



HAL
open science

Unlimited lists of fundamental units of quadratic fields - Applications

Georges Gras

► **To cite this version:**

Georges Gras. Unlimited lists of fundamental units of quadratic fields - Applications: Units of norm -1 , Norm equations, Non- p -rational fields, p -Class groups). 2022. hal-03705446v1

HAL Id: hal-03705446

<https://hal.science/hal-03705446v1>

Preprint submitted on 28 Jun 2022 (v1), last revised 31 May 2023 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNLIMITED LISTS OF FUNDAMENTAL UNITS OF QUADRATIC FIELDS – APPLICATIONS

(UNITS OF NORM -1 , NORM EQUATIONS, NON- p -RATIONAL FIELDS, p -CLASS GROUPS)

GEORGES GRAS

ABSTRACT. We use the polynomials $m_s(t) = t^2 - 4s$, $s \in \{-1, 1\}$, in an elementary process giving arbitrary large lists of *fundamental units* of quadratic fields of discriminants listed in ascending order. More precisely, let $\mathbf{B} \gg 0$; then as t grows from 1 to \mathbf{B} , for each *first occurrence* of a square-free integer $M \geq 2$, in the factorization $m_s(t) =: Mr^2$, the unit $\frac{1}{2}(t + r\sqrt{M})$ is the fundamental unit of norm s of $\mathbb{Q}(\sqrt{M})$, even if $r > 1$ (Theorem 4.6). Using $m_{s\nu}(t) = t^2 - 4s\nu$, $\nu \geq 2$, the algorithm gives arbitrary large lists of *fundamental solutions* to $u^2 - Mv^2 = 4s\nu$ (Theorem 4.11). We deduce, for $p > 2$ prime, arbitrary large lists of *non p -rational* quadratic fields (Theorems 6.3, 6.4, 6.5) and of degree $p - 1$ imaginary fields with non-trivial p -class group (Theorems 7.1, 7.2). PARI programs are given to be copied and pasted.

CONTENTS

1. Introduction and Main results	2
1.1. Quadratic polynomial units	2
1.2. Main Results	2
1.3. Definition of the “F.O.P.” algorithm	3
1.4. Polynomials $m_s(t)$ and associated units $E_s(t)$	4
2. First examples of application of the F.O.P. algorithm	4
2.1. Kummer radicals and discriminants given by the polynomials $m_s(t)$	4
2.2. Application to minimal class numbers	5
2.3. Application to minimal orders of p -ramified torsion groups	6
2.4. Application to minimal orders of logarithmic class groups	6
3. Units $E_s(t)$ vs fundamental units $\varepsilon_{M(t)}$	6
3.1. Programs checking the exponent n in $E_s(t) = \varepsilon_{M(t)}^n$	6
3.2. Remarks on the use of the F.O.P. algorithm	7
4. Accuracy of the F.O.P. algorithm – Application to norm equations	8
4.1. Main property of the trace map	8
4.2. Unlimited lists of fundamental units of norm s , $s \in \{-1, 1\}$	10
4.3. Unlimited lists of fundamental integers of norm $s\nu$, $\nu \geq 2$	11
5. Universality of the polynomials $m_{s\nu}$	13
6. Application to p -rational vs non- p -rational quadratic fields	15
6.1. Remarks about p -rationality and non- p -rationality	16
6.2. Families of units local p -th power at p – Computation of \mathcal{T}_K	17
6.3. Infiniteness of non p -rational real quadratic fields	20
7. Application to p -class groups of some imaginary cyclic fields	21
7.1. Unlimited lists of quadratic fields with non-trivial 3-class group	21
7.2. Lists of degree $p - 1$ imaginary cyclic fields with non-trivial p -class group	23
References	25

Date: June 27, 2022.

2020 *Mathematics Subject Classification*. Primary 11R11, 11R27, 11R37, 08-04.

Key words and phrases. Real quadratic fields; Fundamental units; Norm equations; p -rationality; p -class numbers; PARI programs.

1. INTRODUCTION AND MAIN RESULTS

1.1. Quadratic polynomial units.

1.1.1. *Notations.* 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. There are two ways of writing an element $\alpha \in \mathbf{Z}_K$. The first one is to use the integral basis $\{1, \sqrt{M}\}$ (resp. $\{1, \frac{1+\sqrt{M}}{2}\}$) when $M \not\equiv 1 \pmod{4}$ (resp. $M \equiv 1 \pmod{4}$). The second one is to write $\alpha = \frac{1}{2}(a + b\sqrt{M})$, in which case $a, b \in \mathbb{Z}$ are necessarily of same parity (moreover, a, b may be odd only when $M \equiv 1 \pmod{4}$). We denote by $\mathbf{N}_{K/\mathbb{Q}}$ or simply \mathbf{N} the norm map in K/\mathbb{Q} , so that $\mathbf{N}(\alpha) = \frac{1}{4}(a^2 - Mb^2)$.

Then the norm equation in $x, y \in \mathbb{Z}$ (not necessarily coprime numbers):

$$x^2 - My^2 = 4s\nu, \quad s \in \{-1, 1\}, \nu \in \mathbb{Z}_{\geq 1},$$

has the property that x, y are necessarily of same parity and may be odd only when $M \equiv 1 \pmod{4}$; then $\frac{1}{2}(x + y\sqrt{M}) \in \mathbf{Z}_K$ is of norm $s\nu$.

Finally, we shall write quadratic numbers $\alpha \in \mathbb{Q}(\sqrt{M})$, with positive coefficients on the \mathbb{Q} -basis $\{1, \sqrt{M}\}$; this corresponds to a unique representative modulo sign and conjugation. These viewpoints will be more convenient for our purpose and these conventions of writing and parity will be implicit in all the sequel.

1.1.2. *Polynomial units.* It is classical that the continued fraction expansion of \sqrt{m} , for a positive square-free integer m , gives the fundamental solution, in integers $u, v \in \mathbb{Z}_{\geq 1}$, of the norm equation $u^2 - mv^2 = 4s$, whence the fundamental unit $\varepsilon_m := \frac{1}{2}(u + v\sqrt{m})$ of the quadratic field $\mathbb{Q}(\sqrt{m})$. A similar context of ‘‘polynomial continued fraction expansion’’ does exist and gives polynomial solutions $(u(t), v(t))$, of $u(t)^2 - m(t)v(t)^2 = 4s$, for suitable $m(t) \in \mathbb{Z}[t]$ (see, e.g., [McL, McLZ, Nat, Ram, SaAb]). This gives the quadratic polynomial units $E(t) := \frac{1}{2}(u(t) + v(t)\sqrt{m(t)})$. We will base our study on the following polynomials $m(t)$ that have interesting universal properties.

Definition 1.1. *Consider the square-free polynomials $m_{s\nu}(t) = t^2 - 4s\nu \in \mathbb{Z}[t]$, where $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 1}$. The continued fraction expansion of $\sqrt{t^2 - 4s\nu}$ leads to the integers $A_{s\nu}(t) := \frac{1}{2}(t + \sqrt{t^2 - 4s\nu})$, of norm $s\nu$ and trace t , in a quadratic extension of $\mathbb{Q}(t)$. When $\nu = 1$, one obtains the units $E_s(t) := \frac{1}{2}(t + \sqrt{t^2 - 4s})$, of norm s and trace t .*

The continued fraction expansion, with polynomials, gives the fundamental solution of the norm equation (cf. details in [McL]), but must not be confused with that using evaluations of the polynomials; for instance, for $t_0 = 7$, $m_1(t_0) = 7^2 - 4 = 45$ is not square-free and $E_1(7) = \frac{1}{2}(7 + \sqrt{45}) = \frac{1}{2}(7 + 3\sqrt{5})$ is indeed the fundamental solution of $u^2 - 45v^2 = 4$, but not the fundamental unit ε_5 of $\mathbb{Q}(\sqrt{45}) = \mathbb{Q}(\sqrt{5})$ (one gets $E_1(7) = \varepsilon_5^6$).

1.2. Main Results. We shall prove that the families of polynomials $m_{s\nu}(t) = t^2 - 4s\nu$, $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 1}$, are universal to find all square-free integers M for which there exists a privileged solution $\alpha \in \mathbf{Z}_K \setminus \mathbb{Z}$ to $\mathbf{N}(\alpha) = s\nu$; moreover, the solution obtained is the fundamental one, in the meaning of Definition 4.1 saying that α is of minimal trace. This is obtained by means of an extremely simple algorithmic process (described § 1.3) and allows to get unbounded lists of quadratic fields (given by means of their Kummer radicals¹) having specific properties.

The typical results, admitting several variations, are the following ones, where $\mathbf{B} \gg 0$ is an arbitrary large upper bound, p an odd prime number and where $m(t)$ denotes quadratic polynomial expressions deduced from some $m_{s\nu}(t)$, $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 1}$:

As t grows from 1 up to \mathbf{B} , for each first occurrence of a square-free integer $M \geq 2$, in the factorizations $m(t) =: Mr^2$, we have, the following properties, where $K := \mathbb{Q}(\sqrt{M})$:

(i) Case $m(t) = t^2 - 4s$: The unit $\frac{1}{2}(t + r\sqrt{M})$ is the fundamental unit of norm s of K (Theorem 4.6).

(ii) Case $m(t) = t^2 - 4s\nu$, $\nu \in \mathbb{Z}_{\geq 2}$: The integer $A_{s\nu}(t) = \frac{1}{2}(t + r\sqrt{M})$ is the fundamental solution $\alpha \in \mathbf{Z}_K$ to $\mathbf{N}(\alpha) = s\nu$, in the meaning that $A_{s\nu}(t)$ is the solution with minimal trace (Theorem 4.11).

¹Recall that $M \geq 2$, square-free, is called a ‘‘Kummer radical’’, contrary to any ‘‘radical’’ Mr^2 giving the same field $K = \mathbb{Q}(\sqrt{M})$.

(iii) Case $m(t) \in \{p^{4t^2} \pm 1, p^{4t^2} \pm 2, p^{4t^2} \pm 4, 4p^{4t^2} \pm 2, 9p^{4t^2} \pm 6, 9p^{4t^2} \pm 12, \dots\}$: The field K is non p -rational apart from few explicit cases (Theorem 6.3).

(iv) Case $m(t) = 3^{4t^2} - 4s$: The field $\mathbb{Q}(\sqrt{-3M})$ has a class number divisible by 3, except possibly when the unit $\frac{1}{2}(9t + r\sqrt{M})$ is a third power of a unit. Up to $\mathbf{B} = 10^5$, all the 3-class groups are non-trivial, apart from few explicit cases (Theorem 7.1).

(v) Case $m(t) = p^{4t^2} - 4s, p \geq 5$: The imaginary cyclic extension $\mathbb{Q}((\zeta_p - \zeta_p^{-1})\sqrt{M})$, of degree $p-1$, has a class number divisible by p , except possibly when the unit $\frac{1}{2}(p^2t + r\sqrt{M})$ is a p -th power of unit (Theorem 7.2). For $p = 5$, the quartic cyclic field is defined by the polynomial $P = x^4 + 5Mx^2 + 5M^2$, which leads to a simplified program. Up to $\mathbf{B} = 500$, all the 5-class groups are non-trivial, except for $M = 29$.

Moreover, this principle gives lists of solutions by means of Kummer radicals (or discriminants) of a regularly increasing order of magnitude, these lists being unbounded as $\mathbf{B} \rightarrow \infty$ (e.g., Proposition 1.3 for lists of Kummer radicals and corresponding lists of arithmetic invariants (class groups, p -ramified torsion groups, logarithmic class groups), then Theorems 6.4, 6.5 for unlimited lists of units, local but non global p th powers, etc.). More precisely, all the lists have, at least, $O(\mathbf{B})$ elements, but most often $\mathbf{B} - o(\mathbf{B})$ elements, and even \mathbf{B} elements in some situations. \square

So, we intend to analyze these results in a computational point of view by means of a new strategy to obtain arbitrary large list of fundamental units, other quadratic integers or invariants, even when radicals $m_{s\nu}(t) =: M(t)r(t)^2, t \in \mathbb{Z}_{\geq 1}$, are not square-free; we shall see that many polynomials in the literature, give subfamilies of integers found by means of the $m_{s\nu}$'s with assuming that the radical $m_{s\nu}(t)$ are square-free (especially for $\nu = 1$ to get fundamental units).

Of course, the process has an interest under the use of PARI programs [P]. The programs have been tested as much as possible and may be copied and pasted directly.

1.3. Definition of the “F.O.P.” algorithm. For the convenience of the reader, we give, at once, an outline of this process. We call “*First Occurrence Process*” (F.O.P.) the following algorithm, defined on a large interval $[1, \mathbf{B}]$:

As t grows from $t = 1$ up to $t = \mathbf{B}$, we compute some arithmetic invariant $F(t)$; for instance, a pair of invariants described as a short PARI list:

$$F(t) \mapsto L(t) = \text{List}([M(t) \text{ (Kummer radical)}, \eta(t) \text{ (unit of } \mathbb{Q}(\sqrt{M(t)}) \text{)}]),$$

provided with a natural order on the pairs $L(t)$, then put it in a PARI list LM:

$$\begin{aligned} \text{Listput}(\text{LM}, \text{vector}(2, \text{c}, L[c])) &\mapsto \text{List}([L(1), L(2), \dots, L(t), \dots, L(\mathbf{B})]) \\ &= \text{List}([M(1), \eta(1)], \dots, [M(k), \eta(k)], \dots, [M(\mathbf{B}), \eta(\mathbf{B})]); \end{aligned}$$

after that, we apply the PARI instruction $\text{VM} = \text{vecsort}(\text{LM}, 1, 8)$ which builds the list:

$$\text{VM} = \text{List}([L_1, L_2, \dots, L_j, \dots, L_N]), \quad N \leq \mathbf{B},$$

such that $L_j = L(t_j) = [M(t_j), \eta(t_j)]$ is the *first occurrence* (regarding the selected order, for instance that on the radicals M) of the invariant found by the algorithm and which removes the subsequent duplicate entries; this is the key of the principle since in general duplicate entries are unbounded in number as $\mathbf{B} \rightarrow \infty$ and do not give the suitable information.

Since the length N of the list VM is unknown by nature, one must write LM as a vector and put instead: $\text{VM} = \text{vecsort}(\text{vector}(\mathbf{B}, \text{c}, \text{LM}[c]), 1, 8)$; thus, $N = \text{matsize}(\text{VM})[2]$ makes sense and one can (for possible testing) select elements and components as $X = \text{VM}[k][2]$, etc. If N is not needed, then $\text{VM} = \text{vecsort}(\text{LM}, 1, 8)$ works well.

For instance, the list LM of objects $F(t) = (M(t), \varepsilon(t)), 1 \leq t \leq \mathbf{B} = 10$:

$$\text{LM} = \text{List}([5, \varepsilon_5], [2, \varepsilon_2], [5, \varepsilon'_5], [7, \varepsilon_7], [5, \varepsilon''_5], [3, \varepsilon_3], [2, \varepsilon'_2], [5, \varepsilon'''_5], [6, \varepsilon_6], [7, \varepsilon'_7]),$$

with the natural order on the first components M , leads to the list:

$$\text{VM} = \text{List}([2, \varepsilon_2], [3, \varepsilon_3], [5, \varepsilon_5], [6, \varepsilon_6], [7, \varepsilon_7]).$$

1.4. Polynomials $m_s(t)$ and associated units $E_s(t)$. The polynomials $m_s(t) \in \mathbb{Z}[t]$ define, for $t \in \mathbb{Z}_{\geq 1}$, the parametrized units $E_s(t) = \frac{1}{2}(t + \sqrt{t^2 - 4s})$ of norm s in $K := \mathbb{Q}(\sqrt{M})$, where M is the maximal square-free divisor of $t^2 - 4s$. But M is unpredictable and gives rise to the following discussion depending on the norm $\mathbf{S} := \mathbf{N}(\varepsilon_M)$ of the fundamental unit $\varepsilon_M =: \frac{1}{2}(a + b\sqrt{M})$ of K and of the integral basis of \mathbf{Z}_K :

(i) If $s = 1$, $E_1(t) = \frac{1}{2}(t + \sqrt{t^2 - 4})$ is of norm 1; so, if $\mathbf{S} = 1$, then $E_1(t) \in \langle \varepsilon_M \rangle$, but if $\mathbf{S} = -1$, necessarily $E_1(t) \in \langle \varepsilon_M^2 \rangle$. If $s = -1$, $E_{-1}(t) = \frac{1}{2}(t + \sqrt{t^2 + 4})$ is of norm -1 ; so, necessarily $\mathbf{S} = -1$ (in other words, this particularizes some square-free radicals M).

(ii) If t is odd, $E_s(t)$ is written with half-integer coefficients, $t^2 - 4s \equiv 1 \pmod{4}$, giving $M \equiv 1 \pmod{4}$ and $\mathbf{Z}_K = \mathbb{Z}[\frac{1+\sqrt{M}}{2}]$; so ε_M can not be with integer coefficients (a and b are odd). If t is even, M may be arbitrary as well as ε_M .

We can summarize these constraints by means of the following Table:

$t^2 - 4s$	$\mathbf{S} = \mathbf{N}(\varepsilon_M)$	$E_s(t) \in$	$\varepsilon_M = \frac{1}{2}(a + b\sqrt{M})$
$t^2 - 4$, t even	1 (resp. -1)	$\langle \varepsilon_M \rangle$ (resp. $\langle \varepsilon_M^2 \rangle$)	a, b odd or even
$t^2 - 4$, t odd	1 (resp. -1)	$\langle \varepsilon_M \rangle$ (resp. $\langle \varepsilon_M^2 \rangle$)	a, b odd
$t^2 + 4$, t even	-1	$\langle \varepsilon_M \rangle$	a, b odd or even
$t^2 + 4$, t odd	-1	$\langle \varepsilon_M \rangle$	a, b odd

We shall prove (Theorem 4.6) that, under the F.O.P. algorithm, one always obtains the minimal possible power $n \in \{1, 2\}$ in the writing $E_s(t) = \varepsilon_M^n$, whence $n = 2$ if and only if $s = 1$ and $\mathbf{S} = -1$, which means that $E_s(t)$ is the *fundamental unit of norm s* .

Remark 1.2. It is accepted and often proven that the integers $t^2 - 4s\nu$ are square-free with a non-zero density and an uniform repartition (see, e.g., [FrIw], [Rud]); so an easy heuristic is that the last $M = M_{\mathbf{B}}$ of the list VM is equivalent to \mathbf{B}^2 . This generalizes to the F.O.P. algorithm applied to polynomials of the form $a_n t^n + a_{n-1} t^{n-1} + \dots + a_0$, $n \geq 1$, $a_n \in \mathbb{Z}_{\geq 1}$, and gives the equivalent $M_{\mathbf{B}} \sim a_n \mathbf{B}^n$ as $\mathbf{B} \rightarrow \infty$.

The main fact is that the F.O.P. algorithm will give *fundamental solutions* of norm equations $u^2 - Mv^2 = 4s\nu$ (see Section 4), whatever the order of magnitude of r ; for small values of M , r may be large, even if $r(t)$ tends to 1 as $M(t)$ tends to its maximal value, equivalent to \mathbf{B}^2 , as $t \rightarrow \infty$. Otherwise, without the F.O.P. principle, one must assume $m_{s\nu}(t)$ square-free in the applications, as it is often done in the literature.

The following result shows that any square-free integer $M \geq 2$ may be obtained for \mathbf{B} large enough.

Proposition 1.3. *Consider the polynomial $m_1(t) = t^2 - 4$. For any square-free integer $M \geq 2$, there exists $t \geq 1$ such that $m_1(t) = Mr^2$.*

Proof. The corresponding equation $t^2 - 4 = Mr^2$ becomes of the form $t^2 - Mr^2 = 4$. Depending on the writing in $\mathbb{Z}[\sqrt{M}]$ ($M \equiv 2, 3 \pmod{4}$) or $\mathbb{Z}[\frac{1+\sqrt{M}}{2}]$ ($M \equiv 1 \pmod{4}$) of the powers $\varepsilon_M^n = \frac{1}{2}(t + r\sqrt{M})$, $n \geq 1$, of the fundamental unit ε_M , this selects infinitely many $t \in \mathbb{Z}_{\geq 1}$; if $\mathbf{N}(\varepsilon_M) = -1$, then n is even. \square

Remark 1.4. One may use, instead, the polynomial $m'_1(t) = t^2 - 1$ since for any fundamental unit of the form $\varepsilon_M = \frac{1}{2}(a + b\sqrt{M})$, a, b odd, then $\varepsilon_M^3 \in \mathbb{Z}[\sqrt{M}]$; but some radicals are then obtained with larger values of t (e.g., $m_1(5) = 21$ and $m'_1(55) = 21 \cdot 12^2$ corresponding to $55 + 12\sqrt{21} = (\frac{1}{2}(5 + \sqrt{21}))^2$).

