0.5805775582 \dots$$

We refer to [St], then to [FK2, KoPa2] for history and bibliographical comments about the norm of the fundamental unit of $\mathbb{Q}(\sqrt{M})$ and for his heuristic based on the properties of densities P_t , corresponding to discriminants having t distinct prime factors.

These results involving the 2-class groups structures allow informations about Δ_{disc}^- and especially the determination of lower and upper bounds. For this aspect, we refer to the Chan–Koymans–Milovic–Pagano paper [CKMP] who had proven that Δ_{disc}^- is larger than 0.538220, improving Fouvry–Klüners results [FK1, FK2] saying that Δ_{disc}^- lies between 0.524275 and 0.6666666, which gave $0.538220 \leq \Delta_{\text{disc}}^- \leq 0.6666666$.

For $\mathbf{X} = 10^8$, a PARI [P] calculation gives the experimental density $\frac{\#\mathcal{D}_{\leq \mathbf{X}}^-}{\#\mathcal{D}_{\leq \mathbf{X}}} \approx 0.787255$.

Moreover, it is well known that such partial densities decrease as \mathbf{X} increases; in other words, computer approaches are misleading as explained in [St]. More precisely the arithmetic function $\omega(x)$ giving the number of prime divisors of x fulfills the optimal upper bound $\omega(x) \leq (1 + o(1)) \frac{\log(x)}{\log(\log(x))}$ [Ten, I.5.3], so that large Kummer radicals have “more prime divisors”, whence more important probability to get $\mathbf{S} = -1$.

In the present paper, we do not use these classical ways, so that the main question is to understand how densities may be defined; let’s give the example of classification by ascending traces before giving that of the gcd criterion.

3.2. Classification by ascending traces of fundamental units. In another direction, let’s apply the “First Occurrence Process” algorithm [Gra4, Section 4, Theorem 4.6] in the interval $[1, \mathbf{B}]$, simultaneously for the two cases $s = -1$ and $s = 1$ of the polynomials $m_s(t) = t^2 - 4s$, under the condition $-1 \in \mathbf{N}(K^\times)$ (to be checked only for $s = 1$).

Recall that in the set $\mathcal{T}_{\leq \mathbf{B}}$ of traces $\mathbf{T}(\varepsilon_K) \leq \mathbf{B}$, $\mathcal{T}_{\leq \mathbf{B}}^+$, $\mathcal{T}_{\leq \mathbf{B}}^-$, denote the corresponding subsets of traces $t \leq \mathbf{B}$ of fundamental units, of norm $s = -1$, $s = 1$, respectively.

As $\mathbf{B} \rightarrow \infty$, all units are represented in these lists, as shown with the following PARI program. Indeed, this is clear with $t^2 + 4 = Mr^2$ giving $\mathcal{T}_{\leq \mathbf{B}}^-$, and from [Gra4, Theorem 4.6 and Corollaries], the set $\mathcal{T}_{\leq \mathbf{B}}^+$ deals with minimal traces t for which $t^2 - 4 = Mr^2$ gives the unit ε_K (if $\mathbf{S} = 1$) or ε_K^2 (if $\mathbf{S} = -1$), but the squares of units of norm -1 were obtained with $t^2 + 4$ for a smaller trace, so that the process eliminates this data in the final list. Finally the densities dp, dm are that of units of norms $1, -1$, respectively.

```
PROGRAM FOR DENSITY OF UNITS OF NORM 1 AND OF NORM -1
{B=10^6;Cm=0;Cp=0;LM=List;for(t=1,B,mtm=t^2+4;M=core(mtm);L=List([M,-1]);
listput(LM,vector(2,c,L[c]));mtp=t^2-4;if(mtp<=0,next);M=core(mtp);
r=omega(M);i0=1;if(Mod(M,2)=0,i0=2);f=factor(M);e1lM=component(f,1);
T=1;for(i=i0,r,c=e1lM[i];if(Mod(c,4)!=1,T=0;break));if(T==1,L=List([M,1]);
listput(LM,vector(2,c,L[c])))};VM=vecsort(vector(B,c,LM[c]),1,8);print(VM);
for(k=1,#VM,S=VM[k][2];if(S==1,Cp=Cp+1);if(S==-1,Cm=Cm+1));
print("#VM=",#VM," Cp=",Cp," Cm=",Cm," dp=",Cp/#VM+0., " dm=",Cm/#VM+0.)}
```

