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 $D^{1+\alpha}$ where $\alpha$ 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,
$$t^2 - Du^2 = 1,$$
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
$$\{\eta_D : \eta_D \text{ solution of } (1) \} = \{\pm \varepsilon_D^n ; n \in \mathbb{Z}\},$$
where $\varepsilon_D$ is the so called fundamental solution of (1), that means
$$\varepsilon_D := \inf \{\eta_D ; \eta_D > 1\}.$$ 
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
$$\varepsilon_D \geq 2\sqrt{D}.$$ 
We are interested in counting the $D$’s for which $\varepsilon_D$ 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 $\varepsilon_D$ is not too large (that means less than $D^{1+\alpha}$, where $\alpha < 1$, see [8, Theorem 1]). In the same paper, Hooley develops a heuristic approach to guess the size of $\varepsilon_D$. 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.

Preliminary version – November 25, 2010
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

\begin{align}
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} \}, \\
S^f(x, \alpha) := \{ (\varepsilon_D, D) ; 2 \leq D \leq x, D \text{ non square}, \varepsilon_D \leq D^{\frac{1}{2}+\alpha} \},
\end{align}

Hence, \( S^f(x, \alpha) \) is associated to \( D \) such that the fundamental solution \( \varepsilon_D \) is less than some bound, while in \( S(x, \alpha) \), we consider all the solutions \( \eta_D \), fundamental or not, less than this bound. The cardinalities of \( S(x, \alpha) \) and \( S^f(x, \alpha) \) are respectively denoted by \( S(x, \alpha) \) and \( S^f(x, \alpha) \). Although, \( S^f(x, \alpha) \) 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 \( S^f(x, \alpha) \), see (29) for instance.

Finally, if \( d \) is such that \( d^2 \mid D \), then any \( \eta_D \) is also an \( \eta_D/d^2 \).

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

\begin{equation}
S(x, \alpha) = S^f(x, \alpha) \sim \frac{4\alpha^2}{\pi^2} x^{\frac{3}{2}} \log^2 x,
\end{equation}

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

\begin{align}
S^f(x, \alpha) &\geq \frac{1}{\pi^2} \left( 1 + (2\alpha - 1)(3 - 2\alpha) - o(1) \right) x^{\frac{3}{2}} \log^2 x, \\
S(x, \alpha) &\geq \frac{1}{\pi^2} \left( 1 + (\alpha - \frac{1}{2})(\frac{11}{2} - 3\alpha) - o(1) \right) x^{\frac{3}{2}} \log^2 x,
\end{align}

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 \( S^f(x, \alpha) \) and \( S(x, \alpha) \), for \( \alpha \geq 1 \), via the trivial inequalities \( S^f(x, \alpha) \geq S^f(x, 1) \) and \( S(x, \alpha) \geq S(x, 1) \).

(iii) Hooley (see [8, Conjecture 1]) suggests a conjecture for \( S^f(x, \alpha) \), for \( \alpha > \frac{1}{2} \).

In particular, he thinks that the following is true

\begin{equation}
S^f(x, \alpha) \sim \frac{1}{\pi^2} \left( 1 + 4(\alpha - \frac{1}{2}) \right) x^{\frac{3}{2}} \log^2 x,
\end{equation}

for \( \frac{1}{2} \leq \alpha \leq 1 \) 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

\[ S^f(x, \alpha) \geq \frac{1}{\pi^2} \left( \phi(\alpha) - o(1) \right) x^{\frac{3}{2}} \log^2 x, \]
and (10) as

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

We easily check the following

\[ \phi(\alpha) \leq \phi^{hyp}(\alpha) \text{ for } \frac{1}{2} \leq \alpha \leq 1, \]

\[ \phi(1) = 2 \text{ and } \phi^{hyp}(1) = 3, \]

and finally,

\[ 0 \leq \phi^{hyp}(\alpha) - \phi(\alpha) = O\left( (\alpha - 1/2)^2 \right), \text{ as } \alpha \to 1/2^+. \]