Since for $t = 2t'$, $t^2 + 4s = 4(t'^2 - s)$ gives the same Kummer radical as $t'^2 - s$, in some cases we shall use $m'_s(t) := t^2 - s$ and especially $m'_1(t) := t^2 - 1$ which is “universal” for giving Kummer radicals.

With the polynomials $m_{-1}(t) = t^2 + 4$ or $m'_{-1}(t) = t^2 + 1$ a solution does exist if and only if $\mathbf{N}(\varepsilon_M) = -1$ and one obtains odd powers of ε_M .

2. FIRST EXAMPLES OF APPLICATION OF THE F.O.P. ALGORITHM

2.1. Kummer radicals and discriminants given by the polynomials $m_s(t)$. Recall that, for $t \in \mathbb{Z}_{\geq 1}$, we put $m_s(t) = M(t)r(t)^2$, $M(t)$ square-free.

2.1.1. *Kummer radicals.* The following program gives, as t grows from 1 up to \mathbf{B} , the Kummer radical M and the integer r obtained from the factorizations of $m'_1(t) = t^2 - 1$, under the form Mr^2 ; then we put them in a list \mathbf{LM} and the F.O.P. algorithm gives the pairs $[\mathbf{M}, r]$, in the increasing order of the radicals M and removes the duplicate entries:

```
{B=10^6;LM=List;for(t=1,B,mt=t^2-1;C=core(mt,1);L=List(C);listput(LM,vector(2,c,L[c]));
M=vecsort(vector(B,c,LM[c]),1,8);print(M);print("number of outputs:",matsize(M)[2])}
[2,2],[3,1],[5,4],[6,2],[7,3],[10,6],[11,3],[13,180],[14,4],[15,1],[17,8],[19,39],[21,12],
[22,42],[23,5],[26,10],[29,1820],[30,2],[31,273],[33,4],[34,6],[35,1],[37,12],[38,6],
[39,4],[41,320],[42,2],[43,531],[46,3588],[47,7],[51,7],[53,9100],[55,12],[57,20],
[58,2574],[59,69],[62,8],[65,16],[66,8],[67,5967],[69,936],[70,30],[71,413],[74,430],
(... )
[999976000143,1],[999980000099,1],[999984000063,1],[999988000035,1],[999992000015,1]
number of outputs:999225
time=19,117 ms.
```

Some radicals are not found. Of course they will appear for \mathbf{B} larger according to Proposition 1.3. For instance, the Kummer radical $M = 94$ depends on the fundamental unit $\varepsilon_{94} = 2143295 + 221064\sqrt{94}$ of norm 1; so, using $m'_1(t)$, the minimal solution is $t = 2143295$. For the Kummer radical $M = 193$, $\varepsilon_{193} = 1764132 + 126985\sqrt{193}$ is of norm -1 and $m'_{-1}(1764132) = 193 \times 126985^2$. So $t^2 - 1 = 193r^2$ has the minimal solution $t = 6224323426849$ corresponding to ε_{193}^2 .

2.1.2. *Discriminants.* If one needs the discriminants of the quadratic fields in the ascending order, it suffices to replace the Kummer radical $M = \text{core}(\text{mt})$ by $\text{quaddisc}(\text{core}(\text{mt}))$ giving the discriminant D_M of $\mathbb{Q}(\sqrt{M})$. We use $m'_1(t)$ and $m'_{-1}(t)$ together to get various M modulo 4 (thus the size of the list $[\mathbf{D}]$ is $2 * \mathbf{B}$); this yields the following program and results with outputs $[\mathbf{D}]$:

```
{B=10^6;LD=List;for(t=1,B,L=List([quaddisc(core(t^2-1))]);listput(LD,vector(1,c,L[c]));
L=List([quaddisc(core(t^2+1))]);listput(LD,vector(1,c,L[c]));
D=vecsort(vector(2*B,c,LD[c]),1,8);print(D);print("number of outputs:",matsize(D)[2])}
[[0],[5],[8],[12],[13],[17],[21],[24],[28],[29],[33],[37],[40],[41],[44],[53],[56],[57],[60],
[61],[65],[69],[73],[76],[77],[85],[88],[89],[92],[93],[97],[101],[104],[105],[113],[120],
[124],[129],[136],[137],[140],[141],[145],[149],[152],[156],[161],[165],[168],[172],
[173],[177],[184],[185],[188],[197],[201],[204],[205],[209],[213],[220],[221],[229],
(... )
[3999952000140],[3999960000104],[3999968000060],[3999976000040],[3999992000008]
number of outputs:1998451
time=1min, 40,622 ms.
```

This possibility is valid for all programs of the paper; we will classify the Kummer radicals, instead of discriminants, because radicals are more related to norm equations, but any kind of output can be done easily.

2.2. **Application to minimal class numbers.** One may use this classification of Kummer radicals and compute orders h of some invariants, then apply the F.O.P. principle, with the instruction $\mathbf{VM} = \text{vecsort}(\text{vector}(\mathbf{B}, \mathbf{c}, \mathbf{LM}[\mathbf{c}]), 2, 8)$ to the outputs $[\mathbf{M}, h]$, to get successive possible class numbers h in ascending order (we use here $m_1(t) = t^2 - 4$):

```
{B=10^4;LM=List;for(t=3,B,M=core(t^2-4);h=quadclassunit(quaddisc(M))[1];L=List([M,h]);
listput(LM,vector(2,c,L[c]));VM=vecsort(vector(B-2,c,LM[c]),2,8);print(VM);
print("number of outputs:",matsize(VM)[2])}
[5,1],[15,2],[2021,3],[195,4],[4757,5],[3021,6],[11021,7],[399,8],[27221,9],[7221,10],
[95477,11],[1599,12],[145157,13],[15621,14],[50621,15],[4899,16],[267101,17],[11663,18],
(... )
[24900099,704],[15999999,720],[20884899,728],[20106255,736],[86955621,748],[19483395,760],
[24700899,784],[18062499,832],[15840399,864],[17724099,880],[23232399,920],[24108099,924]
number of outputs:348
time=12,513 ms.
```

One may object that the use of polynomials $m_s(t)$ to obtain radicals, then as above class numbers h , brings nothing new regarding the classical PARI computation:

```
{LM=List;N=0;for(M=2,10^5,if(core(M)!=M,next);N=N+1;h=quadclassunit(quaddisc(M))[1];
L=List([M,h]);listput(LM,vector(2,c,L[c]));VM=vecsort(vector(N,c,LM[c]),2,8);print(VM);
print("number of outputs:",matsize(VM)[2])}
[[2,1],[10,2],[79,3],[82,4],[401,5],[235,6],[577,7],[226,8],[1129,9],[1111,10],[1297,11],
[730,12],[4759,13],[1534,14],[9871,15],[2305,16],[7054,17],[4954,18],[15409,19],
(... )
[78745,60],[68179,62],[57601,63],[71290,64],[87271,66],[53362,68],[56011,70],[45511,72],
[38026,74],[93619,76],[94546,80],[77779,84],[90001,87],[56170,88],[99226,94],[50626,96]]
```


number of outputs:73
time=44,970 ms.

But the F.O.P. algorithm with $m_1(t)$ gives much more examples (348 outputs with $\mathbf{B} = 10^4$ instead of 73 with $\mathbf{B} = 10^5$), in a shorter time. The lists are not comparable but “are equal for $\mathbf{B} = \infty$.”

2.3. Application to minimal orders of p -ramified torsion groups. Let \mathcal{T}_K be the torsion group of the Galois group of the maximal abelian p -ramified (i.e., unramified outside p and ∞) pro- p -extension of $\mathbb{Q}(\sqrt{M})$. The following program, for any $p \geq 3$, gives the results by ascending order (outputs $[M, h = p^a, T = p^b]$, where h is the order of the p -class group and T that of \mathcal{T}_K):

```
{B=10^5;p=3;nu=18;LM=List;for(t=2,B,M=core(t^2-1);K=bnfinit(x^2-M,1);w=valuation(K.no,p);
Kt=bnrinit(K,p^nu);CKt=Kt.cyc;wt=valuation(Kt.no/CKt[1],p);L=List([M,p^w,p^wt]);
listput(LM,vector(3,c,L[c]));VM=vecsort(vector(B-1,c,LM[c]),3,8);print(VM);
print("number of outputs:",matsize(VM)[2])}
[[3,1,1],[15,1,3],[42,1,9],[105,1,27],[1599,3,81],[1095,1,243],[23066,9,729],
[1196835,3,2187],[298662,9,6561],[12629139,27,19683],[6052830,9,59049],
[747366243,243,177147]]
number of outputs:12
time=14min, 1,802 ms.
```

2.4. Application to minimal orders of logarithmic class groups. For the definition of the logarithmic class group $\widetilde{\mathcal{T}}_p$ governing Greenberg’s conjecture [Gre1], see [Jau3, Jau4], and for its computation, see [BeJa] which gives the structure as abelian group. The following program, for $p = 3$, gives the results by ascending orders (all the structures are cyclic):

```
{B=10^5;LM=List;for(t=3,B,M1=core(t^2-4);M2=core(t^2+4);
K1=bnfinit(x^2-M1);Clog=bnflog(K1,3)[1];d=matsize(Clog)[2];C=1;for(j=1,d,C=C*Clog[j]);
L=List([M1,Clog,C]);listput(LM,vector(3,c,L[c]));
K2=bnfinit(x^2-M2);Clog=bnflog(K2,3)[1];d=matsize(Clog)[2];C=1;for(j=1,d,C=C*Clog[j]);
L=List([M2,Clog,C]);listput(LM,vector(3,c,L[c]));
VM=vecsort(vector(2*(B-2),c,LM[c]),3,8);print(VM);
print("number of outputs:",matsize(VM)[2])}
[[5,[],1],[257,[3],3],[2917,[9],9],[26245,[27],27],[577601,[81],81],[236197,[243],243],
[19131877,[729],729],[172186885,[2187],2187],[1549681957,[6561],6561]]
number of outputs:9
time=23min, 31,688 ms.
```

3. UNITS $E_s(t)$ VS FUNDAMENTAL UNITS $\varepsilon_{M(t)}$

We shall use the F.O.P. algorithm to show that the polynomials $m_s(t)$ give the fundamental unit of norm s of $\mathbb{Q}(\sqrt{M})$, whence ε_M or ε_M^2 , regarding the context defined by the choice of s as explained in § 1.4 by means of Table (1.1).

Recall that the algorithm consists, after choosing the upper bound \mathbf{B} , in establishing the list of *first occurrences*, as t increases from 1 up to \mathbf{B} , of any square-free integer $M \geq 2$, in the factorization $m_s(t) = M(t)r(t)^2$ (whence $M = M(t_0)$ for some t_0 and $M \neq M(t)$ for all $t < t_0$), and to consider the unit:

$$E_s(t) := \frac{1}{2}(t + \sqrt{t^2 - 4s}) = \frac{1}{2}(t + r(t)\sqrt{M(t)}), \text{ of norm } s.$$

The F.O.P. is necessary since, if $t_1 > t_0$ give the same Kummer radical M , $E_s(t_0) = \varepsilon_M^{n_0}$ and $E_s(t_1) = \varepsilon_M^{n_1}$ with $n_1 > n_0$; we expect that for t_0 minimal, $E_s(t_0)$ is the fundamental unit of norm s , $\varepsilon_{M(t)}$ or $\varepsilon_{M(t)}^2$, whatever $r(t)$ in the above factorization. This explains that if the upper bound \mathbf{B} increases, the lists give new smaller Kummer radicals M .

3.1. Programs checking the exponent n in $E_s(t) = \varepsilon_{M(t)}^n$. The following programs determine the expression of $E_s(t)$ as power of the fundamental unit of K ; they will find that there is no counterexample to the relation $E_s(t) \in \{\varepsilon_{M(t)}, \varepsilon_{M(t)}^2\}$, depending on \mathbf{S} , from Table (1.1); this will be proved later (Theorem 4.6).

So these programs are only for verification, once for all, because they unnecessarily need much more execution time.

Since $E_s(t)$ is written in $\frac{1}{2}\mathbb{Z}[\sqrt{M}]$ and ε_M on the usual \mathbb{Z} -basis of \mathbf{Z}_K (from the PARI instruction `quadunit`), we write $E_s(t)$ on the PARI basis $\{1, \text{quadgen}(D)\}$, where $D = \text{quaddisc}(M)$ is the discriminant.

One must precise \mathbf{B} and s , the program takes into account the first value $2 + s$ of t since $t = 1, 2$ are not suitable when $s = 1$; then the test $n > (3 + s)/2$ allows the cases $n = 1$ or 2 when $s = 1$. The output of counterexamples is given by the (empty) list V_n :

3.1.1. *Case $s = 1$, $m(t) = t^2 - 4$ (expected exponents $n \in \{1, 2\}$).*

```
{B=10^6;s=1;LM=List;LN=List;for(t=2+s,B,mt=t^2-4*s;C=core(mt,1);M=C[1];r=C[2];
D=quaddisc(M);X=quadgen(D);Y=quadunit(D);res=Mod(M,4);
if(res!=1,Z=1/2*(t+r*X));if(res==1,Z=(t-r)/2+r*X);
z=1;n=0;while(Z!=z,z=z*Y;n=n+1);L=List([M,n]);listput(LM,vector(2,c,L[c]));
VM=vecsort(vector(B-(1+s),c,LM[c]),1,8);print(VM);
print("number of outputs:",matsize(VM)[2]);for(k=1,matsize(VM)[2],n=VM[k][2];
if(n>(3+s)/2,Ln=VM[k];listput(LN,vector(2,c,Ln[c])));Vn=vecsort(LN,1,8);
print("exceptional powers:",Vn)}
[2,2],[3,1],[5,2],[6,1],[7,1],[10,2],[11,1],[13,2],[14,1],[15,1],[17,2],[19,1],[21,1],
[22,1],[23,1],[26,2],[29,2],[30,1],[31,1],[33,1],[34,1],[35,1],[37,2],[38,1],[39,1],
[41,2],[42,1],[43,1],[46,1],[47,1],[51,1],[53,2],[55,1],[57,1],[58,2],[59,1],[61,2],
[62,1],[65,2],[66,1],[67,1],[69,1],[70,1],[71,1],[74,2],[77,1],[78,1],[79,1],[82,2],
(...)
[999978000117,1],[999982000077,1],[999986000045,1],[999990000021,1],[999997999997,1]
number of outputs:998893
exceptional powers:List([])
time=45,665 ms.
```

3.1.2. *Case $s = -1$, $m(t) = t^2 + 4$ (expected exponents $n = 1$).*

```
[2,1],[5,1],[10,1],[13,1],[17,1],[26,1],[29,1],[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],[149,1],[157,1],[170,1],[173,1],[181,1],[185,1],
[197,1],[202,1],[218,1],[226,1],[229,1],[233,1],[257,1],[265,1],[269,1],[274,1],
(...)
[999982000085,1],[999986000053,1],[999990000029,1],[999994000013,1],[999998000005,1]
number of outputs:999874
exceptional powers:List([])
time=1min, 9,473 ms.
```

3.2. **Remarks on the use of the F.O.P. algorithm.** (i) For a matter of space, the programs do not print the units $E_s(t)$ in the outputs, but it may be deduced easily. To obtain a more complete data, it suffices to replace the instructions:

$$L = \text{List}([M, n]), \quad \text{listput}(LM, \text{vector}(2, c, L[c])), \quad \text{listput}(LN, \text{vector}(2, c, Ln[c]))$$

by the following ones (but any information can be put in L ; the sole condition being to put M as first component):

$$L = \text{List}([M, n, t]), \quad \text{listput}(LM, \text{vector}(3, c, L[c])), \quad \text{listput}(LN, \text{vector}(3, c, Ln[c]))$$

or simply:

$$L = \text{List}([M, t]), \quad \text{listput}(LM, \text{vector}(2, c, L[c])), \quad \text{listput}(LN, \text{vector}(2, c, Ln[c]))$$

giving the parameter t whence the trace, then the whole integer of $\mathbb{Q}(\sqrt{M})$; for instance for $m_{-1}(t) = t^2 + 4$ and the general program with outputs $[M, n, t]$:

```
[2,1,2],[5,1,1],[10,1,6],[13,1,3],[17,1,8],[26,1,10],[29,1,5],[37,1,12],[41,1,64],
[53,1,7],[58,1,198],[61,1,39],[65,1,16],[73,1,2136],[74,1,86],[82,1,18],[85,1,9],
[89,1,1000],[97,1,11208],[101,1,20],[106,1,8010],[109,1,261],[113,1,1552],[122,1,22],
[130,1,114],[137,1,3488],...
```

For instance for the data $[41, 1, 64]$, one has $t = 64$ giving $t^2 + 4 = 4100$, whence the fundamental unit $E_{-1}(64) = \varepsilon_{41} = \frac{1}{2}(64 + 10\sqrt{41})$. Another interesting fact is the case of $[137, 1, 3488]$ giving a large fundamental unit at the beginning of the list.

(ii) The programs of § 3.1, computing n , may be used with changing $m_s(t)$ into other polynomials as those given Section 5, or by any $T := f(t)$ with the data $mt = T^2 \pm 4$ and $Z = (T + r * X)/2$ as the following about units $E_s(T) = \frac{1}{2}(T + r\sqrt{M})$.

(a) $T = t^2$ (traces are squares); all are fundamental units ($\mathbf{B} = 10^4$, outputs $[M, n]$):

```
{B=10^4;s=1;LN=List;LM=List;for(t=2+s,B,T=t^2;mt=T^2-4*s;C=core(mt,1);
M=C[1];r=C[2];D=quaddisc(M);X=quadgen(D);Y=quadunit(D);res=Mod(M,4);
if(res!=1,Z=1/2*(T+r*X));if(res==1,Z=(T-r)/2+r*X);
z=1;n=0;while(Z!=z,z=z*Y;n=n+1);L=List([M,n]);listput(LM,vector(2,c,L[c]));
VM=vecsort(vector(B-(1+s),c,LM[c]),1,8);print(VM);
print("number of outputs:",matsize(VM)[2]);for(k=1,matsize(VM)[2],n=VM[k][2];
if(n!=1,Ln=VM[k];listput(LN,vector(2,c,Ln[c])));Vn=vecsort(LN,1,8);
```



```

print("exceptional powers:", Vn)}
[7, 1], [51, 1], [69, 1], [77, 1], [187, 1], [287, 1], [323, 1], [723, 1], [1023, 1], [1067, 1], [1077, 1],
[2397, 1], [3053, 1], [3173, 1], [5183, 1], [6347, 1], [6557, 1], [9799, 1], [14189, 1], [14637, 1],
[15117, 1], [16383, 1], [26243, 1], [29127, 1], [31093, 1], [39999, 1], [43637, 1], [47103, 1],
[47213, 1], [50621, 1], [71111, 1], [71283, 1], [83517, 1], [99763, 1], [102613, 1], [114243, 1],
(...)
[9956072546774637, 1], [9964048570846557, 1], [9988005398920077, 1], [9996000599959997, 1]
number of outputs:9998
exceptional powers:List([])
time=1,980 ms.

