A POSITIVE DENSITY OF FUNDAMENTAL DISCRIMINANTS
WITH LARGE REGULATOR

ÉTIENNE FOUVRY AND FLORENT JOUVE

A POSITIVE DENSITY OF FUNDAMENTAL DISCRIMINANTS WITH LARGE REGULATOR

ÉTIENNE FOUVRY AND FLORENT JOUVE

We prove that there is a positive density of positive fundamental discriminants D such that the fundamental unit $\varepsilon(D)$ of the ring of integers of the field $\mathbb{Q}(\sqrt{D})$ is essentially greater than D^3.

1. Introduction

Let $D > 1$ be a fundamental discriminant which means that D is the discriminant of the quadratic field $K := \mathbb{Q}(\sqrt{D})$. Let $\mathbb{Z}_K$ be its ring of integers and let $\omega = (D + \sqrt{D})/2$. Then $\mathbb{Z}_K$ is a $\mathbb{Z}$-module of rank 2

$$\mathbb{Z}_K = \mathbb{Z} \oplus \mathbb{Z}\,\omega. \tag{1}$$

Furthermore there exists a unique element $\varepsilon(D) > 1$ such that the group $\mathbb{U}_K$ of invertible elements of $\mathbb{Z}_K$ has the shape

$$\mathbb{U}_K = \{\pm\, \varepsilon(D)^n \,;\ n \in \mathbb{Z}\}.$$

The element $\varepsilon(D)$ is called the *fundamental unit* of $\mathbb{Z}_K$ and its logarithm $R(D) := \log \varepsilon(D)$ is called the *regulator*. The regulator $R(D)$ is a central object of algebraic number theory. For instance $R(D)$ plays a role in the computation of the class number (see (34)). The study of the properties of the unruly function $D \mapsto R(D)$ is a fascinating problem in both theoretical and computational aspects (see [Cohen 1993], for instance).

A rather similar but not completely equivalent problem — see the discussion in Section 5 — is the study of the fundamental solution ε_d to the so-called *Pell equation*

$$\text{PE}(d) \qquad\qquad T^2 - dU^2 = 1,$$

where the parameter d is a nonsquare positive integer and the unknown is the pair (T, U) of integers. It is convenient to write any given solution of PE(d) under the form $T + U\sqrt{d}$. Let ε_d be the least of these solutions greater than 1. Then the set of solutions of PE(d) is infinite and also has the shape $\{\pm\, \varepsilon_d^n \,;\ n \in \mathbb{Z}\}$.

It is known that there exists an absolute constant C such that the following inequalities hold

$$(2) \quad \sqrt{D} < \varepsilon(D) \leq \exp(C\sqrt{D}\log D) \quad \text{and} \quad 2\sqrt{d} < \varepsilon_d \leq \exp(C\sqrt{d}\log d).$$

It is widely believed that most of the time $\varepsilon(D)$ and ε_d are huge compared to the size of D or d, and this fact is confirmed by numerical evidence. One can find more precise conjectures ([Hooley 1984; Sarnak 1985], for instance) which would imply in particular that for all $\varepsilon > 0$ the inequality

$$(3) \qquad\qquad \varepsilon_d \geq \exp d^{(1/2)-\varepsilon},$$

holds for almost all nonsquare d (and for almost all fundamental discriminants D, since these D form a subset of positive density). Recall that a subset $\mathcal{A}$ of positive integers is said to have a *positive density* if its counting function satisfies the inequality

$$\liminf \frac{\#\{a \in \mathcal{A} \,;\; 1 \leq a \leq x\}}{x} > 0 \quad (x \to \infty).$$

The set $\mathcal{A}$ is said to be *negligible* (or *with zero density*) if one has

$$\limsup \frac{\#\{a \in \mathcal{A} \,;\; 1 \leq a \leq x\}}{x} = 0 \quad (x \to \infty).$$

Since a proof of (3) still seems to be out of reach, it is a challenging problem to construct infinite sequences of fundamental discriminants D (resp. of nonsquare d) with a huge $\varepsilon(D)$ (resp. with a huge ε_d). In the case of fundamental discriminants D, it is now proved that there exists $c > 1$ such that the inequality $\varepsilon(D) > \exp(\log^c D)$ is true for infinitely many D's; see, for example, [Yamamoto 1971; Reiter 1985; Halter-Koch 1989].

In the case of a nonsquare d the situation is better understood. Indeed we know that for some positive c there exists infinitely many d's such that $\varepsilon_d > \exp(d^c)$. We refer the reader to the pioneering work of Dirichlet [1856] leading to the optimality of (2), and to more recent work on the subject, for instance [Zagier 1981, pp. 74, 85; Fouvry and Jouve 2012, Theorem 2]. See also [Golubeva 1987] for the study of the case $d = 5p^2$. However none of these works manages to produce an infinite family of squarefree d's.

Besides, it is not known whether there exists a constant $c > 1$ such that the inequality $\varepsilon_d \geq \exp(\log^c d)$ holds for a positive density of d's. So we may ask for the frequency of weaker inequalities, such as $\varepsilon_d > d^\theta$ or $\varepsilon(D) > D^\theta$, where $\theta > \frac{1}{2}$ is a fixed constant. In that direction, Hooley [1984, Corollary] proved that for almost every d one has $\varepsilon_d > d^{(3/2)-\varepsilon}$. This was improved to $\varepsilon_d > d^{(7/4)-\varepsilon}$ by Fouvry and Jouve [2013, Corollary 1] ($\varepsilon > 0$ arbitrary).

The same work of Hooley implies that there exists a positive density of d satisfying $\varepsilon_d > d^{3/2}/\log d$. By a complete different technique based on the theory of continued fractions, Golubeva [2002, Theorem] constructed a set of d's of positive density such that $\varepsilon_d \geq d^{2-\varepsilon}$ ($\varepsilon > 0$ arbitrary). It does not seem to be an easy task to extend these two results to the case of a fundamental D because the condition for an integer to be squarefree seems hard to insert in the corresponding proofs of Hooley and Golubeva.

Our main result asserts that there is a positive density of positive fundamental discriminants D with fundamental unit of size essentially larger than D^3. In fact we can say more: first we show it is enough to consider the contribution of positive fundamental discriminants with fundamental unit of positive norm to get our density estimate. Moreover we can further restrict our study to positive fundamental discriminants D that satisfy a very specific divisibility property. This property is of an algebraic nature. To explain precisely what it is, we state the following proposition the first version of which goes back (at least) to Dirichlet (see the beginning of Section 3 for historical background and references).

If $D > 1$ is a fundamental discriminant set

$$D' = \begin{cases} D & \text{if } D \text{ is odd,} \\ D/2 & \text{if } D = 4d, d \equiv 3 \bmod 4, \\ D/4 & \text{if } 8 \mid D. \end{cases}$$

In other words D' is the *kernel* of D. Finally let Fund^+ denote the set of fundamental discriminants $D > 1$ such that $\varepsilon(D)$ has norm 1.

Proposition 1. *For every $D \in \text{Fund}^+$ there exists exactly two distinct positive divisors of D', both different from 1 and $D/(4, D)$, among the set of norms of principal ideals of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$.*

Let Φ be the function on Fund^+ sending D to the minimum of the two distinct divisors of D' the existence of which is guaranteed by Proposition 1. With notation as above our main result can be stated as follows.

Theorem 2. *For every $\delta > 0$ there exists $x_0(\delta) > 0$ and $c_0(\delta) > 0$ such that*

(4) $\#\{D \in \text{Fund}^+ ;\ X < D \leq 2X,\ 2^2 \| D,\ \Phi(D) < D^\delta,\ \varepsilon(D) \geq D^{3-\delta}\} \geq c_0(\delta)X,$

for every $X > x_0(\delta)$.

Similar statements are true when the condition $2^2 \| D$ in the set on the left-hand side is replaced by $8 \mid D$, or $D \equiv 1 \bmod 4$.

We shall mainly concentrate on the case $2^2 \| D$ since the situation is simplified a lot thanks to an easy link between units of $\mathbb{Q}(\sqrt{D})$ and the equation PE($d/4$) via the equality

(5) $$\varepsilon(D) = \varepsilon_{D/4}.$$

Proposition 1 can naturally be seen as a feature of the algebraic interpretation of the transformation of Legendre and Dirichlet we describe in Section 2.1. We devote Section 3 to the proof of this statement. The proof of (4) in Theorem 2 is given in Section 4. The cases $8 \mid D$ and D odd will be treated in Section 5.

The last part of the paper explains another application of the ideas leading to Theorem 2. It is well known that any information on the size of $\varepsilon(D)$ can be interpreted in terms of the ordinary class number $h(D)$ of the field $\mathbb{Q}(\sqrt{D})$. Among the various possible illustrations, we have selected the following one.

Theorem 3. *Let C_0 denote the converging Euler product*:

$$C_0 := \prod_{p \geq 3} \left(1 + \frac{p}{(p+1)^2(p-1)} \right).$$

There exists a constant $\delta > 0$ such that for every sufficiently large x one has the inequality

(6)
$$\sum_{\substack{D \leq x \\ 2^2 \| D}} h(D) \leq \left(\frac{8}{21\pi^2} C_0 - \delta \right) \frac{x^{3/2}}{\log x}.$$

The proof of this theorem is essentially based on [Fouvry and Jouve 2013] and Proposition 7. It will be given in Section 6 where we will explain why the inequality (6) is better than the trivial upper bound by some constant factor strictly larger than 3.5. We shall also use in a crucial way the fact that the set of D's with a large $\varepsilon(D)$ exhibited in Theorem 2 has some regularity. More precisely this set consists, up to a few exceptions, in integers of the form pm with p large (see (29) for the definition of $\mathscr{D}_m^\gamma(x)$). However the inequality (6) is certainly far from giving a crucial step towards the proof of the following expected asymptotic formula

$$\sum_{\substack{D \leq x \\ 2^2 \| D}} h(D) \sim c_0 x \log^2 x,$$

where x tends to infinity and c_0 is some absolute positive constant.