(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 \( \eta_D \) is intimately linked with the study of the congruence \( t^2 - 1 \equiv 0 \mod u^2 \). Such a congruence can be given explicit solutions, which are easily described in terms of the factorization of \( u = u_1 u_2 \), 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 \( u_2^{-2} \mod u_1^2 \) is well distributed. This is achieved by a precise study of the following tridimensional exponential sum, which, roughly speaking, is defined by

\[ \mathfrak{U} := \sum_{h \neq 0} \alpha_h \sum_{u_1} \beta_{u_1} \sum_{u_2} e\left( h \frac{u_2^2}{u_1^2} \right), \]

where the variable \( h \) comes from an application of Poisson summation formula (see Lemma 4 below), where the coefficients \( \alpha_h \) and \( \beta_{u_1} \) 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 \( \mathfrak{U} \) 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 \( \mathfrak{U} \). 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 \( \varepsilon_D \) has an expression based on the expansion of \( \sqrt{D} \) in continued fraction

\[ \sqrt{D} = [a_0; \ a_1, \ldots, a_s], \]

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 \( \delta \), 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 $\vartheta_0$ satisfying

$$0 < \vartheta_0 < 1,$$

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

$$\sum_{m \equiv a \mod 4^k \text{ and } (m,n) = 1} e\left(h \frac{m^2}{n^2}\right) \ll_k (h,n)^{\frac{1}{2}} M^{\vartheta_0},$$

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 $I$ 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 $n^4 \leq M \leq n^2$, when $\delta$ 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 $\vartheta_0$ satisfying $0 < \vartheta_0 < 1$. Then we have

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

and

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

uniformly for $\frac{1}{2} \leq \alpha \leq \min\left(\frac{3}{4}, \frac{1}{1+\vartheta_0}\right)$.

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

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

Preliminary version – November 25, 2010
2. The fundamental transformation

By the definition (5) we have the equality

\[
S(x, \alpha) = \sum_{t \in \mathbb{Z}, \ t > 0} \sum_{D \in \mathbb{N}, \ D^{1/2} \leq \alpha} 1.
\]

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

\[
S(x, \alpha) = \sum_{1 \leq u \leq X_\alpha} \sum_{D \in \mathbb{N}, \ D^{1/2} \leq \alpha} 1,
\]

where

\[
X_\alpha := \frac{1}{2} (x^\alpha - x^{-1-\alpha}),
\]

(14)

\[
Y_3(u) := (xu^2 + 1)^{1/2},
\]

and

(15)

\[
Y_2(u) := Y_2(u, \alpha) := (Y_1(u, \alpha) u^2 + 1)^{1/2}.
\]

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

\[
u = \frac{1}{2} (Y_1(u, \alpha)^\alpha - Y_1(u, \alpha)^{-1-\alpha}).
\]

The relevance of (13) is to replace the inequalities in (12) concerning \(D\) and \(\eta_D\) by conditions on \(t\) and \(u\) separately. Writing \(Y_1\) under the form \(Y_1(u, \alpha) = (A(u) u^\frac{1}{2})\) we shall use

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

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

is of \(C^\infty\) class and satisfies the inequalities

\[
2 \leq A(u) \leq 2 + u^{-1} \cdot (2u)^{-(1+1/\alpha)}.
\]

**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 function \(y \mapsto G_\alpha(x, y)\) 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 \(A(u) u = y\). \(\square\)

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

\[
\begin{align*}
2^{\frac{1}{2+\alpha}} u^{1+\frac{1}{2+\alpha}} < Y_2(u, \alpha) &< (2^{\frac{1}{2+\alpha}} + o(1)) u^{1+\frac{1}{2+\alpha}} \quad (u \to \infty), \\
\frac{dY_2(u, \alpha)}{du} &= O(u^{\frac{1}{2+\alpha}}) \quad (u \to \infty).
\end{align*}
\]
Following [8, formula (15)], we write the equality

$$S(x, \alpha) = \sum_{1 \leq u \leq X\alpha} \sum_{\Omega \in \mathcal{R}(u)} \sum_{t \in \Omega + u^2 \leq Y_3(s)} 1,$$