```

(b) $T = \text{prime}(t)$ (traces are prime), $s = -1$ ($\mathbf{B} = 10^4$, outputs $[M, T = \text{prime}(t), n]$); there is only the exception $[5, 11, 5]$ obtained as $\varepsilon_5^5 = \frac{1}{2}(5 + 11\sqrt{5})$:

```

[5, 11, 5], [29, 5, 1], [53, 7, 1], [149, 61, 1], [173, 13, 1], [293, 17, 1], [317, 89, 1], [365, 19, 1],
[533, 23, 1], [773, 139, 1], [797, 367, 1], [821, 16189, 1], [965, 31, 1], [1373, 37, 1], [1493, 2357, 1],
[1685, 41, 1], [1781, 211, 1], [1853, 43, 1], [1997, 9161, 1], [2213, 47, 1], [2285, 239, 1],
[2309, 17539, 1], [2477, 647, 1], [2813, 53, 1], [3485, 59, 1], [3533, 2437, 1], [3653, 1511, 1],
(..)
[10965650093, 104717, 1], [10966906733, 104723, 1], [10968163445, 104729, 1]
number of outputs:9995
exceptional powers:List([[5, 11, 5]])
time=376 ms.

```

(iii) When several polynomials $m_i(t)$, $1 \leq i \leq N$, are considered together (to get more Kummer radicals solutions of the problem), there is in general commutativity of the two sequences in $\text{for}(t = 1, \mathbf{B}, \text{for}(i = 1, N, \text{mt} = \dots))$ and $\text{for}(i = 1, N, \text{for}(t = 1, \mathbf{B}, \text{mt} = \dots))$. But we will always use the first one.

4. ACCURACY OF THE F.O.P. ALGORITHM – APPLICATION TO NORM EQUATIONS

4.1. Main property of the trace map. We shall speak of solving a norm equation in $K = \mathbb{Q}(\sqrt{M})$, for the search of integers $\alpha \in \mathbf{Z}_K \setminus \mathbb{Z}$ such that $\mathbf{N}(\alpha) = s\nu$, for $s \in \{-1, 1\}$ and $\nu \in \mathbb{Z}_{\geq 1}$ given. We assume to take (up to sign and conjugation) $\alpha = \frac{1}{2}(u + v\sqrt{M})$, with $u, v \in \mathbb{Z}_{\geq 1}$. If the set of solutions is non-empty we will define the notion of *fundamental solution*; we will see that this definition is common to units ($\nu = 1$) and non-units. Then we will prove an elementary property and the main result, involving the F.O.P. algorithm, giving arbitrary large lists of fundamental solutions of norm equations. Note that the resulting PARI programs only use very elementary instructions; whence the rapidity even for large upper bounds \mathbf{B} .

Definition 4.1. Let M be a square-free integer and let $\nu \in \mathbb{Z}_{\geq 1}$, $s \in \{-1, 1\}$. We call *fundamental solution* (if it exists) of the norm equation $u^2 - Mv^2 = 4s\nu$, the corresponding integer $\alpha := \frac{1}{2}(u + v\sqrt{M}) \in \mathbf{Z}_K$ of minimal trace.

In the case $\nu = 1$, let $\mathbf{S} = \mathbf{N}(\varepsilon_M)$; we shall see that α defines the generator of the group of units of norm s of $\mathbb{Q}(\sqrt{M})$ when it exists (whence ε_M if $s = \mathbf{S}$ or ε_M^2 if $\mathbf{S} = -1$ and $s = 1$). We shall explain, in Corollary 4.4, under what conditions such a fundamental solution for $\nu > 1$ does exist, in which case it is necessarily unique and found by means of the F.O.P., algorithm using $m_{-1}(t)$ or $m_1(t)$ (depending in particular on \mathbf{S}).

Theorem 4.2. Let $M \geq 2$ be a square-free integer. Let $\varepsilon = \frac{1}{2}(a + b\sqrt{M}) > 1$ be a unit of $K := \mathbb{Q}(\sqrt{M})$. Then the trace map of ε^n defines a strictly increasing sequence of integers for $n \geq 1$.

Proof. Set $\bar{\varepsilon} = \frac{1}{2}(a - b\sqrt{M})$ for the conjugate of ε and let $s = \varepsilon\bar{\varepsilon} = \pm 1$ be the norm of ε ; then the trace of ε^n is $T_n := \varepsilon^n + \bar{\varepsilon}^n = \varepsilon^n + \frac{s^n}{\varepsilon^n}$. Thus, we have:

$$\frac{T_{n+1}}{T_n} = \frac{\varepsilon^{n+1} + \frac{s^{n+1}}{\varepsilon^{n+1}}}{\varepsilon^n + \frac{s^n}{\varepsilon^n}} = \frac{\varepsilon^{2(n+1)} + s^{n+1}}{\varepsilon^{n+1}} \frac{\varepsilon^n}{\varepsilon^{2n} + s^n} = \frac{\varepsilon^{2(n+1)} + s^{n+1}}{\varepsilon^{2n+1} + s^n \varepsilon}.$$

To prove the increasing, consider, since $\varepsilon^{2n+1} + s^n \varepsilon$ and $\varepsilon^{2(n+1)} + s^{n+1}$ are positive for all n since $\varepsilon > 1$:

$$(4.1) \quad \begin{aligned} \Delta_n(\varepsilon) &:= \varepsilon^{2(n+1)} + s^{n+1} - (\varepsilon^{2n+1} + s^n \varepsilon) = \varepsilon^{2(n+1)} - \varepsilon^{2n+1} + s^{n+1} - s^n \varepsilon \\ &= \varepsilon^{2n+1}(\varepsilon - 1) - s^n(\varepsilon - s). \end{aligned}$$

(i) Case $s = 1$. Then $\Delta_n(\varepsilon) = (\varepsilon - 1)(\varepsilon^{2n+1} - 1)$ is positive.

(ii) Case $s = -1$. Then $\Delta_n(\varepsilon) = \varepsilon^{2(n+1)} - \varepsilon^{2n+1} - (-1)^n(\varepsilon + 1)$. If n is odd, the result is obvious; so, it remains to look at the expression for $n = 2k$, $k \geq 1$:

$$(4.2) \quad \Delta_{2k}(\varepsilon) = \varepsilon^{4k+2} - \varepsilon^{4k+1} - \varepsilon - 1.$$

Let $f(x) := x^{4k+2} - x^{4k+1} - x - 1$; then $f'(x) = (4k+2)x^{4k+1} - (4k+1)x^{4k} - 1$ and $f''(x) = (4k+1)x^{4k-1}[(4k+2)x - 4k] \geq 0$ for all $x \geq 1$. Thus $f'(x)$ is increasing for all $x \geq 1$ and since $f'(1) = 0$, $f(x)$ is an increasing map for all $x \geq 1$; so, for k fixed, $\Delta_{2k}(\varepsilon)$ is increasing regarding ε .

Since the smallest unit $\varepsilon > 1$ with positive coefficients is $\varepsilon_0 := \frac{1+\sqrt{5}}{2} \approx 1.6180\dots$ we have to look, from (4.2), at the map $F(z) := \varepsilon_0^{4z+2} - \varepsilon_0^{4z+1} - \varepsilon_0 - 1$, for $z \geq 1$; so:

$$F'(z) := 4 \log(\varepsilon_0) \varepsilon_0^{4z+2} - 4 \log(\varepsilon_0) \varepsilon_0^{4z+1} = 4 \log(\varepsilon_0) \varepsilon_0^{4z+1} (\varepsilon_0 - 1) > 0.$$

Since $F(1) \approx 4.2360 > 0$, one gets $\Delta_n(\varepsilon) > 0$ in the case $s = -1$, n even. \square

Corollary 4.3. *Let $M \geq 2$ be a square-free integer, let $\varepsilon_M > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{M})$. Let $\alpha = \frac{1}{2}(a + b\sqrt{M})$ be an integer of $\mathbb{Q}(\sqrt{M})$, of norm $s\nu$, $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 2}$. Then the trace map of $\alpha \varepsilon_M^n$ defines a strictly increasing sequence of integers for $n \geq 1$.*

Proof. Put $A = \alpha \varepsilon_M^n$ and $T_n := A + \bar{A} = \alpha \varepsilon_M^n + \bar{\alpha} \bar{\varepsilon}_M^n = \frac{\alpha^2 \varepsilon_M^{2n} + s \mathbf{S}^n \nu}{\alpha \varepsilon_M^n}$, where $\mathbf{S} = \mathbf{N}(\varepsilon_M)$.

We have:

$$\alpha^2 - \nu = \frac{1}{4}(a^2 + 2ab\sqrt{M} + Mb^2 - |a^2 - Mb^2|) = \frac{1}{2}(Mb^2 + ab\sqrt{M}) \text{ or } \frac{1}{2}(a^2 + ab\sqrt{M});$$

so $\alpha^2 > \nu$; then, as in the proof of the theorem, we obtain the expression analogous to (4.1) (since numerator and denominators are positive):

$$\Delta_n(\alpha) := \alpha^2 \varepsilon_M^{2n+1} (\varepsilon_M - 1) - s \mathbf{S}^n \nu (\varepsilon_M - \mathbf{S}).$$

If $s \mathbf{S}^n = -1$, $\Delta_n(\alpha)$ is obviously positive since $\varepsilon_M - \mathbf{S} > 0$. Suppose $s \mathbf{S}^n = 1$; thus:

$$\Delta_n(\alpha) := \alpha^2 \varepsilon_M^{2n+1} (\varepsilon_M - 1) - \nu (\varepsilon_M - \mathbf{S}) \geq \nu [\varepsilon_M^{2n+1} (\varepsilon_M - 1) - (\varepsilon_M - \mathbf{S})],$$

where the most tricky case is $\mathbf{S} = -1$.

As for the case of (4.2), one considers $\varepsilon_M^{2n+1} (\varepsilon_M - 1) - (\varepsilon_M + 1)$, studying the map $f(x) = x^{2n+2} - x^{2n+1} - x - 1$ for $x \geq 1$. We get easily $f''(x) > 0$ for all $x \geq 1$ and $f'(1) = 0$; so $f(x)$ is increasing for $x \geq 1$ and since $f'(1) = 0$, $f(x)$ is an increasing map for all $x \geq 1$. We have to look at the map $F(z) := \varepsilon_0^{2z+2} - \varepsilon_0^{2z+1} - \varepsilon_0 - 1$, for $z \geq 1$; so:

$$F'(z) := 2 \log(\varepsilon_0) \varepsilon_0^{2z+2} - 2 \log(\varepsilon_0) \varepsilon_0^{2z+1} = 2 \log(\varepsilon_0) \varepsilon_0^{2z+1} (\varepsilon_0 - 1) > 0.$$

Surprisingly, $F(1) = \varepsilon_0^4 - \varepsilon_0^3 - \varepsilon_0 - 1 = (\varepsilon_0^2 + 1)(\varepsilon_0^2 - \varepsilon_0 - 1) = 0$. Whence the result. \square

Corollary 4.4. *Let $s \in \{-1, 1\}$ and $\nu \in \mathbb{Z}_{\geq 2}$ be given. A fundamental solution of the norm equation $u^2 - Mv^2 = 4s\nu$ (Definition 4.1) does exist if and only if there exists an integer principal ideal \mathfrak{a} of absolute norm ν with a generator α whose norm is of sign s . If $\mathbf{S} = -1$, the condition is fulfilled whatever s ; If $\mathbf{S} = 1$, the fundamental solution does exist if and only if $\mathbf{N}(\alpha)$ is of sign s .*

When it exists, the fundamental solution α is unique and found by the F.O.P. algorithm using $m_{-1}(t)$ or $m_1(t)$.

Proof. For $\nu \geq 2$, the existence of solutions, regarding the problems of principal ideals and signs, as necessary conditions, is well known. So we can assume that there exists a principal ideal \mathfrak{a} of absolute norm ν giving a solution α with some sign s' of $\mathbf{N}(\alpha)$.

If $\mathbf{S} = -1$, taking α or $\alpha \varepsilon_M$ we may assume that α is a solution of the norm equation $\mathbf{N}(\alpha) = s\nu$. If $\mathbf{S} = 1$ and $s' \neq s$ there is no solution. Thus, assume that the set of solution is non-empty. Let α_0 be the solution of minimal trace. Another arbitrary solution $\alpha \neq \alpha_0$ is such that $\alpha = \alpha_0 \varepsilon_M^\lambda$, $\lambda \in \mathbb{Z}$ under the condition $\mathbf{S}^\lambda = 1$ (since $\mathbf{N}(\alpha) = \mathbf{N}(\alpha_0) = s\nu$). Because of Corollary 4.3 applied to $\alpha = \alpha_0 \varepsilon_M^\lambda$ or to $\alpha_0 = \alpha \varepsilon_M^{-\lambda}$, depending on the sign of λ , necessarily $\lambda \in \mathbb{Z}_{\geq 1}$ and $\alpha = \alpha_0 \varepsilon_M^\lambda$ has a larger trace.

This proves that the F.O.P. algorithm necessarily finds the solution α_0 of norm $s\nu$, the subsequent duplicate entries of the F.O.P. list being the sets $\{\alpha_0 \varepsilon_M, \alpha_0 \varepsilon_M^2, \alpha_0 \varepsilon_M^3, \dots\}$ (in the case $\mathbf{S} = 1$) or $\{\alpha_0 \varepsilon_M^2, \alpha_0 \varepsilon_M^4, \alpha_0 \varepsilon_M^6, \dots\}$ (in the case $\mathbf{S} = -1$).

If $\mathbf{S} = -1$, the two F.O.P. algorithms, using $m_{-1}(t)$ and $m_1(t)$, will find the corresponding fundamental solution; If $\mathbf{S} = 1$, only one of the two F.O.P. algorithms find the fundamental solution when it exists. \square

For instance, the F.O.P. algorithm applied to $M = 13$ (for which $\mathbf{S} = -1$), $\nu = 3$, gives with $m_{-1}(t)$ the solution $[M = 13, \mathbf{t} = 1]$ whence $\alpha = \frac{1}{2}(1 + \sqrt{13})$ of norm -3 ; with $m_1(t)$ it gives $[M = 13, \mathbf{t} = 5]$, $\alpha = \frac{1}{2}(5 + \sqrt{13})$ of norm 3 ; the traces 1 and 5 are minimal for each case. We then compute that $\frac{1}{2}(5 + \sqrt{13}) = \frac{1}{2}(1 - \sqrt{13})(-\varepsilon_{13})$.

But with $M = 7$ (for which $\mathbf{S} = 1$), the F.O.P. algorithm with $m_{-1}(t)$ and $\nu = 3$ gives $[M = 7, \mathbf{t} = 4]$ but nothing with $m_1(t)$.

Remark 4.5. A possible case is when there exist several principal integer ideals of norm $\nu\mathbb{Z}$ (for instance when $\nu = q_1q_2$ is the product of two primes and if there exist two prime ideals $\mathfrak{q}_1, \mathfrak{q}_2$, of degree 1 , over q_1, q_2 , respectively, such that $\mathfrak{q}_1\mathfrak{q}_2$ and $\mathfrak{q}_1\bar{\mathfrak{q}}_2$ are principal). Let $\mathfrak{a} =: (\alpha)$ and $\mathfrak{a}' =: (\alpha')$ of absolute norm ν . We can assume that, in each set of generators, α and α' have minimal trace u and u' , and necessarily we have, for instance, $u' > u$; since the ideals \mathfrak{a} are finite in number, there exists an ‘‘absolute’’ minimal trace u defining the unique fundamental solution which is that found by the suitable F.O.P. algorithm.

4.2. Unlimited lists of fundamental units of norm s , $s \in \{-1, 1\}$.

4.2.1. *Fundamental property of the case $\nu = 1$.* We have the main following result.

Theorem 4.6. *Let $\mathbf{B} \gg 0$ be given. Let $m_s(t) = t^2 - 4s$, $s \in \{-1, 1\}$ fixed. Then, as t grows from 1 up to \mathbf{B} , for each first occurrence of a square-free integer $M \geq 2$ in the factorization $m_s(t) = Mr^2$, the unit $E_s(t) = \frac{1}{2}(t + r\sqrt{M})$ is the fundamental unit of norm s of $\mathbb{Q}(\sqrt{M})$ (whence $E_s(t) = \varepsilon_M$ if $s = -1$ or if $s = \mathbf{S} = 1$, then $E_s(t) = \varepsilon_M^2$ if and only if $s = 1$ and $\mathbf{S} = -1$, according to the Table (1.1) in §1.4).*

Proof. Let $M_0 \geq 2$ be a given square-free integer. Consider the first occurrence $t = t_0$ giving $m_s(t_0) = M_0r(t_0)^2$ if it exists (existence always fulfilled for $s = 1$ by Proposition 1.3); whence $M_0 = M(t_0)$. Suppose that $E_s(t_0) = \frac{1}{2}(t_0 + r(t_0)\sqrt{M(t_0)})$ is not the fundamental unit of norm s , $\varepsilon_{M(t_0)}^{n_0}$ ($n_0 \in \{1, 2\}$) but a non-trivial power $(\varepsilon_{M(t_0)}^{n_0})^n$, $n > 1$.

Put $\varepsilon_{M(t_0)}^{n_0} =: \frac{1}{2}(a + b\sqrt{M(t_0)})$; from Table (1.1), $n_0 \in \{1, 2\}$ is such that $\mathbf{N}(\varepsilon_{M(t_0)}^{n_0}) = s$ (recall that if $s = 1$ and $\mathbf{S} = -1$, $n_0 = 2$, if $\mathbf{S} = s = 1$, $n_0 = 1$; if $s = -1$, necessarily $\mathbf{S} = -1$ and $n_0 = 1$, otherwise there were no occurrence of M_0 for $s = -1$ and $\mathbf{S} = 1$).

Then, Theorem 4.2 on the traces implies $0 < a < t_0$. We have:

$$a^2 - M(t_0)b^2 = 4s \quad \text{and} \quad m_s(a) = a^2 - 4s =: M(a)r(a)^2;$$

but these relations imply $M(t_0)b^2 = M(a)r(a)^2$, whence $M(a) = M(t_0) = M_0$. That is to say, the pair (t_0, M_0) compared to $(a, M(a) = M_0)$, was not the first occurrence of M_0 (absurd). \square

Corollary 4.7. *Let $t \in \mathbb{Z}_{\geq 1}$ and let $E_1(t) = \frac{1}{2}(t + \sqrt{t^2 - 4})$ of norm 1 . Then $E_1(t)$ is a square of a unit of norm -1 , if and only if there exists $t' \in \mathbb{Z}_{\geq 1}$ such that $t = t'^2 + 2$; thus $E_1(t) = (\frac{1}{2}(t' + \sqrt{t'^2 + 4}))^2 = (E_{-1}(t'))^2$. So, the F.O.P. algorithm, with $m_1(t) =: M(t)r(t)^2$, gives the list of $[M(\mathbf{t}), \mathbf{t}]$ for which $\frac{1}{2}(t + \sqrt{t^2 - 4}) = \varepsilon_M^2$ (resp. ε_M) if $t - 2 = t'^2$ (resp. if not).*

Corollary 4.8. *Let $M \geq 2$ be a given square-free integer and consider the two lists given by the F.O.P. algorithm, for m_{-1} and m_1 , respectively. Then, assuming \mathbf{B} large enough, M appears in the two lists if and only if $\mathbf{S} = -1$. Then $t'^2 + 4 = Mr'^2$ for t' minimal gives the fundamental unit $\varepsilon_M = \frac{1}{2}(t' + r'\sqrt{M})$ and $t^2 - 4 = Mr^2$, for t minimal, gives ε_M^2 ; whence $t = t'^2 + 2$ and $r = r't'$.*

4.2.2. *Unlimited lists of fundamental units of norm s , $s \in \{-1, 1\}$.* Consider first $m_{-1}(t) = t^2 + 4$, $t \in [1, \mathbf{B}]$. We know, from Theorem 4.6, that the F.O.P. algorithm gives always the fundamental unit ε_M of $\mathbb{Q}(\sqrt{M})$ whatever its writing in $\mathbb{Z}[\sqrt{M}]$ or in $\mathbb{Z}[\frac{1+\sqrt{M}}{2}]$; for $s = 1$ one obtains ε_M^2 as soon as $\mathbf{S} = -1$. So we can skip checking and use the following simpler program with larger upper bound $\mathbf{B} = 10^7$; the outputs are the Kummer radicals $[M]$ in the ascending order (one must precise \mathbf{B} and s):

```

{B=10^7;s=-1;LM=List;for(t=2+s,B,mt=t^2-4*s;M=core(mt);
L=List([M]);listput(LM,vector(1,c,L[c]));VM=vecsort(vector(B-(1+s),c,LM[c]),1,8);
print(VM);print("number of outputs, up to ",B," : ",matsize(VM)[2])}
s=-1
[2], [5], [10], [13], [17], [26], [29], [37], [41], [53], [58], [61], [65], [73], [74], [82], [85],
[89], [97], [101], [106], [109], [113], [122], [130], [137], [145], [149], [157], [170], [173],
[181], [185], [193], [197], [202], [218], [226], [229], [233], [257], [265], [269], [274], [277],
[281], [290], [293], [298], [314], [317], [346], [349], [353], [362], [365], [370], [373], [389],
(...)
[99999860000053], [99999900000029], [99999940000013], [99999980000005]
number of outputs, up to 10000000 : 9999742
time=10min, 16,132 ms.
s=1
[2], [3], [5], [6], [7], [10], [11], [13], [14], [15], [17], [19], [21], [22], [23], [26], [29], [30],
[31], [33], [34], [35], [37], [38], [39], [41], [42], [43], [46], [47], [51], [53], [55], [57], [58],
[59], [61], [62], [65], [66], [67], [69], [70], [71], [73], [74], [77], [78], [79], [82], [83], [85],
[86], [87], [89], [91], [93], [94], [95], [101], [102], [103], [105], [107], [109], [110], [111],
(...)
[99999780000117], [99999820000077], [99999860000045], [99999900000021], [99999979999997]
number of outputs, up to 10000000 : 9996610
time=7min, 5,233 ms.