2. Preliminaries

2.1. *Legendre and Dirichlet's transformation.* In this subsection d denotes any positive integer, not necessarily a fundamental discriminant. We describe and use an easy transformation of the Pell equation PE(d) which was initiated by Legendre [Legendre 1830, Chapter VII, pp. 61–74] and then extended by Dirichlet [Dirichlet 1834, Section 1]. For the sake of completeness we give the detail of Legendre's argument. For a more detailed presentation together with historical background

and interpretations of this technique we refer to [Lemmermeyer 2003]. See also [Hooley 1984, p. 109; Cremona and Odoni 1989, pp. 18–19].

Let us write PE(d) under the form

$$(7) \qquad \frac{T^2 - 1}{d} = U^2.$$

Since $d \mid T^2 - 1$, we have $d = (T^2 - 1, d) = ((T + 1)(T - 1), d)$. Because the gcd of $T + 1$ and $T - 1$ can only take the values 1 or 2, we are led to consider the two corresponding cases:

- If $T + 1$ and $T - 1$ are coprime (i.e., T is even), we factorize

$$d = (T + 1, d)(T - 1, d) =: d_1 d_2,$$

in a unique way. Combining this splitting of d with (7) yields the four equations

$$T + 1 = d_1 U_1^2, \quad T - 1 = d_2 U_2^2, \quad d = d_1 d_2, \quad U = U_1 U_2,$$

which are equivalent to

$$(8) \quad d_1 U_1^2 - d_2 U_2^2 = 2, \quad T = -1 + d_1 U_1^2, \quad d = d_1 d_2, \quad U = U_1 U_2, \quad 2 \nmid d_1 U_1.$$

- If $2 = (T + 1, T - 1)$, two subcases are to be considered:

  - either $4 \nmid d$, in which case U is even and the Equation (7) can be written

$$\frac{((T + 1)/2) \cdot ((T - 1)/2)}{d} = (U/2)^2.$$

Arguing as in the previous case we are reduced to considering the following set of equations:

$$(9) \quad d_1 U_1^2 - d_2 U_2^2 = 1, \quad T = -1 + 2 d_1 U_1^2, \quad d = d_1 d_2, \quad U = 2 U_1 U_2, \quad 4 \nmid d,$$

  - or $4 \mid d$, in which case we can write (7) as follows:

$$\frac{((T + 1)/2) \cdot ((T - 1)/2)}{(d/4)} = U^2.$$

We factorize $d/4 = ((T + 1)/2, d/4)((T - 1)/2, d/4) =: d_1 d_2$ and get the set of equations

$$(10) \qquad d_1 U_1^2 - d_2 U_2^2 = 1, \quad T = -1 + 2 d_1 U_1^2, \quad d = 4 d_1 d_2, \quad U = U_1 U_2.$$

The following statement summarizes the above decomposition in a more concise and applicable way.

Lemma 4 (Legendre and Dirichlet). *Let $d, U \in \mathbb{N}_{\geq 1}$ be fixed integers. Set*

$$\mathcal{A}(d, U) := \{T \geq 1; \ T^2 - dU^2 = 1\}$$

and

• *if* $2 \nmid dU$:

$$\mathscr{B}(d, U) := \left\{ (d_1, d_2, U_1, U_2) \in \mathbb{N}_{\geq 1}^4 \; ; \; U_1 U_2 = U, \; d_1 d_2 = d, \; d_1 U_1^2 - d_2 U_2^2 = 2 \right\},$$

• *if* $2 \mid dU$ *and* $4 \nmid d$:

$$\mathscr{B}(d, U) := \left\{ (d_1, d_2, U_1, U_2) \in \mathbb{N}_{\geq 1}^4 \; ; \; 2U_1 U_2 = U, \; d_1 d_2 = d, \; d_1 U_1^2 - d_2 U_2^2 = 1 \right\},$$

• *if* $4 \mid d$:

$$\mathscr{B}(d, U) := \left\{ (d_1, d_2, U_1, U_2) \in \mathbb{N}_{\geq 1}^4 \; ; \; U_1 U_2 = U, \; 4d_1 d_2 = d, \; d_1 U_1^2 - d_2 U_2^2 = 1 \right\}.$$

Then in each case, we have

$$\#\mathscr{A}(d, U) = \#\mathscr{B}(d, U) \in \{0, 1\}.$$

Proof. We start with the obvious observation that $\#\mathscr{A}(d, U) \in \{0, 1\}$. We give the rest of the argument in detail only in the first case, the other two cases being exactly similar.

Next, $\#\mathscr{B}(d, U) \in \{0, 1\}$. To see this we fix (d_1, d_2, U_1, U_2) a quadruple in $\mathscr{B}(d, U)$ and we show that the values of d_1, U_1 are prescribed by those of d, U. We compute the square of $d_1 U_1^2 - 1 = d_2 U_2^2 + 1$: it is $(d_1 U_1^2 - 1)(d_2 U_2^2 + 1) = dU^2 + 1$. Thus $d_1 U_1^2 - 1$ is determined by d, U and so is the gcd $(d_1 U_1^2, d)$. We claim this gcd is d_1. Indeed $(d_1, d_2) = 1$ since these integers satisfy $d_1 U_1^2 - d_2 U_2^2 = 2$ and $2 \nmid dU$. Thus if $(d_1 U_1^2, d) \neq d_1$, there is a nontrivial common factor q to U_1 and d_2. Again using the equation satisfied by (d_1, d_2, U_1, U_2) we deduce $q = 2$, contradicting the condition $2 \nmid dU$.

To conclude the proof we observe that both the implications

$$(\#\mathscr{A}(d, U) = 1) \Rightarrow (\#\mathscr{B}(d, U) \geq 1) \quad \text{and} \quad (\#\mathscr{B}(d, U) = 1) \Rightarrow (\#\mathscr{A}(d, U) \geq 1)$$

hold. The first implication is just a way of rephrasing the reduction step explained before the statement of the lemma. To prove the second implication we notice that a quadruple (d_1, d_2, U_1, U_2) gives rise to an element $T := d_2 U_2^2 + 1 = d_1 U_1^2 - 1$ belonging to $\mathscr{A}(d, U)$. $\qquad\square$

2.2. Remarks on Lemma 4. The first remark concerns the implicit decomposition $(d, T, U) \mapsto (d_1, d_2, U_1, U_2)$ of Lemma 4, which should really be seen as a square rooting process. This explains the efficiency of the method as a tool to study the size of the solutions to the Pell equation PE(d). More precisely, a solution $T + U\sqrt{d}$ to PE(d) produces via Lemma 4 the algebraic integer $U_1\sqrt{d_1} + U_2\sqrt{d_2}$ which has degree at most 4 (and at least 2 when d is not a square) over $\mathbb{Q}$ and which satisfies

$$\left(U_1\sqrt{d_1} + U_2\sqrt{d_2} \right)^2 = d_1 U_1^2 + d_2 U_2^2 + 2U_1 U_2 \sqrt{d_1 d_2}.$$

If T is odd this is precisely $T + U\sqrt{d}$. If T is even this number is $2(T + U\sqrt{d})$. Therefore Lemma 4 enables us to significantly reduce the order of magnitude of the algebraic integers we work with.

The second remark concerns the special case where $d = p \equiv \pm 1 \bmod 4$. In that case the integer d can only be factored in two ways under the form $d = d_1 d_2$: either $(d_1, d_2) = (1, p)$ or $(d_1, d_2) = (p, 1)$. Hence the study of the equation $T^2 - pU^2 = 1$ is reduced to the four equations

$$U_1^2 - pU_2^2 = \begin{cases} \pm 2 & \text{if } 2 \nmid U, \\ \pm 1 & \text{if } 2 \mid U. \end{cases}$$

Since $U_2 \geq 1$ we deduce that $U_1 \geq \sqrt{p-2}$, and also that in every case one has the inequality $U \geq \sqrt{p-2}$. Hence any nontrivial solution $\Xi = T + U\sqrt{p}$ of the Pell equation $T^2 - pU^2 = 1$ satisfies the inequality

$$\Xi = \sqrt{pU^2 + 1} + U\sqrt{p} \geq \sqrt{p(p-2) + 1} + \sqrt{p(p-2)} \geq p.$$

This shows that the fundamental solution ε_p of PE(p) satisfies the inequality

(11) $$\varepsilon_p > p.$$

For $p \equiv 3 \bmod 4$ we deduce the lower bound

(12) $$\varepsilon(4p) > p,$$

for the fundamental unit of $\mathbb{Q}(\sqrt{4p})$. In the general case of the equation $T^2 - dU^2 = 1$, the corresponding fundamental solution is greater than $2\sqrt{d}$ and this bound is essentially best possible, as the choice $d = n^2 - 1$ shows.

As E. P. Golubeva pointed out to us, the lower bound (11), which is certainly already in the literature, can be deduced from properties of the continued fraction expansion of $\sqrt{p}$. For instance, by Perron [1913, Satz 14, p. 94] we know that if the nonsquare integer d is such that the period k of the expansion of $\sqrt{d}$ is even then it has the shape

$$\sqrt{d} = \left[b_0; \overline{b_1, \ldots, b_{v-1}, b_v, b_{v-1}, \ldots, b_1, 2b_0} \right],$$

where b_0 is the integral part of $\sqrt{d}$, the central coefficient b_v of index $v := k/2$ either equals b_0 or $b_0 - 1$ or is less than $(2/3)b_0$, and where any b_ℓ, $1 \leq \ell < v$, is less than $(2/3)b_0$. If d is divisible by some prime congruent to 3 mod 4 it is well known that the associated integer k is even. In the particular case where $d = p \equiv 3 \bmod 4$ we even know that $b_v = b_0$ or $b_0 - 1$ (see [Golubeva 1993, p. 1277]). Note that this last property is false if $d \equiv 3 \bmod 4$ is not a prime. Consider for instance $\sqrt{15} = [3; \overline{1, 6}]$.

