ON THE SIZE OF THE FUNDAMENTAL SOLUTION OF PELL EQUATION

ÉTIENNE FOUVRY

Abstract. We give a lower bound for the cardinality of the set of $D \leq x$ for which the fundamental solution of the Pell equation $t^2 - Du^2 = 1$ is less than $D^{\frac{1}{2}+\alpha}$ where α is any fixed constant such that $\alpha \leq 1$. A second result, based on an hypothesis concerning short exponential sums, goes in the direction of a conjecture due to C. Hooley.

1. Introduction and statement of the results

Let D be a non square positive integer. The equation, usually called *Pell equation*,

$$t^2 - Du^2 = 1, \tag{1}$$

where the unknowns are the integers t and u, has a long history (see [13] for instance). As usual, it is more convenient to write any solution of (1) under the form

$$\eta_D := t + u\sqrt{D}.$$

A classical theorem asserts that the set of solutions of (1) is non trivial and is of the form

$$\{\eta_D\,;\ \eta_D \text{ solution of (1)}\,\} = \{\pm\varepsilon_D^n\,;\ n \in \mathbb{Z}\}, \tag{2}$$

where ε_D is the so called *fundamental solution* of (1), that means

$$\varepsilon_D := \inf\big\{\eta_D\,;\ \eta_D > 1\big\}. \tag{3}$$

Writing $\varepsilon_D := t_0 + u_0\sqrt{D}$, we have t_0 and $u_0 \geq 1$, from which we deduce $t_0 = \sqrt{1 + Du_0^2} \geq \sqrt{D}$ and finally

$$\varepsilon_D \geq 2\sqrt{D}. \tag{4}$$

We are interested in counting the D's for which ε_D is less than a fixed power of D and our paper is inspired by a work of Hooley [8], where he investigates the set of D for which the associated ε_D is not too large (that means less than $D^{\frac{1}{2}+\alpha}$, where $\alpha < 1$, see [8, Theorem 1]). In the same paper, Hooley develops a heuristic approach to guess the size of ε_D. As a consequence, he conjectures an asymptotic value for the sum of $H(D)$ $(D \leq x)$ where $H(D)$ is the number of classes of indefinite quadratic forms $aX^2 + 2bXY + cY^2$ with discriminants $D = b^2 - ac$ (see [8, Conjecture 7]). At the same time, Cohen (see [1] & [2]) and Sarnak (see [10] & [11]) were led to conjecture the same type of formula by adopting different points of view.

Date: November 25, 2010.

2010 *Mathematics Subject Classification.* Primary 11D09; Secondary 11L05.

In this work, we shall adopt some notations from [8] and freely borrow some of the preparatory results (see §2, §3 & §9).

For $\alpha > 0$, and, for $x \geq 2$, we consider the two sets

$$\mathcal{S}(x,\alpha) := \{(\eta_D, D)\,;\ 2 \leq D \leq x,\ D \text{ non square},\ \varepsilon_D \leq \eta_D \leq D^{\frac{1}{2}+\alpha}\}, \tag{5}$$

$$\mathcal{S}^{\mathrm{f}}(x,\alpha) := \{(\varepsilon_D, D)\,;\ 2 \leq D \leq x,\ D \text{ non square},\ \varepsilon_D \leq D^{\frac{1}{2}+\alpha}\}, \tag{6}$$

Hence, $\mathcal{S}^{\mathrm{f}}(x,\alpha)$ is associated to D such that the fundamental solution ε_D is less than some bound, while in $\mathcal{S}(x,\alpha)$, we consider all the solutions η_D, fundamental or not, less than this bound. The cardinalities of $\mathcal{S}(x,\alpha)$ and $\mathcal{S}^{\mathrm{f}}(x,\alpha)$ are respectively denoted by $S(x,\alpha)$ and $S^{\mathrm{f}}(x,\alpha)$. Although, $S^{\mathrm{f}}(x,\alpha)$ is more natural, the analytic methods, which will be developed below, only allow to understand $S(x,\alpha)$. However, the equalities (2) and (3) imply relations based on the inclusion–exclusion principle between these cardinalities $S(x,\alpha)$ and $S^{\mathrm{f}}(x,\alpha)$, see (29) for instance. Finally, if d is such that $d^2 \mid D$, then any η_D is also an η_{D/d^2}.

First recall a direct consequence of a theorem of Hooley ([8, Theorem 1]).

Theorem A. *Let $\varepsilon_0 > 0$ satisfying $0 < \varepsilon_0 < 1/2$. As x tends to infinity, one has*

$$S(x,\alpha) = S^{\mathrm{f}}(x,\alpha) \sim \frac{4\alpha^2}{\pi^2} x^{\frac{1}{2}} \log^2 x, \tag{7}$$

uniformly for $\varepsilon_0 \leq \alpha \leq \frac{1}{2}$.

The main purpose of this paper is to prove the following

Theorem 1. *As x tends to infinity, one has the inequalities*

$$S^{\mathrm{f}}(x,\alpha) \geq \frac{1}{\pi^2}\Big(1 + (2\alpha - 1)\,(3 - 2\alpha) - o(1)\Big) x^{\frac{1}{2}} \log^2 x, \tag{8}$$

and

$$S(x,\alpha) \geq \frac{1}{\pi^2}\Big(1 + (\alpha - \frac{1}{2})\,(\frac{11}{2} - 3\alpha) - o(1)\Big) x^{\frac{1}{2}} \log^2 x, \tag{9}$$

uniformly for $\frac{1}{2} \leq \alpha \leq 1$.

Remarks.

(i) The formula (7) is contained in [8, Theorem 1] exactly. We shall briefly give its proof in §3 again. Our contribution will then clearly appear in §4 and in the following sections.

(ii) Actually Theorem 1 also gives non trivial lower bounds of $S^{\mathrm{f}}(x,\alpha)$ and $S(x,\alpha)$, for $\alpha \geq 1$, via the trivial inequalities $S^{\mathrm{f}}(x,\alpha) \geq S^{\mathrm{f}}(x,1)$ and $S(x,\alpha) \geq S(x,1)$.

(iii) Hooley (see [8, Conjecture 1]) suggests a conjecture for $S^{\mathrm{f}}(x,\alpha)$, for $\alpha > \frac{1}{2}$. In particular, he thinks that the following is true

$$S^{\mathrm{f}}(x,\alpha) \sim \frac{1}{\pi^2}\Big(1 + 4(\alpha - \frac{1}{2})\Big) x^{\frac{1}{2}} \log^2 x, \tag{10}$$

for $\frac{1}{2} < \alpha \leq 1$ and $x \to \infty$. Hence the lower bound (8) can be viewed as the first significant step towards the proof of (10).

(iv) To compare our result (8) with (10), write (8) as

$$S^{\mathrm{f}}(x,\alpha) \geq \frac{1}{\pi^2}\,\big(\phi(\alpha) - o(1)\big)\, x^{\frac{1}{2}} \log^2 x,$$

and (10) as

$$S^{\mathrm{f}}(x,\alpha) \sim \frac{1}{\pi^2}\,\phi^{\mathrm{hyp}}(\alpha)\,x^{\frac{1}{2}}\log^2 x.$$

We easily check the following

$$\phi(\alpha) \le \phi^{\mathrm{hyp}}(\alpha) \text{ for } \frac{1}{2} \le \alpha \le 1,$$

$$\phi(1) = 2 \text{ and } \phi^{\mathrm{hyp}}(1) = 3,$$

and finally,

$$0 \le \phi^{\mathrm{hyp}}(\alpha) - \phi(\alpha) = O\big((\alpha - 1/2)^2\big), \text{ as } \alpha \to 1/2^+.$$

(v) In conclusion, the above discussion may give some evidence to support the truth of (10). Another strong evidence will come from Theorem 2 below, which, however, depends on a conjecture on exponential sums (see Conjecture 1 below).

1.1. **Abstract of the proof of Theorem 1.** The main ideas of the present work can be summarized as follows. The search for D with small η_D is intimately linked with the study of the congruence $t^2 - 1 \equiv 0 \bmod u^2$. Such a congruence can be given explicit solutions, which are easily described in terms of the factorization of $u = u_1u_2$, with $(u_1, u_2) = 1$, at least when u is odd (see Lemma 2 below). By Fourier analysis, we are led to prove that the square of the inverse $\overline{u_2}$ of u_2 mod u_1^2 is well distributed. This is achieved by a precise study of the following tridimensional exponential sum, which, roughly speaking, is defined by

$$\mho := \sum_{h\neq 0}\alpha_h \sum_{u_1}\beta_{u_1}\sum_{u_2} e\Big(h\frac{\overline{u_2}^2}{u_1^2}\Big),$$

where the variable h comes from an application of Poisson summation formula (see Lemma 4 below), where the coefficients α_h and β_{u_1} are of modulus less than one. As usual $e(\cdot) = \exp(2\pi i\cdot)$. For a precise definition, see (61) below.

The exponential sum $\mho$ is elementary, which means that, apparently, it is not directly linked with an exponential sum on a curve over a finite field. We will prove that the subsum over u_2 is zero on any interval of length u_1^2, when h and u_1 satisfy some divisibility properties, which are satisfied most of the time (see Lemma 6). This produces an important source of cancellation in the sum $\mho$. When these conditions are not satisfied, classical Gaussian sums appear and we obtain another source of cancellation from the oscillations of the signs of these sums by appealing to the large sieve inequality for Jacobi symbols, due to Heath–Brown (see Lemma 9). However, our method does not cover all the possible cases for the mutual sizes of u_1 and u_2. This is the reason why we can only prove a lower bound.

It is well known that ε_D has an expression based on the expansion of $\sqrt{D}$ in continued fraction

$$\sqrt{D} = \big[a_0;\ \overline{a_1, \cdots, a_s}\big],$$

where s is the period of this expansion. This is the starting point of several papers of Golubeva ([5], [6] for instance). By a delicate study of s and the recurrence relations induced by the a_i, one can prove that, for every fixed positive δ, the inequality $\varepsilon_D > D^{2-\delta}$ is satisfied by a positive proportion of the D (see [6, Theorem]) (Hooley [8, Corollary p.104] obtained the weaker result, with the exponent $2-\delta$ essentially

replaced by 3/2). This type of results deals with a completely different question from the one we investigate here.

1.2. **An hypothetical result.** The above description shows the importance of having stronger bounds for exponential sums to improve Theorem 1. Let us consider the following conjecture on short special exponential sums

Conjecture 1. *There exists an absolute ϑ_0 satisfying*

$$0 < \vartheta_0 < 1,$$

such that, for any odd integer a and for any integer $k \geq 0$ one has the inequality

$$\sum_{\substack{m \in \mathcal{I} \\ m \equiv a \bmod 4^k,\, (m,n)=1}} e\Big(h\frac{\overline{m}^2}{n^2}\Big) \ll_k (h, n^2)^{\frac{1}{2}} M^{\vartheta_0}, \tag{11}$$

uniformly for integers h and n satisfying $h \neq 0$, $n \geq 1$ and $2 \nmid n$, for real number M satisfying $n \leq M \leq n^2$ and $\mathcal{I}$ an interval included in $[M, 2M]$.

Remarks.

(i) The interest of Conjecture 1 is to give some insight on exponential sums, when the length of the interval of summation is just greater than square root of the denominator. We conjecture an upper bound which is slightly better than the trivial one, when the interval is too short to accept an application of the classical Fourier techniques. Conjecture 1 can be compared with the celebrated R^*–conjecture concerning short Kloosterman sums (see [7, p.44]).

(ii) The inequality (11) is proved, when one assumes that M satisfies the condition $n^\delta \leq M \leq n^2$, when δ is any fixed number greater than 1. It suffices to choose $\vartheta_0 := (\delta+1)/2\delta$ and apply (78) below. In other words, we conjecture slightly more than what is proved. Our conjecture seems quite reasonable since it does not deal with very short exponential sums.

(iii) Finally, the inequality (11) is very weak when M is slightly less than n^2 : the inequality (78) is much better.

We have

Theorem 2. *Suppose that Conjecture 1 is true for some ϑ_0 satisfying $0 < \vartheta_0 < 1$. Then we have*

$$S^{\mathrm{f}}(x, \alpha) \geq \frac{4}{\pi^2}\Big(\alpha - \frac{1}{4} - o(1)\Big) x^{\frac{1}{2}} \log^2 x,$$

and

$$S(x, \alpha) \geq \frac{4}{\pi^2}\Big(\alpha - \frac{1}{4} + \big(\frac{\alpha}{2} - \frac{1}{4}\big)^2 - o(1)\Big) x^{\frac{1}{2}} \log^2 x,$$

uniformly for $\dfrac{1}{2} \leq \alpha \leq \min\Big(\dfrac{3}{4}, \dfrac{1}{1+\vartheta_0}\Big)$.

We emphasize the fact that we recover the conjectured formula (10), but only in the lower bound aspect and only for α slightly larger than $\frac{1}{2}$.

Acknowledgement. This research was partially supported by Institut Universitaire de France. The author thanks this institution.