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

$$\mathcal{R}(u) := \{ \Omega \text{ mod } u^2 ; \Omega \equiv 1 \text{ mod } u^2 \}.$$

### 3. The case $\alpha \leq 1/2$

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

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

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

$$S(x, \alpha) = \sum_{1 \leq u \leq X\alpha} \rho(u) \left\{ \frac{Y_3(u) - Y_2(u, \alpha)}{u^2} + O(1) \right\}.$$

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

$$Y_3(u) - Y_2(u, \alpha) = ux^{1/2} + O(u^{1 + 1/2\alpha}).$$

Inserting this into (20), we obtain the equality

$$S(x, \alpha) = x^{1/2} \sum_{1 \leq u \leq X\alpha} \frac{\rho(u)}{u} + O\left( \sum_{1 \leq u \leq X\alpha} \frac{\rho(u)}{u^{1 - 1/\alpha}} \right) + O\left( \sum_{1 \leq u \leq X\alpha} \rho(u) \right).$$

Now consider the Dirichlet series

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

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

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

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 $\Re s < 1/2$. Standard techniques of complex analysis give the existence of an absolute constant $c_0$, such that, for $y \to \infty$, one has

$$\sum_{u \leq y} \rho(u) = \left( \frac{8}{\pi^2} \log y + c_0 \right) y + O(y^{1/2}).$$

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

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

and

$$\sum_{1 \leq u \leq y} \frac{\rho(u)}{u^{1 - 1/\alpha}} = (c_2(\alpha) + o(1)) y^{1/2} \log y.$$
uniformly for $x \geq 1$ and $\alpha \geq \varepsilon_0$, where $\varepsilon_0$ 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

\begin{equation}
S(x, \alpha) = \frac{4\alpha^2}{\pi^2} x^{\frac{3}{2}} \log^2 x + \left( c(\alpha) + o(1) \right) x^{\frac{3}{2}} \log x + O(x^\alpha \log x),
\end{equation}

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

$$\eta_D \geq \varepsilon_2^2 D \geq 4D.$$

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

\begin{equation}
S^f(x, \alpha) = S(x, \alpha).
\end{equation}

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

\begin{equation}
\frac{1}{2} < \alpha \leq 1.
\end{equation}

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 $\eta_D$ which are not fundamental. More precisely, as a consequence of (4) and (28), if $(D, \eta_D)$ belongs to $S(x, \alpha)$, then $\eta_D$ is of the form $\eta_D = \varepsilon_D$ or $\varepsilon_2^2 D$ but not of the form $\eta = \varepsilon_k D$ for some $k \geq 3$. We can measure the intrusion of non fundamental solutions by the following trivial equality

\begin{equation}
S(x, \alpha) = S^f(x, \alpha) + S(x, \frac{\alpha}{2} - \frac{1}{4}) \text{ for } 0 \leq \alpha \leq \frac{3}{2},
\end{equation}

which is a consequence of the equivalence

$$\varepsilon_2^2 D \leq D^{\frac{1}{2} + \alpha} \iff \varepsilon_D \leq D^{\frac{1}{2} + \left( \frac{3}{4} - \frac{1}{4} \right)}.$$

Remark that (29) implies the inequality

\begin{equation}
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}.
\end{equation}

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

\begin{equation}
S\left(x, \frac{1}{2}, \alpha \right) := \{ (t, u, D) \mid 1 \leq u \leq X_{1/2},
\end{equation}

\begin{equation}
D \leq x, Y_2(u, \alpha) \leq t \leq Y_3(u), t^2 - Du^2 = 1 \},
\end{equation}