Classical properties of continued fraction expansions of quadratic integers imply that if $\sqrt{d}$ has even period $k = 2v$, the fundamental solution $T_0 + U_0\sqrt{d}$ of PE(d)

satisfies

$$\frac{T_0}{U_0} = [b_0; b_1, \ldots, b_{\nu-1}, b_\nu, b_{\nu-1}, \ldots, b_1].$$

We deduce from the above discussion that in the case $d = p \equiv 3 \mod 4$ one has

$$U_0 \geq b_\nu \geq b_0 - 1 \geq \sqrt{p} - 2.$$

This gives (11).

3. Proof of Proposition 1

This result has been known for a long time. Dirichlet [1834, Section 5]) was the first to solve the question of the uniqueness of the decomposition $d = d_1 d_2$ (or $d = 4d_1 d_2$) appearing in (8), (9) and (10) but without, of course, using the language of modern algebraic number theory. We reprove this uniqueness result for squarefree d in passing in Section 3.1. For a statement using the language of binary quadratic forms see [Pall 1969], where the author notes that the result at issue essentially follows from a theorem due to Gauss (see the references in [Pall 1969]). For more on this subject we refer the reader to [Lemmermeyer 2003], in particular Theorem 3.3 there and the subsequent discussion. (The statement of that theorem contains a minor typo. One should allow the right-hand side of the equation to be negative since, e.g., the set of integral solutions (r, s) to each of the two equations $pr^2 - s^2 = 1$ and $pr^2 - s^2 = 2$ is empty if $p \equiv 7 \mod 8$.)

3.1. *Applying Gauss's theorem on the 2-rank of C_D.* Let $D \in \text{Fund}^+$. We denote
by Cl_D (resp. C_D) the group of ideal classes of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ in the ordinary (resp. narrow) sense. Let p_i, $1 \leq i \leq t$, be the pairwise distinct prime divisors of D. These primes are precisely the ones ramifying in $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$. For each $1 \leq i \leq t$, let $\mathfrak{p}_i$ be the prime ideal of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ above p_i. Let us define:

(13) $$M = \{\mathfrak{p}_1^{\delta_1} \cdots \mathfrak{p}_t^{\delta_t}; \delta_i \in \{0, 1\} \text{ for all } i\}.$$

It is exactly the set of integral ideals of norm dividing D'.

Let $\mathcal{S}$ be the subgroup of the group of fractional ideals of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ generated by the prime ideals $\mathfrak{p}_i$, $1 \leq i \leq t$. Of course M is a subset of $\mathcal{S}$. Moreover a well known result of Gauss (see, e.g., [Fröhlich and Taylor 1993, Chapter V, Theorem 39]) asserts that the narrow class map

$$\nu : \mathcal{S} \to C_D$$

induces a surjection

$$\mathcal{S}/\mathcal{S}^2 \to C_{D,2} := \{g \in C_D : g^2 = 1\},$$

whose kernel has order 2 and where $\mathscr{S}^2$ denotes the subgroup of squares of the abelian group $\mathscr{S}$.

One deduces that each class in $C_{D,2}$ has exactly two representatives in M. In particular, the image under the narrow class map of

$$P^+_{\mathbb{Q}(\sqrt{D})} :=$$

{fractional principal ideals of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ generated by a totally positive element},

which is the trivial class of $C_{D,2}$, has two representatives in M. These representatives are (1) and a nontrivial ideal $I \in M$. By definition of M the norm of I divides D'. Besides it is easily seen that the norm of I is not $D/(4, D)$. Indeed if by contradiction the norm of I were $D/(4, D)$ then the ideal I would be principal and equal to $(\sqrt{D/(4, D)})$, since $I \in M$. However $D \in \text{Fund}^+$ and $(\sqrt{D/(4, D)})$ is generated by an element of negative norm. Thus $(\sqrt{D/(4, D)})$ cannot be a representative of the trivial class of $C_{D,2}$.

It turns out the ideal I can be described explicitly thanks to the Legendre–Dirichlet transformation. To see this let us analyze each case separately.

(i) *Assume first that $D = 4d$, $d \equiv 3 \mod 4$. The fundamental unit of $\mathbb{Q}(\sqrt{D})$ may be written $\varepsilon(D) = T + U\sqrt{d}$. Applying the transformation described in Section 2.1 to the norm equation $T^2 - dU^2 = 1$ leads either to (8) or (9) depending on whether T is even or odd.*

- In case we are led to (8) (i.e., T is even) the integer $2d_1 > 1$ is a divisor of D' thus the ideal I is $(d_1U_1 + U_2\sqrt{d})$. Indeed the norm of the algebraic integer $d_1U_1 + U_2\sqrt{d}$ is $2d_1 > 0$ (note that $U_1\sqrt{d} + U_2d_2$ has norm $-2d_2 < 0$).

- Otherwise T is odd, hence U is even. Therefore, as explained in Section 2.2, $\varepsilon(D) = T + U\sqrt{d}$ is the square of the algebraic integer $U_1\sqrt{d_1} + U_2\sqrt{d_2}$. We deduce $d_1 > 1$ since otherwise this algebraic integer would be a unit (it would have norm 1) of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ contradicting the minimality of $\varepsilon(D)$. Thus one also has $I = (d_1U_1 + U_2\sqrt{d})$, the element $d_1U_1 + U_2\sqrt{d}$ having norm $d_1 > 0$.

(ii) *The second case we consider is $D \equiv 1 \mod 4$. For convenience and to unify the notation we set in that case $d := D$. We may write $\varepsilon(D) = T/2 + (U/2)\sqrt{d}$, where $T \equiv U \mod 2$. If T and U are both even we argue as in the previous case (note that by reducing modulo 4 we see that $T/2$ has to be odd). Otherwise T and U are both odd and satisfy $T^2 - dU^2 = 4$. Mimicking the transformation of Legendre and Dirichlet described in Section 2.1 (see also Lemma 9) one easily gets a set of equalities analogous to (8) and (9):*

$$(14) \qquad d_1U_1^2 - d_2U_2^2 = 4, \quad T = -2 + d_1U_1^2, \quad d = d_1d_2, \quad U = U_1U_2.$$

Therefore the integral principal ideal $(d_1U_1/2 + (U_2/2)\sqrt{d})$ (note that both d_1U_1

and U_2 are odd) is generated by an element of norm $d_1 > 0$. To see that this ideal is I it is enough to prove that $d_1 > 1$. Indeed if by contradiction $d_1 = 1$ then $(U_1/2)\sqrt{d_1} + (U_2/2)\sqrt{d_2}$ would be a unit of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ the square of which equals $\varepsilon(D)$ contradicting the minimality of the fundamental unit.

(iii) *Finally let us consider the case where $D = 4d$, $d \equiv 2 \bmod 4$.* As in the first case the fundamental unit may be written $\varepsilon(D) = T + U\sqrt{d}$. From the norm equation $T^2 - dU^2 = 1$ we deduce that T is odd and U is even; i.e., the transformation of Legendre and Dirichlet leads to (9). As in the first case one easily shows that $I = (d_1 U_1 + U_2\sqrt{d})$.

However what we want to understand is how (the narrow classes of) the elements of $P_{\mathbb{Q}(\sqrt{D})} := \{$ fractional principal ideals of $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}\} \supset P^+_{\mathbb{Q}(\sqrt{D})}$ are represented in M. It turns out (see [Fouvry and Klüners 2010a, (6)], for instance) that one has a short exact sequence

$$1 \to F_\infty \to C_D \to Cl_D \to 1,$$

where F_∞ has order at most 2. It is straightforward from the definitions that $|F_\infty| = [P_{\mathbb{Q}(\sqrt{D})} : P^+_{\mathbb{Q}(\sqrt{D})}]$. Moreover one knows that $|F_\infty| = 2$ if and only if $\varepsilon(D)$ has norm 1 (see the discussion following [Fouvry and Klüners 2010a, (6)] and the references therein). Since we have assumed $D \in \text{Fund}^+$ we have $[P_{\mathbb{Q}(\sqrt{D})} : P^+_{\mathbb{Q}(\sqrt{D})}] = 2$ and the above discussion then implies that $P_{\mathbb{Q}(\sqrt{D})}$ has four representatives in M. We can even argue in a completely explicit way: $P_{\mathbb{Q}(\sqrt{D})}$ is the disjoint union of two left cosets with respect to the subgroup $P^+_{\mathbb{Q}(\sqrt{D})}$. We have exhibited two elements ((1) and $I =: (a)$) in the coset $P^+_{\mathbb{Q}(\sqrt{D})}$. In the other coset obviously lies the ideal $(\sqrt{d})$: the algebraic integer $\sqrt{d}$ has norm $-d$ dividing D'. Using (a) and $(\sqrt{d})$ we easily deduce the construction of the fourth suitable ideal. Indeed in the decomposition of $(a\sqrt{d})$ as a product of prime ideals, the $\mathfrak{p}_i$'s are the only prime ideals that may appear. Reducing the exponent of each $\mathfrak{p}_i$ appearing modulo 2 we get a principal ideal (recall that $\mathfrak{p}_j^2 = (p_j)$ for each j) the norm of which divides D'. Clearly this ideal is different from (1), (a) and $(\sqrt{d})$. (We can deduce more: since both I and $(\sqrt{d})$ are elements of M and since d differs from D' by at most a factor 2 then either the norm $\tilde{d}$ of $I = (a)$ divides d and therefore the norm of the "fourth" ideal is $d/\tilde{d}$ or $\tilde{d}$ is even and the norm of the fourth ideal is $4d/\tilde{d}$.)