2. The fundamental transformation

By the definition (5) we have the equality

$$S(x,\alpha)=\sum_{\substack{(t,u,D),\ t^2-Du^2=1\\ 1<t+u\sqrt{D}\le D^{\frac12+\alpha}}}\sum\sum 1. \tag{12}$$

Following Hooley [8, formula (15)], one has the equality

$$S(x,\alpha)=\sum_{1\le u\le X_\alpha}\ \sum_{\substack{Du^2=t^2-1\\ Y_2(u,\alpha)\le t\le Y_3(u)}} 1, \tag{13}$$

where

$$X_\alpha:=\frac12(x^\alpha-x^{-1-\alpha}),$$

$$Y_3(u):=\big(xu^2+1\big)^{\frac12}, \tag{14}$$

and

$$Y_2(u)=Y_2(u,\alpha):=\big(Y_1(u,\alpha)u^2+1\big)^{\frac12}. \tag{15}$$

In that last expression, $Y_1(u,\alpha)$ is the function of u, implicitly defined by the equation

$$u=\frac12\big(Y_1(u,\alpha)^\alpha-Y_1(u,\alpha)^{-1-\alpha}\big).$$

The relevance of (13) is to replace the inequalities in (12) concerning D and η_D by conditions on t and u separately. Writing Y_1 under the form $Y_1(u,\alpha)=(A(u)\,u)^{\frac1\alpha}$ we shall use

Lemma 1. *Let $\alpha>0$. Then the function $u\mapsto A(u)$ defined, for $u\ge1$, by the equality*

$$A(u)\,u-\big(A(u)u\big)^{-(1+1/\alpha)}=2u,$$

is of $\mathcal{C}^\infty$–class and satisfies the inequalities

$$2\le A(u)\le 2+u^{-1}\cdot(2u)^{-(1+1/\alpha)}.$$

Proof. Consider the function

$$(x,y)\in]0,+\infty[^2\mapsto G_\alpha(x,y):=2x-y+y^{-(1+1/\alpha)}.$$

For every fixed x, the funtion $y\mapsto G_\alpha(x,y)$ is decreasing. We trivially have $G(x,2x)>0$ and

$$G(x,2x+(2x)^{-(1+1/\alpha)})=-(2x)^{-(1+1/\alpha)}+(2x+(2x)^{-(1+1/\alpha)}))^{-(1+1/\alpha)}<0.$$

Hence the result by the obvious change of notations $u=x$ and $A(u)u=y$. □

This lemma implies that the function $u\mapsto Y_2(u,\alpha)$ is of $\mathcal{C}^\infty$–class and satisfies the inequalities

$$\begin{cases} 2^{\frac{1}{2\alpha}}\,u^{1+\frac{1}{2\alpha}}<Y_2(u,\alpha)<\big(2^{\frac{1}{2\alpha}}+o(1)\big)\,u^{1+\frac{1}{2\alpha}} \quad (u\to\infty),\\[2ex] \dfrac{\mathrm{d}Y_2(u,\alpha)}{\mathrm{d}u}=O\big(u^{\frac{1}{2\alpha}}\big) \quad (u\to\infty). \end{cases} \tag{16}$$

Following [8, formula (15)], we write the equality

$$S(x,\alpha)=\sum_{1\le u\le X_\alpha}\ \sum_{\Omega\in\mathcal{R}(u)}\ \sum_{\substack{t\equiv\Omega \bmod u^2\\ Y_2(u,\alpha)\le t\le Y_3(u)}} 1, \tag{17}$$

where $\mathcal{R}(u)$ denotes the set of congruence classes

$$\mathcal{R}(u):=\big\{\Omega \bmod u^2\,;\ \Omega^2\equiv 1 \bmod u^2\big\}. \tag{18}$$

3. The case $\alpha\le 1/2$

The most direct way of studying (17) is to introduce the function $\rho(d)$ which is the cardinality of $\mathcal{R}(d)$. The function $d\mapsto\rho(d)$ is a multiplicative function, which satisfies the equalities

$$\rho(2)=2,\ \rho(2^k)=4 \text{ for } k\ge 2 \text{ and } \rho(p^\ell)=2 \text{ for } p\ge 3 \text{ and } \ell\ge 1. \tag{19}$$

As usual we reserve the letter p for prime numbers. Hence, by (18), we write (17) as

$$S(x,\alpha)=\sum_{1\le u\le X_\alpha}\rho(u)\Big\{\frac{Y_3(u)-Y_2(u,\alpha)}{u^2}+O(1)\Big\}. \tag{20}$$

By the definitions of the functions Y_2 and Y_3 and by (16), we deduce the equality

$$Y_3(u)-Y_2(u,\alpha)=ux^{\frac12}+O\big(u^{1+\frac{1}{2\alpha}}\big). \tag{21}$$

Inserting this into (20), we obtain the equality

$$S(x,\alpha)=x^{\frac12}\sum_{1\le u\le X_\alpha}\frac{\rho(u)}{u}+O\Big(\sum_{1\le u\le X_\alpha}\frac{\rho(u)}{u^{1-\frac{1}{2\alpha}}}\Big)+O\Big(\sum_{1\le u\le X_\alpha}\rho(u)\Big). \tag{22}$$

Now consider the Dirichlet series

$$F(s):=\sum_{d\ge1}\frac{\rho(d)}{d^s}\ (\Re s>1).$$

By (19), we get the equality (see [8, p.103])

$$F(s)=\Big(1+\frac{1}{2^s}+\frac{2}{2^{2s}}\Big)\Big(1+\frac{1}{2^s}\Big)^{-1}\ \frac{\zeta^2(s)}{\zeta(2s)},$$

which shows that this function has a meromorphic continuation to $\mathbb{C}$, with a double pole at $s=1$, the other poles lying in the half plane $\Re s<\frac12$. Standard techniques of complex analysis give the existence of an absolute constant c_0, such that, for $y\to\infty$, one has

$$\sum_{u\le y}\rho(u)=\Big(\frac{8}{\pi^2}\log y+c_0\Big)y+O(y^{\frac34}). \tag{23}$$

An application of Abel summation to (23) gives the equalities

$$\sum_{1\le u\le y}\frac{\rho(u)}{u}=\frac{4}{\pi^2}\ \log^2 y+\big(c_1+o(1)\big)\log y, \tag{24}$$

and

$$\sum_{1\le u\le y}\frac{\rho(u)}{u^{1-\frac{1}{2\alpha}}}=\big(c_2(\alpha)+o(1)\big)\,y^{\frac{1}{2\alpha}}\log y, \tag{25}$$

uniformly for $x \geq 1$ and $\alpha \geq \varepsilon_0$, where ε_0 is any fixed positive constant. It remains to fix $y = X_\alpha$ (so $\log X_\alpha = \alpha \log x - \log 2 + o(1)$) and to insert (23), (24) and (25) into (22) to get the equality

$$S(x,\alpha) = \frac{4\alpha^2}{\pi^2} x^{\frac{1}{2}} \log^2 x + \big(c(\alpha) + o(1)\big) x^{\frac{1}{2}} \log x + O(x^\alpha \log x), \tag{26}$$

uniformly for $\varepsilon_0 \leq \alpha \leq 1$ and $x \geq x_0(\alpha)$. The function $c(\alpha)$ could be given an explicit form. Hence we get the first part of Theorem A.

From (4), we deduce that if $\eta_D > 1$ is not a fundamental solution of (1), we necessarily have

$$\eta_D \geq \varepsilon_D^2 \geq 4D.$$

Hence, for $\alpha \leq \frac{1}{2}$, we have

$$S^{\mathrm{f}}(x,\alpha) = S(x,\alpha). \tag{27}$$

This completes the proof of Theorem A. We have recovered [8, Theorem 1].

4. Preparation of $S(x,\alpha)$ for $\alpha > 1/2$

4.1. **The trivial lower bound.** Throughout the end of this paper, we shall suppose that the inequalities

$$\frac{1}{2} < \alpha \leq 1. \tag{28}$$

hold. The situation now is different from the case $\alpha \leq \frac{1}{2}$ for two reasons at least. The first one is that the $O(1)$–term in (20) surpasses the main term. The second one is that we may count in $S(x,\alpha)$ some η_D which are not fondamental. More precisely, as a consequence of (4) and (28), if (D,η_D) belongs to $\mathcal{S}(x,\alpha)$, then η_D is of the form $\eta_D = \varepsilon_D$ or ε_D^2 but not of the form $\eta = \varepsilon_D^k$ for some $k \geq 3$. We can measure the intrusion of non fundamental solutions by the following trivial equality

$$S(x,\alpha) = S^{\mathrm{f}}(x,\alpha) + S(x, \frac{\alpha}{2} - \frac{1}{4}) \text{ for } 0 \leq \alpha \leq \frac{3}{2}, \tag{29}$$

which is a consequence of the equivalence

$$\varepsilon_D^2 \leq D^{\frac{1}{2}+\alpha} \iff \varepsilon_D \leq D^{\frac{1}{2}+(\frac{\alpha}{2}-\frac{1}{4})}.$$

Remark that (29) implies the inequality

$$S(x,\alpha) \geq S(x,\frac{1}{2}) + S(x, \frac{\alpha}{2} - \frac{1}{4}) \text{ for } \frac{1}{2} \leq \alpha \leq \frac{3}{2}, \tag{30}$$

4.2. **A first dissection of the sum.** Let $\mathcal{S}(x,\frac{1}{2},\alpha)$ be the following set

$$\mathcal{S}(x,\frac{1}{2},\alpha) := \big\{(t,u,D),\ ;\ 1 \leq u \leq X_{1/2}, \\ D \leq x, Y_2(u,\alpha) \leq t \leq Y_3(u), t^2 - Du^2 = 1\big\}, \tag{31}$$

where $Y_2(u,\alpha)$ is defined by (15) always. The cardinality of this set is denoted by $S(x,\frac{1}{2},\alpha)$ and can be seen as a subsum of $S(x,\frac{1}{2})$ since we have the equality

$$S(x,\frac{1}{2},\alpha) := \sum_{1\leq u\leq X_{1/2}} \sum_{\Omega\in\mathcal{R}(u)} \sum_{\substack{t\equiv\Omega \bmod u^2 \\ Y_2(u,\alpha)\leq t\leq Y_3(u)}} 1, \tag{32}$$

(compare (32) and (17)). By similar techniques leading to (26), one proves that

$$S(x,\frac{1}{2},\alpha)\sim S(x,\frac{1}{2})\ \sim \frac{1}{\pi^2}x^{\frac{1}{2}}\log^2 x, \tag{33}$$

as x tends to infinity.

We now consider the difference

$$L(x,\alpha):=S(x,\alpha)-S_\alpha(x,\frac{1}{2},\alpha). \tag{34}$$

By (17), (32) and (34), we have the equality

$$L(x,\alpha)=\sum_{X_{1/2}<u\leq X_\alpha}\ \sum_{\substack{Du^2=t^2-1\\ Y_2(u)\leq t\leq Y_3(u)}} 1. \tag{35}$$

Of course, $L(x,\alpha)$ is the cardinality of the set

$$\begin{aligned}\mathcal{L}(x,\alpha):=\big\{(t,u,D)\,;\ X_{1/2}<u\leq X_\alpha,\\ D\leq x, Y_2(u,\alpha)\leq t\leq Y_3(u), t^2-Du^2=1\big\}.\end{aligned} \tag{36}$$

Since α is fixed, we write $Y_2(u)$ instead of $Y_2(u,\alpha)$. We also denote by $\mathcal{S}^{\mathrm{f}}(x,\frac{1}{2},\alpha)$ and $\mathcal{L}^{\mathrm{f}}(x,\alpha)$ the subsets of $\mathcal{S}(x,\frac{1}{2},\alpha)$ and $\mathcal{L}(x,\alpha)$ where the triples (t,u,D) satisfy the extra condition $t+u\sqrt{D}=\varepsilon_D$. Their cardinalities are respectively denoted by $S^{\mathrm{f}}(x,\frac{1}{2},\alpha)$ and $L^{\mathrm{f}}(x,\alpha)$.

By (33) & (34), the proof of (9) is now reduced to proving a lower bound for $L(x,\alpha)$.

4.3. **An arithmetical preparation.** Fix k an integer ≥ 0. Let $u\geq 1$ such that $u=2^k u_0$, where u_0 is an odd integer. We then have

$$\Omega^2-1\equiv 0 \bmod u^2 \iff \begin{cases}\Omega^2-1\equiv 0 \bmod u_0^2\\ \text{ and }\\ \Omega^2-1\equiv 0 \bmod 4^k.\end{cases} \tag{37}$$

In other words, (37) describes $\mathcal{R}(u)$ in terms of $\mathcal{R}(2^k)$ and $\mathcal{R}(u_0)$ (recall the definition (18)). Starting from (35), we decompose $L(x,\alpha)$ as follows

$$L(x,\alpha)=\sum_{k=0}^{\infty}\ \sum_{\xi\in\mathcal{R}(2^k)} L(x,\alpha,\xi,k), \tag{38}$$

with

$$L(x,\alpha,\xi,k):=\sum_{\substack{X_{1/2}2^{-k}<u\leq X_\alpha 2^{-k}\\ u\text{ odd}}}\ \sum_{\Omega\in\mathcal{R}(u)}\ \sum_{\substack{t\equiv\Omega \bmod u^2\\ t\equiv\xi \bmod 4^k\\ Y_2(2^k u)\leq t\leq Y_3(2^k u)}} 1. \tag{39}$$

Remark that (38) and (39) only contain positive terms. Hence, when dropping the too difficult terms, we arrive at a lower bound for $L(x,\alpha)$.