VM=
 [2,-1],[5,-1],[10,-1],[13,-1],[17,-1],[26,-1],[29,-1],[34,1],[37,-1],[41,-1],
 [53,-1],[58,-1],[61,-1],[65,-1],[73,-1],[74,-1],[82,-1],[85,-1],[89,-1],[97,-1],
 [101,-1],[106,-1],[109,-1],[113,-1],[122,-1],[130,-1],[137,-1],[145,-1],[146,1],
 [149,-1],[157,-1],[170,-1],[173,-1],[178,1],[181,-1],[185,-1],[194,1],[197,-1],
 [202,-1],[205,1],[218,-1],[221,1],[226,-1],[229,-1],[233,-1],[257,-1],[265,-1],
 [269,-1],[274,-1],[277,-1],[290,-1],[293,-1],[298,-1],[305,1],[314,-1],[317,-1],
 [346,-1],[349,-1],[353,-1],[362,-1],[365,-1],[370,-1],[373,-1],[377,1],[386,1],
 [389,-1],[397,-1],[401,-1],[410,1],[421,-1],[442,-1],[445,-1],[458,-1],[461,-1],
 [482,1],[485,-1],[493,-1],[505,1],[509,-1],[514,1],[530,-1],[533,-1],[538,-1],
 [545,1],[554,-1],[557,-1],[565,-1],[577,-1],[610,-1],[613,-1],[626,-1],[629,-1],
 [653,-1],[674,1],[677,-1],[685,-1],[689,1],[697,-1],[698,-1],[701,-1],[706,1],
 (...)
 [906781966997,1],[906781967005,-1],[906785776013,-1],[906789585029,-1],
 [906793394053,-1],[906797203085,-1],[906804821173,-1],[906808630229,-1],
 [906812439293,-1],[906816248365,-1],[906820057445,-1],[906823866533,-1],
 [906827675629,-1],[906831484733,-1],[906835293845,-1],[906839102965,-1],
 [906842912093,-1],[906846721229,-1]
 #VM=998781 Cp=46622 Cm=952159 dp=0.0466789015 dm=0.9533210984

For $\mathbf{B} = 10^7$, the data becomes:

#VM=9996335 Cp=400433 Cm=9595902 dp=0.0400579812 dm=0.9599420187

In that context, $\varepsilon_K = a + b\sqrt{M}$ is written $\frac{1}{2}(t + r\sqrt{M})$ and only units with too large traces are missing in the above finite list. Restricting to the density Δ_{trace}^- of the set of units of norm -1 inside the set of units classified by ascending traces, one gets:

Theorem 3.2. We have $\Delta_{\text{trace}}^- := \lim_{\mathbf{B} \rightarrow \infty} \frac{\#\mathcal{T}_{\leq \mathbf{B}}^-}{\#\mathcal{T}_{\leq \mathbf{B}}} = 1$.

Proof. From [Gra4, Theorem 4.5], we have $\#\mathcal{T}_{\leq \mathbf{B}}^- \sim \mathbf{B} - O(\sqrt[3]{\mathbf{B}})$. □

3.3. Approximations of the density from the gcd principle. Theorem 2.4, on the characterization of the norm \mathbf{S} of ε_K , allows heuristics for densities since the statement reduces to elementary arithmetic properties. The criterion only depends on properties of $m = \mathbf{gcd}(A, M)$ and $m' = \mathbf{gcd}(A', M)$ whose “probabilities” may be computed, assuming that the the pairs (A, M) and (A', M) are random with Kummer radicals taken in the subset of square-free integers, without using the natural order of radicals or discriminants, nor that of the order of magnitude of the integers A, A' depending on the unpredictable trace of the unit.

Before giving some heuristics, we introduce the partial densities corresponding to the six cases summarized by the following array, with numerical values obtained for M in various intervals $[bM, BM]$:

$M \in [bM, BM]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	↓	$\delta_{2,2}^{\text{even}}$
even	= 2	> 2	= 1	↓	$\delta_{2,m'}^{\text{even}}$
even	> 2	= 2	= 1	↓	$\delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	↑	$\delta_{m,m'}^{\text{odd}}$