In terms of the Legendre–Dirichlet transformation and besides (1) and $I = (a)$ the ideals $(\sqrt{d})$ and $(U_1\sqrt{d} + d_2 U_2)$ (or $((U_1/2)\sqrt{d} + d_2 U_2/2)$ in the case $d = D \equiv 1 \bmod 4$) are representatives of $P_{\mathbb{Q}(\sqrt{D})}$ in M. Of these four integral principal ideals one has norm 1 and one has norm d. The norms of the other two are d_1 and d_2 (or $2d_1$ and $2d_2$ in the case where $D = 4d$, $d \equiv 3 \bmod 4$, and the coordinate T of the fundamental unit $\varepsilon(D) = T + U\sqrt{d}$ is even) respectively. This concludes the proof of Proposition 1.

3.2. Remarks on Proposition 1 and its proof. Among the constraints defining the sets on the left-hand side of (4) one may object that there is some redundancy in imposing both the conditions $D \in \mathrm{Fund}^+$ and $2^2 \| D$. However the norm of the fundamental unit is of course no longer automatically positive in the cases D odd or $8 \mid D$.

In view of the above proof of Proposition 1, we see that the integer $\Phi(D)$ can be given explicitly via the Legendre–Dirichlet transformation. Indeed we deduce from the proof the following explicit version of Proposition 1.

Proposition 5. *Let $D \in \mathrm{Fund}^+$ and $d := D/(4, D)$. Let $d = d_1 d_2$ be the coprime factorization of d obtained by applying (8), (9) or (14) to the norm equation satisfied by the fundamental unit $\varepsilon(D)$. Then*

$$
\Phi(D) = \begin{cases} \min(2d_1, 2d_2) & \text{if } D = 4d, \ d \equiv 3 \bmod 4, \ T \equiv 0 \bmod 2, \\ \min(d_1, d_2) & \text{otherwise,} \end{cases}
$$

where in the first case $\varepsilon(D) = T + U\sqrt{d}$.

As a consequence one deduces $\Phi(D) < \sqrt{d}$ unless $D = 4d$, $d \equiv 3 \bmod 4$ and the coordinate T of the fundamental unit $\varepsilon(D) = T + U\sqrt{d}$ is even. In the latter case one can only infer $\Phi(D) < \sqrt{D}$.

Example 6. Assuming $D \in \mathrm{Fund}^+$ one might get the intuitive idea that among the four integral principal ideals of norm dividing D', the ideal $(\sqrt{d})$ is the one with norm of maximal absolute value. Of course this is true if the norms of the four ideals in question divide d which is always the case unless $D = 4d$, $d \equiv 3 \pmod 4$, and $\varepsilon(D) = T + U\sqrt{d}$ with T even. However this intuitive idea is not necessarily true in the latter situation. Consider the case $D = 12$. Thus $D' = 6$ and $d = 3$. If $\mathscr{N}$ denotes the norm map relative to the extension $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, one easily checks that

$$
\mathscr{N}(\sqrt{3}) = -3, \quad \mathscr{N}(1 + \sqrt{3}) = -2, \quad \mathscr{N}(3 + \sqrt{3}) = 6.
$$

In the notation of the Legendre–Dirichlet transformation the maximum of the absolute values of the three norms above is $2d_1 = 6$. Moreover $\Phi(12) = 2$ and one notices as expected the identity among ideals:

$$
(\sqrt{3}) \cdot (3 + \sqrt{3}) = (3) \cdot (1 + \sqrt{3}),
$$

which is congruent to $(1 + \sqrt{3})$ modulo squares (i.e., modulo $\mathscr{S}^2$ in the notation of the proof of Proposition 1).

This example contains even more information. Not only does it show that d is not in general the maximum of the four divisors of D' among the norms of integral principal ideals, but also that at most one of the other three divisors is larger than d. Otherwise we would have $2d_1 \geq d$ and $2d_2 \geq d$, by virtue of Proposition 5. Since

$d = d_1 d_2 \equiv 3 \bmod 4$ this implies $d = 3$. This corresponds to $D = 12$, in which case $d_2 = 1$, as shown above.

4. Proof of Theorem 2 when $2^2 \| D$

4.1. *Notation.* The letter p is reserved for prime numbers. The Möbius function is denoted by μ, the number of distinct prime divisors of the integer n is $\omega(n)$, the cardinality of the set of primes $p \leq x$ which are congruent to $a \bmod q$ is denoted by $\pi(x; q, a)$. The condition $n \sim N$ means that the variable n has to satisfy the inequalities $N < n \leq 2N$. As it shall not lead to confusion the symbol $\sim$ will also be used in the usual sense: if f, g are two functions of the real variable x defined on a neighborhood of a on which g does not vanish, $f(x) \sim g(x)$ as $x \to a$ means that f/g approaches 1 as $x \to a$.

4.2. *The basic splitting.* Let D be a fundamental discriminant such that $2^2 \| D$. Hence $d := D/4$ is squarefree and congruent to 3 mod 4. In that particular case (1) simplifies into $\mathbb{Z}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. As already mentioned both the facts that $D \in \mathrm{Fund}^+$ and that D is divisible by some $p \equiv 3 \bmod 4$ imply that there is no unit with norm -1. Hence $T + U\sqrt{d}$ belongs to $\mathbb{U}_K$ if and only if $T^2 - dU^2 = 1$, i.e., (5) holds.

We construct a sequence of fundamental discriminants $D = 4d$ with a large $\varepsilon(D) = \varepsilon_d$ by starting from

$$d = pm,$$

where $p \equiv 3 \bmod 4$ and $m \equiv 1 \bmod 4$ is squarefree. We keep in mind that m is small compared to p, hence m is coprime with p.

For any squarefree integer m and any $x \geq 2$ let

$$(15) \qquad \mathscr{D}_m(x) := \{pm \; ; \; pm \sim x, \; p \geq 7, \; p \equiv 3 \bmod 4\}.$$

Dirichlet's Theorem on primes in arithmetic progressions directly implies

$$(16) \qquad \#\mathscr{D}_m(x) \sim \frac{x}{2m \log(x/m)},$$

as $x \to \infty$ uniformly for $m \leq \sqrt{x}$. We now introduce the following subset of $\mathscr{D}_m(x)$ consisting of elements pm with a small ε_{pm}: for $\delta = \delta(x) > 0$, we consider

$$\mathscr{D}_m(x, \delta) := \{pm \; ; \; pm \in \mathscr{D}_m(x), \, \varepsilon_{pm} \leq (4pm)^{3-\delta}\}.$$

By counting solutions that may not be fundamental, we have the inequality

$$(17) \quad \#\mathscr{D}_m(x, \delta) \leq \# \big\{(p, T, U) \; ; \; T, \, U \geq 1, \; pm \in \mathscr{D}_m(x), \; T^2 - pmU^2 = 1,$$
$$T + U\sqrt{pm} \leq (4pm)^{3-\delta}\big\}.$$

We now want to apply Lemma 4 with the choice $d = pm$, where m satisfies

(18) $$2 \nmid m \text{ and } \mu^2(m) = 1.$$

Let $m_1 m_2 = m$ be a decomposition of m. For

(19) $$\eta \in \{\pm 1, \pm 2\}.$$

we consider the equation

$$E(m_1, m_2, \eta) \qquad m_1 U_1^2 - pm_2 U_2^2 = \eta.$$

By (17) and using the values of T appearing in (8) & (9) we get the inequality

(20) $\#\mathcal{D}_m(x, \delta)$
$$\leq \sum_{m_1 m_2 = m} \sum_{\eta = \pm 1} \# \left\{ (p, U_1, U_2) \, ; \; pm \in \mathcal{D}_m(x), \, m_1 U_1^2 - pm_2 U_2^2 = \eta, \right.$$
$$\left. -1 + 2m_1 U_1^2 + 2U_1 U_2 \sqrt{pm} \leq (4pm)^{3-\delta} \right\}$$
$$+ \sum_{m_1 m_2 = m} \sum_{\eta = \pm 2} \# \left\{ (p, U_1, U_2) \, ; \; pm \in \mathcal{D}_m(x), \, m_1 U_1^2 - pm_2 U_2^2 = \eta, \right.$$
$$\left. -1 + m_1 U_1^2 + U_1 U_2 \sqrt{pm} \leq (4pm)^{3-\delta} \right\}.$$

We now want to simplify the above inequality by studying the orders of magnitude of the variables U_1 and U_2. The equation $E(m_1, m_2, \eta)$ and the assumption $p \geq 7$ in (15) imply that we have

$$\tfrac{1}{2} m_1 U_1^2 \leq pm_2 U_2^2 \leq 2m_1 U_1^2.$$

Multiplying these inequalities by m_1 and using the assumption $pm \sim x$ we obtain:

(21) $$\tfrac{1}{2} m_1 U_1 x^{-1/2} \leq U_2 \leq 2m_1 U_1 x^{-1/2}.$$

From the inequalities defining the sets in the right-hand side of (20) we deduce

$$U_1 U_2 \sqrt{pm} \leq 64 \, (pm)^{3-\delta},$$

which implies in turn

(22) $$U_1 U_2 \leq 400 \, x^{(5/2)-\delta}.$$

Also note that (21) and (22) imply the inequalities

(23) $$U_2 \leq 30 \, m_1^{1/2} x^{1-(\delta/2)} \quad \text{and} \quad U_1 \leq 2m_1^{-1} x^{1/2} U_2.$$

Now we drop the condition that p is prime in (20). We deduce the inequality

(24) $$\#\mathcal{D}_m(x, \delta) \leq \sum_{m_1 m_2 = m} \sum_{\eta = \pm 1, \pm 2} F(m_1, m_2, \eta).$$