4.4. **Description of $\mathcal{R}(u)$ for odd u.** The following easy lemma gives a precise description of the set $\mathcal{R}(u)$. This idea was not use in [8]. As usual, for m and n coprime integers, we denote by $\overline{m} \bmod n$, $(\overline{m})_{\bmod n}$ (or simply $\overline{m}$ when the context is clear, for instance in the fraction $\frac{\overline{m}}{n}$), the multiplicative inverse of m modulo n. This notation was already used in §1.1 & §1.2. We have

Lemma 2. *Let u be a positive odd integer. Then there is a bijection Φ between the set of coprime decompositions of u*

$$\mathcal{D}(u) := \big\{(u_1,u_2)\,;\ u_1u_2=u,\ (u_1,u_2)=1,\ u_1,u_2\geq 1\big\},$$

and the set of roots of congruence

$$\mathcal{R}(u) := \big\{\Omega \bmod u^2\,;\ \Omega^2\equiv 1 \bmod u^2\big\}.$$

Such a bijection can be defined by $\Phi(u_1,u_2)=\Omega$, where Ω is uniquely determined by $\Omega\equiv 1 \bmod u_1^2$ and $\Omega\equiv -1 \bmod u_2^2$. In an equivalent manner we have the equalities

$$\begin{aligned}\Phi(u_1,u_2) &\equiv -\overline{u_1}^2u_1^2+\overline{u_2}^2u_2^2 \bmod u^2\\ &\equiv -2\,\overline{u_1}^2u_1^2+1 \bmod u^2 \qquad (40)\\ &\equiv 2\,\overline{u_2}^2u_2^2-1 \bmod u^2. \qquad (41)\end{aligned}$$

Of course $\overline{u_1}^2$ and $\overline{u_2}^2$ are considered modulo u_2^2 and u_1^2 respectively.

Proof. Let Φ defined as in Lemma 2. We now prove that Φ is a bijection. We easily see that $\Phi(\mathcal{D}(u))\subset\mathcal{R}(u)$ and that Φ is injective. Conversely, let $\Omega\in\mathcal{R}(u)$. Since u is odd, we have

$$u^2=(u^2,\Omega^2-1)=(u^2,\Omega-1)(u^2,\Omega+1).$$

Since $(u^2,\Omega-1)$ and $(u^2,\Omega+1)$ are coprime, we deduce that $(u^2,\Omega-1)$ is necessarily of the form $(u^2,\Omega-1)=u_1^2$, where $u_1\mid u$. Similarly, one has $(u^2,\Omega+1)=u_2^2$, with $u=u_1u_2$ and $(u_1,u_2)=1$. Thus we have proved that $\Phi(u_1,u_2)=\Omega$. Hence Φ is a bijection. □

4.5. **Arithmetic decomposition of $L(x,\alpha,\xi,k)$.** We implement Lemma 2 in (39) to obtain the equality

$$\begin{aligned}L(x,\alpha,\xi,k) &= \sum_{\substack{u_1,\ u_2\\ X_{1/2}<2^ku_1u_2\leq X_\alpha\\ (u_1u_2,2)=(u_1,u_2)=1}}\ \sum_{\substack{t\equiv\Phi(u_1,u_2)\bmod u_1^2u_2^2\\ t\equiv\xi \bmod 4^k\\ Y_2(2^ku_1u_2)\leq t\leq Y_3(2^ku_1u_2)}} 1\\ &:= L^{>}(x,\alpha,\xi,k)+L^{<}(x,\alpha,\xi,k), \qquad (42)\end{aligned}$$

where $L^{>}(x,\alpha,\xi,k)$ is the subsum of $L(x,\alpha,\xi,k)$ corresponding to the extra condition $u_1>u_2$. Of course $L^{<}(x,\alpha,\xi,k)$ corresponds to the case $u_1<u_2$. Due to the symmetric expressions of the Φ–function (see Lemma 2, formulas (40) and (41)), the treatments of $L^{>}$ and $L^{<}$ are similar. We shall only study $L^{<}(x,\alpha,\xi,k)$.

4.6. **A further dissection of $L^{<}(x,\alpha,\xi,k)$.** We want to drop the multiplicative constraints $X_{1/2}\leq 2^ku_1u_2\leq X_\alpha$ and control the order of magnitude of u_1 and u_2, so we denote by $\boldsymbol{U}=(U_1,U_2)$ any couple of integers taken in the sequence 1, 2, 4, 8, 16, ... and satisfying the extra conditions

$$U_1<U_2,\ \text{and}\ X_{1/2}\leq 2^kU_1U_2\leq X_\alpha/4. \qquad (43)$$

The notation $n \sim N$ means that the variable n must satisfy the inequality $N < n \leq 2N$. Later on, we will have to control the congruence classes of u_1 and u_2 modulo 4^k, so we denote by ξ_1 and ξ_2 any congruence classes modulo 4^k, satisfying $(\xi_1\xi_2, 4^k) = 1$. The following inequality is straightforward

$$L^{<}(x,\alpha,\xi,k) \geq \sum_{\boldsymbol{U}} \sum_{\xi_1} \sum_{\xi_2} L(x,\alpha,\boldsymbol{U},\xi,\xi_1,\xi_2,k), \tag{44}$$

where
- the summation is over all $\boldsymbol{U} = (U_1, U_2)$ satisfying (43),
- the summation is over all ξ_1 and ξ_2 mod 4^k satisfying $(\xi_1\xi_2, 4^k) = 1$,
- we have defined

$$L(x,\alpha,\boldsymbol{U},\xi,\xi_1,\xi_2,k) := \sum_{\substack{u_1,\ u_2\\ u_1\sim U_1,\ u_2\sim U_2\\ u_1\equiv\xi_1,\ u_2\equiv\xi_2 \bmod 4^k\\ (u_1u_2,2)=1}} \sum_{\substack{t\equiv\Phi(u_1,u_2) \bmod u_1^2u_2^2\\ t\equiv\xi \bmod 4^k\\ Y_2(2^ku_1u_2)\leq t\leq Y_3(2^ku_1u_2)}} 1. \tag{45}$$

Of course the condition $(u_1u_2, 2) = 1$ can be dropped when $k \geq 1$. The parameter α is supposed to be fixed and the congruence conditions modulo 4^k are harmless. So to shorten the notations, we write

$$L(x,\boldsymbol{U}) := L(x,\alpha,\boldsymbol{U},\xi,\xi_1,\xi_2,k). \tag{46}$$

The coprimality condition $(u_1, u_2) = 1$ is implicitly supposed in all the computations below. Finally we shall not precise the dependence on k of some O–symbols, since we shall work with a finite number of values of k (see (103) and Proposition **??** below). The case $k = 0$ is typical and really reflects the difficulties of the method.

5. Expansion in Fourier series

5.1. **Reduction of a congruence.** First, we study the congruence conditions appearing in the last sum of (45). In particular, this congruence implies that, necessarily the integer t is congruent to -1 mod u_2^2, hence it has the shape $t = -1 + \ell u_2^2$, where ℓ is some integer (see the definition of Φ in Lemma 2). It must also belong to the interval $]Y_2(2^ku_1u_2), Y_3(2^ku_1u_2)]$. However the definitions of Y_2 and Y_3 imply that there is no such t when u_2 is too large, for instance when $u_2^2 > \big(4^kxu_1^2u_2^2 + 1\big)^{\frac{1}{2}} + 1$. Hence we can suppose

$$U_2 \leq 2^{k+2}x^{\frac{1}{2}}U_1, \tag{47}$$

otherwise $L(x, \boldsymbol{U}) = 0$.

Since u_1u_2 is odd, we deduce from (41) the equivalence

$$t \equiv \Phi(u_1,u_2) \bmod u_1^2u_2^2 \text{ and } t \equiv \xi \bmod 4^k \iff t \equiv t_0 \bmod 4^ku_1^2u_2^2, \tag{48}$$

where

$$t_0 := \xi\, u_1^2u_2^2 \cdot \big(\overline{u_1}^2\overline{u_2}^2\big)_{\bmod 4^k} + \Big(2\big(\overline{u_2}^2\big)_{\bmod u_1^2}u_2^2 - 1\Big)4^k \cdot \big(\overline{4^k}\big)_{\bmod u_1^2u_2^2} \bmod 4^ku_1^2u_2^2. \tag{49}$$

Modulo 1, this congruence implies the equality

$$\frac{t_0}{4^k u_1^2 u_2^2} = \frac{\xi \overline{u_1}^2 \overline{u_2}^2}{4^k} + \frac{\overline{4^k}\,\big(2\,\overline{u_2}^2 u_2^2 - 1\big)}{u_1^2 u_2^2}$$

$$= \kappa - \frac{1}{4^k u_1^2 u_2^2} + 2\frac{\overline{4^k}\,\overline{u_2}^2}{u_1^2} \bmod 1, \tag{50}$$

with

$$\kappa := \frac{(\xi+1)\overline{\xi_1}^2 \overline{\xi_2}^2}{4^k}.$$

In the proof of (50), we used Bézout's relation

$$\frac{1}{ab} = \frac{\overline{a}}{b} + \frac{\overline{b}}{a} \bmod 1,$$

for coprime integers a and b and the fact that $u_i \equiv \xi_i \bmod 4^k$ (see the conditions in (45)). The three terms in the right part of (50) have completely different structures: the first one is constant, the second one oscillates very slowly when u_1 and u_2 vary, the third one has a deep arithmetic meaning and it oscillates a lot when u_2 varies. Our project is to benefit from this chaotic behaviour via the theory of exponential sums.

5.2. **The smooth function.** The last sum in (45) counts the number of integers of an arithmetic progression lying in an interval. We want to avoid the crude formula

$$\sum_{\substack{t \equiv t_0 \bmod 4^k u_1^2 u_2^2 \\ Y_2(2^k u_1 u_2) \le t \le Y_3(2^k u_1 u_2)}} 1 = \frac{Y_3(2^k u_1 u_2) - Y_2(2^k u_1 u_2)}{4^k u_1^2 u_2^2} + O(1), \tag{51}$$

by appealing to Fourier techniques to obtain cancellation from the summation over u_2 via the explicit expression of t_0 contained in (50). However our pretension is only to give a lower bound of $L(x, \boldsymbol{U})$, so we gain in efficiency by introducing a smooth function which plays the role of a lower bound of the characteristic function $\mathbf{1}_{[Y_2,Y_3]}$ of the interval $[Y_2, Y_3]$. To do so, we recall two standard tools of analytic number theory.

Lemma 3. *For every $\delta > 0$ there exists a $\mathcal{C}^\infty$–function $g : \mathbb{R} \to \mathbb{R}$, which has the two properties*

$$0 \le g \le \mathbf{1}_{[-1/2,1/2]},$$

and

$$\int_{-\infty}^{\infty} g(y)\,\mathrm{d}y = 1 - \delta.$$

It is well known that the Fourier coefficients $\hat{g}(u)$, defined by

$$\hat{g}(u) := \int_{-\infty}^{\infty} g(y) e(-uy)\,\mathrm{d}y,$$

go to 0 very quickly as $u \to \infty$, since, for every $n \ge 0$ we have

$$\hat{g}(u) = O_n(|u|^{-n}), \tag{52}$$

uniformly for $|u| \ge 1$.

Let $m_0 \in \mathbb{R}$ and $L_0 > 0$. The function

$$f_{m_0,L_0}(y) := g\Big(\frac{y - m_0}{L_0}\Big),$$

will appear as a good approximation from below of the characteristic function of the interval $\Big[m_0 - \frac{L_0}{2}, m_0 + \frac{L_0}{2}\Big]$. We now write a Poisson summation formula for the function f.

Lemma 4. *Let m_0 and L_0 as above and let $f = f_{m_0,L_0}$ be the corresponding function. Then for every integers a and q with $q \geq 1$, one has the equality*

$$\sum_{m \equiv a \bmod q} f(m) = \frac{L_0}{q} \sum_h e\Big(h \cdot \frac{a - m_0}{q}\Big)\, \hat{g}\Big(h \cdot \frac{L_0}{q}\Big).$$

For the rest of the paper, $\delta > 0$ is fixed, so is the function g which satisfies Lemma 3. We choose

$$m_0 := \frac{1}{2}(Y_2 + Y_3),\ L_0 := Y_3 - Y_2,\ q = 4^k u_1^2 u_2^2 \text{ and } a := t_0,$$

where t_0 is defined in (49). Turning our attention to the last sum in the right part of (45), we use (50) and apply Lemmas 3 and 4 to get the inequality

$$\sum_t 1 \geq \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} \sum_h e\Big(h \cdot \Big[\kappa - \frac{1}{4^k u_1^2 u_2^2} + 2\frac{\overline{4^k}\,\overline{u_2}^2}{u_1^2} - \frac{Y_2 + Y_3}{2 \cdot 4^k u_1^2 u_2^2}\Big]\Big)\hat{g}\Big(h . \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}\Big). \tag{53}$$

For $h = 0$ we recognize the main term

$$\mathrm{MT}(u_1, u_2) := (1 - \delta)\, \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}. \tag{54}$$

We now want to transform the series appearing in (53) into a finite sum by appealing to the property (52). Let ε be a small positive number and define

$$H = H(\boldsymbol{U}) := U_1 U_2 x^{-\frac{1}{2} + \varepsilon}. \tag{55}$$

If $x > x_0(\varepsilon, k)$, we have $H \geq 1$, as a consequence of (43). For $|h| \geq H$, one has the inequality the inequality

$$\Big|\hat{g}\Big(h . \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}\Big)\Big| \ll \Big(\frac{|h| \cdot u_1 u_2 x^{\frac{1}{2}}}{2^k u_1^2 u_2^2}\Big)^{-n} \ll \Big(\frac{|h|}{H} x^{\varepsilon}\Big)^{-2} (x^{\varepsilon})^{-(n-2)},$$

where n is an arbitrary positive integer. Choosing n very large, we see that the contribution of the terms with $|h| \geq H$ in (53), is in $O(x^{-10})$. It is now time to condense notations. Let

$$G(h, y, u_1, u_2) := g(y)\, \frac{Y_3 - Y_2}{4^k\, u_1^2 u_2^2}\, e\Big(-h \frac{2 + Y_2 + Y_3}{2 \cdot 4^k u_1^2 u_2^2}\Big)\, e\Big(-hy \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}\Big).$$