Notations of partial densities are given in the right column; the densities $\delta_{2,m'}^{\text{even}}$ and $\delta_{m,2}^{\text{even}}$, corresponding to each sign in formulas of $\varepsilon_K \pm 1$, are indistinguishable about the cases $m = 2 \ \& \ m' > 2$ or $m > 2 \ \& \ m' = 2$, so we will only give the sum $\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$. Then $\delta_{2,2}^{\text{even}}$ represent the cases M even, $\mathbf{S} = -1$ where \mathfrak{q}_2 is not principal. The densities $\delta_{1,1}^{\text{odd}}$ (resp. $\delta_{m,m'}^{\text{odd}}$) represent the cases $\mathbf{S} = -1$ with no principality relations (resp. $\mathbf{S} = 1$ with the two complementary principality relations). We put $\Delta_{\text{gcd}}^- := \delta_{1,1}^{\text{odd}} + \delta_{2,2}^{\text{even}}$.

Many tests, using the following program, have been done and have shown that some densities increase while the others decrease as the Kummer radicals are taken in larger intervals (indicated with arrows \uparrow and \downarrow):

```
{bM=2;BM=10^6;CM=0;C22=0;C2p=0;Cm2=0;Cmp=0;CC11=0;CCmp=0;
for (M=bM, BM, res8=Mod(M, 8); if (res8!=1&res8!=2&res8!=5, next);
if (core(M)!=M, next); res=Mod(M, 2); i0=1; if (res==0, i0=2);
```

```

r=omega(M);f=factor(M);ellM=component(f,1);for(i=i0,r,ell=ellM[i];
if(Mod(ell,4)==3,next(2));D=M;if(res==0,D=4*M);CM=CM+1;e=quadunit(D);
res=lift(res);Y=component(e,3)/(res+1);X=component(e,2)+res*Y;
g=gcd(X+1,Y);A=(X+1)/g;m=gcd(A,M);gp=gcd(X-1,Y);Ap=(X-1)/gp;mp=gcd(Ap,M);
if(res==0,
if(m==2 & mp==2,C22=C22+1);if(m==2 & mp>2,C2p=C2p+1);
if(m>2 & mp==2,Cm2=Cm2+1);if(m>2 & mp>2,Cmp=Cmp+1));
if(res==1,
if(m==1 & mp==1,CC11=CC11+1);if(m>2 & mp>2,CCmp=CCmp+1));
print("CM=",CM," C22=",C22," C2p=",C2p," Cm2=",Cm2," Cmp= ",Cmp,
" CC11=",CC11," CCmp= ",CCmp);
d22=C22/CM+0.0;d2p=C2p/CM+0.0;dm2=Cm2/CM+0.0;
dmp=Cmp/CM+0.0;dd11=CC11/CM+0.0;ddmp=CCmp/CM+0.0;
print("Sum=",C22+C2p+Cm2+Cmp+CC11+CCmp);
print("d22=",d22," d2p=",d2p," dm2=",dm2," dmp=",dmp,
" dd11=",dd11," ddmp=",ddmp)}

```

$M \in [1, 10^6]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2347176480 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.0652421881 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0389107558 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5475861515 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1135432564 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 124490,

C22 = 29220 C2p = 4079, Cm2 = 4043, Cmp = 4844, CC11 = 68169, CCmp = 14135,

$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.3388705920 \downarrow$,

$\delta_{2,2}^{\text{even}} = 0.2347176480 \downarrow$, $(\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1041529440 \uparrow$,

$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.6611294079 \uparrow$, $\Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = 0.7823037995 \downarrow$.

$M \in [10^6, 10^7]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2312433670 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.0614862378 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0452699271 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5374200520 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1245804159 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 1029889,

C22 = 238155, C2p = 31753, Cm2 = 31571, Cmp = 46623, CC11 = 553483, CCmp = 128304,

$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.33767663 \downarrow$,

$\delta_{2,2}^{\text{even}} = 0.2312433670 \downarrow$, $(\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1067561648 \uparrow$,

$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.66232334 \uparrow$, $\Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = 0.768663419 \downarrow$.

$M \in [10^7, 10^8]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2290897913 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.058607396 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0497431369 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5297912763 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1327683993 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 9652809,

C22 = 2211360, C2p = 283421, Cm2 = 282305, Cmp = 480161, CC11 = 5113974, CCmp = 1281588,

$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.3374403243 \downarrow$,

$\delta_{2,2}^{\text{even}} = 0.2290897913 \downarrow$, $(\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1083505329 \uparrow$,

$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.6625596756 \uparrow$, $\Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = .7588810676 \downarrow$.