Here $F(m_1, m_2, \eta)$ is the number of solutions to the congruence

(25) $$m_1 U_1^2 \equiv \eta \bmod m_2 U_2^2,$$

where (U_1, U_2) is subject to (23). Let $\rho_{\eta, m_1}(t)$ be the number of solutions to the congruence

$$m_1 u^2 - \eta \equiv 0 \bmod t,$$

where η satisfies (19) and m_1 is odd. The study of the function $\rho_{\eta, m_1}(t)$ is classically reduced to the study of $\rho_{\eta, m_1}(p^k)$. Since we always have $(m_1, \eta) = 1$ in every case one has $\rho_{\eta, m_1}(2^k) \leq 4$ and $\rho_{\eta, m_1}(p^k) \leq 2$ ($k \geq 1$ and $p \geq 3$). This leads to the inequality

$$(26) \qquad \rho_{\eta, m_1}(t) \leq 2 \cdot 2^{\omega(t)} \text{ for any } t \geq 1.$$

Looking back at (24) we split the interval of variation of U_1 into intervals of length $m_2 U_2^2$ together with perhaps an incomplete one. Inserting (26) and noting that η can take four distinct values we obtain the inequality

$$(27) \qquad \#\mathcal{D}_m(x, \delta) \leq 8 \sum_{m_1 m_2 = m} \sum_{U_2 \leq 30 \, m_1^{1/2} x^{1-\delta/2}} 2^{\omega(m_2 U_2)} \left(2 \frac{x^{1/2}}{m_1 m_2 U_2} + 1 \right)$$

$$\leq 16 \frac{x^{1/2}}{m} \Sigma_1 + 8 \Sigma_2,$$

with

$$\Sigma_1 := \sum_{m_1 m_2 = m} 2^{\omega(m_2)} \sum_{U_2 \leq 30 \, m_1^{1/2} x^{1-\delta/2}} \frac{2^{\omega(U_2)}}{U_2},$$

and

$$\Sigma_2 := \sum_{m_1 m_2 = m} 2^{\omega(m_2)} \sum_{U_2 \leq 30 \, m_1^{1/2} x^{1-\delta/2}} 2^{\omega(U_2)}.$$

It remains to apply techniques for summing multiplicative functions (recall that m is squarefree). We obtain

$$\Sigma_1 \ll \sum_{m_1 m_2 = m} 2^{\omega(m_2)} \log^2 x \ll 3^{\omega(m)} \log^2 x,$$

and

$$\Sigma_2 \ll x^{1-\delta/2} \log x \sum_{m_1 m_2 = m} 2^{\omega(m_2)} m_1^{1/2} = (x^{1-\delta/2} \log x) m^{1/2} \sum_{m_2 \mid m} \frac{2^{\omega(m_2)}}{\sqrt{m_2}},$$

$$\ll_\kappa \kappa^{\omega(m)} m^{1/2} x^{1-\delta/2} \log x,$$

for any fixed $\kappa > 1$. Putting everything together via (27) we have finally proved:

Proposition 7. *For every $\kappa > 1$ there exists $c(\kappa) > 0$ such that the inequality*

$$(28) \qquad \#\mathcal{D}_m(x, \delta) \leq c(\kappa)(3^{\omega(m)} m^{-1} x^{1/2} \log^2 x + \kappa^{\omega(m)} m^{1/2} x^{1-\delta/2} \log x),$$

holds for every $x \geq 2$, for every odd squarefree $m \leq \sqrt{x}$ and for every $\delta = \delta(x) \geq 0$.

Applying this proposition with $m = 1$ one instantly deduces:

Corollary 8. *Let $t \mapsto \psi(t)$ be any increasing function of the variable $t \geq 1$, approaching infinity as $t \to \infty$. Then as x tends to infinity one has*

$$\# \{ p \leq x \, ; \; p \equiv 3 \bmod 4, \; \varepsilon(4p) \leq p^3 / (\psi(p) \log^4 p) \} = o(x/(\log x)).$$

In other words, this corollary tells us that for almost every $p \equiv 3 \bmod 4$, the regulator $R(4p)$ of the field $\mathbb{Q}(\sqrt{4p})$ is greater than $(3 - \varepsilon) \log p$ (where $\varepsilon > 0$ is arbitrary). However Corollary 8 is not new: it is slightly weaker by a power of $\log p$ than [Golubeva 1993, Corollary 5] which was obtained by Golubeva via the theory of continued fractions. In the statement of Corollary 8 it is possible to make the power of $\log p$ decrease. It requires a better control of the function $\rho_{\eta,1}(p)$ which can be achieved by appealing to oscillations of some Legendre symbol. One essentially deduces the fact that this ρ-function has mean value 1 as long as $\eta \neq 1$. Actually, requiring that $T + U \sqrt{p}$ be a fundamental solution to PE(p) is enough to reduce to this case.

4.3. *End of the proof of the lower bound in Theorem 2.* Let γ be a constant satisfying $0 \leq \gamma \leq \frac{1}{2}$. Let

$$(29) \qquad \mathcal{D}^\gamma(x) := \bigcup_m \mathcal{D}_m(x),$$

where the union is taken over the integers m satisfying

$$(30) \qquad 1 \leq m \leq x^\gamma, \quad \mu^2(m) = 1 \text{ and } m \equiv 1 \bmod 4.$$

Since the sets $\mathcal{D}_m(x)$ are pairwise disjoint (when m runs over the set of integers satisfying (30)) we have the equality

$$\# \mathcal{D}^\gamma(x) = \sum_{m \text{ satisfies } (30)} \# \mathcal{D}_m(x).$$

Inserting (16), summing over m, and using the formula

$$\sum_{\substack{m \leq y \\ m \equiv 1 \bmod 4}} \mu^2(m) \sim \frac{2}{\pi^2} y \; (y \to \infty),$$

we deduce that for every $\gamma_0 > 0$ and for $x \to \infty$, one has

$$(31) \qquad \# \mathcal{D}^\gamma(x) \sim -\frac{\log(1 - \gamma)}{\pi^2} x,$$

uniformly for $\gamma_0 \leq \gamma \leq \frac{1}{2}$.

Now we apply Proposition 7 and (31) with the choice $\gamma = \delta/4$. Consider

$$\mathscr{E}(x, \delta) := \bigcup_m (\mathscr{D}_m(x) \setminus \mathscr{D}_m(x, \delta)),$$

where the union is taken over the indices m satisfying (30). Every element $pm \in \mathscr{E}(x, \delta)$ is squarefree and congruent to 3 mod 4. Hence $D := 4pm$ is a fundamental discriminant and it satisfies the inequality $\varepsilon_d = \varepsilon(D) \geq D^{3-\delta}$ and the inequality $D \leq 8x$. Furthermore, because the sets $\mathscr{D}_m(x)$ appearing in the definition of $\mathscr{E}(x, \delta)$ are pairwise disjoint, one trivially has:

$$\mathscr{E}(x, \delta) = \mathscr{D}^\gamma(x) \setminus \left(\bigcup_m \mathscr{D}_m(x, \delta) \right),$$

where the union appearing on the right-hand side is a disjoint union. Therefore,

$$\#\mathscr{E}(x, \delta) \geq -\frac{(1 - o(1)) \log(1 - \delta/4)}{\pi^2} \cdot x - O\left(x^{1-\delta/2} \log x \sum_{m \leq x^{\delta/4}} (3/2)^{\omega(m)} m^{1/2} \right)$$

$$\geq -\frac{(1 - o(1)) \log(1 - \delta/4)}{\pi^2} \cdot x.$$

This gives the first case of Theorem 2. Indeed the argument so far has only involved splittings of positive fundamental discriminants D of type $D/4 = d_1 d_2$ with $d_1 = m_1$ and $d_2 = pm_2$ (see (20)). Since $m = m_1 m_2$ is a divisor of D of very small size (see (30)) the condition on $\Phi(D)$ on the left-hand side of (4) is automatically fulfilled for the particular D's under consideration in view of Proposition 1 or rather its explicit version Proposition 5.

4.4. *Comments on the proof of Proposition 7.* To obtain the inequality (24) we have dropped the condition p prime. By sieve techniques it is possible to handle this constraint. The upshot of this would consist in saving a power of $\log x$ in the first term of the right-hand side of (28). This improvement does not seem to affect the exponent $3 - \delta$ in the statement of (4).

A more promising way to improve this exponent is to apply a better treatment of the congruence (25) in small intervals. After a classical expansion via Fourier techniques we would be led to bound the general exponential sum

$$\sum_{m_1 m_2 = m} \sum_{U_2 \leq 30\, m^{1/2} x^{1-\delta/2}} \sum_{\substack{U_1 \bmod m_2 U_2^2 \\ m_1 U_1^2 \equiv \eta \bmod m_2 U_2^2}} \sum_{\substack{1 \leq |h| \leq \\ m_1 m_2 x^{-1/2} U_2^{1+\varepsilon}}} \exp\left(2\pi \iota h \frac{U_1}{m_2 U_2^2} \right).$$

5. Proof of the remaining cases

5.1. *The case D divisible by 8.* In that case set $d := D/4$. We still have

$$K := \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d}) \quad \text{and} \quad \mathbb{Z}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}.$$

However, contrary to the case $2^2 \| D$, the fact that $D \in \text{Fund}^+$ is no longer guaranteed which means that the negative Pell equation $T^2 - dU^2 = -1$ may be solvable.

Since we are only dealing with discriminants in Fund^+ we are led to modify (15):

$$\mathcal{D}_m(x) := \{2pm \; ; \; 2pm \sim x, \; p \equiv 3 \bmod 4\},$$

hence $d \in \mathcal{D}_m(x)$ implies $D \in \text{Fund}^+$. We shall consider these sets for m squarefree and congruent to 1 mod 4. The proof of Theorem 2 is essentially the same in this case.

5.2. *The case D odd.* In that case D is squarefree and congruent to 1 mod 4, write $d := D$. Then $K = \mathbb{Q}(\sqrt{D})$ and $\mathbb{Z}_K = \{(a + b\sqrt{d})/2 \; ; \; a, b \in \mathbb{Z}, \; a \equiv b \bmod 2\}$. Hence the study of the fundamental unit of K is reduced to the question of finding the smallest nontrivial solution to the equation

$$T^2 - dU^2 = \pm 4.$$

As above we can ensure the equation $T^2 - dU^2 = -4$ has no integral solution (thus $D \in \text{Fund}^+$) by imposing d to be divisible by some $p \equiv 3 \bmod 4$. To deal with the equation $T^2 - dU^2 = 4$ we appeal to a variant of Lemma 4 that we state without proof.