```

The same program with outputs of the form $[M, r, t]$ for $s = 1$ gives many examples of squares of fundamental units. For instance, the data $[29, 5, 27]$ defines the unit $E_1(27) = \frac{1}{2}(27 + 5\sqrt{29})$ and since $27 - 2 = 5^2$, then $t' = 5$, $r' = 1$ and $E_1(27) = (\frac{1}{2}(5 + \sqrt{29}))^2 = \varepsilon_{29}^2$.

4.2.3. Remark on the repartition of units of norm -1 . Some Kummer radicals giving units ε_M of norm -1 do not appear up to $\mathbf{B} = 10^7$, e.g., $M \in \{241, 313, 337, 394, \dots\}$; but all the Kummer radicals M , such that $\mathbf{S} = -1$, ultimately appear as \mathbf{B} increases. So, as $\mathbf{B} \rightarrow \infty$, any unit is obtained, which suggests the existence of natural densities in the framework of the F.O.P. algorithm. More precisely, in the list \mathbf{LM} (i.e., before using $\mathbf{VM} = \text{vecsort}(\text{vector}(\mathbf{B}, c, \mathbf{LM}[c]), 1, 8)$), any Kummer radical M does appear in the list as many times as the trace of ε_M^n (n odd) is less than \mathbf{B} , which gives for instance ($\mathbf{B} = 10^3$):

```

[5], [2], [13], [5], [29], [10], [53], [17], [85], [26], [5], [37], [173], [2],
[229], [65], [293], [82], [365], [101], [445], [122], [533], [145], [629],
[170], [733], [197], [5], [226], [965], [257], [1093], [290], [1229], [13],

```

This fact with Corollaries 4.7, 4.8 may suggest some analytic computation of the density. In [St, Conjecture 1.4], Stevenhagen uses the subset of fields of discriminants D for which -1 is local norm everywhere (whence, any odd $p \mid M$ fulfills the condition $p \equiv 1 \pmod{4}$); the conjectured density in this set is $0.5805\dots$ and is tested in large intervals. This conjecture is strengthened by the proof in [CKMP] that the infimum of this density is at least 0.538 .

4.3. Unlimited lists of fundamental integers of norm $s\nu$, $\nu \geq 2$. This framework being different from the case of units when $\nu \in \mathbb{Z}_{>2}$, we give a separate study, even if some statements may be common to both problems.

4.3.1. Generalities. We begin with an obvious necessary condition depending on the class group of K .

Proposition 4.9. *Consider the polynomials $m_{s\nu}(t) = t^2 - 4s\nu$, $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 2}$. For a given square-free integer $M \geq 2$, there exists $s \in \{-1, 1\}$ and $t \geq 1$ such that $m_{s\nu}(t) = Mr^2$, if and only if there exists an integer ideal \mathfrak{a} of $K = \mathbb{Q}(\sqrt{M})$, of absolute norm ν , and if this ideal is principal.*

Proof. If $\mathfrak{a} = (\alpha)$, of absolute norm ν , with $\alpha = \frac{1}{2}(a + b\sqrt{M}) \in \mathbf{Z}_K$, one obtains $a^2 - Mb^2 = 4s\nu$ for a suitable $s \in \{-1, 1\}$ giving a solution with $t = a$; then $m_{s\nu}(a) = a^2 - 4s\nu = M(a)r^2 = Mb^2$, whence $M = M(a)$ and $r = b$.

Reciprocally, we assume that the corresponding equation (in unknowns t, s) $t^2 - 4s\nu = Mr^2$ has a solution, whence $t^2 - Mr^2 = 4s\nu$. Set $\alpha := \frac{1}{2}(t + r\sqrt{M}) \in \mathbf{Z}_K$; then one obtains the principal ideal $\mathfrak{a} = (\alpha)\mathbf{Z}_K$ of absolute norm ν . \square

Remark 4.10. If $\nu = \prod_{q|\nu} q^{n_q}$, where q denotes distinct prime numbers, there exist integer ideals \mathfrak{a} of absolute norm $\nu\mathbb{Z}$ if and only if, for each inert $q \mid \nu$ then n_q is even. In the F.O.P. algorithm this will select particular Kummer radicals M for which each $q \mid \nu$,

such that n_q is odd, ramifies or splits in $K = \mathbb{Q}(\sqrt{M})$; this is equivalent to $q \mid D_K$ (the discriminant, M or $4M$, of K) or to $\rho_q := \left(\frac{M}{q}\right) = 1$ in terms of quadratic residues. If so, we then have ideal solutions $\mathbf{N}(\mathbf{a}) = \nu\mathbb{Z}$; let's write, with obvious notations:

$$\mathbf{a} = \prod_{q, \rho_q=0} \mathfrak{q}^{n_q} \prod_{q, \rho_q=-1} \mathfrak{q}^{2n'_q} \prod_{q, \rho_q=1} \mathfrak{q}^{n'_q} \bar{\mathfrak{q}}^{n''_q}.$$

Then the equation becomes $\mathbf{N}(\mathbf{a}') = \nu'\mathbb{Z}$ for another integral ideal \mathbf{a}' and another $\nu' \mid \nu$, where \mathbf{a}' is an integer ideal "without any rational integer factor". Thus, $\mathbf{N}(\alpha') = s\nu'$ is equivalent to $\mathbf{a}' = \alpha'\mathbf{Z}_K$. This depends on relations in the class group of K and gives obstructions for some Kummer radicals M . Once a solution \mathbf{a}' principal exists (non unique) we can apply Corollary 4.4 using Corollary 4.3, and conclude as follows.

Theorem 4.11. *Let $\mathbf{B} \gg 0$ be given. Let $m_{s\nu}(t) = t^2 - 4s\nu$, $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 2}$. Then, as t grows from 1 up to \mathbf{B} , for each first occurrence of a square-free integer $M \geq 2$ in the factorization $m_{s\nu}(t) = Mr^2$, the integer $A_{s\nu}(t) = \frac{1}{2}(t + r\sqrt{M})$, is the fundamental solution α of $\mathbb{Q}(\sqrt{M})$ to $\mathbf{N}(\alpha) = s\nu$, $\alpha \in \mathbf{Z}_K$, in the meaning that the trace of α is minimal.*

4.3.2. *Program for lists of quadratic integers of norm $\nu \geq 2$.* The previous program (without any checking) can be modified by choosing an integer $\nu \geq 2$, a sign $s \in \{-1, 1\}$ and the polynomial $m_{s\nu}(t) = t^2 - 4s\nu$ (outputs $[\mathbf{M}(t), \mathbf{t}]$):

```
{B=10^6;s=1;nu=2;LM=List;for(t=1,B,mt=t^2-4*s*nu;M=core(mt);
L=List([M,t]);listput(LM,vector(2,c,L[c]));VM=vecsort(vector(B,c,LM[c]),1,8);
print(VM);print("number of outputs, up to ",B," = ",matsize(VM)[2])}
```

(i) $s = 1$, $\nu = 2$.

```
[-7,1],[ -1,2],[1,3],
[2,4],[7,6],[14,8],[17,5],[23,10],[31,78],[34,12],[41,7],[46,312],[47,14],[62,16],
[71,118],[73,9],[79,18],[89,217],[94,2928],[97,69],[103,954],[113,11],[119,22],
[127,4350],[137,199],[142,24],[151,83142],[158,176],[161,13],[167,26],[191,5998],
[193,56445],[194,28],[199,255078],[206,488],[217,15],[223,30],[233,6121],[238,216],
(... )
[999986000041,999993],[999990000017,999995],[999994000001,999997],[999997999993,999999]
number of outputs, up to 1000000 = 999909
```

(ii) $s = -1$, $\nu = 3$.

```
[1, 2],
[3,6],[7,4],[13,1],[19,8],[21,3],[31,22],[37,5],[39,12],[43,26],[57,30],[61,7],[67,16],
[73,34],[91,38],[93,9],[97,1694],[103,20],[109,73],[111,42],[127,586],[129,318],[133,11],
[139,448],[151,172],[157,50],[163,1864],[181,13],[183,54],[193,379486],[199,28],
[201,1758],[211,58],[217,766],[237,15],[241,62],[247,220],[259,32],[271,428],
(... )
[999986000061,999993],[999990000037,999995],[999994000021,999997],[999998000013,999999]
number of outputs, up to 1000000 = 999866
```

Consider the output $[93, 9]$ ($M = 3 \cdot 31$, $t = 9$, $r = 1$); then $\alpha = A_{-3}(9) = \frac{1}{2}(9 + \sqrt{3 \cdot 31})$ of norm -3 with ramified prime 3; it is indeed the minimal solution since the equation reduces to $3x'^2 + 4 = 31y^2$ with minimal $x' = 3$, then minimal trace $x = 9$.

For the output $[193, 379486]$, $\alpha = A_{-3}(379486) = \frac{1}{2}(379486 + 27316\sqrt{193})$ of norm -3 ; this is the minimal solution despite of a large trace, but $\varepsilon_{193} = \frac{1}{2}(1764132 + 126985\sqrt{193})$ is very large and cannot intervene to decrease the size.

(iii) $s = 1$, $\nu = 15$.

```
[-59,1],[ -51,3],[ -35,5],[ -14,2],[ -11,4],[ -6,6],[1,8],
[10,10],[21,9],[34,14],[61,11],[66,18],[85,20],[106,22],[109,13],[129,24],[154,26],
[165,15],[181,28],[201,312],[210,30],[229,17],[241,32],[265,1400],[274,34],[301,19],
[309,36],[346,38],[349,131],[354,414],[381,21],[385,40],[394,278],[409,41216],[421,3919],
(... )
[999982000021,999991],[999985999989,999993],[999993999949,999997],[999997999941,999999]
number of outputs, up to 1000000 = 999815
s=-1 nu=15
[1,2],
[6,6],[10,10],[15,30],[19,4],[31,8],[34,22],[46,26],[51,12],[61,1],[69,3],[79,16],
[85,5],[94,38],[106,82],[109,7],[114,42],[115,20],[139,94],[141,9],[151,98],[159,24],
[166,206],[181,11],[186,54],[190,110],[199,536],[211,28],[214,58],[229,13],[241,52658],
[249,126],[265,130],[271,32],[274,1258],[285,15],[310,70],[331,7714],[334,146],[339,36],
(... )
[999986000109,999993],[999990000085,999995],[999994000069,999997],[999998000061,999999]
number of outputs, up to 1000000 = 999782
```

For instance, [85, 5] illustrates Proposition 4.9 with the solution $\alpha = \frac{1}{2}(5 + \sqrt{85})$ of norm -15 , with $(\alpha)\mathbf{Z}_K = \mathfrak{q}_3\mathfrak{q}_5$, where 3 splits in K and 5 is ramified; one verifies that the ideals \mathfrak{q}_3 and \mathfrak{q}_5 are non-principal, but their product is of course principal. For this, one obtains the following PARI checkings:

```
k=bnfinit(x^2-85)
k.clgp=[2, [2], [[3, 1; 0, 1]]]
idealfactor(k, 3)=[[3, [0, 2]~, 1, 1, [-1, -1]~]1], [[3, [2, 2]~, 1, 1, [0, -1]~]1]
idealfactor(k, 5)=[[5, [1, 2]~, 2, 1, [1, 2]~]2]
bnfisprincipal(k, [3, [2, 2]~, 1, 1, [0, -1]~])=[[1]~, [1, 0]~]
bnfisprincipal(k, [5, [1, 2]~, 2, 1, [1, 2]~])=[[1]~, [1, 1/3]~]
bnfisprincipal(k, idealmul(k, [3, [2, 2]~, 1, 1, [0, -1]~], [5, [1, 2]~, 2, 1, [1, 2]~]))=[[0]~, [2, -1]~]
nfbasis(x^2-85)=[1, 1/2*x-1/2]
```

The data $[[0], [2, -1]]$ gives the principality with generator $[2, -1]$ denoting (because of the integral basis $\{1, \frac{1}{2}x - \frac{1}{2}\}$ used by PARI), $2 - [\frac{1}{2}\sqrt{85} - \frac{1}{2}] = \frac{1}{2}(5 - \sqrt{85}) = \bar{\alpha}$.

(iv) $s = -1$, $\nu = 9 \times 25$.

```
[1, 16],
[2, 30], [5, 15], [10, 10], [13, 20], [17, 120], [26, 6], [29, 12], [34, 18], [37, 5], [41, 24],
[53, 105], [58, 70], [61, 25], [65, 240], [73, 80], [74, 42], [82, 270], [85, 35], [89, 48], [97, 1280],
[101, 3], [106, 54], [109, 9], [113, 23280], [122, 330], [130, 110], [137, 52320], [145, 360],
[146, 66], [149, 21], [157, 55], [170, 390], [173, 195], [178, 130], [181, 27], [185, 2040],
(... )
[999966001189, 999983], [999978001021, 999989], [999982000981, 999991], [999994000909, 999997]
number of outputs, up to 1000000 = 999448
```

The case [37, 5] may be interpreted as follows: $m_{-1}(5) = 5^2 + 4 \cdot 9 \cdot 25 = 5^2 \cdot 37$, whence $A_{-1}(5) = \frac{1}{2}(5 + 5\sqrt{37}) = 5 \cdot \frac{1}{2}(1 + \sqrt{37}) =: 5B$, where $B := \frac{1}{2}(1 + \sqrt{37})$ is of norm -9 and 5 is indeed inert in K . Thus $\frac{1}{2}(1 + \sqrt{37})\mathbf{Z}_K$ is the square of a prime ideal \mathfrak{p}_3 over 3. The field K is principal and we compute that $\mathfrak{p}_3 = \frac{1}{2}(5 \pm \sqrt{37})\mathbf{Z}_K$, $\mathfrak{p}_3^2 = \frac{1}{2}(31 \pm 5\sqrt{37})\mathbf{Z}_K$. So, $B\mathbf{Z}_K = \frac{1}{2}(1 + \sqrt{37})\mathbf{Z}_K = \frac{1}{2}(31 + 5\sqrt{37})\mathbf{Z}_K$ or $\frac{1}{2}(31 - 5\sqrt{37})\mathbf{Z}_K$. We have $\varepsilon_{37} = 6 + \sqrt{37}$ and we obtain that $B = \frac{1}{2}(31 - 5\sqrt{37}) \cdot \varepsilon_{37}$, showing that $\alpha = 5 \cdot \frac{1}{2}(1 + \sqrt{37})$ is the fundamental solution of the equation $\mathbf{N}(\alpha) = 3^2 \cdot 5^2$ with minimal trace 5.

For larger integers ν , fundamental solutions are obtained easily, as shown by the following example with the prime $\nu = 1009$:

(v) $s = -1$, $\nu = 1009$.

```
[2, 14], [5, 13], [10, 102], [29, 100], [37, 21], [41, 8], [58, 42], [74, 58], [101, 305],
[109, 1617], [113, 656], [137, 2504], [157, 108], [173, 17], [185, 1168], [197, 259], [202, 35958],
[205, 33], [209, 4192], [218, 854], [241, 380808], [253, 681], [269, 620], [290, 158], [313, 384],
[314, 2090], [317, 1316], [337, 6792], [341, 67], [353, 16496], [370, 1422], [394, 86742],
(... )
[999986004085, 999993], [999990004061, 999995], [999994004045, 999997], [999998004037, 999999]
number of outputs, up to 1000000 = 999664
```

We finish with a highly composed number ν , not obvious for a calculation by hand:

(vi) $s = 1$, $\nu = 2 \times 3 \times 5 \times 7$.

```
[-839, 1], [-831, 3], [-815, 5], [-791, 7], [-759, 9], [-719, 11], [-671, 13], [-615, 15], [-551, 17],
[-479, 19], [-399, 21], [-311, 23], [-215, 25], [-209, 2], [-206, 4], [-201, 6], [-194, 8], [-185, 10],
[-174, 12], [-161, 14], [-146, 16], [-129, 18], [-111, 27], [-110, 20], [-89, 22], [-66, 24], [-41, 26],
[-14, 28], [1, 29],
[15, 30], [46, 32], [79, 34], [114, 36], [151, 38], [190, 40], [226, 332], [231, 42], [249, 33],
[274, 44], [319, 46], [366, 48], [385, 35], [415, 50], [466, 52], [511, 2758], [519, 54], [526, 872],
[574, 56], [609, 273], [610, 4100], [631, 58], [679, 574], [681, 39], [690, 60], [721, 511], [751, 62],
[814, 64], [834, 636], [865, 1265], [879, 66], [919, 2486], [946, 68], [991, 30158], [1009, 43],
(... )
[999985999209, 999993], [999989999185, 999995], [999993999169, 999997], [999997999161, 999999]
number of outputs, up to 1000000 = 999715
```

We have not dropped the negative radicals meaning, for instance with $M = -839$, that a solution of the norm equation does exist in $\mathbb{Q}(\sqrt{-839})$ with $\alpha = \frac{1}{2}(1 + \sqrt{-839})$, or with $M = -14$ giving $\alpha = 14 + \sqrt{-14}$.

5. UNIVERSALITY OF THE POLYNOMIALS $m_{s\nu}$

Let's begin with the following obvious result making a link with polynomials $m_{s\nu}$.

Lemma 5.1. *Let $M \geq 2$ be a square-free integer; then, any $\alpha = \frac{1}{2}(a + b\sqrt{M}) \in \mathbf{Z}_K \setminus \mathbb{Z}$ is characterized by its trace a and its norm $s\nu$, $s \in \{-1, 1\}$, $\nu \in \mathbb{Z}_{\geq 1}$, and is given by $m_{s\nu}(a)$, which determines the coefficient b .*

Proof. From the equation $\alpha^2 - a\alpha + s\nu = 0$, we get $\alpha = \frac{1}{2}(a + \sqrt{a^2 - 4s\nu})$, where necessarily $a^2 - 4s\nu =: Mb^2$ giving $b > 0$ from the knowledge of a and $s\nu$. \square

Consider some polynomials that one finds in the literature; for instance that of Mc Laughlin [McL] obtained from ‘‘polynomial continued fraction expansion’’, giving formal units, and defined as follows.

Let $m \geq 2$ be a given square-free integer and let $E_m = u + v\sqrt{m}$, $u, v \in \mathbb{Z}_{\geq 1}$, be the fundamental solution of the norm equation (or Pell–Fermat equation) $u^2 - mv^2 = 1$ (thus, $E_m = \varepsilon_m^{n_0}$, $n_0 \in \{1, 2, 3, 6\}$). For such m, u, v , each of the data below leads to the *fundamental polynomial solution* of the norm equation $U(t)^2 - m(t)V(t)^2 = 1$ (see [McL, Theorems 1–5]), giving the parametrized units $E_{M(t)} = U(t) + V(t)r\sqrt{M(t)}$, of norm 1 of $\mathbb{Q}(\sqrt{M(t)})$, where $m(t) =: M(t)r(t)^2$, $M(t)$ square-free.