$M \in [10^8, 10^8 + 10^6]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2285032150 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.0571186698 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0518491039 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5276699767 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1348590343 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 105132,

C22 = 24023, C2p = 2971, Cm2 = 3034, Cmp = 5451, CC11 = 55475, CCmp = 14178,

$$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.3374709887 \downarrow,$$

$$\delta_{2,2}^{\text{even}} = 0.2285032150 \downarrow, \quad (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1089677737 \uparrow,$$

$$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.662529011 \uparrow, \quad \Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = 0.7561731917 \downarrow.$$

$M \in [10^9, 10^9 + 10^6]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2262061480 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.0563555787 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0540844730 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5226055410 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1407482589 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 99511,

C22 = 22510, C2p = 2808, Cm2 = 2800, Cmp = 5382, CC11 = 52005, CCmp = 14006,

$$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.3366461999 \downarrow,$$

$$\delta_{2,2}^{\text{even}} = 0.2262061480 \downarrow, \quad (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1104400517 \uparrow,$$

$$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.6633538000 \uparrow, \quad \Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = 0.748811689 \downarrow.$$

$M \in [10^{10}, 10^{10} + 10^6]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2252429443 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.0535799257 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0571751842 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5164271590 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1475747866 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 94569,

C22 = 21301, C2p = 2494, Cm2 = 2573, Cmp = 5407, CC11 = 48838, CCmp = 13956,

$$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.3359980543 \downarrow,$$

$$\delta_{2,2}^{\text{even}} = 0.2252429443 \downarrow, \quad (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1107551099 \uparrow,$$

$$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.6640019456 \uparrow, \quad \Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = 0.7416701033 \downarrow.$$

$M \in [10^{11}, 10^{11} + 2.5 \cdot 10^5]$	m	m'	$\mathbf{S} = \mathbf{N}(\varepsilon_K)$	densities	δ
even	= 2	= 2	-1	0.2240462381 ↓	$\delta_{2,2}^{\text{even}}$
even	= 2, > 2	> 2, = 2	= 1	0.0514559794 ↓	$\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}$
even	> 2	> 2	= 1	0.0607678259 ↑	$\delta_{m,m'}^{\text{even}}$
odd	= 1	= 1	-1	0.5127736860 ↓	$\delta_{1,1}^{\text{odd}}$
odd	> 2	> 2	= 1	0.1509562704 ↑	$\delta_{m,m'}^{\text{odd}}$

CM = 49829,

C22 = 11164, C2p = 1308, Cm2 = 1256, Cmp = 3028, CC11 = 25551, CCmp = 7522,

$$\delta_{2,2}^{\text{even}} + (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.3362700435 \downarrow \uparrow,$$

$$\delta_{2,2}^{\text{even}} = 0.2240462381 \downarrow, \quad (\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}}) + \delta_{m,m'}^{\text{even}} = 0.1122238054 \uparrow,$$

$$\delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} = 0.6637299564 \uparrow \downarrow, \quad \Delta_{\text{gcd}}^- = \delta_{2,2}^{\text{even}} + \delta_{1,1}^{\text{odd}} = 0.7368199241 \downarrow.$$

3.3.1. *First heuristic from the above data.* It is difficult to go further because of the execution time, but some rules appear, that are not proved, but allow possible heuristics:

- $\delta^{\text{even}} := \delta_{2,2}^{\text{even}} + \delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}} + \delta_{m,m'}^{\text{even}} \rightarrow \frac{1}{3};$

$$\bullet \delta^{\text{odd}} := \delta_{1,1}^{\text{odd}} + \delta_{m,m'}^{\text{odd}} \rightarrow \frac{2}{3};$$

this is almost obvious since random Kummer radicals M , such that $-1 \in \mathbf{N}(K^\times)$, are in the classes 1, 2 or 5 modulo 8, whence with uniform repartition $\frac{1}{3}$ for M even (class of 2) and $\frac{2}{3}$ for the case M odd (classes of 1 and 5).

The indications \uparrow and \downarrow give some interesting phenomena:

$\bullet \delta_{m,m'}^{\text{even}}$ must have a hight increasing, since $\delta_{2,m'}^{\text{even}}$ and $\delta_{m,2}^{\text{even}}$ are decreasing, but the sum $\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}} + \delta_{m,m'}^{\text{even}}$ is increasing.