Recall that Y_2 and Y_3 are functions of u_1 and u_2 and are defined by

$$Y_2 = Y_2(2^k u_1 u_2, \alpha) \text{ and } Y_3 = Y_3(2^k u_1 u_2), \tag{56}$$

(see (14) and (15)). With the above discussion, we write (53) as

$$\sum_t 1 \geq \mathrm{MT}(u_1, u_2) + \int_{-\infty}^{\infty} \sum_{1 \leq |h| \leq H} G(h, y, u_1, u_2) e(h\kappa) e\Big(2h \frac{\overline{4^k}\,\overline{u_2}^2}{u_1^2}\Big)\, \mathrm{d}y + O(x^{-10}). \tag{57}$$

Our aim in to obtain cancellation from the summation over u_2, so we carry (57) into (45) and (46) to write the inequality

$$L(x, \boldsymbol{U}) \geq (1 - \delta)\, \mathrm{EMT}(x, \boldsymbol{U}) + \mathrm{Err}(x, \boldsymbol{U}) + O(1), \tag{58}$$

where $\mathrm{EMT}(x,\boldsymbol{U})$ is the expected main term (see (54))

$$\mathrm{EMT}(x,\boldsymbol{U}) := \sum_{\substack{u_1,\ u_2\\ u_1\sim U_1,\ u_2\sim U_2\\ u_1\equiv\xi_1,\ u_2\equiv\xi_2 \bmod 4^k\\ (u_1u_2,2)=1}} \frac{Y_3-Y_2}{4^k u_1^2u_2^2},$$

where the error term is

(59)
$$\mathrm{Err}(x,\boldsymbol{U}) := \int_{-\infty}^{\infty} \sum_{1\le|h|\le H} e(h\kappa) \sum_{\substack{u_1,\ u_2\\ u_1\sim U_1,\ u_2\sim U_2\\ u_1\equiv\xi_1,\ u_2\equiv\xi_2 \bmod 4^k\\ (u_1u_2,2)=1}} G(h,y,u_1,u_2)e\Big(2h\frac{\overline{4^k}\,\overline{u_2}^2}{u_1^2}\Big)\,\mathrm{d}y.$$

We now simplify $\mathrm{Err}(x,\boldsymbol{U})$ by Abel summation over the variables u_1 and u_2. As a consequence of (14) and (16), we have

$$\frac{\partial^{\varepsilon_1+\varepsilon_2}}{\partial^{\varepsilon_1}u_1\partial^{\varepsilon_2}u_2}G(h,y,u_1,u_2) \ll x^{\frac12+\varepsilon}U_1^{-1}U_2^{-1}\left(x^{3\varepsilon}U_1^{-1}\right)^{\varepsilon_1}\left(x^{3\varepsilon}U_2^{-1}\right)^{\varepsilon_2},$$

for $\varepsilon_1,\varepsilon_2=0$ or 1, uniformly for $1\le|h|\le H$ and $y\in\mathbb{R}$. From these inequalities, we deduce the existence of U_1^* and U_2^*, satisfying $U_1\le U_1^*\le 2U_1$ and $U_2\le U_2^*\le 2U_2$, such that we have

$$\mathrm{Err}(x,\boldsymbol{U}) \ll \frac{x^{\frac12+6\varepsilon}}{U_1U_2}\left|\sum_{1\le|h|\le H} e(h\kappa) \sum_{\substack{u_1\\ U_1<u_1\le U_1^*,\ U_2<u_2\le U_2^*\\ u_1\equiv\xi_1,\ u_2\equiv\xi_2 \bmod 4^k\\ (u_1u_2,2)=1}}\ \sum_{u_2} e\Big(2h\frac{\overline{4^k}\,\overline{u_2}^2}{u_1^2}\Big)\right|. \tag{60}$$

So, after a multiplicative shift $2H\mapsto H$, we are led to consider the more general triple exponential sum

$$\mathfrak{V}(H,U_1,U_2,k) := \sum_{1\le|h|\le H}\alpha_h \sum_{u_1\sim U_1}\beta_{u_1} \sum_{U_2<u_2\le U_2^*}{}^{\dagger} e\Big(h\frac{\overline{4^k}\overline{u_2}^2}{u_1^2}\Big), \tag{61}$$

where

- H, U_1 and $U_2\ge1$, $U_2\le U_2^*\le 2U_2$, k is an integer ≥0,
- α_h is some complex coefficient, satisfying $|\alpha_h|\le1$ and $h\equiv h' \bmod 2\cdot4^k \Rightarrow \alpha_h=\alpha_{h'}$,
- β_{u_1} is some complex coefficient, satisfying $|\beta_{u_1}|\le1$ and $2\mid u_1\Rightarrow\beta_{u_1}=0$,
- the †–symbol means that the summation over u_2 is restricted to some fixed congruence class $u_2\equiv\xi_2 \bmod 4^k$ with ξ_2 odd if $k\ge1$, or $u_2\equiv1 \bmod 2$ if $k=0$ (see (59)). In the notation, it is useless to specify the value of ξ_2 and to recall the dependence on U_2^*. Of course the most typical cases are $k=0$ and $U_2^*=2U_2$, and the trivial bound is

$$\mathfrak{V}(H,U_1,U_2,k)\ll HU_1U_2.$$

We want to know under which conditions, we have

$$\mathfrak{V}(H,U_1,U_2,k)\ll U_1U_2x^{-7\varepsilon}, \tag{62}$$

for H as in (55). When (62) is satisfied, we deduce from (60) the inequality $\mathrm{Err}(x,\boldsymbol{U})\ll x^{\frac12-\varepsilon}$, which shows that $\mathrm{Err}(x,\boldsymbol{U})$ really behaves as an error term in (58).

In the next section, we give general results on some related exponential sums leading to sufficient conditions to ensure the veracity of (62).

6. Exponential sums

The purpose of this section is to give a description as accurate as possible of the exponential sum $\sum_{u_2\sim U_2} e(h\overline{u_2}^2/u_1^2)$, which appears to be central in our proof.

6.1. **The complete exponential sum.** Let $h\neq 0$, $k\geq 0$ and $n\geq 1$ be three integers with odd n. Let $\Sigma(h;n^2,k)$ be the complete sum

$$\Sigma(h;n^2,k):=\begin{cases}\displaystyle\sum_{\substack{m \bmod 4^k n^2\\(m,n)=1}}^{\dagger} e\Big(h\frac{\overline{m}^2}{n^2}\Big), & \text{if } k\geq 1,\\[2ex] \displaystyle\sum_{\substack{m \bmod 2n^2\\(m,n)=1}}^{\dagger} e\Big(h\frac{\overline{m}^2}{n^2}\Big), & \text{if } k=0.\end{cases}$$

The †–symbol indicates the same restriction of summation for the variable m as for the variable u_2 in the definition (61). Let also $\Sigma(h;n^2)$ be defined by

$$\Sigma(h;n^2):=\sum_{\substack{m \bmod n^2\\(m,n)=1}} e\Big(h\frac{\overline{m}^2}{n^2}\Big).$$

The Chinese Remainder Theorem directly gives

Lemma 5. *For every h, for every $k\geq 0$ and for every positive odd n, one has the equality*

$$\Sigma(h;n^2,k)=\Sigma(h;n^2).$$

Thus, the congruence condition modulo 4^k or 2 induced by the †–symbol is momentarily forgotten. We are now searching for a practical expression of $\Sigma(h;n^2)$. We first use the bijection $n\mapsto\overline{n}$. Thus the sum $\Sigma(h;n^2)$ is transformed into the reduced Gaussian sum

$$\Sigma(h;n^2)=\sum_{\substack{m \bmod n^2\\(m,n)=1}} e\Big(h\frac{m^2}{n^2}\Big),$$

which appears as a subsum of the classical Gauss sum $G(h;n^2)$ where

$$G(h;n):=\sum_{m \bmod n} e\Big(h\frac{m^2}{n}\Big).$$

We now recall some classical formulas for $G(h;n)$ (see [9, Chap.7.5, p.162–169] for instance). The first one is

$$G(h;n_1n_2)=G(hn_2;n_1)G(hn_1;n_2) \text{ when } (n_1,n_2)=1.$$

In particular, after a linear change of variables, under the same conditions we have

$$G(h;n_1^2n_2^2)=G(h;n_1^2)G(h;n_2^2). \tag{63}$$

For $(2h, n) = 1$, we also have

$$G(h;n) = \begin{cases} \left(\frac{h}{n}\right)\sqrt{n} & \text{if } n \equiv 1 \bmod 4, \\ i\left(\frac{h}{n}\right)\sqrt{n} & \text{if } n \equiv 3 \bmod 4, \end{cases}$$

and finally

$$G(h;p^\ell) = (h,p^\ell)\, G\Big(\frac{h}{(h,p^\ell)}; \frac{p^\ell}{(h,p^\ell)}\Big). \tag{64}$$

We decompose $n := p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, with distinct p_i and $\alpha_i \geq 1$. By the Chinese Remainder Theorem and a linear change of variables, we obtain the equality

$$\Sigma(h;n^2) = \prod_{i=1}^{k} \Sigma(h;p_i^{2\alpha_i}), \tag{65}$$

which is an analogue of (63). By the exclusion principle, we have

$$\Sigma(h;p^{2\ell}) = G(h;p^{2\ell}) - \sum_{m'=1}^{p^{2\ell-1}} e\Big(h\frac{(pm')^2}{p^{2\ell}}\Big),$$

which is

$$\Sigma(h;p^{2\ell}) = G(h;p^{2\ell}) - p\, G(h;p^{2\ell-2}). \tag{66}$$

In particular, the above formulas give the equality

$$\Sigma(h;p^{2\ell}) = 0, \text{ when } p \nmid 2h \text{ and } \ell \geq 1.$$

By (65) we deduce that

$$\Sigma(h;n^2) = 0 \text{ if there exists } p \text{ such that } p \mid n \text{ and } p \nmid 2h.$$

It remains to study the cases corresponding to $2 \nmid n$ and $n \mid h^\infty$. Let p odd and t be such that $p^t \| h$. This implies that $(h, p^{2\ell}) = p^t$ or $p^{2\ell}$. By (64) and (66), we have the equalities

$$\Sigma(h;p^{2\ell}) = \begin{cases} p^t\left(\frac{hp^{-t}}{p^{2\ell-t}}\right)G(1;p^{2\ell-t}) - p^{1+t}\left(\frac{hp^{-t}}{p^{2\ell-2-t}}\right)G(1;p^{2\ell-2-t}) & \text{if } t < 2\ell-2, \\ p^t\left(\frac{hp^{-t}}{p^{2\ell-t}}\right)G(1;p^{2\ell-t}) - p^{2\ell-1} & \text{if } 2\ell-2 \leq t < 2\ell, \\ p^{2\ell-1}(p-1) & \text{if } t \geq 2\ell. \end{cases} \tag{67}$$

For $t = 0$, we recover the fact that $\Sigma(h;p^{2\ell}) = 0$. We now simplify (67) as follows

$$\Sigma(h;p^{2\ell}) = \begin{cases} 0 & \text{for } t \leq 2\ell-2, \\ p^{2\ell-1}\left(\frac{hp^{-t}}{p}\right)G(1;p) - p^{2\ell-1} & \text{for } t = 2\ell-1, \\ p^{2\ell-1}(p-1) & \text{for } t \geq 2\ell. \end{cases} \tag{68}$$

To use (65), we recall the definition of the kernel $\kappa(n)$ of an integer $n \geq 1$

$$\kappa(n) := \prod_{p|n} p,$$

and introduce the following arithmetical function $\gamma(m;n)$ defined, for $m \neq 0$ and odd $n \geq 1$ by the formula (ℓ is an integer ≥ 1)

$$\gamma(m;n) = \prod_{\substack{p^\ell \| n \\ p^{2\ell-1} \| m}} \Big(p^{2\ell-1} \Big(\frac{mp^{-2\ell+1}}{p} \Big) G(1;p) - p^{2\ell-1} \Big) \prod_{\substack{p^\ell \| n \\ p^{2\ell} | m}} p^{2\ell-1}(p-1). \tag{69}$$

Remark that, for any integer a such that $(a,n)=1$, one has the equality

$$\gamma(m;n) = \gamma(a^2 m;n). \tag{70}$$

From (65), (68) and (69), we deduce

Lemma 6. *For every odd n and for every non zero h, one has the equality*

$$\Sigma(h;n^2) = \begin{cases} 0 & \text{for } \big(n^2/\kappa(n)\big) \nmid h, \\ \\ \gamma(h;n) & \text{otherwise.} \end{cases} \tag{71}$$

6.2. **The incomplete exponential sum.** We want to generalize the content of the above subsection, to the exponential sum

$$\Sigma(\mathcal{I},h;n^2,k) := \sum_{\substack{m\in\mathcal{I} \\ (m,n)=1}}^{\dagger} e\Big(h\frac{\overline{m}^2}{n^2}\Big) = \sum_{\substack{m\in\mathcal{I} \\ (m,2n)=1}}^{\dagger} e\Big(h\frac{\overline{m}^2}{n^2}\Big),$$

where $\mathcal{I}$ is an interval included in $[0,4^k n^2[$ if $k \geq 1$, or in $[0,2n^2[$ if $k=0$. As usual, h is an integer and n an odd positive integer. We shall only work on the case $k \geq 1$, since the case $k=0$ is totally similar after slight modifications. We write the characteristic function of the set $\{m\,;\ m \in \mathcal{I},\, m \text{ satisfies } \dagger\}$ under the form

$$\frac{1}{4^k n^2} \sum_{\ell=1}^{4^k n^2} \sum_{u\in\mathcal{I}}{}^{\dagger} e\Big(\frac{\ell(m-u)}{4^k n^2}\Big).$$