Lemma 9. *Let d and U be positive integers such that $2 \nmid d$. Define $\mathcal{A}(d, U)$ as in Lemma 4. Set*

$$\tilde{\mathcal{A}}(d, U) := \{T \geq 1 \; ; \; T^2 - dU^2 = 4\},$$
$$\tilde{\mathcal{B}}(d, U) := \big\{(d_1, d_2, U_1, U_2) \in \mathbb{N}_{\geq 1}^4 \; ; \; U_1 U_2 = U, \; d_1 d_2 = d, \; d_1 U_1^2 - d_2 U_2^2 = 4\big\}.$$

Then we have

(32) $\qquad\qquad\qquad \tilde{\mathcal{A}}(d, U) = 2 \cdot \mathcal{A}(d, U/2) \qquad$ *if $2 | U$,*

(33) $\qquad\qquad\qquad \# \tilde{\mathcal{A}}(d, U) = \# \tilde{\mathcal{B}}(d, U) \in \{0, 1\} \quad$ *if $2 \nmid U$.*

We are led to modify (15) in the following way:

$$\mathcal{D}_m(x) := \{pm \; ; \; pm \sim x, \; p \equiv 3 \bmod 4\}.$$

We shall consider these sets for m squarefree and congruent to 3 mod 4. Thanks to Lemma 9 the proof of Theorem 2 in this last case is once more essentially the same.

The proof of Theorem 2 is now complete.

Remark 10. The "algebraic interpretation" provided by Proposition 1 and translated by the condition on the function Φ in (4) relies heavily on the assumption that for the D's under consideration the fundamental unit $\varepsilon(D)$ has norm 1 (see Section 3). If $\varepsilon(D)$ has norm -1 then $d = D/(4, D)$ is the norm of the algebraic integer $\varepsilon(D)\sqrt{d}$. Gauss's theorem on the 2-rank of C_D still applies and shows that the only two

divisors of D' among norms of integral principal ideals generated by totally positive elements are 1 and d. Recall that if $\varepsilon(D)$ has norm -1 then the groups $P_{\mathbb{Q}(\sqrt{D})}$ and $P_{\mathbb{Q}(\sqrt{D})}^{+}$ coincide.

Remark 11. One may wonder why neglecting the contribution of positive fundamental discriminants with fundamental unit of negative norm has such little influence on the difficulty of showing the lower bound (4). This comes from the fact that the set of fundamental discriminants with fundamental unit of norm -1 is negligible. More precisely the number of *special discriminants* (i.e., positive fundamental discriminants only divisible by 2 or primes congruent to 1 modulo 4) up to X is asymptotic to $c \cdot X (\log X)^{-1/2}$, where c is an absolute constant (see [Fouvry and Klüners 2010a, Section 1] and the references therein).

6. Proof of Theorem 3

Our starting point is the following well known *class number formula* (see [Cohen 1993, Proposition 5.6.9, p. 262], for instance)

$$(34) \qquad h(D) = \frac{L(1, \chi_D)}{2 R(D)} \sqrt{D},$$

where D is a positive fundamental discriminant and $L(s, \chi_D)$ is the Dirichlet L-function associated to the Kronecker symbol $\chi_D = (D/\cdot)$

$$L(s, \chi_D) := \sum_{n=1}^{\infty} \chi_D(n) \, n^{-s} \ (\Re s > 1).$$

Recall the classical upper bound

$$(35) \qquad L(1, \chi) \ll \log(q + 1),$$

which holds for any nonprincipal Dirichlet character χ modulo $q > 1$. To prove Theorem 3 we have to study the sum

$$\Sigma(x) := \sum_{\substack{D \leq x \\ 2^2 \| D}} h(D),$$

and prove the inequality

$$(36) \qquad \Sigma(x) \leq \left(\frac{8}{21\pi^2} C_0 - \delta \right) \frac{x^{3/2}}{\log x},$$

for sufficiently large x. Define the two positive valued functions

$$\kappa(D) := R(D)/\log D, \quad \xi(D) := L(1, \chi_D)\sqrt{D}$$

and

$$(37) \qquad \tilde{\Sigma}(x) := \sum_{\substack{D \leq x \\ 2^2 \| D}} \frac{\xi(D)}{\kappa(D)}.$$

By (34) and by partial summation, we see that (36) can be deduced from the inequality

$$(38) \qquad \tilde{\Sigma}(x) \leq 2 \left(\frac{8}{21\pi^2} C_0 - 2\delta \right) x^{3/2},$$

for sufficiently large x.

Let γ, η and η' be small positive numbers and let $\mathscr{E}(x)$ be the set of indices over which the summation (37) is performed. We write any $D \in \mathscr{E}(x)$ under the form $D = 4d$. Hence $D \in \mathscr{E}(x)$ if and only if $d \in \mathscr{F}(x)$ where

$$(39) \qquad \mathscr{F}(x) := \left\{ d \, ; \, \mu^2(d) = 1, \ d \equiv 3 \bmod 4 \text{ and } d \leq x/4 \right\}.$$

We now consider two disjoint subsets of $\mathscr{F}(x)$ defined as follows:

$$\mathscr{F}_1(x) := \left\{ d \in \mathscr{F}(x) \, ; \, \kappa(4d) \leq \tfrac{7}{4} - \eta' \right\},$$
$$\mathscr{F}_2(x) := \left\{ d \in \mathscr{F}(x) \, ; \, \kappa(4d) > \tfrac{7}{4} - \eta', \right.$$
$$\left. d = pm, \ pm \sim x/8, \ p \equiv 3 \bmod 4, m \equiv 1 \bmod 4, m \leq x^\gamma \right\}.$$

We denote by $\mathscr{G}(x)$ the complement of $\mathscr{F}_1(x) \cup \mathscr{F}_2(x)$ in $\mathscr{F}(x)$. Let us then use the condition $\kappa(4d) \leq (7/4) + \eta$ to split further $\mathscr{F}_2(x)$ into the partition $\mathscr{F}_2^+(x) \cup \mathscr{F}_2^-(x)$ where:

$$\mathscr{F}_2^-(x) := \left\{ d \in \mathscr{F}_2(x) \, ; \, \kappa(4d) \leq \tfrac{7}{4} + \eta \right\},$$
$$\mathscr{F}_2^+(x) := \left\{ d \in \mathscr{F}_2(x) \, ; \, \kappa(4d) > \tfrac{7}{4} + \eta \right\}.$$

Using this decomposition we split the sum $\tilde{\Sigma}(x)$ accordingly:

$$(40) \qquad \tilde{\Sigma}(x) = \sigma_{\mathscr{F}_1}(x) + \sigma_{\mathscr{F}_2^-}(x) + \sigma_{\mathscr{F}_2^+}(x) + \sigma_{\mathscr{G}}(x),$$

where each term on the right-hand side is a sum over the corresponding obvious subset of $\mathscr{F}(x)$ we have just defined. To upper bound $\sigma_{\mathscr{F}_1}(x)$ we use [Fouvry and Jouve 2013, Theorem 1] which asserts that for any $\varepsilon > 0$ one has

$$\#\left\{ (D, \varepsilon_D); D \text{ nonsquare} , \ 2 \leq D \leq x, \ \varepsilon_D \leq D^{(1/2)+\alpha} \right\} = O_\varepsilon(x^{(\alpha/3)+(7/12)+\varepsilon}),$$

uniformly for $\alpha \geq 0$ and $x \geq 2$. Together with (5) the above formula (with the choices $\varepsilon = \eta'/12$ and $\alpha = 5/4 - \eta'$) implies:

$$\#\mathscr{F}_1(x) \ll_\gamma x^{1-\eta'/4}.$$

Hence by the inequality $\kappa(4d) \geq 1/2$ (see (2)) and by (35), we deduce the inequality

$$(41) \qquad \sigma_{\mathscr{F}_1}(x) \ll x^{(3/2)-(\eta'/4)} \log x.$$

By (28), we also know that

$$\# \mathscr{F}_2^-(x) \ll x^{1-\eta/10},$$

with the choice $\gamma = \eta/10$. As for the proof of (41) we deduce that

$$(42) \qquad \sigma_{\mathscr{F}_2^-}(x) \ll x^{(3/2)-(\eta/10)} \log x.$$

Next note the following easy inequality, consequence of the definitions of the sets $\mathscr{F}_2^+(x)$, $\mathscr{F}_2^-(x)$ and $\mathscr{G}(x)$:

$$\sigma_{\mathscr{F}_2^+}(x) + \sigma_{\mathscr{G}}(x) \leq \frac{1}{7/4+\eta} \sum_{d\in\mathscr{F}_2^+(x)} \xi(4d) + \frac{1}{7/4-\eta'} \sum_{d\in\mathscr{G}(x)} \xi(4d).$$

Set

$$(43) \quad \tilde{\mathscr{F}}_2(x) := \big\{ d\,;\; d = pm,\; \mu^2(d) = 1,\; pm \sim x/8,\; m \leq x^\gamma,$$
$$p \equiv 3 \bmod 4, m \equiv 1 \bmod 4 \big\}.$$

From the inclusion $\mathscr{F}_1(x) \cup \mathscr{F}_2(x) \supset \tilde{\mathscr{F}}_2(x)$ one deduces

$$\sum_{d\in\mathscr{F}_1(x)\cup\mathscr{F}_2(x)} \xi(4d) \geq \sum_{d\in\tilde{\mathscr{F}}_2(x)} \xi(4d).$$