The five polynomials $m(t)$ are:

$$\left\{ \begin{array}{l} mcl_1(t) = v^2t^2 + 2ut + m, U(t) = v^2t + u, V(t) = v; \\ mcl_2(t) = (u-1)^2(v^2t^2 + 2t) + m, U(t) = (u-1)(v^4t^2 + 2v^2t) + u, V(t) = v^3t + v; \\ mcl_3(t) = (u+1)^2(v^2t^2 + 2t) + m, U(t) = (u+1)(v^4t^2 + 2v^2t) + u, V(t) = v^3t + v; \\ mcl_4(t) = (u+1)^2v^2t^2 + 2(u^2 - 1)t + m, \\ \quad U(t) = \frac{(u+1)^2}{u-1}v^4t^2 + 2(u+1)v^2t + u, V(t) = \frac{u+1}{u-1}v^3t + v; \\ mcl_5(t) = (u-1)^2(v^6t^4 + 4v^4t^3 + 6v^2t^2) + 2(u-1)(2u-1)t + m, \\ \quad U(t) = (u-1)(v^6t^3 + 3v^4t^2 + 3v^2t) + u, V(t) = v^3t + v. \end{array} \right.$$

Note that for $mcl_1(t)$ one may also use a unit $E_m = u + v\sqrt{m}$ of norm -1 since $U(t)^2 - mcl_1(t)V(t)^2 = u^2 - mv^2$, which is not possible for the other polynomials.

We may enlarge the previous list with cases where the coefficients of E_m may be half-integers defining more general units (as $\varepsilon_5, \varepsilon_{13}$ of norm -1 in the case of $mcl_1(t)$, then as ε_{21} of norm 1 for the other $mcl(t)$). This will give $E_m = \varepsilon_m$ or ε_m^2 .

So we have the following transformation of the $mcl(t), U(t), V(t)$, that we explain with $mcl_1(t)$. The polynomial $mcl_1(t)$ fulfills the condition $U(t)^2 - mcl_1(t)V(t)^2 = u^2 - mv^2$, which is the norm of $E_m = u + v\sqrt{m}$; so we can use any square-free integer $m \equiv 1 \pmod{4}$ such that $E_m = \frac{1}{2}(u + v\sqrt{m})$, $u, v \in \mathbb{Z}_{\geq 1}$ odd, and we obtain the formal unit $E_{M(t)} = \frac{1}{2}(U(t) + V(t)\sqrt{mcl_1(t)})$ under the condition t even to get $U(t), V(t) \in \mathbb{Z}_{\geq 1}$. This gives the polynomials $mcl_6(t) = v^2t^2 + 2ut + m$ and the coefficients $U(t) = \frac{1}{2}(v^2t + u)$, $V(t) = \frac{1}{2}v$ of a new unit, with $mcl_6(t) = M(t)r(t)^2$, for all $t \geq 0$.

For the other $mcl(t)$ one applies the maps $t \mapsto 2t, t \mapsto 4t$, depending on the degrees; so we obtain the following list, where the resulting unit is $E_{M(t)} = U(t) + V(t)\sqrt{m(t)}$, of norm ± 1 , under the conditions $m \equiv 1 \pmod{4}$ and $\varepsilon_m = \frac{1}{2}(u + v\sqrt{m})$, u, v odd:

$$\left\{ \begin{array}{l} mcl_6(t) = v^2t^2 + 2ut + m, U(t) = \frac{1}{2}(v^2t + u), V(t) = \frac{1}{2}v; \\ mcl_7(t) = (u-2)^2(v^2t^2 + 2t) + m, \\ \quad U(t) = \frac{1}{2}((u-2)(v^4t^2 + 2v^2t) + u), V(t) = \frac{1}{2}(v^3t + v); \\ mcl_8(t) = (u+2)^2(v^2t^2 + 2t) + m, \\ \quad U(t) = \frac{1}{2}((u+2)(v^4t^2 + 2v^2t) + u), V(t) = \frac{1}{2}(v^3t + v); \\ mcl_9(t) = (u+2)^2v^2t^2 + 2(u^2 - 4)t + m, \\ \quad U(t) = \frac{1}{2}\left(\frac{(u+2)^2}{u-2}v^4t^2 + 2(u+2)v^2t + u\right), V(t) = \frac{1}{2}\left(\frac{u+2}{u-2}v^3t + v\right); \\ mcl_{10}(t) = (u-2)^2(v^6t^4 + 4v^4t^3 + 6v^2t^2) + 4(u-2)(u-1)t + m, \\ \quad U(t) = \frac{1}{2}((u-2)(v^6t^3 + 3v^4t^2 + 3v^2t) + u), V(t) = \frac{1}{2}(v^3t + v). \end{array} \right.$$

In other words, these numerous families of parametrized units are nothing but the units $E_s(T) = \frac{1}{2}(T + \sqrt{T^2 - 4s})$ when the parameter $T = U(t)$ is a given polynomial expression. This explain that the properties of the units $E_s(T)$ are similar to that of the

two universal units $E_s(t)$, for $t \in \mathbb{Z}_{\geq 1}$, but, a priori, the F.O.P. algorithm does not give fundamental units when $T(t)$ is not a degree 1 monic polynomial; nevertheless it seems that the algorithm gives most often fundamental units, at least for all $t \gg 0$.

We give the following example, using for instance the Mc Laughlin polynomial $mcl_{10}(t)$ with $m = 301$, $u = 22745$, $v = 1311$, corresponding to, $\varepsilon_m = \frac{1}{2}(22745 + 1311\sqrt{301})$ of norm 1 (program of Section 3); this will give enormous units $E_{M(t)} =: \varepsilon_{M(t)}^n$. The output is of the form $[M(t), r(t), n]$. Then there is no exception to $E_{M(t)} = \varepsilon_{M(t)}$ (i.e., $n = 1$); moreover, one sees many cases of non-square-free integers $mcl_{10}(t)$:

```
{B=10^3;LN=List;LM=List;u=22745;v=1311;for(t=1,B,
mt=(u-2)^2*(v^6*t^4+4*v^4*t^3+6*v^2*t^2)+4*(u-2)*(u-1)*t+301;
ut=1/2*((u-2)*(v^6*t^3+3*v^4*t^2+3*v^2*t)+u);vt=1/2*(v^3*t+v);
C=core(mt,1);M=C[1];r=C[2];D=quaddisc(M);X=quadgen(D);Y=quadunit(D);
res=Mod(M,4);if(res!=1,Z=ut+r*vt*X);if(res==1,Z=ut-r*vt+2*r*vt*X);
z=1;n=0;while(Z!=z,z=z*Y;n=n+1);L=List([M,r,n]);listput(LM,vector(3,c,L[c]));
VM=vecsort(vector(B,c,LM[c]),1,8);print(VM);
print("number of outputs:",matsize(VM)[2]);for(k=1,matsize(VM)[2],n=VM[k][3]);
if(n>1,Ln=VM[k];listput(LN,vector(3,c,Ln[c]))) ;Vn=vecsort(LN,1,8);
print("exceptional powers:",Vn)}
[656527122296918386395032242,2,1],[1594671238615711306590405613,63245,1],
[6538031892707128354912512481,1400,1],[8374054846220987469202089646,14,1],
[13294653599300065679245260247,4,1],[17461037237177260272395675419,140,1],
[28515629817043220531451663970,7672,1],[42017686932862256394245096245,1,1],
(...)
[2626102383534535069268098426753041168301,1,1]
number of outputs:1000
exceptional powers:List([])
time=15,483 ms.
```

Using the Remark 1.2, with $\mathbf{B} = 10^3$ and $m(t)$ of degree 4, with leading coefficient $a_4\mathbf{B}^4 = (22745 - 2)^2 \cdot 1311^6 \cdot 10^{12} = 262610237742277549987973268900000000000$, one gets $\log(2626102383534535069268098426753041168301)/\log(a_4\mathbf{B}^4) \approx 1.00000000025\dots$

6. APPLICATION TO p -RATIONAL VS NON- p -RATIONAL QUADRATIC FIELDS

Let $p \geq 2$ be a prime number. Recall the definition of p -rationality of a number field in the framework of abelian p -ramification theory. The references we give in this article are insufficient to cover the subject and concern essentially recent papers; so the reader may look at the historical of the abelian p -ramification theory, in [Gra5, Appendix], for precise attribution from Šafarevič's pioneering results of the numerous approaches (class field theory, Galois cohomology, pro- p -group theory, infinitesimal theory) and use its references concerning developments of this theory (from our Crelle's papers 1982–1983, Jaulent's infinitesimals [Jau1] (1984), Jaulent's thesis [Jau2] (1986), Nguyen Quang Do's article [Ng] (1986), Movahhedi's thesis [Mov] (1988)); all prerequisites and developments are available in our book [Gra1] (2005).

Definition 6.1. *A number field K is said to be p -rational if K fulfills the Leopoldt conjecture for p and if the torsion group \mathcal{T}_K of the Galois group of the maximal abelian p -ramified (i.e., unramified outside p and ∞) pro- p -extension of K is trivial.*

We will use the fact that, for totally real fields K , we have the formula:

$$(6.1) \quad \#\mathcal{T}_K = \#\mathcal{C}'_K \cdot \#\mathcal{R}_K \cdot \#\mathcal{W}_K,$$

where \mathcal{C}'_K is a quotient of the p -class group \mathcal{C}_K and \mathcal{W}_K depends on local p -roots of unity; for $K = \mathbb{Q}(\sqrt{M})$ and $p > 2$, $\mathcal{C}'_K = \mathcal{C}_K$ and $\mathcal{W}_K = 1$ except if $p = 3$ and $M \equiv -3 \pmod{9}$. Then \mathcal{R}_K is the “normalized p -adic regulator” of K (see the definition for any number field in [Gra4, Proposition 5.2]). For $K = \mathbb{Q}(\sqrt{M})$, $\#\mathcal{R}_K \sim \frac{1}{p} \log_p(\varepsilon_M)$.

So $\#\mathcal{T}_K$ is divisible by the order of \mathcal{R}_K , which gives a sufficient condition for the non- p -rationality of K . Since the p -class group of a field is trivial for $p \gg 0$, the p -rationality only depends on \mathcal{R}_K in that cases.

Proposition 6.2. ([Gra6, Proposition 5.1]) *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of fundamental unit ε_m . Let $p > 2$ be a prime number with residue degree $f \in \{1, 2\}$.*

(i) *For $p \geq 3$ unramified in K , $v_p(\#\mathcal{R}_K) = v_p(\varepsilon_m^{p^f-1} - 1) - 1$.*

(ii) *For $p > 3$ ramified in K , $v_p(\#\mathcal{R}_K) = \frac{1}{2}(v_p(\varepsilon^{p-1} - 1) - 1)$, where $\mathfrak{p}^2 = (p)$.*

(iii) For $p = 3$ ramified in K , $v_3(\#\mathcal{R}_K) = \frac{1}{2}(v_p(\varepsilon^6 - 1) - 2 - \delta)$, where $\mathfrak{p}^2 = (3)$ and $\delta = 1$ (resp. $\delta = 3$) if $m \not\equiv -3 \pmod{9}$ (resp. $m \equiv -3 \pmod{9}$).

A sufficient condition for the non-triviality of \mathcal{R}_K that encompasses all cases (since the decomposition of p in $\mathbb{Q}(\sqrt{M(t)})$ is unpredictable in the F.O.P. algorithm) is $\log_p(\varepsilon_m) \equiv 0 \pmod{p^2}$; this implies that ε_m is a local p th power at p . It suffices to force the parameter t to be such that a suitable power, prime to p , of $E_s(t) = \frac{1}{2}(t + r(t)\sqrt{M(t)})$ is congruent to 1 modulo p^2 . So, exceptions may arrive only when $E_s(t)$ is a global p th power.

6.1. Remarks about p -rationality and non- p -rationality. (a) In general, most papers intend to find p -rational fields, the main purpose being to prove the existence, in our context, of families of real p -rational quadratic fields (see, e.g., [AsBo, Ben, BGKK, BeMo, Bou, BaRa, By, Gra2, Gra6, Kop, MaRo1, MaRo2]); for this there are three frameworks that may exist for arbitrary number fields, but we restrict ourselves to the already non-trivial real quadratic case:

(i) The field K is fixed and it is conjectured that there exist only finitely many primes $p > 2$ for which K is non p -rational, which is equivalent to the existence of finitely many p for which $\frac{1}{p} \log_p(\varepsilon_K) \equiv 0 \pmod{p}$.

(ii) The prime $p > 2$ is fixed and it is proved/conjectured that there exist infinitely many p -rational quadratic field K , which is equivalent to the existence of infinitely many fields K for which the p -class group is trivial and such that $\frac{1}{p} \log_p(\varepsilon_K)$ is a p -adic unit; this aspect is more difficult because of the p -class group.

(iii) One constructs some families of fields $K(p)$ indexed by p prime. These examples of quadratic fields often make use of Lemma 5.1 to get interesting radicals and units.

For instance we have considered in [Gra6, §5.3] (as many authors), the polynomials $t^2 p^{2\rho} + s$ for p -adic properties of the unit $E = t^2 p^{2\rho} + s + t p^\rho \sqrt{t^2 p^{2\rho} + 2s}$ of norm 1.

Taking " $\rho = \frac{1}{2}$, $t = 1$ ", one gets the unit $E = p + s + \sqrt{p(p+2s)}$ considered in [Ben] where it is proved that for $p > 3$, the fields $\mathbb{Q}(\sqrt{p(p+2)})$ are p -rational since the p -class group is trivial (for analytic reasons) and the unit $p+1 + \sqrt{p(p+2)}$ is not a local p -power. Note that $4p(p+2s) = m_1(2p+2s)$, since $\mathbf{N}(E) = 1$ for all s .

Similarly, in [BeMo], is considered the bi-quadratic fields $\mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)})$, containing the quadratic field $\mathbb{Q}(\sqrt{p^2-4})$ giving the unit $\frac{1}{2}(p + \sqrt{p^2-4})$ still associated to $m_1(p)$; the p -rationality comes from the control of the p -class group since the p -adic regulators are obviously p -adic units.

Finally, in [Kop], is considered the tri-quadratic fields $\mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1})$ which are proven to be p -rational for infinitely many primes p ; but these fields are imaginary, so that one has to control the p -class group by means of non-trivial analytic arguments.

The p -rational fields, having the most trivial arithmetic as possible, allow many existence theorems, conjectures (as the Greenberg's conjecture [Gre2] on Galois representations with open images, and many subsequent papers as [AsBo, Ben, BeMo, Bou, BaRa, GrJa, Jau2, Kop]), and they give results in the pro- p -group Galois theory [MaRo1]. Algorithmic aspects may be found in [Gra3, Gra5, PiVa] and in [BeJa] for the logarithmic class group having strong connexions with \mathcal{T}_K and associated to another Greenberg conjecture [Gre1] (Iwasawa's invariants $\lambda = \mu = 0$ for totally real fields).

(b) We observe with the following program that the polynomials:

$$m_s(p+1) = (p+1)^2 - 4s, \text{ and } m_s(2p+2) = 4(p+1)^2 - 4s$$

always give p -rational quadratic fields, apart from very rare exceptions (only four ones up to 10^6) due to the fact that the units $E_s(p+1) = \frac{1}{2}(p+1 + \sqrt{(p+1)^2 - 4s})$ and $E_s(2p+2) = p+1 + \sqrt{(p+1)^2 - s}$ may be a local p -power as studied in [Gra2] in a probabilistic point of view (except in the case of $E_1(2p+2) = 1 + p + \sqrt{p^2 + 2p} \equiv 1 \pmod{p}$, with $\mathfrak{p}^2 = (p)$, thus never local p th power):

```
{nu=8;L=List([-4,-1,1,4]);for(j=1,4,d=L[j];print("m(p)=(p+1)^2-(",d,")");
forprime(p=3,10^6,M=core((p+1)^2-d);K=bnfinit(x^2-M);wh=valuation(K.no,p);
Kmod=bnrinit(K,p~nu);CKmod=Kmod.cyc;dCK=matsize(CKmod)[2];val=0;
for(k=1,dCK-1,C1=Ckmod[dCK-k+1];w=valuation(C1,p);if(w>0,val=val+w));if(val>0,
print("p=",p," M=",M," v_p(#(p-class group))=",wh," v_p(#(p-torsion group))=",val))}}
```

$m(p)=(p+1)^2+4$, $p=13$	$M=2$	$v_p(\#(p\text{-class group}))=0$	$v_p(\#(p\text{-torsion group}))=1$
$m(p)=(p+1)^2+1$, $p=11$	$M=145$	$v_p(\#(p\text{-class group}))=0$	$v_p(\#(p\text{-torsion group}))=2$
$p=16651$	$M=277289105$	$v_p(\#(p\text{-class group}))=0$	$v_p(\#(p\text{-torsion group}))=1$
$m(p)=(p+1)^2-1$, $p=3$	$M=15$	$v_p(\#(p\text{-class group}))=0$	$v_p(\#(p\text{-torsion group}))=1$
$m(p)=(p+1)^2-4$			

The case of $p = 3$, $M = 15$ does not come from the regulator, nor the class group, but of the factor $\#\mathcal{W}_K = 3$ since $15 \equiv -3 \pmod{9}$; but this case must be considered as a trivial case of non- p -rationality.

(c) For real quadratic fields, the 2-rational fields are characterized via a specific genus theory and are exactly the subfields of the form $\mathbb{Q}(\sqrt{m})$ for $m = 2$, $m = \ell$, $m = 2\ell$, where ℓ is a prime number congruent to $\pm 3 \pmod{8}$ (see proof and history in [Gra3, Examples IV.3.5.1]). So we shall not consider the case $p = 2$ since the non-2-rational quadratic fields may be easily deduced, as well as fields with non-trivial 2-class group.

(d) Nevertheless, these torsion groups \mathcal{T}_K are “essentially” the Tate–Šafarevič groups (see their cohomological interpretations in [Ng]):

$$\text{III}_K^2 := \text{Ker} \left[\text{H}^2(\mathcal{G}_{K,S_p}, \mathbb{F}_p) \rightarrow \bigoplus_{p \in S_p} \text{H}^2(\mathcal{G}_{K_p}, \mathbb{F}_p) \right],$$

where S_p is the set of p -places of K , \mathcal{G}_{K,S_p} the Galois group of the maximal S_p -ramified pro- p -extension of K and \mathcal{G}_{K_p} the local analogue over K_p ; so their non-triviality has an important arithmetic meaning about the arithmetic complexity of the number fields (see for instance computational approach of this context in [Gra7] for the pro-cyclic extension of \mathbb{Q} and the analysis of the Greenberg’s conjecture [Gre1] in [Gra8]). When the set of places S does not contain S_p , few things are known about $\mathcal{G}_{K,S}$; see for instance Maire’s survey [Mai] and its bibliography, then [Gra5, Section 3] for numerical computations.

In other words, the non- p -rationality (equivalent, for $p > 2$, to $\text{III}_K^2 \neq 0$) is an obstruction to a local-global principle and is probably more mysterious than p -rationality. Indeed, in an unsophisticated context, it is the question of the number of primes p such that the Fermat quotient $\frac{2^{p-1} - 1}{p}$ is divisible by p , for which only two solutions are known; then non- p -rationality is the same problem applied to algebraic numbers, as units ε_M ; this aspect is extensively developed in [Gra2] for arbitrary Galois number fields).

6.2. Families of units local p -th power at p – Computation of \mathcal{T}_K . We shall force the non triviality of \mathcal{R}_K to obtain the non- p -rationality of K .

6.2.1. Definitions of the units. Taking polynomials stemming from suitable polynomials m_s we can state:

Theorem 6.3. *Let $p > 2$ be a prime number and let $s \in \{-1, 1\}$.*

(a) *Let $a \in \mathbb{Z}_{\geq 1}$ and $\delta \in \{1, 2\}$. We consider $T := 2\delta^{-1}(ap^4t^2 - \delta s)$ and $m_1(T)$ giving rise to the unit $E_1(T) = \frac{1}{2}(T + \sqrt{T^2 - 4}) = \frac{1}{2}(ap^4t^2 - \delta s + p^2t\sqrt{a^2p^4t^2 - 2\delta as})$, of norm 1 and local p th power at p .*

The cases $(a, \delta) \in \{(1, 1), (1, 2), (2, 1), (3, 1), (3, 2), (4, 1), (5, 1), (5, 2)\}$ give distinct units.