This gives the equality

$$\Sigma(\mathcal{I},h;n^2,k) = \frac{1}{4^k n^2} \sum_{\ell=1}^{4^k n^2} \sum_{u\in\mathcal{I}}{}^{\dagger} e\Big(-\ell\frac{u}{4^k n^2}\Big) \mathfrak{S}(4^k h,\ell;4^k n^2), \tag{72}$$

with

$$\mathfrak{S}(h,\ell;n^2) := \sum_{\substack{m \bmod n^2 \\ (m,n)=1}} e\Big(\frac{h\overline{m}^2 + \ell m}{n^2}\Big).$$

Since $\mathfrak{S}(h,\ell;n^2) = \mathfrak{S}(h,-\ell;n)$, we shall use (72) under the form

$$|\Sigma(\mathcal{I},h;n^2,k)| \leq |\Sigma(4^k h;4^k n^2)| + O\Big(\sum_{\ell=1}^{(4^k n^2)/2} \frac{1}{\ell} |\mathfrak{S}(4^k h,\ell;4^k n^2)| \Big). \tag{73}$$

Write $\mathfrak{S}(h,\ell;n^2)$ under the form

$$\mathfrak{S}(h,\ell;n^2) := \sum_{\substack{m \bmod n^2\\(m,n)=1}} e\Big(\frac{hm^2+\ell\overline{m}}{n^2}\Big).$$

If $n = p_1^{\alpha_1}\cdots p_t^{\alpha_t}$ with distinct odd p_i, we see that the Chinese Remainder Theorem gives the inequality

$$\Big|\,\mathfrak{S}(4^k h,\ell;4^k n^2)\,\Big| \le 4^k \Big|\prod_{i=1}^{t}\mathfrak{S}\Big(\overline{16}^k\, h\,\overline{(n/p_i^{\alpha_i})}^2, \ell\,\overline{(n/p_i^{\alpha_i})}^2; p_i^{2\alpha_i}\Big)\,\Big|. \tag{74}$$

Hence, we are reduced to study $\mathfrak{S}(a,b;p^{2\alpha})$, for an odd p, for integers a and b and $\alpha \ge 1$. We write $\mathfrak{S}(a,b;p^{2\alpha})$ under the form

$$\mathfrak{S}(a,b;p^{2\alpha}) = \sum_{\substack{s=0\\(s,p)=1}}^{p^\alpha-1}\sum_{t=0}^{p^\alpha-1} e\Big(\frac{a\,(s+tp^\alpha)^2 + b\,\overline{(s+tp^\alpha)}}{p^{2\alpha}}\Big). \tag{75}$$

We now appeal to the following formula which reduces the expression of the inverse modulo p^k when $k \ge 2$.

Lemma 7. *(see* [3, Lemma 1]*) Let m and n be integers such that*

$$\frac{1}{2}m \le n < m,$$

s and p such that $p \nmid s$. Then we have the following equality, where all the inverses are taken modulo p^m

$$\overline{s+p^n t} \equiv \overline{s} - p^n\, t\, \overline{s}^2 \bmod p^m.$$

This lemma simplifies (75) into

$$\mathfrak{S}(a,b;p^{2\alpha}) = \sum_{\substack{s=1\\(s,p)=1}}^{p^\alpha-1} e\Big(\frac{as^2+b\overline{s}}{p^{2\alpha}}\Big)\sum_{t=0}^{p^\alpha-1} e\Big(\frac{(2as-b\overline{s}^2)t}{p^\alpha}\Big). \tag{76}$$

The last sum of the above expression is 0 unless $p^\alpha \mid 2as - b\overline{s}^2$, in which case, its value is p^α. Remark that

$$2as - b\overline{s}^2 \equiv 0 \bmod p^\alpha \iff 2as^3 \equiv b \bmod p^\alpha.$$

Dividing both sides by (a,b,p^α), we see that this equation has less than $3(a,b,p^\alpha)$ solutions in $s \bmod p^\alpha$, with $p \nmid s$. Returning to (76), we get the inequality

$$\big|\mathfrak{S}(a,b;p^{2\alpha})\big| \le 3p^\alpha(a,b,p^\alpha),$$

and by the multiplicativity property (74), we obtain

Lemma 8. *For any odd n, for any integers a and b, one has the inequalities*

$$\big|\mathfrak{S}(a,b;n^2)\big| \le 3^{\omega(n)}\, n\,(a,b,n).$$

and

$$\big|\mathfrak{S}(a,b;4^k n^2)\big| \le 4^k\, 3^{\omega(n)}\, n\,(a,b,n).$$

As usual $\omega(n)$ is the number of distinct prime factors of n.

Coming back to (73), applying Lemma 8 and summing over ℓ, we deduce the inequality

$$|\Sigma(\mathcal{I},h;n^2,k)|\leq |\Sigma(4^kh;4^kn^2)|+O(n^{1+\varepsilon}), \tag{77}$$

for any interval $\mathcal{I}$ of length smaller than 4^kn^2. The following consequence of (65)

$$|\Sigma(4^kh;4^kn^2)|\leq 4^k|\Sigma(h;n^2)| \text{ if } 2\nmid n,$$

simplifies (77) into

$$|\Sigma(\mathcal{I},h;n^2,k)|\ll |\Sigma(h;n^2)|+n^{1+\varepsilon}, \tag{78}$$

6.3. **The final result.** Consider the general exponential sum

$$\Sigma=\Sigma(Y,Z,h;n^2,k):=\sum_{\substack{Y<m\leq Z\\(m,n)=1}}^{\dagger} e\Big(h\frac{\overline{m}^2}{n^2}\Big), \tag{79}$$

where the †–symbol is always defined in (61), n is an odd integer. We split the interval of summation in $\big[([Z]-[Y])/(4^kn^2)\big]$ intervals of length $L=4^kn^2$ when $k\geq 1$ and in $\big[([Z]-[Y])/(2n^2)\big]$ intervals of length $L=2n^2$ when when $k=0$ (as usual, $[y]$ is the integer part of the real number y). We then apply Lemmas 5 and 6 to each of the intervals of length L and (78) to the incomplete interval. So we obtain

Proposition 1. *Let Σ defined in (79). Then for every positive ε, for every integer $k\geq 1$, the following equality holds*

$$\Sigma=\begin{cases}\Big[\frac{[Z]-[Y]}{4^kn^2}\Big]\gamma(h;n)+O\big(|\gamma(h;n)|\big)+O(n^{1+\varepsilon}) & \text{if } \big(n^2/\kappa(n)\big)\mid h,\\ \\ O(n^{1+\varepsilon}) & \text{otherwise,}\end{cases}$$

uniformly for $Y\leq Z$, for any integer $h\neq 0$, for any odd and positive n. In the case where $k=0$, it suffices to replace 4^k by 2.

We stress the fact that, in the first case, we hope to benefit from oscillations of the coefficient γ, since it contains Jacobi symbols in its definition.

7. Application to $\mathfrak{U}(H,U_1,U_2,k)$

7.1. **A first approach.** We turn our attention to the sum $\mathfrak{U}(H,U_1,U_2,k)$ defined in (61). For simplicity, we only consider the case $k\geq 1$. We first start from the crude upper bound of the γ–function defined in (69):

$$|\gamma(m;n)|\leq n^2, \tag{80}$$

which is true for every non zero m and every odd n. We simplify the first case of Lemma 1 in writing

$$\Sigma=\frac{Z-Y}{4^kn^2}\gamma(h;n)+O(n^2) \text{ if } \big(n^2/\kappa(n)\big)\mid h.$$

By this remark, by (70) and by the second case of Proposition 1, we directly have the equality

$$\begin{aligned}\mho(H,U_1,U_2,k) &= 4^{-k}(U_2^*-U_2)\sum_{1\le|h|\le H}\alpha_h\sum_{\substack{u_1\sim U_1\\(u_1^2/\kappa(u_1))\mid h}}\beta_{u_1}\,u_1^{-2}\gamma(h;u_1)\\ &\quad+O\Big(\sum_{1\le|h|\le H}\sum_{\substack{u_1\sim U_1\\u_1^2\mid h\kappa(u_1)}}u_1^2\Big)\\ &\quad+O\Big(\sum_{1\le|h|\le H}\sum_{u_1\sim U_1}u_1^{1+\varepsilon}\Big)\\ &= 4^{-k}(U_2^*-U_2)\,E_1(H,U_1)+O(E_2(H,U_1))+O(E_3(H,U_1)),\end{aligned}\tag{81}$$

by definition. We trivially have

$$E_3(H,U_1)=O\big(H\,U_1^{2+\varepsilon}\big).\tag{82}$$

For the second term of (81), we sum over $\nu:=\kappa(u_1)$ and write $u_1:=\nu v_1$ with $v_1\mid\nu^\infty$. This gives the relation

$$E_2(H,U_1)\ll U_1^2\sum_{\nu}\sum_{\substack{v_1\mid\nu^\infty\\ \nu v_1\sim U_1}}\sum_{\substack{1\le|h|\le H\\ \nu v_1^2\mid h}}1,$$

which is

$$E_2(H,U_1)=O\big(HU_1^{2+\varepsilon}\big).\tag{83}$$

Firstly, we give a trivial upper bound of $E_1(H,U_1)$. By (80) and by a similar computation as leading to (83), we deduce the inequality

$$E_1(H,U_1)=O(H).\tag{84}$$

As written at the end of §5.2, we are searching for sufficient conditions to ensure that the inequality (62) holds. By (81), (82), (83), (84) and the definition (55), we deduce that (62) is satisfied when one has the inequalities

$$U_1\le x^{\frac14-5\varepsilon}\text{ and }U_2\le x^{\frac12-9\varepsilon}.\tag{85}$$

By (43), we see that these rather easy investigations give a non trivial lower bound on the function $L(x,\boldsymbol{U})$, for some choices of (U_1,U_2) up to $U_1U_2\le x^{\frac34-6\varepsilon}$. Thus the trivial bound $U_1U_2=x^{\frac12-\varepsilon}$ is passed.

7.2. **A precise upper bound.** Our purpose is to loosen the conditions (85) by a deeper study of the γ–function which takes into account the oscillations of the Jacobi symbol. We first elaborate a more practical form of the function γ. As above, we define $\nu:=\kappa(u_1)$ and write

$$u_1:=\nu v_1\text{ with }v_1\mid\nu^\infty.$$

The condition $(u_1^2/\kappa(u_1))\mid h$ is equivalent to the fact that h can be written as

$$h=\nu\,h'\,v_1^2.$$

Recall that u_1 is odd. With these conventions, we have the equality

$$\gamma(h;u_1)=\nu\,v_1^2\prod_{\substack{p\mid\nu\\ p\nmid h'}}\Big(\Big(\frac{h'\nu/p}{p}\Big)G(1;p)-1\Big)\prod_{\substack{p\mid\nu\\ p\mid h'}}(p-1),$$

and the first step is the equality

$$\gamma(h;u_1)=\nu\,v_1^2\,\varphi\big((h',\nu)\big)\prod_{\substack{p\mid\nu\\ p\nmid h'}}\Big(\Big(\frac{h'\nu/p}{p}\Big)G(1;p)-1\Big). \tag{86}$$

To simplify the notations, we define for any odd squarefree δ the function $G(\delta)$ by

$$G(\delta):=\delta^{\frac12}\Big(\prod_{\substack{p\mid\delta\\ p\equiv 3 \bmod 4}} i\Big)=\prod_{p\mid\delta}G(1;p). \tag{87}$$

With these remarks we expand (86) as

$$\gamma(h;u_1)=\nu\,v_1^2\,\varphi\big((h',\nu)\big)\sum_{\delta\mid\frac{\nu}{(\nu,h')}}\Big(\frac{h'}{\delta}\Big)\,G(\delta)\prod_{p\mid\delta}\Big(\frac{\nu/p}{p}\Big)\,\mu\Big(\frac{\nu}{(\nu,h')\delta}\Big).$$

Since ν is squarefree, we can simplify the μ–factor, and we also notice that if $\delta\mid\nu$ but $\delta\nmid\frac{\nu}{(\nu,h')}$ then we have $\Big(\frac{h'}{\delta}\Big)=0$. These remarks simplify the above formula into

$$\gamma(h;u_1)=\nu\,v_1^2\,\mu(\nu)\,\varphi\big((h',\nu)\big)\mu\big((h',\nu)\big)\sum_{\delta\mid\nu}\Big(\frac{h'}{\delta}\Big)\,G(\delta)\prod_{p\mid\delta}\Big(\frac{\nu/p}{p}\Big)\mu(\delta).$$

Then write

$$\nu:=\delta\eta,$$

and define, for every odd squarefree integer a, the function $\varpi(a)=\pm1$ by the formula

$$\varpi(a):=\prod_{p\mid a}\Big(\frac{a/p}{p}\Big),$$

to rewrite $\gamma(h;u_1)$ as

$$\gamma(h;u_1)=\nu\,v_1^2\,\mu(\nu)\,\varphi\big((h',\nu)\big)\mu\big((h',\nu)\big)\sum_{\delta\,\eta=\nu}\Big(\frac{h'}{\delta}\Big)\,G(\delta)\,\Big(\frac{\eta}{\delta}\Big)\varpi(\delta)\mu(\delta).$$