$\bullet \delta_{2,2}^{\text{even}}$ must have a hight decreasing, since $\delta^{\text{even}} = \delta_{2,2}^{\text{even}} + \delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}} + \delta_{m,m'}^{\text{even}}$ is decreasing while the partial sum $\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}} + \delta_{m,m'}^{\text{even}}$ is increasing.

\bullet The sum $\Delta_{\text{gcd}}^- = \delta_{1,1}^{\text{odd}} + \delta_{2,2}^{\text{even}}$ is much decreasing.

\bullet The quotient $\frac{\delta_{2,2}^{\text{even}}}{\delta_{1,1}^{\text{odd}}}$ seems to be increasing and the quotient $\frac{\delta_{1,1}^{\text{odd}}}{\delta_{m,m'}^{\text{odd}}}$ seems to be rapidly decreasing.

\bullet The quotient $\frac{\delta_{2,2}^{\text{even}}}{\delta_{2,m'}^{\text{even}} + \delta_{m,2}^{\text{even}} + \delta_{m,m'}^{\text{even}}}$ seems to be decreasing up to a constant $\rho \approx 2$.

To reinforce this last heuristic, let's consider the computation of the parity of the component b of $\varepsilon_K = a + b\sqrt{M}$, for M even and $-1 \in \mathbf{N}(K^\times)$; indeed, recall that in that cases $\mathbf{S} = -1$ is equivalent to b odd. The following program examines this question taking $M \equiv 2 \pmod{8}$, in the intervals $[k * 10^7, (k + 1) * 10^7]$, $k \geq 1$:

```
{for(k=0,50,bM=k*10^7;BM=bM+10^7;CM=0;CP=0;CI=0;forstep(M=bM+2,BM,8,
if(core(M)!=M,next);r=omega(M);f=factor(M);e11M=component(f,1);for(i=2,r,
e11=e11M[i];if(Mod(e11,4)==3,next(2)));CM=CM+1;e=quadunit(4*M);
Y=component(e,3);if(Mod(Y,2)==0,CP=CP+1);if(Mod(Y,2)==1,CI=CI+1));
print("k=",k," CM=",CM," CP=",CP," CI=",CI," rho=",CI/CP+0.0)}}
```

k	CM	CP	CI	rho
0	390288	122913	267375	2.1753191281638231920138634644016499475
1	373804	119118	254686	2.1380983562517839453315200053728235867
2	368305	117555	250750	2.1330441070137382501807664497469269704
3	364879	117142	247737	2.1148435232452920387222345529357531884
4	362321	116164	246157	2.1190472091181433146241520608794463001
5	360344	115669	244675	2.1153031495041886763091234470774364782
6	358748	115431	243317	2.1078999575503980733078635721773180515
7	357459	115340	242119	2.0991763481879660135252297555054621120
8	356212	114959	241253	2.0986003705668977635504832157551822824
9	355175	114509	240666	2.1017212620842029884113912443563388031
10	354229	114366	239863	2.0973278771662906807967402899463127153
11	353458	113972	239486	2.1012704874881549854350191275050012284
12	352631	113688	238943	2.1017433678136654704102455844064457111
13	351987	113671	238316	2.0965417740672642978420177529888889866
14	351367	113626	237741	2.0923116188196363508351961698906940313
15	350705	113407	237298	2.0924457925877591330341160598552117594
16	350238	113342	236896	2.0900989924299906477739937534188562051
17	349650	112900	236750	2.0969884853852967227635075287865367582
18	349183	112760	236423	2.0966920893934019155728981908478183753
19	348671	112975	235696	2.0862668732020358486390794423545032087
20	348262	112572	235690	2.0936822655722559783960487510215684184
21	347881	112435	235446	2.0940632365366656290301062836305420910
22	347434	112209	235225	2.0963113475746152269425803634289584614
23	347070	112571	234499	2.0831208748256655799451013138374892290
24	346697	112323	234374	2.0866073733785600455828280939789713594
25	346469	112613	233856	2.0766341363785708577162494561018710096
26	346065	112086	233979	2.0874953160965687061720464643220384348
27	345684	111830	233854	2.0911562192613788786551014933381024770
28	345428	111827	233601	2.0889498958212238547041412181315782414
29	345159	111590	233569	2.0930997401200824446635003136481763599
30	344767	112211	232556	2.0724884369625081320013189437755656754
31	344530	112094	232436	2.0735811015754634503184827020179492212
32	344346	111732	232614	2.0818923853506605090752872945977875631
33	343975	111378	232597	2.0883567670455565731113864497477060102
34	343833	111710	232123	2.0779070808343031062572732969295497270
35	343605	111150	232455	2.0913630229419703103913630229419703104
36	343315	111288	232027	2.0849238013083171590827402774782546187
37	343185	111320	231865	2.0828692058929213079410707869205892921