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

\begin{equation}
S\left(x, \frac{1}{2}, \alpha \right) := \sum_{1 \leq u \leq X_{1/2}} \sum_{\Omega \in R(u)} \sum_{t \equiv \Omega \mod u^2} \sum_{Y_2(u, \alpha) \leq t \leq Y_3(u)} 1,
\end{equation}

Preliminary version – November 25, 2010
(compare (32) and (17)). By similar techniques leading to (26), one proves that

\[(33)\quad S(x, \frac{1}{2}, \alpha) \sim S(x, \frac{1}{2}) \sim \frac{1}{x^{\frac{3}{2}}} x^2 \log^2 x,\]
as \(x\) tends to infinity.

We now consider the difference

\[(34)\quad L(x, \alpha) := S(x, \alpha) - S_{\alpha}(x, \frac{1}{2}, \alpha).\]

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

\[(35)\quad L(x, \alpha) = \sum_{X_{1/2} < u \leq X_\alpha} \sum_{D \leq u, Y_2(u) \leq \frac{t^2}{2} - Du^2 = 1} 1.\]

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

\[(36)\quad \mathcal{L}(x, \alpha) := \{(t, u, D) ; X_{1/2} < u \leq X_\alpha, D \leq u, Y_2(u) \leq t \leq Y_3(u), t^2 - Du^2 = 1\}.\]

Since \(\alpha\) is fixed, we write \(Y_2(u)\) instead of \(Y_2(u, \alpha)\). We also denote by \(S^t(x, \frac{1}{2}, \alpha)\) and \(\mathcal{L}(x, \alpha)\) the subsets of \(S(x, \frac{1}{2}, \alpha)\) 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 \(S^t(x, \frac{1}{2}, \alpha)\) and \(\mathcal{L}(x, \alpha)\).

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 \(\geq 0\). Let \(u \geq 1\) such that \(u = 2^k u_0\), where \(u_0\) is an odd integer. We then have

\[(37)\quad \Omega^2 - 1 \equiv 0 \mod u^2 \iff \begin{cases} \Omega^2 - 1 \equiv 0 \mod u_0^2 \\ \Omega^2 - 1 \equiv 0 \mod 4^k. \end{cases}\]

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

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

with

\[(39)\quad L(x, \alpha, \xi, k) := \sum_{X_{1/2} \leq u \leq X_\alpha} \sum_{\Omega \in \mathcal{R}(u)} \sum_{\begin{vmatrix} t \equiv 0 \mod u^2 \\ t \equiv \xi \mod 4^k \\ Y_2(2^k u) \leq t \leq Y_3(2^k u) \end{vmatrix}} 1.\]

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 used in [8]. As usual, for $m$ and $n$ coprime integers, we denote by $\overline{m} \mod n$, $(\overline{m}) \mod n$ (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 $\Phi$ between the set of coprime decompositions of $u$
\[
\mathcal{D}(u) := \{(u_1, u_2); \ u_1u_2 = u, (u_1, u_2) = 1, u_1, u_2 \geq 1\},
\]
and the set of roots of congruence
\[
\mathcal{R}(u) := \{\Omega \mod u^2; \ \Omega^2 \equiv 1 \mod u^2\}.
\]
Such a bijection can be defined by $\Phi(u_1, u_2) = \Omega$, where $\Omega$ is uniquely determined by $\Omega \equiv 1 \mod u_1^2$ and $\Omega \equiv -1 \mod u_2^2$. In an equivalent manner we have the equalities
\[
\begin{align*}
\Phi(u_1, u_2) &\equiv -\overline{u_1^2}u_1^2 + \overline{u_2^2}u_2^2 \mod u^2 \\
&\equiv -2\overline{u_1^2}u_1^2 + 1 \mod u^2 \\
&\equiv 2\overline{u_2^2}u_2^2 - 1 \mod u^2.
\end{align*}
\]
Of course $\overline{u_1^2}$ and $\overline{u_2^2}$ are considered modulo $u_2^2$ and $u_1^2$ respectively.