From this we deduce the following expression of $E_1(H,U_1)$ defined in (81)

$$\begin{aligned}E_1(H,U_1)=\sum_{\substack{\nu\\ 2\nmid\nu}}\nu^{-1}\mu(\nu)\sum_{\substack{v_1\mid\nu^\infty\\ \nu v_1\sim U_1}}\beta_{\nu v_1}\\ \sum_{1\le|h'|\le H/(\nu v_1^2)}\alpha_{\nu h' v_1^2}\,\varphi\big((h',\nu)\big)\,\mu\big((h',\nu)\big)\sum_{\delta\,\eta=\nu}\Big(\frac{h'}{\delta}\Big)\,G(\delta)\,\Big(\frac{\eta}{\delta}\Big)\varpi(\delta)\mu(\delta).\end{aligned} \tag{88}$$

We can always suppose that $(h',\delta)=1$, otherwise $\Big(\frac{h'}{\delta}\Big)=0$. This remark gives the equality $(h',\nu)=(h',\eta)$ and transforms (88) into

$$\begin{aligned}E_1(H,U_1)=\sum_{\delta}\delta^{-1}\varpi(\delta)\;G(\delta)\sum_{\eta}\eta^{-1}\,\mu(\eta)\,\mu^2(2\delta\eta)\Big(\frac{\eta}{\delta}\Big)\\ \sum_{\substack{v_1\mid(\delta\,\eta)^\infty\\ \delta\eta v_1\sim U_1}}\beta_{\delta\eta v_1}\sum_{1\le|h'|\le H/(\delta\eta v_1^2)}\alpha_{\delta\eta h' v_1^2}\,\varphi((\eta,h'))\,\mu((\eta,h'))\Big(\frac{h'}{\delta}\Big).\end{aligned} \tag{89}$$

To circumvent the difficulty of the g.c.d.(η,h'), we compose η into

$$\eta:=\eta_1\eta_2,$$

and impose $(\eta, h') = \eta_1$. This is equivalent to write

$$h' := \eta_1\lambda \text{ with } (\lambda, \eta_2) = 1.$$

With these conventions, we transform (89) in

$$E_1(H,U_1) = \sum_{\delta} \delta^{-1}\,\varpi(\delta)\,G(\delta) \sum_{\eta_1}\sum_{\eta_2} \eta_1^{-1}\eta_2^{-1}\,\mu^2(2\delta\eta_1\eta_2)\mu(\eta_2)\varphi(\eta_1)\Big(\frac{\eta_2}{\delta}\Big) \sum_{\substack{v_1\,|\,(\delta\eta_1\eta_2)^\infty\\ \delta\eta_1\eta_2 v_1\sim U_1}} \beta_{\delta\eta_1\eta_2 v_1} \sum_{\substack{1\le|\lambda|\le H/(\delta\eta_1^2\eta_2 v_1^2)\\ (\lambda,\eta_2)=1}} \alpha_{\delta\eta_1^2\eta_2\lambda v_1^2}\left(\frac{\lambda}{\delta}\right). \tag{90}$$

We now split the above sum into subsums where the congruence classes modulo 4^k of each of the five variables δ, η_1, η_2, v_1 and λ are fixed (this implies that, by hypothesis, the coefficient $\alpha_{\delta\eta_1^2\eta_2\lambda v_1^2}$ has a constant value). We also fix the order of magnitude of each variables by imposing

$$\eta_1 \sim Y_1,\ \eta_2 \sim Y_2,\ \delta \sim \Delta, v_1 \sim V_1,\ \lambda \sim L. \tag{91}$$

These orders of magnitude are constrained as follows

$$V_1Y_1Y_2\Delta \sim U_1,\ L \le \frac{H}{Y_1^2Y_2V_1^2\Delta}\ \Big(\asymp \frac{H}{Y_1U_1V_1} := L_0\Big). \tag{92}$$

This double splitting process gives the inequality

$$E_1(H,U_1) \ll (HU_1)^{\varepsilon}\,\mathcal{E}^*(L,V_1,Y_1,Y_2,\Delta), \tag{93}$$

for some (L,V_1,Y_1,Y_2,Δ) satisfying (92), and where we define

$$\mathcal{E}^*(L,V_1,Y_1,Y_2,\Delta) := \sum_{\delta}{}^*\delta^{-1}\,\varpi(\delta)\,G(\delta) \times \sum_{\eta_1}{}^*\sum_{\eta_2}{}^*\eta_1^{-1}\eta_2^{-1}\,\mu^2(2\delta\eta_1\eta_2)\mu(\eta_2)\varphi(\eta_1)\Big(\frac{\eta_2}{\delta}\Big) \sum_{\substack{v_1\,|\,(\delta\eta_1\eta_2)^\infty\\ \delta\eta_1\eta_2 v_1\sim U_1}}{}^* \beta_{\delta\eta_1\eta_2 v_1} \sum_{\substack{\lambda\le H/(\delta\eta_1^2\eta_2 v_1^2)\\ (\lambda,\eta_2)=1}}{}^* \left(\frac{\lambda}{\delta}\right), \tag{94}$$

where the variables are controlled (91) and where the upper *–symbol means that the involved variable must satisfy a congruence condition modulo 4^k, which is useless to specify.

We now want to separate the variable λ from the variables δ and v_1 in the inequality $\lambda \le H/(\delta\eta_1^2\eta_2 v_1^2)$, which still remains in the definition (94). To do so, we use the following form of Perron's formula (see [12, Lemma 1.1, p.131] for instance)

$$\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} y^s\frac{\mathrm{d}s}{s} = \begin{cases} 1 + O\big(\,y^{\sigma_0}\,T^{-1}(\log y)^{-1}\big) & \text{if } y>1,\\[2ex] O\big(\,y^{\sigma_0}\,T^{-1}(\log y\ )^{-1}\big) & \text{if } 0<y<1, \end{cases}$$

uniformly for $T \ge 1$, and $\sigma_0 > 0$. In our context, we can suppose that H is of the form $H = [H] + \frac{1}{2}$, and we fix $y := H/(\delta\eta_1^2\eta_2\lambda v_1^2)$. Hence, we always have $|\log y| \gg H^{-1}$. We choose

$$T := (HU_1)^{100} \text{ and } 0 < \sigma_0 \le \frac{1}{100}.$$

This transforms (94) into

$$\mathcal{E}^* = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\Big\{\sum_{\delta}{}^{*}\delta^{-1-s}\,\varpi(\delta)\,G(\delta)\sum_{\eta_1}{}^{*}\sum_{\eta_2}{}^{*}\eta_1^{-1-2s}\eta_2^{-1-s} \tag{95}$$
$$\times\mu^2(2\delta\eta_1\eta_2)\,\mu(\eta_2)\,\varphi(\eta_1)\Big(\frac{\eta_2}{\delta}\Big)\sum_{\substack{v_1\mid(\delta\eta_1\eta_2)^\infty\\ \delta\eta_1\eta_2 v_1\sim U_1}}{}^{*}\beta_{\delta\eta_1\eta_2 v_1}v_1^{-2s}\sum_{(\lambda,\eta_2)=1}^{*}\lambda^{-s}\left(\frac{\lambda}{\delta}\right)\Big\}H^s\frac{\mathrm{d}s}{s}+O(1),$$

where the variables continue to satisfy (91). After inverting summations, we have the equality

$$\mathcal{E}^* = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\Big\{\sum_{\eta_1}{}^{*}\sum_{\eta_2}{}^{*}\eta_1^{-1-2s}\eta_2^{-1-s}\mu(\eta_2)\varphi(\eta_1) \tag{96}$$
$$\sum_{(\lambda,\eta_2)=1}^{*}\sum_{\delta}{}^{*}\lambda^{-s}A(\delta,\eta_1,\eta_2,s)\left(\frac{\lambda}{\delta}\right)\Big\}H^s\frac{\mathrm{d}s}{s}+O(1),$$

where

$$A(\delta,\eta_1,\eta_2,s) = \delta^{-1-s}\,\varpi(\delta)\,G(\delta)\,\mu^2(2\delta\eta_1\eta_2)\,\Big(\frac{\eta_2}{\delta}\Big)\sum_{\substack{v_1\mid(\delta\eta_1\eta_2)^\infty\\ \delta\eta_1\eta_2 v_1\sim U_1}}{}^{*}\beta_{\delta\eta_1\eta_2 v_1}v_1^{-2s}. \tag{97}$$

Of course, the variables continue to satisfy (91). It is crucial to remark that in (96), the variables δ and λ simultaneously appear in the Jacobi symbol $\big(\frac{\lambda}{\delta}\big)$ only. So we are in good position to apply the following deep result of Heath–Brown (see [4, Corollary 4, p.238])

Lemma 9. *Let M, N be positive integers, and let $a_1,\dots a_M$ and $b_1,\dots,b_N$ be arbitrary complex numbers satisfying $|a_m|$, $|b_n|\leq 1$. Then, we have*

$$\sum_{m\leq M,\,2\nmid m}\sum_{n\leq N}a_m b_n\Big(\frac{n}{m}\Big)\ll_\varepsilon (MN)^{1+\varepsilon}(M^{-\frac12}+N^{-\frac12}),$$

for every positive ε.

To bound the function $A(\delta,\eta_1,\eta_2,s)$ we shall use the following classical lemma.

Lemma 10. *For every positive ε, one has the inequality*

$$\sum_{\substack{n\leq N\\ n\mid m^\infty}}1\ll_\varepsilon N^\varepsilon 2^{\omega(m)}.$$

Proof. It is an application of Rankin's method. For every $\varepsilon>0$, one has the inequalities

$$\sum_{\substack{n\leq N\\ n\mid m^\infty}}1\leq\sum_{n\mid m^\infty}\Big(\frac{N}{n}\Big)^\varepsilon = N^\varepsilon\prod_{p\mid m}\Big(1+\frac{1}{p^\varepsilon}+\frac{1}{p^{2\varepsilon}}+\cdots\Big)\ll N^\varepsilon\prod_{\substack{p\mid m\\ p^\varepsilon>2}}\Big(1-\frac{1}{p^\varepsilon}\Big)^{-1}.$$

□

By (87), (97) and Lemma 10, we get the inequality

$$A(\delta,\eta_1,\eta_2,s)\ll\Delta^{-\frac12}(HU_1)^\varepsilon,$$

uniformly over s, η_1 and η_2. By Lemma 9 and after an integration over s (with the choice $\sigma_0 = \varepsilon/10$), we get the inequality

$$\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{L,V_1,Y_1,Y_2,\Delta} \Big\{ Y_1\, \Delta^{-\frac12} \Big(L\ \Delta\big(\Delta^{-\frac12} + L^{-\frac12}\big)\Big)\Big\},$$

where the supremum is considered on the set of constraints (92). The above bound is an increasing function of L. So we have

$$\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{V_1,Y_1,Y_2,\Delta} \Big\{ Y_1\, \Delta^{-\frac12} \Big(L_0\ \Delta\big(\Delta^{-\frac12} + L_0^{-\frac12}\big)\Big)\Big\}.$$

Replacing L_0 by its value, we obtain the inequality

$$\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{V_1,Y_1,Y_2,\Delta} \Big\{ HU_1^{-1}V_1^{-1} + H^{\frac12}U_1^{-\frac12}V_1^{-\frac12}Y_1^{\frac12}\Delta^{\frac12}\Big\}.$$

We now insert the fact that $V_1Y_1Y_2\Delta \asymp U_1$ in order to simplify the above upper bound as

$$\begin{aligned}\mathcal{E}^* &\ll (HU_1)^{3\varepsilon} \sup_{Y_1,Y_2,V_1} \Big\{ HU_1^{-1}V_1^{-1} + H^{\frac12}V_1^{-1}Y_2^{-\frac12}\Big\}\\ &\ll \big(HU_1^{-1} + H^{\frac12}\big)\,(HU_1)^{3\varepsilon}. \qquad (98)\end{aligned}$$

Gathering (81), (82), (83), (93) and (98) we obtain the following

Proposition 2. *Let $\mathfrak{V}(H,U_1,U_2,k)$ defined as in (61). Then for every $\varepsilon > 0$, for every integer $k \geq 0$, one has the inequality*

$$\mathfrak{V}(H,U_1,U_2,k) \ll_{\varepsilon,k} (HU_1U_2)^{\varepsilon}\big(HU_1^{-1}U_2 + H^{\frac12}U_2 + HU_1^2\big),$$

uniformly for H, U_1 and $U_2 \geq 1$.

In particular, the inequality (62) holds, when H is defined by (55), as soon as the following inequalities hold

$$U_2 \leq x^{\frac12-10\varepsilon}U_1 \text{ and } U_1 \leq x^{\frac14-10\varepsilon}. \qquad (99)$$

This is a quite substantial improvement of (85). The first inequality of (99) is almost optimal when compared with (47). In our opinion, this is not the case of the second one. We conjecture that it should be replaced by $U_1 \leq U_2$, at least when α is slightly larger than $1/2$ (see the proof of the conditional Theorem 2 given in §10).