38	342857	111017	231840	2.0883288145058864858535179296864444184
39	342577	111231	231346	2.0798698204637196465014249624654997258
40	342591	111345	231246	2.0768422470699178229826215815707934797
41	342144	111123	231021	2.0789665505790880375799789422531789099
42	342078	111320	230758	2.0729249011857707509881422924901185771
43	341911	110739	231172	2.0875391686758955742782578856590722329
44	341767	110973	230794	2.0797311057644652302812395807989330738
45	341313	110928	230385	2.0768877109476417135439203807875378624
46	341356	110701	230655	2.0835855141326636615748728557104271868
47	341177	110800	230377	2.0792148014440433212996389891696750903
48	341010	110847	230163	2.0764026090015967955831010311510460364
49	340781	110667	230114	2.0793371104303902699088255758265788356
50	340700	110734	229966	2.0767424639225531453754041215886719526

Many oscillations can be observed, on the successive intervals $[k * 10^7, (k + 1) * 10^7]$, which support the idea of a slow convergence of CI/CP towards $\rho = 2^+$.

With the same principle, but in intervals of the form $[k * 10^9, k * 10^9 + 10^7]$, $k \geq 1$ (long calculation time), we obtain, as expected, a slow global decreasing of the data:

1	334971	109266	225705	2.0656471363461644061281642963044313876
2	329775	107868	221907	2.0572088107687173211703192791189231283
3	326962	106943	220019	2.0573483070420691396351327342603068925
4	324916	107023	217893	2.0359455444156863477943993347224428394
5	323273	105998	217275	2.0498028264684239325270288118643747995

To conclude, one may say that these heuristics are compatible with the next one suggesting that $\delta_{1,1}^{\text{odd}} \rightarrow \left(\frac{6}{\pi^2}\right)^2 \approx 0.3695\dots$, then $\Delta_{\text{gcd}}^- := \delta_{1,1}^{\text{odd}} + \delta_{2,2}^{\text{even}} \rightarrow \left(\frac{6}{\pi^2}\right)^2 (1 + 0.5) \approx 0.5543\dots$

3.3.2. *Second heuristic from randomness of A, A' .* In our viewpoint, we are reduced to use the well-known fact that the density of pairs of independent co-prime integers is $\frac{6}{\pi^2} \approx 0.6079\dots$; but this implies that no condition is assumed, especially for a radical R taken at random, and we must take into account that a radical lies in the subset of square-free integers, whose relative density is also given by $\frac{6}{\pi^2}$. The integers $a \pm 1$ giving A, A' may be considered as random and independent regarding M .

- When M is odd, $\mathbf{S} = -1$ is equivalent to $m := \mathbf{gcd}(A, M) = 1$; which gives the partial density $\delta_{1,1}^{\text{odd}} = \left(\frac{6}{\pi^2}\right)^2$.

- When M is even, $\mathbf{S} = -1$ is equivalent to $m' := \mathbf{gcd}(A', M) = 2$ and this may be written $\frac{m'}{2} := \mathbf{gcd}\left(\frac{A'}{2}, \frac{M}{2}\right) = 1$; we know this is equivalent to b odd and that a good heuristic is that this occur with probability $\frac{1}{2}$.

The specific case $m = 2$ (with the alternative $m' > 2$ or $m' = 2$) occurs only for M even, whence a coefficients $\frac{1}{2}$ for the corresponding densities; indeed, M even and

We then obtain the following discussion, on m and m' , from Theorem 2.4:

- $m = 1$ (M of any parity); thus $\mathbf{S} = -1$ with density $\left(\frac{6}{\pi^2}\right)^2$;
- $m = m' = 2$ (M even); thus $\mathbf{S} = -1$ with density $\frac{1}{2} \left(\frac{6}{\pi^2}\right)^2$.

Taking into account the previous interpretation, we propose, for \mathcal{D}^- inside \mathcal{D} , the conjectural density:

$$(3.1) \quad \Delta_{\text{gcd}}^- = \left(\frac{6}{\pi^2}\right)^2 \left(1 + \frac{1}{2}\right) \approx 0.554363041753.$$

To be compared with the density 0.5805775582 [St, Conjecture 1.4], proven in [KoPa1, KoPa2] depending on the natural order of discriminants.