(b) *Consider $T := t_0 + p^2t$ and $m_s(T) = T^2 - 4s$ and the units of norm s :*

$$E_s(T) = \frac{1}{2}(T + \sqrt{T^2 - 4s});$$

they are, for all t , local p th power at p for suitable t_0 depending on p and s , as follows:

(i) *For $t_0 = 0$, the units $E_s(T) = E_s(p^2t)$ are local p th powers at p .*

(ii) *For $p \not\equiv 5 \pmod{8}$, there exist $s \in \{-1, 1\}$ and $t_0 \in \mathbb{Z}_{\geq 1}$ solution of the congruence $t_0^2 \equiv 2s \pmod{p^2}$ such that the units $E_s(T)$ are local p th powers at p .*

(iii) *We get the data $(p = 3, s = -1, t_0 \in \{4, 5\})$, $(p = 7, s = 1, t_0 \in \{10, 39\})$, $(p = 11, s = -1, t_0 \in \{19, 102\})$, $(p = 17, s = -1, t_0 \in \{24, 265\}; s = 1, t_0 \in \{45, 244\})$.*

As t grows from 1 up to \mathbf{B} , for each first occurrence of a square-free integer $M \geq 2$ in the factorization $m(t) = a^2p^4t^2 - 2\delta as = M(t)r(t)^2$ (case (a)), or the factorization $m(t) = (t_0 + p^2t)^2 - 4s = M(t)r(t)^2$ (case (b)), the quadratic fields $\mathbb{Q}(\sqrt{M(t)})$, are non- p -rational, apart possibly when $\frac{1}{2}(ap^4t^2 - \delta s + p^2tr(t)\sqrt{M(t)}) \in \langle \varepsilon_{M(t)}^p \rangle$ (case (a)), or $\frac{1}{2}(t_0 + p^2t + \sqrt{(t_0 + p^2t)^2 - 4s}) \in \langle \varepsilon_{M(t)}^p \rangle$ (case (b)).

Proof. The case (a) is obvious. Since the case (b) (i) is also obvious, assume $t_0 \not\equiv 0 \pmod{p^2}$. We have:

$$(E_s(T))^2 \equiv \frac{1}{2}(T^2 - 2s + T\sqrt{T^2 - 4s}) \pmod{p^2},$$

whence $(E_s(T))^2 \equiv \frac{t_0}{2}\sqrt{T^2 - 4s} \pmod{p^2}$ under the condition $t_0^2 \equiv 2s \pmod{p^2}$. So, $E_s(T)^4 \equiv \frac{1}{4}t_0^2(t_0^2 - 4s) \equiv -1 \pmod{p^2}$, whence the result. One computes that $t_0^2 \equiv 2s \pmod{p^2}$ has solutions for $(p-1)(p+1) \equiv 0 \pmod{16}$ when $s = 1$ and $(p-1)(p+5) \equiv 0 \pmod{16}$ when $s = -1$. \square

For instance, in case (a) we shall use $m(t) = p^4t^2 - s$, $m(t) = p^4t^2 - 2s$, $m(t) = p^4t^2 - 4s$, $m(t) = 9p^4t^2 - 6s$, $m(t) = 9p^4t^2 - 12s$, $m(t) = 4p^4t^2 - 2s$, $m(t) = 25p^4t^2 - 10s$, $m(t) = 25p^4t^2 - 20s$. The case (b) has the advantage that the traces of the units are in $O(t)$ instead of $O(t^2)$ for case (a).

Since in many computations we are testing if some unit $E_s(T)$ is a global p th power, we state the following result which will be extremely useful in practice because it means that the exceptional cases are present only at the beginning of the F.O.P. list:

Theorem 6.4. *Let T be a polynomial of the form $T = ct^h + c_0$, $c \geq 1$, $h \geq 1$, $c_0 \in \mathbb{Z}$ and set $T^2 - 4s = M(t)r(t)^2$. For $\mathbf{B} \gg 0$, the maximal bound $M_{\mathbf{B}}^{\text{exc}}$ of the square-free integers $M(t)$, obtained by the F.O.P. algorithm, for which $E_s(T) := \frac{1}{2}(T + \sqrt{T^2 - 4s})$ may be a p th power of $\varepsilon_{M(t)}$ (whence the field $\mathbb{Q}(\sqrt{M(t)})$ being p -rational by exception), is of the order of $(c^2\mathbf{B}^{2h})^{\frac{1}{p}}$ as $\mathbf{B} \rightarrow \infty$.*

Proof. Put $\varepsilon_M = \frac{1}{2}(a + b\sqrt{M})$ as usual; then we can write $\varepsilon_M \sim b\sqrt{M}$ and $E_s(T) \sim T$ so that T and $(b\sqrt{M})^p$ are equivalent as M and \mathbf{B} tend to infinity; taking the most unfavorable case $b = 1$, we conclude that $M_{\mathbf{B}}^{\text{exc}} \ll (c^2\mathbf{B}^{2h})^{2/p}$ in general. \square

For instance $T = t_0 + p^2t$, of the case (b) of Theorem 6.3, gives a bound $M_{\mathbf{B}}^{\text{exc}}$, of possible exceptional Kummer radicals, of the order of $(p^4\mathbf{B}^2)^{1/p}$. This implies that when $\mathbf{B} \rightarrow \infty$, the density of Kummer radicals M such that $E_s(T)$ is not a global p th power is equal to 1. With $\mathbf{B} = 10^6$, often used in the programs, the bound $M_{\mathbf{B}}^{\text{exc}}$ tends to 1 quickly as p increases. In practice, for almost all primes p , the F.O.P. lists are without any exception (only the case $p = 3$ gives larger bounds, as $M_{10^6}^{\text{exc}} \approx 43267$ for the above example; but it remains around $10^6 - 43267 = 956733$ certified solutions M).

6.2.2. *Program of computation of \mathcal{T}_K .* We give the program using together the above 16 parametrized radicals (case (a)) and we print short excerpts. The parameter nu must be large enough such that p^ν annihilates \mathcal{T}_K ; any prime number $p > 2$ may be illustrated (here we take $p = 3, 5, 7$). A part of the program is that given in [Gra3] for any number field. For convenience, we replace the data [7784110, List([9])], in the outputs, by [7784110, [9]] giving a 3-group \mathcal{T}_K of $\mathbb{Q}(\sqrt{7784110})$ isomorphic to $\mathbb{Z}/9\mathbb{Z}$.

```
{B=10^4;p=3;Lm=List([List([1,-4]),List([1,-2]),List([1,-1]),List([1,1]),List([1,2]),
List([1,4]),List([4,-2]),List([4,2]),List([9,-6]),List([9,6]),List([9,-12]),List([9,12]),
List([25,-10]),List([25,10]),List([25,-20]),List([25,20])]);nu=8;p4=p^4;Ln=List;LM=List;
for(t=1,B,for(e11=1,16,a=Lm[e11][1];b=Lm[e11][2];mt=a*t^2*p4+b;M=core(mt);
K=bnfinit(x^2-M,1);Kmod=bnrinit(K,p^nu);CKmod=Kmod.cyc;Tn=List;d=matsize(CKmod)[2];
for(k=1,d-1,C1=CKmod[d-k+1];w=valuation(C1,p);if(w>0,listinsert(Tn,p^w,1)));
L=List([M,Tn]);listput(LM,vector(2,c,L[c]));VM=vecsort(vector(16*B,c,LM[c]),1,8);
print(VM);print("number of outputs:",matsize(VM)[2]);
for(k=1,matsize(VM)[2],T=VM[k];if(T[2]==List([]),listput(Ln,vector(1,c,T[c])));
Vn=vecsort(Ln,1,8);print("exceptions:",Vn)}
p=3
[[2, []], [3, []], [5, []], [6, [3]], [7, []], [10, []], [11, []], [13, []], [14, []], [15, [3]], [21, []],
[23, []], [29, [9]], [33, [3]], [34, []], [35, []], [37, []], [38, []], [42, [9]], [53, []], [55, []],
[58, [3]], [61, []], [62, [3]], [69, [3]], [74, [9]], [77, [3]], [78, [3]], [79, [9]], [82, [3]],
[83, [3]], [85, [3]], [87, [3]], [93, [3]], [103, [3]], [106, [3]], [109, [3]], [110, []], [115, []],
[122, [81]], [141, [9]], [142, [3]], [143, []], [145, []], [146, []], [151, [3]], [159, [3]], [173, [3]],
(...)]
[202378518245, [3]], [202419008110, [27, 3]], [202459502005, [27, 9]], [202459502015, [81]],
[202459502035, [81]], [202459502045, [81, 3]], [202499999990, [3]], [202500000010, [3]]]
number of outputs:139954
exceptions:List([[2], [3], [5], [7], [10], [11], [13], [14], [21], [23], [34], [35], [37], [38], [53],
[55], [61], [110], [115], [143], [145], [146], [205], [215], [221], [226], [227], [230], [437], [439],
```



```

[442], [445], [577], [890], [902], [905], [910], [1085], [1087], [1093], [1517], [1762], [1766],
[2605], [3595], [3605], [5605], [5615], [5645], [11005]])
time=34min, 12,215 ms.
p=5
[[2, []], [3, []], [5, []], [6, []], [21, []], [23, []], [26, []], [29, []], [38, [5]], [39, [5]], [51, [5]],
[62, [25]], [69, [5]], [89, [25]], [102, []], [107, [5]], [114, [5]], [127, [5]], [134, [5]], [161, [5]],
[183, [5]], [186, [5]], [213, []], [219, []], [231, []], [237, []], [278, [5]], [287, [5]], [295, [25]],
[326, [5]], [382, [5]], [422, [5]], [434, [25]], [453, [5]], [467, [5]], [501, [5]], [509, [5]],
[514, [25]], [519, [5]], [574, [5]], [581, [5]], [606, [125]], [623, [5]], [626, [5]], [627, [5]],
[629, [5]], [645, [5]], [662, [5]], [674, [5]], [761, [5]],
(...)]
[1561562640635, [125]], [1561562640645, [25]], [1561875062510, [25]], [1562187515605, [625]],
[1562187515615, [125]], [1562187515635, [25]], [1562187515645, [625]], [1562500000010, [15625]])]
number of outputs:139982
exceptions>List([[2], [3], [5], [6], [21], [23], [26], [29], [102], [213], [219], [231], [237]])
time=58min, 12,328 ms.
p=7
[[6, [7]], [37, [7]], [74, [7]], [101, [7]], [123, [7]], [145, [49]], [149, [7]], [206, [7]], [214, [7]],
[215, [7]], [219, [7]], [267, [7]], [505, [7]], [554, [7]], [570, [7]], [629, [7]], [663, [7]], [741, [7]],
[817, [49]], [834, [49]], [887, [49]], [894, [7]], [1067, [7]], [1373, [49]], [1446, [7]], [1517, [7]],
[1590, [7]], [1893, [7]], [2085, [7]], [2162, [7]], [2302, [49]], [2355, [7]], [2397, [7]], [2399, [7]],
[2402, [7]], [2405, [7]], [2498, [7]], [2567, [7]], [2615, [7]], [2679, [7]], [2742, [7]], [2778, [7]],
(...)]
[5998899040235, [49]], [6000099240090, [7]], [6000099240110, [7]], [6001299560005, [7]],
[6001299560015, [7]], [6001299560035, [7]], [6001299560045, [7]], [6002499999990, [7]])]
number of outputs:139991
exceptions>List([])
time=1h, 29min, 18,262 ms.

```

For $p = 11$ and 13 no exception is found for $B = 10^4$.

The case (b) gives an analogous program and will be also illustrated in the Section 7 about p -class groups, especially for the case $p = 3$. The results are similar and give, in almost cases, non-trivial p -adic regulators \mathcal{R}_K , hence non- p -rational fields K .

```

{B=10^4;p=3;nu=8;p4=p^4;Ln=List;LM=List;for(t=1,B,forstep(s=-1,1,2,mt=p4*t^2-4*s;
M=core(mt);K=bnfinit(x^2-M,1);Kmod=bnrinit(K,p^nu);CKmod=Kmod.cyc;Tn=List;
d=matsize(CKmod)[2];for(k=1,d-1,C1=CKmod[d-k+1];w=valuation(C1,p);
if(w>0,listinsert(Tn,p^w,1));L=List([M,Tn]);listput(LM,vector(2,c,L[c])));
VM=vecsort(vector(2*B,c,LM[c]),1,8);print(VM);
print("number of outputs:",matsize(VM)[2]);for(k=1,matsize(VM)[2],T=VM[k];
if(T[2]==List([],listput(Ln,vector(1,c,T[c]))));Vn=vecsort(Ln,1,8);
print("exceptions:",Vn)}
p=3
[[2, []], [5, []], [10, []], [13, []], [14, []], [29, [9]], [35, []], [37, []], [58, [3]], [61, []], [62, [3]],
[74, [9]], [77, [3]], [82, [3]], [85, [3]], [106, [3]], [109, [3]], [110, []], [122, [81]], [143, []],
[145, []], [173, [3]], [181, [3]], [182, [9]], [202, [3]], [221, []], [226, []], [229, [3]], [257, [27]],
[287, [3]], [323, [3]], [359, [9]], [397, [3]], [401, [3]], [410, [27]], [437, []], [442, []], [445, []],
[506, [9]], [515, [3]], [518, [3]], [533, [3]], [626, [3]], [635, [3]], [674, [9]], [730, [27]],
(...)]
[8078953685, [81]], [8078953693, [9]], [8082189805, [3, 3]], [8085426557, [9]], [8085426565, [9]],
[8088663965, [9]], [8091902021, [3]], [8095140733, [3]], [8098380077, [27, 3]], [8098380085, [27]]]
number of outputs:19990
exceptions>List([[2], [5], [10], [13], [14], [35], [37], [61], [110], [143], [145], [221], [226],
[437], [442], [445], [1085], [1093], [1517]])
time = 2min, 52,051 ms.
p=5
[[6, []], [21, []], [26, []], [29, []], [39, [5]], [51, [5]], [69, [5]], [89, [25]], [114, [5]], [161, [5]],
[326, [5]], [434, [25]], [501, [5]], [509, [5]], [514, [25]], [574, [5]], [581, [5]], [626, [5]],
[629, [5]], [674, [5]], [761, [5]], [789, [5]], [791, [5]], [874, [5]], [1086, [5]], [1111, [5, 5]],
[1191, [5]], [1351, [5]], [1406, [5]], [1641, [625]], [1761, [5]], [1851, [5]], [1914, [5]],
(...)]
[62412530621, [5]], [62412530629, [5]], [62437515621, [25]], [62437515629, [125]],
[62462505621, [5]], [62462505629, [5]], [62487500621, [5]], [62487500629, [5]]]
number of outputs:19996
exceptions>List([[6], [21], [26], [29]])
time = 4min, 9,555 ms.
p=7
[[6, [7]], [37, [7]], [101, [7]], [145, [49]], [149, [7]], [206, [7]], [215, [7]], [554, [7]], [570, [7]],
[629, [7]], [663, [7]], [741, [7]], [817, [49]], [894, [7]], [1067, [7]], [1373, [49]], [1517, [7]],
[1893, [7]], [2085, [7]], [2162, [7]], [2302, [49]], [2355, [7]], [2397, [7]], [2402, [7]], [2405, [7]],
[2498, [7]], [2567, [7]], [2679, [7]], [2742, [7]], [2845, [7]], [2915, [49]], [3162, [7]], [3477, [7]],

```



```
(... )
[239668014477, [7]], [239668014485, [7]], [239763977645, [343]], [239763977653, [7]],
[239859960029, [7]], [239955961613, [7]], [240051982397, [7]], [240051982405, [7]]]
number of outputs:19998
exceptions:List([])
time = 5min, 33,455 ms.
```

6.3. Infiniteness of non p -rational real quadratic fields. All these experiments raise the question of the infiniteness, for any given prime $p > 2$, of non p -rational real quadratic fields when the non p -rationality is due to $\mathcal{R}_K \equiv 0 \pmod{p}$ (i.e., $\log(\varepsilon_M) \equiv 0 \pmod{p^2}$).

6.3.1. *Explicit families of units.* We will built parametrized Kummer radicals and units, in the corresponding fields, which are not p th power of a unit; the method relies on the choice of suitable values of the parameter trace t . This will imply the infiniteness of degree $p - 1$ imaginary cyclic fields of the Section 7 having non trivial p -class groups.

Theorem 6.5. (i) *Let $q \equiv 1 \pmod{p}$ be prime, let $\bar{c} \notin \mathbb{F}_q^{\times p}$ and $t_q \in \mathbb{Z}_{\geq 1}$ such that $t_q \equiv \frac{c^2 + s}{2cp^2} \pmod{q}$. Then, whatever the bound \mathbf{B} , the F.O.P. algorithm applied to the polynomial $m(t_q + qx) = p^4(t_q + qx)^2 - s$, $x \in \mathbb{Z}_{\geq 0}$, gives lists of distinct Kummer radicals M , in the ascending order, such that $\mathbb{Q}(\sqrt{M})$ is non- p -rational.*

(ii) *For any given prime $p > 2$ there exist infinitely many real quadratic fields K such that $\mathcal{R}_K \equiv 0 \pmod{p}$, whence infinitely many non p -rational real quadratic fields.*

Proof. (i) *Criterion of non p th power.* Consider $m(t) = p^4t^2 - s$ and the unit $E_s(2p^2t) = p^2t + \sqrt{p^4t^2 - s}$ of norm s and local p th power at p . Choose a prime $q \equiv 1 \pmod{p}$ and let $c \in \mathbb{Z}_{>1}$ be non p th power modulo q (whence $(q - 1)(1 - \frac{1}{p})$ possibilities). Let $t \equiv \frac{c^2 + s}{2cp^2} \pmod{q}$; then:

$$\begin{aligned} \mathbf{N}(E_s(2p^2t) - c) &= \mathbf{N}(p^2t - c + \sqrt{p^4t^2 - s}) \\ &= (p^2t - c)^2 - p^4t^2 + s = c^2 + s - 2cp^2t \equiv 0 \pmod{q}. \end{aligned}$$

Such value of t defines the field $\mathbb{Q}(\sqrt{M(t)})$, via $p^4t^2 - s = M(t)r(t)^2$, and whatever its residue field at q (\mathbb{F}_q or \mathbb{F}_{q^2}), we get $E_s(2p^2t) \equiv c \pmod{q}$, for some $q \mid q\mathbb{Z}$; since in the inert case, $\#\mathbb{F}_{q^2}^{\times} = (q - 1)(q + 1)$, with $q + 1 \not\equiv 0 \pmod{p}$, c is still non p th power, and $E_s(2p^2t)$ is not a local p th power modulo q , hence not a global p th power.

(ii) *Infiniteness.* Now, for simplicity to prove the infiniteness, we restrict ourselves to the case $m(t) = p^4t^2 - 1$ (the case $m(t) = p^4t^2 + 1$ may be considered with a similar reasoning in $\mathbb{Z}[\sqrt{-1}]$ instead of \mathbb{Z}). Let ℓ be a prime number arbitrary large and consider the congruence:

$$p^2(t_q + qx) \equiv 1 \pmod{\ell};$$

it is equivalent to $x = x_0 + y\ell$, $y \in \mathbb{Z}_{\geq 0}$, where x_0 is a residue modulo ℓ of the constant $\frac{1 - t_q p^2}{qp^2}$; so, we have $p^2(t_q + qx_0) - 1 = \lambda\ell^n$, $n \geq 1$, $\ell \nmid \lambda$. Computing these $m(t)$'s, with $t = t_q + (x_0 + y\ell)q$, gives:

$$p^4(t_q + q(x_0 + y\ell))^2 - 1 = [p^2(t_q + q(x_0 + y\ell)) - 1] \cdot [p^2(t_q + q(x_0 + y\ell)) + 1] \equiv 0 \pmod{\ell};$$

the right factor is prime to ℓ ; the left one is of the form $\lambda\ell^n + qyp^2\ell$, and whatever n , it is possible to choose y such that the ℓ -valuation of $\lambda\ell^{n-1} + qyp^2$ is zero. So, for such integers t , we have the factorization $m(t) = \ell M' r^2$, where $M' \geq 1$ is square-free and $M' r^2$ prime to ℓ , which defines $M := \ell M'$ arbitrary large.