8. Proof of a weakened form of Theorem 1

As a consequence of Proposition 2, we have seen that the error term $\mathrm{Err}(x,\boldsymbol{U})$ (controlled by (60)) satisfies the inequality

$$\mathrm{Err}(x,\boldsymbol{U}) \ll x^{\frac12-\varepsilon}, \qquad (100)$$

as soon as (99) is satisfied. Gathering (38), (39), (42), (43), (44), (46), (58) and (100), we have proved that, for every ε and $\delta > 0$, for every $k_0 \geq 0$, and for sufficiently large x, the following inequality

$$\begin{aligned}L(x,\alpha) &\geq 2(1-\delta)\\ &\times \sum_{k=0}^{k_0} \sum_{\xi\in\mathcal{R}(2^k)} \sum_{\substack{\xi_1,\xi_2 \bmod 4^k\\ 2\nmid\xi_1\xi_2}} \sum_{U_1,\ U_2} \sum_{\substack{u_i\equiv\xi_i \bmod 4^k\\ u_i\sim U_i,\,(u_1,u_2)=(u_1u_2,2)=1}} \frac{Y_3-Y_2}{4^k u_1^2u_2^2} - O(x^{\frac12}),\end{aligned} \qquad (101)$$

holds provided that U_1 and U_2 are powers of 2, satisfying the inequalities

$$\frac{1}{2}x^{\frac12} < 2^k U_1U_2 < \frac{1}{8}x^\alpha,\ U_1 < U_2,\ U_2 \le x^{\frac12-\varepsilon}U_1 \text{ and } U_1 \le x^{\frac14-\varepsilon}.$$

We insert (21) under the form

$$Y_3 - Y_2 = Y_3(2^k u_1u_2) - Y_2(2^k u_1u_2, \alpha) = 2^k u_1u_2 x^{\frac12} + O((u_1u_2)^{1+\frac{1}{2\alpha}})). \tag{102}$$

The contribution of the error term in (102) to the right hand side of (101), is handled as in (22) and (25) and is in $O(x^{\frac12}\log x)$. Recalling the definition of $\rho(2^k) = \sharp\mathcal{R}(2^k)$, summing over all possible ξ_1 and ξ_2 modulo 4^k, and gluing the intervals $]U_i, 2U_i]$ back together, we get the inequality

$$L(x,\alpha) \ge 2(1-2\delta)\Big(\sum_{k=0}^{k_0}\frac{\rho(2^k)}{2^k}\Big)x^{\frac12} \sum_{\substack{u_1,\\ (u_1,u_2)=(u_1u_2,2)=1}}\sum_{u_2}\frac{1}{u_1u_2} - O(x^{\frac12}\log x), \tag{103}$$

where the integer variables u_1 and u_2 satisfy the inequalities

$$x^{\frac12} < u_1u_2 < x^\alpha,\ u_1 \le u_2,\ u_2 \le u_1x^{\frac12-\varepsilon} \text{ and } u_1 \le x^{\frac14-\varepsilon}.$$

In the proof of (103), we used the inequalities

$$\sum_{y\le u_1u_2\le Ay}\sum\frac{1}{u_1u_2} \ll_A \log 2y \text{ and } \sum_{\substack{u_1u_2\le y\\ u_1\le u_2\le Au_1}}\sum\frac{1}{u_1u_2} \ll_A \log 2y,$$

for any fixed constant $A \ge 1$. Appealing to (19), choosing $k_0 = k_0(\delta)$ very large and $\varepsilon = \varepsilon(\delta)$ very small and redefining the constant δ, the inequality (103) is simplified in

$$L(x,\alpha) \ge 8\,x^{\frac12} \sum_{\substack{u_1,\\ (u_1,u_2)=(u_1u_2,2)=1}}\sum_{u_2}\frac{1}{u_1u_2} - O(\delta x^{\frac12}\log^2 x) - O_\delta(x^{\frac12}\log x), \tag{104}$$

where the conditions of summation now are

$$x^{\frac12} < u_1u_2 < x^\alpha,\ u_1 \le u_2,\ u_2 \le u_1x^{\frac12} \text{ and } u_1 \le x^{\frac14}.$$

The inequality (104) is true for any positive δ and the corresponding region of summation can be written as

$$\big\{(u_1,u_2);\ u_1 \le x^{\frac14},\, x^{\frac12}u_1^{-1} \le u_2 \le \min\big(x^\alpha u_1^{-1}, x^{\frac12}u_1\big),\, (u_1,u_2) = (u_1u_2,2) = 1\big\}.$$

We now appeal to the classical

Lemma 11. *For any integer $m \ge 1$ and for any $y \ge 1$, one has the equality*

$$\sum_{\substack{n\le y\\ (m,n)=1}}\frac{1}{n} = \frac{\varphi(m)}{m}\log y + O\Big(1 + \sum_{d\mid m}\frac{\log d}{d}\Big).$$

Proof. By Möbius' inversion formula, one may write

$$\begin{aligned}\sum_{\substack{n\le y\\ (m,n)=1}}\frac{1}{n} &= \sum_{\substack{d\mid m\\ d\le y}}\mu(d)\sum_{n'\le y/d}\frac{1}{dn'}\\ &= \sum_{\substack{d\mid m\\ d\le y}}\frac{\mu(d)}{d}\big(\log(y/d) + O(1)\big).\end{aligned}$$

□

Lemma 11 combined with the inequality

$$\sum_{u_1\le x^{\frac14}}\frac{1}{u_1}\cdot\Big(1+\sum_{d\mid u_1}\frac{\log d}{d}\Big)\ll\log x,$$

transforms (104) in

$$L(x,\alpha)\ge 8x^{\frac12}\sum_{\substack{u_1\le x^{\frac14}\\ 2\nmid u_1}}\frac{\varphi(u_1)}{2u_1^2}\Big(\log\min\big(x^{\alpha-\frac12},u_1^2\big)\Big)\\ -O(\delta x^{\frac12}\log^2 x)-O_\delta(x^{\frac12}\log x). \tag{105}$$

We now appeal to a classical consequence of the theory of Dirichlet series.

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

$$\sum_{\substack{n\le y\\ 2\nmid y}}\frac{\varphi(n)}{n^2}\sim\frac{4}{\pi^2}\log y, \tag{106}$$

and

$$\sum_{\substack{n\le y\\ 2\nmid y}}\log n\frac{\varphi(n)}{n^2}\sim\frac{2}{\pi^2}\log^2 y. \tag{107}$$

Proof. For $\Re s>1$, consider the Dirichlet series

$$F(s):=\sum_{2\nmid n}\frac{\varphi(n)/n}{n^s}=\zeta(s)\Big(1-\frac{1}{2^s}\Big)\prod_{p\ge3}\Big(1-\frac{1}{p^{s+1}}\Big).$$

As $s\to1$, one has $F(s)\sim(4/\pi^2)(s-1)^{-1}$. By the Hardy–Littlewood–Karamata's Theorem (see [12, Theorem 8, p.227]), one deduces (106). Then (107) is obtained by Abel's summation. □

Returning to (105), one gets the inequality

$$L(x,\alpha)\ge 8\,x^{\frac12}\Big\{\sum_{\substack{u_1\le x^{\frac{\alpha}{2}-\frac14}\\ 2\nmid u_1}}\frac{\varphi(u_1)}{u_1^2}\log u_1\\ +(\alpha-\frac12)\log x\sum_{\substack{x^{\frac{\alpha}{2}-\frac14}<u_1\le x^{\frac14}\\ 2\nmid u_1}}\frac{\varphi(u_1)}{2u_1^2}\Big\}-O(\delta x^{\frac12}\log^2 x)-O_\delta(x^{\frac12}\log x). \tag{108}$$

The second sum on the right hand side of (108) is empty for $\alpha\ge1$. Lemma 12 now leads to the inequality

$$\begin{aligned}L(x,\alpha)&\ge 8\Big\{\frac{2}{\pi^2}\big(\frac{\alpha}{2}-\frac14\big)^2+\frac{2}{\pi^2}(\alpha-\frac12)(\frac12-\frac{\alpha}{2})-\delta\Big\}x^{\frac12}\log^2 x\\ &\ge\frac{1}{\pi^2}\Big((2\alpha-1)(3-2\alpha)-\delta\Big)x^{\frac12}\log^2 x,\end{aligned} \tag{109}$$

which holds for every $\delta>0$ and $x>x_0(\delta)$. It remains to take δ tending to 0 and insert the above lower bound in (33) and (34) to obtain the following inequality

$$S(x,\alpha)\ge\frac{1}{\pi^2}\big(1+(2\alpha-1)\,(3-2\alpha)-o(1)\big)x^{\frac12}\log^2 x, \tag{110}$$

uniformly for $\frac{1}{2} \leq \alpha \leq 1$. To pass from a lower bound of $S(x,\alpha)$ to a lower bound on $S^{\mathrm{f}}(x,\alpha)$ ($\alpha \leq 1$), we have to substract the cardinality of the set of (D,η_D) where η_D is of the shape $\eta_D = \varepsilon_D^2$. So we use (29) and appeal to (7) and (110) to deduce the following lower bound

$$S^{\mathrm{f}}(x,\alpha) \geq \frac{1}{\pi^2}\Big(1+(2\alpha-1)(\frac{13}{4}-\frac{5\alpha}{2})-o(1)\Big)x^{\frac{1}{2}}\log^2 x, \tag{111}$$

which is valid for $\frac{1}{2} \leq \alpha \leq 1$. However, the function $\alpha \mapsto (\alpha-\frac{1}{2})(\frac{13}{4}-\frac{5\alpha}{2})$ is decreasing for $\alpha > \frac{9}{10}$. Hence (111) is useful for $\frac{1}{2} \leq \alpha \leq \frac{9}{10}$ only.

In conclusion the inequalities (110) and (111) appear as a weakened form of Theorem 1. In particular, our next task will be to prove that (110) is actually satisfied by $S^{\mathrm{f}}(x,\alpha)$.

9. Proof of Theorem 1

The proof of Theorem 1 itself depends on a more elaborate study of the contribution of the non fondamental solutions. In other words, we shall prove that the non fundamental solutions create negligible subsets of $\mathcal{S}(x,\frac{1}{2},\alpha)$ and $\mathcal{L}(x,\alpha)$, defined in (31) and in (36).

We first prove

Lemma 13. *Uniformly for $1/2 \leq \alpha \leq 1$ and $x \geq 2$, one has*

$$S(x,\frac{1}{2},\alpha) - S^{\mathrm{f}}(x,\frac{1}{2},\alpha) = O(x^{\frac{1}{2}}\log x).$$

Proof. Let $\eta_D = t+u\sqrt{D}$ be a non fundamental solution, satisfying the inequalities $u \leq X_{1/2}$ and $\eta_D \leq D^{\frac{1}{2}+\alpha}$. Hence, for some positive integers t_0 and u_0, we have the equality

$$t+u\sqrt{D} = (t_0+u_0\sqrt{D})^2 = t_0^2+u_0^2D+2t_0u_0\sqrt{D}. \tag{112}$$

From this, we deduce the inequality $2 \leq 2t_0u_0 \leq X_{1/2} \leq x^{\frac{1}{2}}$. It is well know that the cardinality of such (t_0,u_0) is $O(x^{\frac{1}{2}}\log x)$. The same upper bound applies to the associated triples (t_0,u_0,D) and the investigated triples (t,u,D). □

To deal with the contribution of the non fundamental solutions to $L(x,\alpha)$, we exploit a pertinent remark of Hooley [8, p.108] describing the anatomy of ε_D^2, in particular the fact that the integer u_2 associated to ε_D^2 (see (42)) is very large, thus very close to the upper limit of the inequality (47). We now summarize what we proved in §4 and §8 without forgetting the least information as possible. To do so, we introduce the following set $\mathcal{Z}(x,\alpha,\varepsilon,k_0)$ of 5–uples of integers defined by

$$\begin{aligned}\mathcal{Z}(x,\alpha,\varepsilon,k_0) := \Big\{&(k,t,u_1,u_2,D)\,;\, 2\nmid u_1u_2,\ (u_1,u_2)=1,\ 0\leq k\leq k_0,\\ &D\leq x,\ X_{1/2}\leq 2^k u_1u_2\leq X_\alpha,\ t+2^ku_1u_2\sqrt{D}\leq D^{\frac{1}{2}+\alpha},\\ &t^2-1\equiv 0 \bmod 4^k,\ t\equiv 1 \bmod u_1^2,\ t\equiv -1 \bmod u_2^2,\ t^2-4^ku_1^2u_2^2D=1,\\ &(u_1\leq u_2\leq u_1x^{\frac{1}{2}-\varepsilon} \text{ and } u_1\leq x^{\frac{1}{4}-\varepsilon}) \text{ or } (u_2\leq u_1\leq u_2x^{\frac{1}{2}-\varepsilon} \text{ and } u_2\leq x^{\frac{1}{4}-\varepsilon})\Big\}.\end{aligned} \tag{113}$$

We also consider the subset $\mathcal{Z}^{\mathrm{f}}(x,\alpha,\varepsilon,k_0)$ where the 5–uples (k,t,u_1,u_2,D) satisfy the extra condition

$$t+2^ku_1u_2\sqrt{D} = \varepsilon_D.$$

The cardinalities are respectively denoted by $Z(x,\alpha,\varepsilon,k_0)$ and $Z^{\mathrm{f}}(x,\alpha,\varepsilon,k_0)$.

The arithmetical preparation made in §4 can be summarized in the following inequality

$$L(x,\alpha) \geq Z(x,\alpha,\varepsilon,k_0) \text{ and } L^{\mathrm{f}}(x,\alpha) \geq Z^{\mathrm{f}}(x,\alpha,\varepsilon,k_0) \tag{114}$$

which is true for every positive ε and for every $k_0 \geq 0$, (see (38), (39) and (42)).