Our method, assumes the independence and randomness of the parameters; moreover it does not classify the radicals (or discriminants), nor the units (for example by means of their traces), so one can only notice that the density (3.1) may be an lower bound for the classical case; fortunately it is greater than the lower bound 0.538220, which was proved in [CKMP], and also less than 0.666666..., proved in [FK1, FK2].

REFERENCES

- [BoSt] W. Bosma, P. Stevenhagen, Density computations for real quadratic units, *Math. Comp.* **65** (1996), 1327–1337. <https://doi.org/10.1090/S0025-5718-96-00725-9> 10
- [CKMP] S. Chan, P. Koymans, D. Milovic, C. Pagano, On the negative Pell equation, arXiv (2019). <https://arxiv.org/abs/1908.01752> 10, 15
- [Che] C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, Thèse 155, Jour. of the Faculty of Sciences Tokyo **2** (1933), 365–476. http://archive.numdam.org/item/THESE_1934_155_365_0/ 2
- [FK1] E. Fouvry, J. Klüners, The parity of the period of the continued fraction of \sqrt{d} , *Proc. Lond. Math. Soc.* (3) **101**(2) (2010), 337–391. <http://doi.org/10.1112/PLMS/PDP057> 10, 15
- [FK2] E. Fouvry, J. Klüners, On the negative Pell equation, *Ann. of Math.* (2) **172**(3) (2010), 2035–2104. <http://doi.org/10.4007/annals.2010.172.2035> 10, 15
- [Fu] Y. Furuta, Norm of units of quadratic fields, *J. Math. Soc. Japan* **11**(2) (1959), 139–145. <https://doi.org/10.2969/jmsj/01120139> 9
- [Gra1] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005). 2, 3
- [Gra2] G. Gras, Sur la norme du groupe des unités d’extensions quadratiques relatives, *Acta Arithmetica* **61** (1992), 307–317. <https://doi.org/10.4064/aa-61-4-307-317> 2, 10
- [Gra3] G. Gras, Invariant generalized ideal classes – Structure theorems for p -class groups in p -extensions, *Proc. Indian Acad. Sci. (Math. Sci.)* **127**(1) (2017), 1–34. <https://doi.org/10.1007/s12044-016-0324-1> 9
- [Gra4] G. Gras, Unlimited lists of fundamental units of quadratic fields – Applications, arXiv (2022). <https://doi.org/10.48550/arXiv.2206.13931> 10, 11
- [KoPa1] P. Koymans, C. Pagano, On the distribution of $Cl(K)[\ell^\infty]$ for degree ℓ cyclic fields, *J. Eur. Math. Soc.* **24**(4) (2022), 1189–1283. <https://doi.org/10.4171/JEMS/1112> 2, 15
- [KoPa2] P. Koymans, C. Pagano, On Stevenhagen’s conjecture, arXiv (2022). <https://arxiv.org/abs/2201.13424> 2, 10, 15
- [P] The PARI Group, PARI/GP, version 2.9.0, Université de Bordeaux (2016). <http://pari.math.u-bordeaux.fr/> 10
- [Rie] G.J. Rieger, Über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. II, *Journal für die reine und angewandte Mathematik* **217** (1965), 200–216. <http://eudml.org/doc/150667> 9
- [Sm] A. Smith, 2^∞ -Selmer groups, 2^∞ -class groups and Goldfeld’s conjecture, arXiv (2017). <https://arxiv.org/abs/1702.02325> 2
- [St] P. Stevenhagen, The number of real quadratic fields having units of negative norm, *Experiment. Math.* **2**(2) (1993), 121–136. <http://eudml.org/doc/230043> 2, 10, 15
- [Ten] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 4^e édition mise à jour, Coll. Échelles, Belin, 592 pages (2015). 10
- [Tro] H.F. Trotter, On the Norms of Units in Quadratic Fields, *Proc. Amer. Math. Soc.* **22**(1) (1969), 198–201. <https://doi.org/10.2307/2036951> 3

VILLA LA GARDETTE – 4, CHEMIN DE CHÂTEAU GAGNIÈRE – 38520 LE BOURG D’OISANS, FRANCE –
 URL: <http://orcid.org/0000-0002-1318-4414>
 Email address: g.mn.gras@wanadoo.fr