This proves that in the F.O.P. algorithm, when $\mathbf{B} \rightarrow \infty$, one can find arbitrary large Kummer radicals $M(t_q + (x_0 + y\ell)q)$ such that the corresponding unit $E_1(t_q + (x_0 + y\ell)q)$ is a local p th power modulo p , but not a global p -th power. \square

The main property of the F.O.P. algorithm is that the Kummer radicals obtained are distinct and listed in the ascending order; without the F.O.P. process, all the integers $t = t_q + (x_0 + y\ell)q$ giving the same M give $E_1(t_q + (x_0 + y\ell)q) = \varepsilon_M^n$ with $n \not\equiv 0 \pmod{p}$.

6.3.2. *Unlimited lists of non- p -rational real quadratic fields.* Take $p = 3$, $q = 7$, $c \in \{2, 3, 4, 5\}$. With $m(t) = 81t^2 - 1$, then $t_q \in \{2, 5\}$; with $m(t) = 81t^2 + 1$, then $t_q \in \{3, 4\}$ and $t = t_q + 7x$, $x \geq 0$. The F.O.P. list is without any exception, giving non 3-rational quadratic fields $\mathbb{Q}(\sqrt{M})$ (in the first case, $p = 3$ is inert and in the second one, $p = 3$ splits. We give the corresponding list using together the four possibilities:

```
{B=10^6;p=3;Lm=List([List([-1,3]),List([-1,4]),List([1,2]),List([1,5])]);
Ln=List;LM=List;for(t=1,B,for(ell=1,4,s=Lm[ell][1];tq=Lm[ell][2];M=core(81*(tq+7*t)^2-s);
L=List([M]);listput(LM,vector(1,c,L[c])));VM=vecsort(vector(4*B,c,LM[c]),1,8);print(VM);
print("number of outputs:",matsize(VM)[2])}
[58], [74], [106], [113], [137], [359], [386], [401], [410], [494], [515], [610], [674], [743], [806],
[842], [877], [1009], [1010], [1157], [1367], [1430], [1934], [1901], [1934], [2006], [2153], [2255], [2522],
[2678], [2822], [2986], [3014], [5266], [5513], [6262], [6707], [6722], [6890], [7310], [7610],
[7858], [7919], [8101], [8465], [8555], [8738], [8761], [9410], [9634], [9998], [11183], [11195],
[11237], [11447], [11509], [11537], [11663], [11890], [11965], [13427], [13645], [14795], [16895],
[16913], [17266], [18530], [19223], [19826], [20066], [20735], [21023], [21317], [21389], [22730],
[23066], [23102], [23410], [23626], [23783], [23963],
(...)
[248061649500730], [248061933000323], [248063067000323], [248063350500730], [248063634001297]
number of outputs:4000000
time=7min, 1,706 ms.
```

In case of doubt about the results, one may use the same program with the computation of $\#\mathcal{T}_K$; but the execution time is much larger and it is not possible to take a large \mathbf{B} since the computations need the instructions $K = \text{bnfinit}(x^2 - M)$ and $K\text{mod} = \text{bnrinit}(K, p^n u)$ of class field theory package (the list below contains 42 outputs up to $M = 23963$, while the first one contains 80 Kummer radicals):

```
{B=10^3;p=3;Lm=List([List([-1,3]),List([-1,4]),List([1,2]),List([1,5])]);nu=8;p4=p^4;
Ln=List;LM=List;for(t=1,B,for(ell=1,4,s=Lm[ell][1];t0=Lm[ell][2];M=core(81*(t0+7*t)^2-s);
K=bnfinit(x^2-M);Kmod=bnrinit(K,p^nu);CKmod=Kmod.cyc;Tn=List;d=matsize(CKmod)[2];
for(k=1,d-1,C1=CKmod[d-k+1];w=valuation(C1,p);if(w>0,listinsert(Tn,p^w,1));L=List([M,Tn]);
listput(LM,vector(2,c,L[c])));VM=vecsort(vector(4*B,c,LM[c]),1,8);print(VM);
print("number of outputs:",matsize(VM)[2]);for(k=1,matsize(VM)[2],T=VM[k];
if(T[2]==List([]),listput(Ln,vector(1,c,T[c])));
Vn=vecsort(Ln,1,8);print("exceptions:",Vn)}
```

```
[58, [3]], [74, [9]], [106, [3]], [359, [9]], [401, [3]], [410, [27]], [515, [3]], [674, [9]], [842, [9]],
[1009, [9]], [1157, [3]], [1367, [9]], [1430, [9]], [1934, [3]], [2255, [3]], [2678, [9]], [2822, [9]],
[3014, [3]], [5513, [9]], [6722, [27]], [6890, [3]], [7310, [3, 3]], [7858, [9]], [7919, [3]], [8101, [3]],
[8465, [27]], [8555, [27]], [8738, [3]], [8761, [81]], [9410, [9]], [9634, [27, 3]], [9998, [9, 3]],
(...)
[3949745410, [3]], [3950876735, [81]], [3955403663, [27]], [3956535802, [3]], [3957668101, [27, 3]],
[3965598730, [3]], [3966732323, [9, 3]], [3971268323, [81]], [3972402730, [3]], [3973537297, [27]]]
number of outputs:4000
exceptions:List([])
time=32,886 ms.
```

7. APPLICATION TO p -CLASS GROUPS OF SOME IMAGINARY CYCLIC FIELDS

Considering, now, the case (b) of Theorem 6.3, we use the polynomial $m_s(T) = T^2 - 4s$, with $T = t_0 + p^2t$, and the unit of norm s :

$$E_s(T) = \frac{1}{2}(T + \sqrt{T^2 - 4s}),$$

for suitable s and t_0 such that $E_s(T)$ be a local p th power at p , which is in particular the case for all $p > 2$ and all s when $t_0 = 0$. For $t_0 \neq 0$, we get the particular data when the equation $t_0^2 \equiv 2s \pmod{p^2}$ has solutions (which is equivalent to $p \not\equiv 5 \pmod{8}$): ($p = 3, s \in \{-1, 1\}, t_0 = 0$), ($p = 3, s = -1, t_0 \in \{4, 5\}$), ($p = 7, s = 1, t_0 \in \{10, 39\}$), ($p = 11, s = -1, t_0 \in \{19, 102\}$), ($p = 17, s = -1, t_0 \in \{24, 265\}$; $s = 1, t_0 \in \{45, 244\}$).

The programs are testing that $E_s(T)$ is not the p th power of a unit.

7.1. Unlimited lists of quadratic fields with non-trivial 3-class group. From the above, we obtain, as consequence, the following selection of illustrations (see Theorem 6.5 claiming that the F.O.P. lists are unbounded as $\mathbf{B} \rightarrow \infty$):

Theorem 7.1. *Let $t_0 \in \{0, 4, 5\}$ and $m(t) := (t_0 + 9t)^2 + 4$ if $t_0 \neq 0$, or $m(t) := (t_0 + 9t)^2 \pm 4$ if $t_0 = 0$. As t grows from 1 up to \mathbf{B} , each first occurrence of a square-free integer $M \geq 2$ in the factorization $m(t) = Mr^2$, the quadratic field $\mathbb{Q}(\sqrt{-3M})$ has a*

class number divisible by 3, except possibly when the unit $E_s(t_0 + 9t) := \frac{1}{2}(t_0 + 9t + r\sqrt{M})$ is a third power of a unit.

The F.O.P. algorithm applied to the subset of parameters $t = 2 + 7x$ or $t = 5 + 7x$, $x \in \mathbb{Z}_{\geq 0}$ with $m(t) = 81t^2 - 1$, always gives non-trivial 3-class groups. Same results with $t = \pm 3 + 7x$ with $m(t) = 81t^2 + 1$.

Proof. If $E_s(t_0 + 9t)$ is not a third power of ε_M but a local 3th power at 3, it is 3-primary in the meaning that if ζ_3 is a primitive 3th root of unity, then $K(\zeta_3, \sqrt[3]{E_s(t_0 + 9t)})/K(\zeta_3)$ is unramified (in fact 3 splits in this extension). From reflection theorem (Scholz's Theorem in the present case), 3 divides the class number of $\mathbb{Q}(\sqrt{-3M})$, even when $r > 1$ in the factorization $m(t) = Mr^2$. The case of $t_0 = 0$ and $s = \pm 1$ is obvious.

The second claim comes from Theorem 6.5 (see numerical part below). \square

7.1.1. *Program for lists of 3-class groups of imaginary quadratic fields.* Note that the case where $E_s(t_0 + 9t)$ is a third power is very rare because it happens only for very large $t_0 + 9t$ giving a small Kummer radical M . One may verify the claim by means of the following program, in the case $s = -1$ valid for all t_0 , where $[M, Vh]$ gives in Vh the 3-structure of the class group of $\mathbb{Q}(\sqrt{-3M})$; at the end of each output, one sees the list of exceptions (case of third powers), where the output $[M, n]$ means that for the Kummer radical $M = M(t)$, then $E_{-1}(t_0 + 9t) = \varepsilon_M^n$. We may see that any excerpt for t large enough give no exceptions:

```
{p=3;B=10^5;L3=List;Lh=List;Lt0=List([0,4,5]);for(t=1,B,for(e11=1,3,t0=Lt0[e11]);
mt=(t0+9*t)^2+4;ut=(t0+9*t)/2;vt=1/2;C=core(mt,1);M=C[1];r=C[2];
D=quaddisc(M);X=quadgen(D);Y=quadunit(D);res=Mod(M,4);
if(res!=1,Z=ut+r*vt*X);if(res==1,Z=ut-r*vt+2*r*vt*X);z=1;n=0;
while(Z!=z,z=z*Y;n=n+1);C3=List;K=bnfinit(x^2+3*M,1);CK=K.cyc;d=matsize(CK)[2];
for(j=1,d,C1=CK[d-j+1];w=valuation(C1,3);if(w>0,listinsert(C3,3^w,1));L=List([M,C3,n]);
listput(Lh,vector(3,c,L[c]));Vh=vecsort(vector(3*B,c,Lh[c]),1,8);print(Vh);
print("number of outputs:",matsize(Vh)[2]);
for(k=1,matsize(Vh)[2],LC=Vh[k][2];if(LC==List([]),Ln=List([Vh[k][1],Vh[k][3]]));
listput(L3,vector(2,c,Ln[c]));V3=vecsort(L3,1,8);print("exceptional powers:",V3)}
[[2, [], 15], [5, [], 9], [10, [], 3], [13, [], 3], [17, [], 3], [26, [], 3], [29, [3], 5], [37, [], 3],
[41, [], 3], [53, [], 3], [58, [3], 1], [61, [], 3], [65, [], 3], [74, [3], 1], [82, [3], 1], [85, [3], 1],
[101, [], 3], [106, [3], 1], [109, [3], 1], [113, [3], 1], [122, [3], 1], [137, [3], 1], [145, [], 3],
[149, [], 3], [170, [], 3], [173, [9], 1], [181, [3], 1], [197, [], 3], [202, [3], 1], [226, [], 3],
[229, [3], 3], [257, [3], 1], [290, [], 3], [293, [], 3], [314, [3], 1], [317, [], 3], [353, [3], 1],
[362, [], 3], [365, [], 3], [397, [3], 1], [401, [3], 1], [442, [], 3], [445, [], 3], [461, [9], 1],
[485, [], 3], [530, [], 3], [533, [9], 1], [577, [], 3], [610, [3], 1], [626, [3], 1], [629, [], 3],
[653, [3], 1], [677, [], 3], [730, [3], 1], [733, [9], 1], [754, [3], 1], [773, [3], 1], [785, [3], 3],
[842, [3], 1], [877, [3], 1], [901, [], 3], [962, [], 3], [965, [9], 1], [997, [3], 1], [1009, [3], 1],
(...)]
[809976600173, [27], 1], [809983800085, [81], 1], [809991000029, [27], 1], [810009000029, [9], 1]]
number of outputs:299963
exceptional powers:List([[2,15], [5,9], [10,3], [13,3], [17,3], [26,3], [37,3], [41,3], [53,3],
[61,3], [65,3], [101,3], [145,3], [149,3], [170,3], [197,3], [226,3], [290,3], [293,3], [317,3],
[362,3], [365,3], [442,3], [445,3], [485,3], [530,3], [577,3], [629,3], [677,3], [901,3], [962,3],
[1093,3], [1226,3], [1370,3], [1601,3], [1853,3], [2117,3], [2305,3], [2605,3], [2813,3],
[3029,3], [3253,3], [4229,3], [5045,3], [6245,3], [6893,3], [8653,3]])
time = 2h, 32min, 56,578 ms.
```

Then $M_B = 810016200085$ and $\log(810016200085)/\log(81 \cdot 10^{10}) \approx 1.0000007293$; then $M_B^{\frac{1}{3}} \approx 9321.76$ give a good verification of the Heuristic 6.4. This also means that *all the integers M larger than 9029* leads to non-trivial 3-class groups, and they are very numerous !

We note that some M 's (as 29, 74, 82, 85, ...) are in the list of exceptions despite a non-trivial 3-class group; this is equivalent to the fact that, even if $E_{-1}(t_0 + 9t) \in \langle \varepsilon_M^3 \rangle$, either the 3-regulator \mathcal{R}_K of K is non-trivial or its 3-class group is non-trivial.

7.1.2. *Unlimited lists of non-trivial 3-class groups.* To finish, let's give the case where the F.O.P. algorithm *always* gives non-trivial 3-class groups in $\mathbb{Q}(\sqrt{-3M})$; we use together the 4 parametrizations given by Theorem 7.1 (outputs $[M, [3 \text{ class group}]]$):

```
{p=3;B=10^4;Lh=List;Lm=List([List([-1,3]),List([-1,4]),List([1,2]),List([1,5])]);
for(t=1,B,for(e11=1,4,s=Lm[e11][1];t0=Lm[e11][2];M=core(81*(t0+7*t)^2-s);C3=List;
K=bnfinit(x^2+3*M);CK=K.cyc;d=matsize(CK)[2];for(j=1,d,C1=CK[d-j+1];w=valuation(C1,3);
if(w>0,listinsert(C3,3^w,1));L=List([M,C3]);listput(Lh,vector(2,c,L[c])););
```

```
Vh=vecsort(vector(4*B,c,Lh[c]),1,8);print(Vh);print("number of outputs:",matsize(Vh)[2])
[[58, [3]], [74, [3]], [106, [3]], [359, [3]], [386, [3]], [401, [3]], [410, [3]], [494, [3]], [515, [3]],
[610, [3]], [674, [3]], [842, [3]], [877, [3]], [1009, [3]], [1157, [3]], [1367, [3]], [1430, [3]],
[1901, [9, 3]], [1934, [9]], [2153, [3]], [2255, [3]], [2678, [9]], [2822, [3]], [2986, [3]], [3014, [3]],
[5266, [3]], [5513, [3]], [6626, [9]], [6707, [3]], [6722, [3]], [6890, [3]], [7310, [3, 3]], [7858, [27]],
[7919, [3]], [8101, [3]], [8465, [9]], [8555, [9]], [8738, [3]], [8761, [9]], [9410, [3]], [9634, [9, 3]],
[9998, [3, 3]], [11183, [3]], [11237, [3]], [11447, [3]], [11509, [27]], [11537, [3]], [11663, [3, 3]],
[11965, [3]], [13427, [3]], [16895, [3]], [16913, [3, 3]], [17266, [9]], [18530, [3]], [20066, [3]],
(...)]
[396877320323, [3]], [396922680323, [9]], [396934020730, [3]], [396945361297, [3]]]
number of outputs:40000
time=22min, 6,490 ms.
```

7.2. Lists of degree $p - 1$ imaginary cyclic fields with non-trivial p -class group.

Let χ be the even character of order 2 defining $K := \mathbb{Q}(\sqrt{M})$, let $p \geq 3$ and let $L := K(\zeta_p)$ be the field obtained by adjunction of a primitive p th root of unity; we may assume that $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, otherwise $M = p \equiv 1 \pmod{4}$ for which there is no known examples of p -primary fundamental unit. Let ω be the p -adic Teichmüller character (so that for all $\tau \in \text{Gal}(L/\mathbb{Q})$, $\zeta_p^\tau = \zeta_p^{\omega(\tau)}$).

Then, for any list of quadratic fields $\mathbb{Q}(\sqrt{M})$ obtained by the previous F.O.P. algorithm giving p -primary units E , the $\omega\chi^{-1}$ -component of the p -class group of L is non-trivial as soon as $E \notin \langle \varepsilon_M^p \rangle$; it gives an odd component of the whole p -class group of L .

Theorem 7.2. *As t grows from 1 up to \mathbf{B} , each first occurrence of a square-free integer $M \geq 2$ in the factorization $m(t) := p^4 t^2 - 4s = Mr^2$, the degree $p - 1$ cyclic imaginary subfield of $\mathbb{Q}(\sqrt{M}, \zeta_p)$, distinct from $\mathbb{Q}(\zeta_p)$, has a class number divisible by p , except possibly when the unit $E_s(p^2 t) := \frac{1}{2}[p^2 t + r\sqrt{M}]$ is a p -th power of a unit.*

7.2.1. *Lists of 5-class groups of cyclic imaginary quartic fields.* The following program for $p = 5$ verifies the claim with the above parametrized family; it tests if $E_s(p^2 t)$ is a p -power of unit. For $p = 5$, the “mirror field” is defined by the polynomial

$$P = x^4 + 5 * M * x^2 + 5 * M^2$$

still giving a particular faster program than the forthcoming one, valuable for any $p \geq 3$:

```
{p=5;B=100;s=-1;Lp=List;Lh=List;p2=p^2;p4=p^4;
for(t=1,B,mt=p4*t^2-4*s;ut=p2*t/2;vt=1/2;C=core(mt,1);M=C[1];r=C[2];
D=quaddisc(M);X=quadgen(D);Y=quadunit(D);res=Mod(M,4);
if(res!=1,Z=ut+r*vt*X);if(res==1,Z=ut-r*vt+2*r*vt*X);z=1;n=0;
while(Z!=z,z=z*Y;n=n+1);P=x^4+5*M*x^2+5*M^2;K=bnfinit(P,1);CK=N.cyc;C5=List;
d=matsize(CK)[2];for(i=1,d,C1=CK[d-i+1];w=valuation(C1,p);if(w>0,listinsert(C5,p^w,1)));
L=List([M,C5]);listput(Lh,vector(2,c,L[c]));Vh=vecsort(vector(B,c,Lh[c]),1,8);print(Vh);
print("number of outputs:",matsize(Vh)[2]);
for(k=1,matsize(Vh)[2],if(Vh[k][2]==List([]),listput(Lp,Vh[k]));Vp=vecsort(Lp,1,8);
print("exceptions:",Vp)}
s=-1
[[89, [5]], [509, [5, 5]], [626, [25, 5]], [629, [5, 5]], [761, [5]], [2501, [5]], [3554, [25]],
[5626, [5, 5]], [5629, [5]], [10001, [5]], [15626, [5, 5]], [15629, [25]], [22501, [5]],
[30626, [5, 5]], [30629, [5]], [40001, [5]], [50626, [25, 5]], [50629, [5]], [62501, [25, 25]],
[75626, [5]], [75629, [5]], [90001, [5, 5]], [105626, [125, 25]], [105629, [5, 5]], [122501, [5]],
(...)]
[5175629, [125]], [5405629, [5]], [5640629, [5]], [5880629, [5]], [6125629, [5]]]
number of outputs:100
exceptions:List([])
time=19,705 ms.
s=1
[[39, [5]], [51, [5]], [69, [5]], [114, [5]], [326, [5]], [434, [25]], [574, [5, 5]], [674, [5]],
[791, [5]], [1086, [5]], [1111, [5, 5]], [1406, [5]], [1761, [5]], [1914, [5, 5]], [3981, [5]],
[4171, [5, 5]], [5621, [5]], [8789, [5, 5]], [10421, [5]], [11289, [5, 5]], [13611, [5]],
[14189, [5]], [15621, [25]], [18906, [5]], [20069, [5, 5]], [20501, [5, 5]], [22499, [25, 25]],
(...)]
[4730621, [25, 5]], [5405621, [5]], [5640621, [25]], [5880621, [5, 5, 5]], [6125621, [5]]]
number of outputs:100
exceptions:List([])
time=17,011 ms.
```