Combining the last two inequalities with the following obvious facts:

$$\sum_{d\in\mathscr{G}(x)} \xi(4d) = \sum_{d\in\mathscr{F}(x)} \xi(4d) - \sum_{d\in\mathscr{F}_1(x)\cup\mathscr{F}_2(x)} \xi(4d), \qquad \sum_{d\in\mathscr{F}_2^+(x)} \xi(4d) \leq \sum_{d\in\tilde{\mathscr{F}}_2(x)} \xi(4d)$$

we deduce the inequality
$$(44)$$
$$\sigma_{\mathscr{F}_2^+}(x) + \sigma_{\mathscr{G}}(x) \leq \frac{1}{7/4-\eta'} \sum_{d\in\mathscr{F}(x)} \xi(4d) - \frac{\eta+\eta'}{(7/4+\eta)(7/4-\eta')} \sum_{d\in\tilde{\mathscr{F}}_2(x)} \xi(4d).$$

It remains to evaluate each of the two sums in (44). To that end we state and prove two lemmas, the most classical of which is the following:

Lemma 12. *As $y \to \infty$, one has*

$$\sum_{\substack{d\leq y \\ d\equiv 3 \bmod 4}} \mu^2(d) L(1, \chi_{4d}) \sqrt{d} \sim \frac{4C_0}{3\pi^2} y^{3/2}.$$

Proof. Let $A_1(y)$ be the sum we want to evaluate. By the properties of the Kronecker symbol we have the equality

$$A_1(y) = \sum_{\substack{d \leq y \\ d \equiv 3 \bmod 4}} \mu^2(d)\sqrt{d} \sum_{n \geq 1,\, 2 \nmid n} \frac{(d/n)}{n},$$

that now involves a Jacobi symbol. By the fact that the sum over n varying in any interval of length $4d$ of the symbols $(4d/n)$ equals zero, we can express using partial summation the above infinite series as a finite sum with a small enough error term:

$$\sum_{\substack{n \geq 1 \\ 2 \nmid n}} \frac{(d/n)}{n} = \sum_{\substack{1 \leq n \leq y^2 \\ 2 \nmid n}} \frac{(d/n)}{n} + O(y^{-1}),$$

uniformly for $d \leq y$. Inserting this equality in the definition of $A_1(y)$ and splitting the sum according to whether n is a square or not, we get the equality

$$(45) \qquad A_1(y) = \mathrm{MT}_1(y) + \mathrm{Err}_1(y) + O(y^{1/2}).$$

In the above equality the sum $\mathrm{MT}_1(y)$ which will appear as the main term is the following

$$(46) \qquad \mathrm{MT}_1(y) := \sum_{\substack{d \leq y \\ d \equiv 3 \bmod 4}} \sum_{\substack{1 \leq t \leq y \\ (t, 2d) = 1}} \mu^2(d) \frac{\sqrt{d}}{t^2},$$

whereas $\mathrm{Err}_1(y)$ is defined by

$$(47) \qquad \mathrm{Err}_1(y) := \sum_{\substack{d \leq y \\ d \equiv 3 \bmod 4}} \sum_{\substack{1 \leq n \leq y^2 \\ 2 \nmid n,\, n \neq \square}} \mu^2(d) \frac{\sqrt{d}}{n} \left(\frac{d}{n}\right).$$

We first consider $\mathrm{Err}_1(y)$. We want to prove that it behaves as an error term. More precisely we want to show:

$$(48) \qquad \mathrm{Err}_1(y) = o(y^{3/2}) \quad (y \to \infty).$$

To do so we split the double sum in (47) in $O(\log^2 y)$ subsums $\mathrm{Err}_1(D, N)$ where the sizes of d and n are controlled:

$$(49) \qquad \mathrm{Err}_1(D, N) := \sum_{\substack{d \sim D \\ d \equiv 3 \bmod 4}} \sum_{\substack{n \sim N \\ 2 \nmid n,\, n \neq \square}} \mu^2(d) \frac{\sqrt{d}}{n} \left(\frac{d}{n}\right),$$

with $D \le y/2$ and $N \le y^2/2$. Our purpose is to prove that in all these cases we have

$$\text{(50)} \qquad \text{Err}_1(D, N) = O(y^{3/2} \log^{-3} y).$$

Of course the trivial bound is $\text{Err}_1(D, N) \ll D^{3/2}$. Hence (50) is proved for any (D, N) such that $D \le y \log^{-2} y$. Thus for the rest of the proof we suppose that

$$\text{(51)} \qquad D > y \log^{-2} y.$$

The sum $\text{Err}_1(y)$ is a particular case of a double sum of Jacobi or Kronecker symbols, which is nowadays quite common in analytic number theory. For instance we have (see [Fouvry and Klüners 2010b, Proposition 10]):

Lemma 13. *For every $A > 0$, there exists $c(A) > 0$, such that for every bounded complex sequences (α_m) and (β_n) and for every M and N satisfying the inequalities $M, N \ge \max(2, \log^A(MN))$, one has the inequality*

$$\left| \sum_{m \sim M} \sum_{n \sim N} \alpha_m \beta_n \mu^2(2m) \, \mu^2(2n) \left(\frac{m}{n} \right) \right| \le c(A) \, \|(\alpha)\|_\infty \, \|(\beta)\|_\infty \, MN \log^{-A/2}(MN).$$

However in the definition (49) of $\text{Err}_1(D, N)$ the variable n is not squarefree. To circumvent this difficulty we decompose $n = \ell^2 n'$ where now n' is squarefree and we consider two cases. Either $\ell \le N^{1/4}$ and we apply Lemma 13 where the parameters M and N respectively have the values D and $N\ell^{-2}$. Or $\ell > N^{1/4}$ and we apply the trivial bound. Summing over ℓ, choosing a big enough A in Lemma 13 and appealing to (51), we finally deduce the inequality

$$\text{Err}_1(D, N) \ll D^{3/2} \log^{-10}(DN) \ll y^{3/2} \log^{-3} y,$$

which holds uniformly for $N \ge \log^{100} y$. Hence we have also proved (50) in that case. Combining with (51) it remains to prove (50) in the case where D is large and N is small:

$$\text{(52)} \qquad D \ge y \log^{-2} y \text{ and } N \le \log^{100} y.$$

We shall now benefit from the oscillations of the character $d \mapsto (d/n)$ when d runs over squarefree integers $d \equiv 3 \bmod 4$ as follows. Our argument uses the following rather standard lemma which can be found in [Prachar 1958, formula (1)].

Lemma 14. *The following equality*

$$\sum_{\substack{n \le x \\ n \equiv \ell \bmod k}} \mu^2(n) = \frac{6}{\pi^2} \prod_{p \mid k} \left(1 - \frac{1}{p^2} \right)^{-1} \frac{x}{k} + O(x^{1/2}),$$

holds uniformly for $x \ge 2$, $k \ge 1$ and ℓ coprime with k.

Applying Lemma 14 to each of the reduced classes ℓ modulo $4n$ such that $\ell \equiv 3 \bmod 4$ and summing over these ℓ, we obtain the equality

$$(53) \qquad \sum_{\substack{d \leq t \\ d \equiv 3 \bmod 4}} \mu^2(d)\left(\frac{d}{n}\right) = O(nt^{1/2}),$$

uniformly for $t \geq 1$ and for $n \geq 1$ odd and nonsquare.

Integrating by part and summing over $n \sim N$, we easily see that (50) also holds under the condition (52). As a conclusion the proof of (48) is now complete.

We now deal with $\mathrm{MT}_1(y)$. From Lemma 14 we deduce that for any given $A > 0$ the formula

$$\sum_{\substack{d \leq z \\ (d,t)=1 \\ d \equiv 3 \bmod 4}} \mu^2(d) \sim \frac{2}{\pi^2} \prod_{p \mid t}\left(1+\frac{1}{p}\right)^{-1} z,$$

holds as $z \to \infty$ uniformly for t odd satisfying $t \leq z^A$. By a partial summation and by comparison with an integral we have

$$\sum_{\substack{d \leq z \\ (d,t)=1 \\ d \equiv 3 \bmod 4}} \mu^2(d)\sqrt{d} \sim \frac{4}{3\,\pi^2} \cdot \prod_{p \mid t}\left(1+\frac{1}{p}\right)^{-1} z^{3/2}.$$

Inserting this formula in the definition (46) and summing over every odd $t \leq y$ yields:

$$\mathrm{MT}_1(y) \sim_{y \to \infty} \frac{4}{3\pi^2} y^{3/2} \sum_{2 \nmid t} t^{-2} \prod_{p \mid t}\left(1+\frac{1}{p}\right)^{-1}.$$

The infinite series above admits an expansion as an Euler product

$$(54) \qquad \mathrm{MT}_1(y) \sim_{y \to \infty} \frac{4}{3\pi^2} \prod_{p \geq 3}\left(1+\frac{p}{(p+1)^2(p-1)}\right) y^{3/2} = \frac{4C_0}{3\pi^2} y^{3/2}.$$

Putting together (45), (48) and (54) we complete the proof of Lemma 12. $\qquad\square$

The second lemma we need in order to evaluate the sums in (44) is the following.

Lemma 15. *Let $0 < \gamma < \frac{1}{2}$ and, for any $x \geqslant 0$, let $\widetilde{\mathscr{F}}_2(x)$ be defined as in (43). Then there exists $c(\gamma) > 0$, such that as $x \to \infty$ one has*

$$\sum_{d \in \widetilde{\mathscr{F}}_2(x)} L(1, \chi_{4d})\sqrt{d} \sim c(\gamma)x^{3/2}.$$

The asymptotics is uniform for $\gamma_0 \leq \gamma \leq \frac{1}{2} - \gamma_0$, whenever $0 < \gamma_0 < \frac{1}{4}$.