By (103) and (109), we also have the following lower bound

$$Z(x,\alpha,\varepsilon,k_0) \geq \frac{1}{\pi^2}\big\{(2\alpha-1)(3-2\alpha)-\delta\big\}\, x^{\frac{1}{2}} \log^2 x, \tag{115}$$

which is true for every δ, for every $0 < \varepsilon < \varepsilon_0(\delta)$, $k_0 > k_0(\delta)$ and $x > x_0(\delta)$.

We now prove

Lemma 14. *For every integer $k_0 \geq 0$, for every $\varepsilon > 0$, one has*

$$Z(x,\alpha,\varepsilon,k_0) - Z^{\mathrm{f}}(x,\alpha,\varepsilon,k_0) = O_{\varepsilon,k_0}(x^{\frac{1}{2}} \log x),$$

uniformly for $\frac{1}{2} \leq \alpha \leq 1$ and $x \geq 2$.

Proof. Let $(k,t,u_1,u_2) \in \mathcal{Z}(x,\alpha,\varepsilon,k_0)$ such that

$$t + 2^k u_1 u_2 \sqrt{D} = \varepsilon_D^2 := (t_0 + u_0\sqrt{D})^2. \tag{116}$$

In particular we have

$$\varepsilon_D \leq D^{\frac{3}{4}}. \tag{117}$$

The relation (116) is equivalent to the two equalities

$$t = t_0^2 + Du_0^2 \text{ and } 2^{k-1} u_1 u_2 = t_0 u_0.$$

So we suppose $1 \leq k \leq k_0$. By the equality $t_0^2 - Du_0^2 = 1$, we deduce that

$$\text{either } \Big(2^{k-1} \| t_0 \text{ and } 2 \nmid u_0 \Big) \text{ or } \Big(2^{k-1} \| u_0 \text{ and } 2 \nmid t_0 \Big),$$

and we denote by $\tilde{t}_0$ and $\tilde{u}_0$ the greatest odd divisors of t_0 and u_0. We also have the equalities

$$\begin{cases} t = 1 + 2Du_0^2, \\ \\ t = -1 + 2t_0^2, \end{cases}$$

which imply the set of congruences

$$\begin{cases} t^2 & \equiv 1 \bmod 4^k, \\ t & \equiv 1 \bmod \tilde{u}_0^2, \\ t & \equiv -1 \bmod \tilde{t}_0^2. \end{cases}$$

Since $(\tilde{t}_0, \tilde{u}_0) = 1$, we recognize the congruences appearing in the definition of $\mathcal{Z}(k,\alpha,\varepsilon,k_0)$. In other words, we proved the equalities

$$\tilde{t}_0 = u_2 \text{ and } \tilde{u}_0 = u_1. \tag{118}$$

From the general inequality $u_0\sqrt{D} \leq t_0 \leq u_0\sqrt{D} + 1 < 2u_0\sqrt{D}$, we deduce the general inequality

$$2^{-k+1} \tilde{u}_1 \sqrt{D} \leq \tilde{u}_2 \leq 2^k \tilde{u}_1 \sqrt{D}. \tag{119}$$

We end the proof as follows.

• If $D \leq x(\log x)^{-2}$, by Theorem A and by (117), we know that the cardinality of the corresponding (ε_D, D) is $\ll (x(\log x)^{-2})^{\frac{1}{2}} \log^2 x \ll x^{\frac{1}{2}} (\log x)$.

• Now suppose $x(\log x)^{-2} \le D \le x$. In these circumstances, (119) implies that $u_2 \ge 2^{-k_0+1} u_1 x^{\frac12} (\log x)^{-1}$. If we choose $x \ge x_1(k_0, \varepsilon)$, this inequality is incompatible with the inequality $u_2 \le u_1 x^{\frac12 - \varepsilon}$ appearing in the definition of $\mathcal{Z}(k, \alpha, \varepsilon, k_0)$. □

9.1. **The final step.** We gather the relations (34), (114) to write the following inequality

$$\begin{aligned} S^{\mathrm{f}}(x,\alpha) &= S^{\mathrm{f}}(x,\frac12,\alpha) + L^{\mathrm{f}}(x,\alpha) \\ &\ge S(x,\frac12,\alpha) + Z(x,\alpha,\varepsilon,k_0) + \Big(S^{\mathrm{f}}(x,\frac12,\alpha) - S(x,\frac12,\alpha)\Big) \\ &\quad + \Big(Z^{\mathrm{f}}(x,\alpha,\varepsilon,k_0) - Z(x,\alpha,\varepsilon,k_0)\Big), \end{aligned}$$

which is true for every $\varepsilon > 0$ and every k_0. By (33), (115), Lemmas 13 & 14 and by choosing k_0 sufficiently large and ε sufficiently small, in terms of the parameter δ, we deduce the following inequality

$$S^{\mathrm{f}}(x,\alpha) \ge \frac{1-o(1)}{\pi^2} x^{\frac12} \log^2 x + \frac{1}{\pi^2}\big\{(2\alpha-1)(3-2\alpha) - \delta\big\} x^{\frac12} \log^2 x - O_\delta\big(x^{\frac12} \log x\big),$$

which is true for any positive δ. Letting δ tend to zero, we get (8).

The second inequality (9), of Theorem 1 is deduced from (8) by adding the contribution of the non fundamental solutions, as it is written in (29).

The proof of Theorem 1 is now complete.

10. Proof of Theorem 2

In that section we suppose the truth of Conjecture 1. We first prove an easy upper bound for the sum $\mho$ defined in (61).

Proposition 3. *Suppose that Conjecture 1, is true for some ϑ_0, satisfying $0 < \vartheta_0 < 1$. Then we have the inequality*

$$\mho(H, U_1, U_2, k) \ll_k H U_1 U_2^{\vartheta_0},$$

uniformly for $H \ge 1$ and $U_1 < U_2 \le U_1^2$.

Proof. By a direct application of Conjecture 1, we have

$$\mho(H, U_1, U_2, k) \ll U_2^{\vartheta_0} \sum_{1 \le |h| \le H} \sum_{u_1 \sim U_1} (h, u_1^2)^{\frac12}. \tag{120}$$

For $n \ge 1$, let $n^\ddagger$ be the integer defined by

$$n^\ddagger := \prod_{p^k \| n} p^{[\frac{k+1}{2}]}.$$

Summing over $\delta := (h, u_1^2)$, we have

$$\begin{aligned} \sum_{1 \le |h| \le H} \sum_{u_1 \sim U_1} (h, u_1^2)^{\frac12} &\le \sum_{\delta \le 4HU_1^2} \delta^{\frac12} \sum_{\substack{1 \le |h| \le H \\ \delta \mid h}} \sum_{\substack{u_1 \sim U_1 \\ \delta^\ddagger \mid u_1}} 1 \\ &\le 2HU_1 \sum_{\delta \le 4HU_1^2} \frac{1}{\delta^{\frac12} \delta^\ddagger} \\ &\ll HU_1. \end{aligned}$$

Inserting this bound in (120), we complete the proof of Proposition 3. □

We can now pass to the proof of Theorem 2 itself. We first remark that we have the inequality (62), that is

$$\mathfrak{V}(H,U_1,U_2,k)\ll U_1U_2x^{-7\varepsilon},$$

as soon as we have the inequalities

$$U_1<U_2<U_1^2,\ \text{and}\ U_1U_2^{\vartheta_0}\leq x^{\frac12-8\varepsilon}. \tag{121}$$

This is a direct consequence of Proposition 3. This implies that, under the assumption of Conjecture 1, the lower bound (104) is improved into

$$L(x,\alpha)\geq 8\,x^{\frac12}\sum_{\substack{u_1,\ u_2\\(u_1,u_2)=(u_1u_2,2)=1}}\sum\frac{1}{u_1u_2}-O(\delta x^{\frac12}\log^2x)-O_\delta(x^{\frac12}\log x), \tag{122}$$

where the conditions of summation are

$$x^{\frac12}<u_1u_2<x^\alpha\ \text{and}\ \begin{cases}u_1<u_2,\ u_2\leq u_1x^{\frac12}\ \text{and}\ u_1\leq x^{\frac14},\\ \text{or}\\ u_1<u_2<u_1^2\ \text{and}\ \ u_1<x^{\frac12}u_2^{-\vartheta_0}.\end{cases} \tag{123}$$

If we suppose the inequality

$$\frac12\leq\alpha\leq\min\Big(\frac34,\frac{1}{1+\vartheta_0}\Big), \tag{124}$$

by drawing a picture in the (u_1,u_2)–plane, we see that the domain of summation (123) is simplified into

$$x^{\frac12}<u_1u_2<x^\alpha,\ u_1<u_2\ \text{and}\ \ u_2\leq u_1x^{\frac12}. \tag{125}$$

After this simplification we can compute the right part of (122). Applying Lemma 11 and following the computation leading to (108), we have

$$\begin{aligned}L(x,\alpha)\geq 8\,x^{\frac12}\Bigg\{&\sum_{\substack{u_1\leq x^{\frac{\alpha}{2}-\frac14}\\2\nmid u_1}}\frac{\varphi(u_1)}{u_1^2}\log u_1+(\alpha-\frac12)\log x\sum_{\substack{x^{\frac{\alpha}{2}-\frac14}<u_1<x^{\frac14}\\2\nmid u_1}}\frac{\varphi(u_1)}{2u_1^2}\\&+\sum_{\substack{x^{\frac14}<u_1<x^{\frac{\alpha}{2}}\\2\nmid u_1}}\frac{\varphi(u_1)}{2u_1^2}\log(x^\alpha u_1^{-2})\Bigg\}-O(\delta x^{\frac12}\log^2x)-O_\delta(x^{\frac12}\log x).\end{aligned}$$

By Lemma 12, we obtain the inequality

$$\begin{aligned}L(x,\alpha)\geq 8x^{\frac12}\log^2x\Bigg\{&\frac{2}{\pi^2}\,\big(\frac{\alpha}{2}-\frac14\big)^2+\frac{2}{\pi^2}\,\big(\alpha-\frac12\big)\,\big(\frac12-\frac{\alpha}{2}\big)\\&+\frac{2}{\pi^2}\,\alpha\,\big(\frac{\alpha}{2}-\frac14\big)-\frac{2}{\pi^2}\,\Big(\big(\frac{\alpha}{2}\big)^2-\frac{1}{16}\Big)\Bigg\}-O(\delta x^{\frac12}\log^2x)-O_\delta(x^{\frac12}\log x).\end{aligned}$$

This gives the inequality

$$L(x,\alpha)\geq\frac{8}{\pi^2}(\frac{\alpha}{2}-\frac14)x^{\frac12}\log^2x-O(\delta x^{\frac12}\log^2x), \tag{126}$$

which is true under the condition (124), for every $\delta > 0$ and $x > x_0(\delta)$. The inequality (126) is a substantial improvement of (109). Actually, we also have the inequality

$$L^{\mathrm{f}}(x,\alpha) \geq \frac{8}{\pi^2}\big(\frac{\alpha}{2}-\frac{1}{4}\big)x^{\frac{1}{2}}\log^2 x - O(\delta x^{\frac{1}{2}}\log^2 x), \tag{127}$$

by the technique developed in §9. It is unnecessary to give all the details to describe the modifications. We only mention that the set $Z(x,\alpha,\varepsilon,k_0)$ is now defined by (113) by dropping the conditions $u_1 \leq x^{\frac{1}{4}-\varepsilon}$ and $u_2 \leq x^{\frac{1}{4}-\varepsilon}$.

The rest of the proof of Theorem 2 is similar to §9.1.

References

[1] H. Cohen, Sur la distribution asymptotique des groupes de classes, *C. R. Acad. Sci. Paris Sér. I Math.*, 296 : 245–247, 1983.

[2] H. Cohen and H.W. Lenstra, Heuristics on class groups of number fields. *in* Number Theory, Noordwijkerhout 1983. *Lecture Notes in Math.*, vol. 1068: 33–62, Springer, Berlin, 1984.

[3] D.R. Heath–Brown, A mean value estimate for real character sums, *Acta Arithm.*, 72 : 235–275, 1995.

[4] T. Estermann, On Kloosterman's sum, *Mathematika*, 8 : 83–86, 1960.

[5] E.P. Golubeva, The class numbers of real quadratic fields of discriminant $4p$, J. Math. Sci., 79 no. 5, 1277–1292, 1996.

[6] E.P. Golubeva, On the Pellian equation. J. Math. Sci., 122 no. 6, 3600–3602, 2004.

[7] C. Hooley, On the greatest prime factor of a cubic polynomial, *J. für reine Angew. Math.*, 303/304 : 921–50, 1978.

[8] C. Hooley, On the Pellian equation and the class number of indefinite binary quadratic forms, *J. für reine Angew. Math.*, 353 : 98–131, 1984.

[9] L.K. Hua, Introduction to Number Theory. *Springer Verlag*, Berlin Heidelberg New York, 1982.

[10] P. Sarnak, Class numbers of indefinite binary quadratic forms. II, *J. Number Theory*, 21 : 333–346, 1985.

[11] P. Sarnak, Reciprocal geodesics. *Analytic Number Theory. Clay Math. Proc.*, American Math. Soc., Providence, R.I., vol. 7 : 217–237, 2007.

[12] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory. *Cambridge Studies in Advanced mathematics* vol. 46. C.U.P., 1995.

[13] A.Weil, Number Theory: An Approach through History, *Birkhaüser, Boston*, 1984.

Univ. Paris–Sud, Laboratoire de Mathématique, UMR 8628, Orsay, F–91405 France, CNRS, Orsay, F–91405, France

E-mail address: Etienne.Fouvry@math.u-psud.fr