7.2.2. *General program giving p -class groups of degree $p - 1$ imaginary fields.* The following general program computes the defining polynomial P of the algebraic number $(\zeta_p - \zeta_p^{-1})\sqrt{M}$; it tests if the unit $E_s(p^2t)$ is the p th power of ε_M (choose B and s):

```

{p=5;B=500;s=-1;Lp=List;Lh=List;Zeta=exp(2*I*Pi/p);p2=p^2;p4=p^4;
for(t=1,B,mt=p4*t^2-4*s;ut=p2*t/2;vt=1/2;C=core(mt,1);M=C[1];r=C[2];
D=quaddisc(M);X=quadgen(D);Y=quadunit(D);res=Mod(M,4);
if(res!=1,Z=ut+r*vt*X);if(res==1,Z=ut-r*vt+2*r*vt*X);
z=1;n=0;while(Z!=z,z=z*Y;n=n+1);P=1;for(i=1,(p-1)/2,A=(Zeta^i+Zeta^-i-2)*M;
P=(x^2-A)*P);P=round(P);k=bnfinit(P,1);Ck=k.cyc;Cp=List;d=matsize(Ck)[2];
for(i=1,d,C1=Ck[d-i+1];w=valuation(C1,p);if(w>0,listinsert(Cp,p^w,1));L=List([M,Cp]);
listput(Lh,vector(2,c,L[c]));Vh=vecsort(vector(B,c,Lh[c]),1,8);print(Vh);
print("number of outputs:",matsize(Vh)[2]);
for(k=1,matsize(Vh)[2],if(Vh[k][2]==List([]),listput(Lp,Vh[k]));Vp=vecsort(Lp,1,8);
print("exceptions:",Vp)}
s=-1
[[29, []], [89, [5]], [509, [5, 5]], [626, [25, 5]], [629, [5, 5]], [761, [5]], [2501, [5]], [3554, [25]],
[5626, [5, 5]], [5629, [5]], [10001, [5]], [15626, [5, 5]], [15629, [25]], [19109, [5]], [22061, [5, 5]],
[22501, [5]], [30626, [5, 5]], [30629, [5]], [40001, [5]], [42341, [5]], [50626, [25, 5]], [50629, [5]],
[62501, [25, 25]], [70429, [25]], [75626, [5]], [75629, [5]], [82234, [5]], [90001, [5, 5]],
[105626, [125, 25]], [105629, [5, 5]], [122501, [5]], [140626, [5]], [140629, [5, 5]], [147929, [5]],
(... )
[147015629, [5]], [148230629, [5]], [149450629, [5]], [150675629, [5, 5, 5]],
[151905629, [5]], [153140629, [5]], [154380629, [5]], [155625629, [5, 5]]
number of outputs:500
exceptions:List([[29, List([])]])
time=6min, 2,236 ms.
s=1
[21, []], [39, [5]], [51, [5]], [69, [5]], [114, [5]], [326, [5]], [434, [25]], [514, [5]], [574, [5, 5]],
[581, [5, 5]], [674, [5]], [791, [5]], [874, [5]], [1086, [5]], [1111, [5, 5]], [1191, [5]], [1351, [25]],
[1406, [5]], [1641, [5]], [1761, [5]], [1851, [5]], [1914, [5, 5]], [2399, [5]], [2599, [25]],
[3251, [25]], [3981, [5]], [4171, [5, 5]], [5474, [5]], [5621, [5]], [5774, [5]], [8294, [25, 5]],
[8789, [5, 5]], [10421, [5]], [11289, [5, 5]], [13611, [5]], [14189, [5]], [15621, [25]],
(... )
[141015621, [5, 5]], [142205621, [5, 5]], [143400621, [25, 5]], [144600621, [25, 5]], [145805621, [25]],
[149450621, [5]], [150675621, [5, 5]], [151905621, [5]], [153140621, [5]], [155625621, [625, 5]]
number of outputs:500
exceptions:List([[21, List([])]])
time=4min, 49,301 ms.

```

In this interval, all the 5-class groups obtained are non-trivial, except for $M = 29$ for $s = -1$. From Remark 1.2, we compute $\log(155625629)/\log(5^4 \cdot 25 \cdot 10^4) \approx 0.999787777$. Theorem 6.4 gives possible exceptions up to $M_{\mathbb{B}}^{\frac{1}{5}} = 155625629^{\frac{1}{5}} \approx 43.49268545$.

One observes the spectacular decrease of counterexamples and the unique exception obtained for $t = 151$, $p^2t = 25 \cdot 151 = 3775$, $m_{-1}(3775) = 701^2 \times 29$; whence the PARI data $Y = \text{Mod}(1/2 * x + 5/2, x^2 - 29)$, $Z = \text{Mod}(2646275/2 * x + 14250627/2, x^2 - 29)$ (for ε_{29} and $E_{-1}(3775)$, respectively). One obtains easily the relation $E_{-1}(3775) = \varepsilon_{29}^{10}$. The case $s = 1$ gives no exception:

Consider the case $p = 7$, $s \in \{-1, 1\}$; exceptionally, we give the complete lists:

```

p=7 B=100 s=-1
[[37, [7]], [2402, [7]], [2405, [7]], [4706, [7]], [9605, [7]], [10357, [7]], [11621, [49, 7]],
[21610, [7, 7]], [21613, [7, 7]], [38417, [7]], [60026, [7, 7]], [60029, [7]], [86437, [7, 7]],
[98345, [7]], [117653, [7]], [146077, [7]], [153665, [7, 7]], [177578, [7, 7]], [194482, [7, 7]],
[194485, [49, 7]], [240101, [7]], [290522, [49]], [345745, [49]], [357365, [7]], [405770, [7, 7]],
[405773, [49, 7]], [470597, [7, 7]], [540226, [7]], [540229, [7, 7]], [614657, [7, 7]], [693890, [7, 7]],
[693893, [7]], [760733, [7, 7, 7]], [866762, [7, 7]], [866765, [7, 7]], [960401, [7, 7]], [1058842, [7]],
[1058845, [7, 7]], [1162085, [49, 7]], [1270130, [49, 7, 7]], [1270133, [7]], [1382977, [7, 7]],
[1500626, [49]], [1500629, [7]], [1623077, [7]], [1750330, [7]], [1882385, [7]], [2019242, [49]],
[2019245, [7, 7]], [2160901, [7]], [2307362, [343]], [2307365, [7, 7]], [2614690, [7, 7]],
[2614693, [7]], [2775557, [7]], [2941226, [7]], [2941229, [49]], [3111697, [7]], [3286970, [7]],
[3286973, [7, 7]], [3467045, [7]], [3651922, [7]], [3841601, [7]], [4036082, [7]], [4036085, [49]],
[4235365, [7]], [4439453, [49]], [4648337, [49, 7]], [4862026, [7, 7]], [4862029, [7]],
[5080517, [7, 7]], [5303810, [7]], [5303813, [7]], [5531905, [7]], [5764802, [7, 7]], [5764805, [7]],
[6002501, [7]], [6245005, [7, 7]], [6744413, [49, 7]], [7263029, [7]], [7800853, [7]], [8357885, [7]],
[9529573, [49, 7, 7]], [10144229, [7]], [10778093, [7, 7]], [11431165, [49]], [12103445, [49, 7]],
[12794933, [7]], [13505629, [7]], [14235533, [7]], [14984645, [7]], [15752965, [7]], [16540493, [7]],
[17347229, [7]], [18173173, [7, 7, 7]], [19882685, [7]], [20766253, [7]], [21669029, [7, 7]],
[22591013, [7]], [23532205, [7, 7]]
number of outputs:100

```

```

exceptions>List([])
time=11min, 42,990 ms.
p=7 B=100 s=1
[6, [7]], [741, [7, 7]], [817, [7, 7]], [1067, [7, 7]], [1517, [49]], [2302, [49]], [2397, [49]],
[3477, [7]], [3603, [49, 7]], [5402, [2401, 7]], [5645, [7, 7]], [8070, [49]], [8441, [7, 7]],
[10421, [7]], [10842, [7, 7]], [12155, [7]], [13702, [7]], [15006, [49]], [21605, [7, 7]], [27165, [7]],
[35003, [7]], [38415, [7]], [42803, [7]], [43637, [7]], [45085, [49]], [55319, [7]], [56090, [7, 7]],
[63269, [7]], [64923, [7]], [68295, [7]], [70013, [7]], [79383, [7]], [86435, [7]], [101442, [7]],
[106711, [7]], [117645, [49, 7]], [144210, [49]], [153663, [7, 7]], [163418, [7]], [194477, [7]],
[216690, [7, 7]], [228245, [7]], [240099, [49, 7]], [252255, [7, 7]], [264710, [7]], [290517, [49, 7]],
[308395, [7]], [345743, [7]], [437582, [7, 7]], [448453, [49, 7]], [470595, [7]], [511797, [7]],
[540221, [7]], [640533, [7, 7]], [693885, [7]], [735306, [49, 7]], [777923, [7]], [821742, [7]],
[866757, [7]], [928653, [49]], [1058837, [49, 7]], [1162083, [7]], [1197565, [343]], [1215506, [7, 7]],
[1500621, [7, 7]], [1882383, [49, 7]], [1927469, [7]], [2019237, [7]], [2160899, [7]], [2407669, [7]],
[2458623, [49]], [2614685, [7, 7]], [2941221, [7, 7]], [3111695, [7]], [3651917, [7]], [3841599, [7, 7]],
[4439445, [7]], [4648335, [7]], [4862021, [49, 49, 7]], [5080515, [7]], [5303805, [7]], [5531903, [7]],
[6002499, [7]], [6244997, [7]], [6744405, [7, 7]], [7263021, [7, 7]], [7800845, [7]], [8934117, [7]],
[9529565, [7]], [10144221, [7]], [11431157, [7]], [13505621, [7]], [14984637, [7]], [16540485, [7]],
[18173165, [7]], [19018317, [7]], [19882677, [7]], [20766245, [7]], [22591005, [7]], [23532197, [7]]
number of outputs:100
exceptions>List([])
time=8min, 34,556 ms.

```

Of course, $\mathbf{B} = 100$ is insufficient to give smaller Kummer radicals, but it is only a question of execution time and memory due to the instruction `bnfinit(P, 1)` for P of degree $p - 1$. It is clear that the same program for the F.O.P. algorithm, without computation of the p -class group, gives unlimited lists of degree $p - 1$ imaginary cyclic fields with non-trivial p -class group, as soon as $M > M_{\mathbf{B}}^{\text{exc}}$ (cf. Theorem 6.4):

```

{p=7;B=10^5;s=-1;LM=List;p4=p^4;for(t=1,B,mt=p4*t^2-4*s;M=core(mt);L=List([M]);
listput(LM,vector(1,c,L[c]));VM=vecsort(vector(B-(1+s),c,LM[c]),1,8);print(s);print(VM)}

```

REFERENCES

- [AsBo] J. Assim, Z. Bouazzaoui, Half-integral weight modular forms and real quadratic p -rational fields, *Funct. Approx. Comment. Math.* **63**(2) (2020), 201–213. <https://doi.org/10.7169/facm/1851> [16](#)
- [Ben] Y. Benmerieme, Les corps multi-quadratiques p -rationnels, Thèse (2021LIMO0100), Université de Limoges (2021). <https://tel.archives-ouvertes.fr/tel-03559781> [16](#)
- [By] D. Byeon, Indivisibility of special values of Dedekind zeta functions of real quadratic fields, *Acta Arithmetica* **109**(3) (2003), 231–235. <https://doi.org/10.4064/AA109-3-3> [16](#)
- [BGKK] G. Boeckle, D.A. Guiraud, S. Kalyanswamy, C. Khare, Wieferich Primes and a mod p Leopoldt Conjecture (2018). <https://doi.org/10.48550/arXiv.1805.00131> [16](#)
- [BeJa] K. Belabas, J.-F. Jaulent, The logarithmic class group package in PARI/GP, *Pub. Math. Besançon, Algèbre et théorie des nombres* **2016**, 5–18. <https://doi.org/10.5802/pmb.o-1> [6](#), [16](#)
- [BeMo] Y. Benmerieme, A. Movahhedi, Multi-quadratic p -rational number fields, *Jour. Pure Appl. Algebra* **225**(9) (2021), 1–17. <https://doi.org/10.1016/j.jpaa.2020.106657> [16](#)
- [Bou] Z. Bouazzaoui, Fibonacci numbers and real quadratic p -rational fields, *Period. Math. Hungar.* **81**(1) (2020), 123–133. <https://doi.org/10.1007/s10998-020-00320-7> [16](#)
- [BaRa] R. Barbulescu, J. Ray, Some remarks and experiments on Greenberg’s p -rationality conjecture, *arXiv* (2019). <https://arxiv.org/abs/1706.04847v3> [16](#)
- [CKMP] S. Chan, P. Koymans, D. Milovic, C. Pagano, On the negative Pell equation, *arXiv* (2019). <https://arxiv.org/abs/1908.01752> [11](#)
- [FrIw] J.B. Friedlander, H. Iwaniec, Square-free values of quadratic polynomials, *Proceedings of the Edinburgh Mathematical Society* **53**(2) (2010), 385–392. <https://doi.org/10.1017/S0013091508000989> [4](#)
- [GrJa] G. Gras, J.-F. Jaulent, Note on 2-rational fields, *Jour. Number Theory* **129**(2) (2009), 495–498. <https://doi.org/10.1016/j.jnt.2008.06.012> [16](#)
- [Gra1] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005). [15](#)
- [Gra2] G. Gras, Les θ -régulateurs locaux d’un nombre algébrique : Conjectures p -adiques, *Canadian Jour. Math.* **68**(3) (2016), 571–624. <http://dx.doi.org/10.4153/CJM-2015-026-3> [16](#), [17](#)
English translation: <https://arxiv.org/pdf/1701.02618>
- [Gra3] G. Gras, On p -rationality of number fields. Applications–PARI/GP programs, *Pub. Math. Besançon (Théorie des Nombres)*, *Années 2018/2019*. <https://doi.org/10.5802/pmb.35> [16](#), [17](#), [18](#)
- [Gra4] G. Gras, The p -adic Kummer–Leopoldt Constant: Normalized p -adic Regulator, *Int. Jour. Number Theory* **14**(2) (2018), 329–337. <https://doi.org/10.1142/S1793042118500203> [15](#)
- [Gra5] G. GRAS, Practice of the Incomplete p -Ramification Over a Number Field – History of Abelian p -Ramification, *Communications in Advanced Mathematical Sciences* **2**(4) (2019), 251–280. <https://doi.org/10.33434/cams.573729> [15](#), [16](#), [17](#)
- [Gra6] G. Gras, Heuristics and conjectures in the direction of a p -adic Brauer–Siegel theorem, *Math. Comp.* **88**(318) (2019), 1929–1965. <https://doi.org/10.1090/mcom/3395> [15](#), [16](#)

- [Gra7] G. Gras, Tate–Shafarevich groups in the cyclotomic $\widehat{\mathbb{Z}}$ -extension and Weber’s class number problem, *Jour. Number Theory* **228** (2021), 219–252. <https://doi.org/10.1016/j.jnt.2021.04.019> 17
- [Gra8] G. Gras, Algorithmic complexity of Greenberg’s conjecture, *Arch. Math.* **117** (2021), 277–289. <https://doi.org/10.1007/s00013-021-01618-9> 17
- [Gre1] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98**(1) (1976), 263–284. <https://doi.org/10.2307/2373625> 6, 16, 17
- [Gre2] R. Greenberg, Galois representation with open image, *Ann. Math. Qué.* **40**(1) (2016), 83–119. <https://doi.org/10.1007/s40316-015-0050-6> 16
- [Jau1] J-F. Jaulent, S -classes infinitésimales d’un corps de nombres algébriques, *Ann. Inst. Fourier* **34**(2) (1984), 1–27. <https://doi.org/10.5802/aif.960> 15
- [Jau2] J-F. Jaulent, L’arithmétique des ℓ -extensions Thèse de doctorat d’Etat, *Pub. Math. Besançon (Théorie des Nombres)* (1986), 1–349. http://pmb.univ-fcomte.fr/1986/Jaulent_these.pdf 15, 16
- [Jau3] J-F. Jaulent, Classes logarithmiques des corps de nombres, *J. Théorie des Nombres de Bordeaux* **6** (1994), 301–325. <https://doi.org/10.5802/jtnb.117> 6
- [Jau4] J-F. Jaulent, Note sur la conjecture de Greenberg, *Jour. Ramanujan Math. Soc.* **34** (2019), 59–80. <http://www.mathjournals.org/jrms/2019-034-001/2019-034-001-005.html> 6
- [Kop] J. Koperecz, Triquadratic p -rational fields, *Jour. Number Theory*, In Press, Journal Pre–proof (2022). <https://doi.org/10.1016/j.jnt.2022.04.011> 16
- [Mai] C. Maire, Sur la dimension cohomologique des pro- p -extensions des corps de nombres, *J. Théor. Nombres Bordeaux*, **17**(2) (2005), 575–606. <https://doi.org/10.5802/jtnb.509> 17
- [MaRo1] C. Maire, M. Rognant, Composantes isotypiques de pro- p -extensions de corps de nombres et p -rationalité, *Publicationes Mathematicae Debrecen* **94**(1/2) (2019), 123–155. <https://doi.org/10.5486/PMD.2019.8281> 16
- [MaRo2] C. Maire, M. Rognant, A note on p -rational fields and the abc -conjecture, *Proc. Amer. Math. Soc.* **148**(8) (2020), 3263–3271. <https://doi.org/10.1090/proc/14983> 16
- [McL] J. Mc Laughlin, Polynomial Solutions of Pell’s Equation and Fundamental Units in Real Quadratic Fields, *Jour. London Math. Soc.* (2) **67**(1) (2003), 16–28. <https://doi.org/10.1112/S002461070200371X> 2, 14
- [McLZ] J. Mc Laughlin, P. Zimmer, Some more Long Continued Fractions, I, *Acta Arithmetica* **127**(4) (2007), 365–389. <http://eudml.org/doc/278353> 2
- [Mov] A. Movahhedi, Sur les p -extensions des corps p -rationnels, Thèse, Univ. Paris VII, 1988. http://www.unilim.fr/pages_perso/chazad.movahhedi/These_1988.pdf 15
- [Nat] M. B. Nathanson, Polynomial pell’s equations, *Proceedings of the American Mathematical Society*, vol. **56**(1) (1976), 89–92. <https://doi.org/10.2307/2041581> 2
- [Ng] T. Nguyen Quang Do, Sur la \mathbb{Z}_p -torsion de certains modules galoisiens, *Ann. Inst. Fourier*, **36**(2) (1986), 27–46. <https://doi.org/10.5802/aif.1045> 15, 17
- [P] The PARI Group, PARI/GP, version 2.9.0, Université de Bordeaux (2016). 3 <http://pari.math.u-bordeaux.fr/>
- [PiVa] F. Pitoun, F. Varescon, Computing the torsion of the p -ramified module of a number field, *Math. Comp.* **84**(291) (2015), 371–383. <https://doi.org/10.1090/S0025-5718-2014-02838-X> 16
- [Ram] A. M. S. Ramasamy, Polynomial solutions for the Pell’s equation, *Indian Jour. of Pure and Applied Mathematics*, **25** (1994), 577–581. <https://www.academia.edu/33430848/> 2
- [Rud] Z. Rudnick, Square-free values of quadratic polynomials, *Lecture notes* (2015).4 <http://www.math.tau.ac.il/~rudnick/courses/sieves2015/squarefrees.pdf>
- [SaAb] H. Sankari, A. Abdo, On Polynomial Solutions of Pell’s Equation, *Hindawi Jour. of Mathematics* **2021** (2021), 1–4. <https://doi.org/10.1155/2021/5379284> 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> 11

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