Proof. The proof is very similar to the proof of Lemma 12. The main difference being that (53) is replaced by the following consequence of the classical Siegel–Walfisz theorem

$$
(55) \qquad \sum_{\substack{m \equiv 1 \bmod 4 \\ m \leq x^\gamma}} \mu^2(d) \sum_{\substack{p \equiv 3 \bmod 4 \\ p \sim D/m}} \left(\frac{pm}{n} \right) = O_A(\sqrt{n} D \log^{-A} D),
$$

which holds for any constant $A > 0$. Note that the upper bound contained in (55) is only interesting if $n \leq \log^{2A} D$. This exactly fits the constraint we have on the summation over n (see (52)).

The corresponding main term will have the shape (see (46))

$$
\sum_{\substack{m \leq x^\gamma \\ m \equiv 1 \bmod 4}} \mu^2(m)\sqrt{m} \sum_{\substack{p \sim x/(8m) \\ p \equiv 3 \bmod 4}} \sqrt{p} \sum_{t,(t,2pm)=1} \frac{1}{t^2}.
$$

Inverting summations we first sum over p (where we use a variant of (16)), then over m and finally over t, as in the proof of (54). We note in passing that $c(\gamma)$ could be given an explicit value. $\qquad \square$

6.1. *End of the proof of Theorem 3 and remarks.* Putting together the definition (40), Lemma 12, Lemma 15 (with the choice $\gamma = \eta/10$), and the equalities (41), (42) and (44), we get the inequality

$$
\tilde{\Sigma}(x)
$$

$$
\leq \left\{ \frac{4C_0}{3\pi^2(7/4 - \eta')}(1 + o(1)) - \frac{(\eta + \eta')c(\eta/10)}{(7/4 + \eta)(7/4 - \eta')}(1 - o_\eta(1)) \right\} x^{3/2} + o_{\eta,\eta'}(x^{3/2}).
$$

Now fix $\eta = \frac{1}{10}$. Then by fixing a very small $\eta' > 0$ the above upper bound can be written

$$
\tilde{\Sigma}(x) \leq K_0 x^{3/2},
$$

for sufficiently large x and for some fixed K_0 satisfying the inequality

$$
K_0 < \frac{16\,C_0}{21\pi^2}.
$$

This proves (38) hence (36) and completes the proof of Theorem 3.

We now discuss the influence of the different results about the size of $\varepsilon(D)$ we have used on the sum we have studied. If our only input is the trivial lower bound $\varepsilon(D) \geq 2\sqrt{D}$ (see (2)), we cannot get anything better than

$$
(56) \qquad \sum_{\substack{D \leq x \\ 2^2 \| D}} h(D) \leq \left(\frac{4\,C_0}{3\pi^2} + \delta \right) \frac{x^{3/2}}{\log x},
$$

for every positive δ and every sufficiently large x.

Using [Fouvry and Jouve 2013, Theorem 1] has enabled us to improve the multiplicative coefficient in the above upper bound by the factor 3.5. Finally the purpose of our Proposition 7 has been to improve the inequality (56) by some factor slightly larger than 3.5.

6.2. *A consequence of Corollary 8.* A natural question is to ask for some upper bound on average for the class number $h(D)$ when D is essentially prime. So we consider the sum

$$S(x) := \sum_{\substack{p \leq x \\ p \equiv 3 \bmod 4}} h(4p).$$

By techniques very similar to those presented in the beginning of Section 6 and the trivial bound $\varepsilon(4p) \geq 2\sqrt{p}$, we can prove that we have the trivial asymptotic inequality

$$S(x) \leq \left(\frac{1}{2} + o(1)\right) \frac{x^{3/2}}{\log^2 x}.$$

When appealing instead to (12), we improve this upper bound by a factor 2. Finally, Corollary 8 improves by a factor 6 the trivial asymptotic inequality. More precisely we get the following result the proof of which easily follows from Corollary 8 and is left to the reader.

Corollary 16. *As $x \to \infty$, one has the inequality*

$$S(x) \leq \left(\frac{1}{12} + o(1)\right) \frac{x^{3/2}}{\log^2 x}.$$

Acknowledgements

References

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993. MR 94i:11105 Zbl 0786.11071

[Cremona and Odoni 1989] J. E. Cremona and R. W. K. Odoni, "Some density results for negative Pell equations: An application of graph theory", *J. London Math. Soc.* (2) **39**:1 (1989), 16–28. MR 90b:11019 Zbl 0678.10015

[Dirichlet 1834] P. G. Lejeune-Dirichlet, "Einige neue Sätze über unbestimmte Gleichungen", pp. 649–604 [i.e., 664], 1834. Reprinted as pp. 219–236 in his *Werke*, vol. I, G. Reimer, Berlin, 1889; available at http://archive.org/stream/abhandlungenderk1834deut#page/n734. JFM 21.0016.01

[Dirichlet 1856] P. G. Lejeune-Dirichlet, "Sur une propriété des formes quadratiques à déterminant positif", *J. Math. Pure Appl.* (2) **1** (1856), 76–79. Reprinted as pp. 191–194 in his *Werke*, vol. II, G.

Reimer, Berlin, 1897; available at http://portail.mathdoc.fr/JMPA/PDF/JMPA_1856_2_1_A7_0.pdf. JFM 28.0014.01

[Fouvry and Jouve 2012] É. Fouvry and F. Jouve, "Fundamental solutions to Pell equation with prescribed size", *Proc. Steklov Inst. Math.* **276**:1 (2012), 40–50.

[Fouvry and Jouve 2013] É. Fouvry and F. Jouve, "Size of regulators and consecutive square–free numbers", *Math. Z.* **273**:3-4 (2013), 869–882. MR 3030681

[Fouvry and Klüners 2010a] É. Fouvry and J. Klüners, "On the negative Pell equation", *Ann. of Math.* (2) **172**:3 (2010), 2035–2104. MR 2011h:11122 Zbl 1230.11136

[Fouvry and Klüners 2010b] É. Fouvry and J. Klüners, "The parity of the period of the continued fraction of $\sqrt{d}$", *Proc. Lond. Math. Soc.* (3) **101**:2 (2010), 337–391. MR 2011g:11213 Zbl 1244.11092

[Fröhlich and Taylor 1993] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, 1993. MR 94d:11078 Zbl 0744.11001

[Golubeva 1987] E. P. Golubeva, "On the lengths of the periods of a continued fraction expansion of quadratic irrationalities and on the class numbers of real quadratic fields", *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* (*LOMI*) **160**:Anal. Teor. Chisel i Teor. Funktsii. 8 (1987), 72–81. In Russian; translated in *J. Soviet Math.* **52**:3 (1990), 3049–3056. MR 88j:11055 Zbl 0900.11015

[Golubeva 1993] E. P. Golubeva, "Class numbers of real quadratic fields of discriminant $4p$", *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov.* (*POMI*) **204**:Anal. Teor. Chisel i Teor. Funktsii. 11 (1993), 11–36. In Russian; translated in *J. Math. Sc.* **79**:5 (1996), 1277–1292. MR 94f:11115 Zbl 0814.11023

[Golubeva 2002] E. P. Golubeva, "On the Pell equation", *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov.* (*POMI*) **286**:Anal. Teor. Chisel i Teor. Funkts. 18 (2002), 36–39. In Russian; translated in *J. Math. Sc.* **12**:6 (2004), 3600–3602. MR 2003j:11027 Zbl 1077.11021

[Halter-Koch 1989] F. Halter-Koch, "Reell-quadratische Zahlkörper mit großer Grundeinheit", *Abh. Math. Sem. Univ. Hamburg* **59** (1989), 171–181. MR 91h:11116 Zbl 0718.11054

[Hooley 1984] C. Hooley, "On the Pellian equation and the class number of indefinite binary quadratic forms", *J. Reine Angew. Math.* **353** (1984), 98–131. MR 86d:11032 Zbl 0539.10019

[Legendre 1830] A.-M. Legendre, *Théorie des nombres, I*, 3rd ed., Didot, Paris, 1830.

[Lemmermeyer 2003] F. Lemmermeyer, "Higher descent on Pell conics, I: From Legendre to Selmer", preprint, 2003. arXiv math/0311309v1

[Pall 1969] G. Pall, "Discriminantal divisors of binary quadratic forms", *J. Number Theory* **1** (1969), 525–533. MR 40 #1335 Zbl 0186.08602

[Perron 1913] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, Berlin, 1913. JFM 43.0283.04

[Prachar 1958] K. Prachar, "Über die kleinste quadratfreie Zahl einer arithmetischen Reihe", *Monatsh. Math.* **62** (1958), 173–176. MR 19,1160g Zbl 0083.03704

[Reiter 1985] C. Reiter, "Effective lower bounds on large fundamental units of real quadratic fields", *Osaka J. Math.* **22**:4 (1985), 755–765. MR 87h:11107 Zbl 0586.12005

[Sarnak 1985] P. C. Sarnak, "Class numbers of indefinite binary quadratic forms, II", *J. Number Theory* **21**:3 (1985), 333–346. MR 87h:11027 Zbl 0571.10022

[Yamamoto 1971] Y. Yamamoto, "Real quadratic number fields with large fundamental units", *Osaka J. Math.* **8** (1971), 261–270. MR 45 #5107 Zbl 0243.12001

[Zagier 1981] D. B. Zagier, *Zetafunktionen und quadratische Körper: Eine Einführung in die höhere Zahlentheorie*, Springer, Berlin, 1981. MR 82m:10002 Zbl 0459.10001

ÉTIENNE FOUVRY
LABORATOIRE DE MATHÉMATIQUE
CAMPUS D'ORSAY, UNIVERSITÉ DE PARIS-SUD
BATIMENT 425 UMR 8628
91405 ORSAY CEDEX
FRANCE
etienne.fouvry@math.u-psud.fr

FLORENT JOUVE
LABORATOIRE DE MATHÉMATIQUE
CAMPUS D'ORSAY, UNIVERSITÉ DE PARIS-SUD
BATIMENT 425 UMR 8628
91405 ORSAY CEDEX
FRANCE
florent.jouve@math.u-psud.fr

See inside back cover or msp.org/pjm for submission instructions.

PACIFIC JOURNAL OF MATHEMATICS