**Proof.** Let $\Phi$ defined as in Lemma 2. We now prove that $\Phi$ is a bijection. We easily see that $\Phi(\mathcal{D}(u)) \subset \mathcal{R}(u)$ and that $\Phi$ 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 $(u^2, \Omega - 1) = u_2^2$, where $u_1 \mid u$. Similarly, one has $(u^2, \Omega + 1) = u_1^2$, with $u = u_1u_2$ and $(u_1, u_2) = 1$. Thus we have proved that $\Phi(u_1, u_2) = \Omega$. Hence $\Phi$ is a bijection. 

4.5. Arithmetic decomposition of $L(x, \alpha, \xi, k)$. We implement Lemma 2 in (39) to obtain the equality
\[
L(x, \alpha, \xi, k) = \sum_{u_1, u_2: X_{1/2} < 2^k u_1 u_2 \leq X_x} \sum_{t \equiv \Phi(u_1, u_2) \mod 4^k} \sum_{t \equiv \xi \mod 4^k} 1 \quad (42)
\]
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 $\Phi$–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 $X_{1/2} \leq 2^k u_1 u_2 \leq X_x$ and control the order of magnitude of $u_1$ and $u_2$, so we denote by $U = (U_1, U_2)$ any couple of integers taken in the sequence $1, 2, 4, 6, 8, 16$, ... and satisfying the extra conditions
\[
U_1 < U_2, \text{ and } X_{1/2} \leq 2^k U_1 U_2 \leq X_x/4.
\]
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 \( \xi_1 \) and \( \xi_2 \) any congruence classes modulo \( 4^k \), satisfying \((\xi_1 \xi_2, 4^k) = 1\). The following inequality is straightforward

\[
L^< (x, \alpha, \xi, k) \geq \sum_{U} \sum_{\xi_1} \sum_{\xi_2} L(x, \alpha, U, \xi, \xi_1, \xi_2, k),
\]

where

- the summation is over all \( U = (U_1, U_2) \) satisfying (43),
- the summation is over all \( \xi_1 \) and \( \xi_2 \) mod \( 4^k \) satisfying \((\xi_1 \xi_2, 4^k) = 1\),
- we have defined

\[
L(x, \alpha, U, \xi, \xi_1, \xi_2, k) := \sum_{u_1 \sim U_1, \ u_2 \sim U_2} \sum_{u_1 \equiv \xi_1, \ u_2 \equiv \xi_2 \mod 4^k \atop (u_1 u_2, 2) = 1} \sum_{t \equiv \Phi(u_1, u_2) \mod 4^k} \sum_{t \equiv \xi \mod 4^k} \sum_{Y_2(2^k u_1 u_2) \leq t \leq Y_3(2^k u_1 u_2)} 1.
\]

Of course the condition \((u_1 u_2, 2) = 1\) can be dropped when \( k \geq 1 \). The parameter \( \alpha \) is supposed to be fixed and the congruence conditions modulo \( 4^k \) are harmless. So to shorten the notations, we write

\[
L(x, U) := L(x, \alpha, U, \xi, \xi_1, \xi_2, k).
\]

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 \( \ell \) is some integer (see the definition of \( \Phi \) in Lemma 2). It must also belong to the interval \([Y_2(2^k u_1 u_2), Y_3(2^k u_1 u_2)]\). 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 \( u_2^2 > (4^k x u_1^2 u_2^2 + 1)^2 + 1 \). Hence we can suppose

\[
U_2 \leq 2^{k+2} x^{\frac{1}{4}} U_1,
\]

otherwise \( L(x, U) = 0 \).

Since \( u_1 u_2 \) is odd, we deduce from (41) the equivalence

\[
t \equiv \Phi(u_1, u_2) \mod u_1^2 u_2^2 \quad \text{and} \quad t \equiv \xi \mod 4^k \iff t \equiv t_0 \mod 4^k u_1^2 u_2^2,
\]

where

\[
t_0 := \xi u_1^2 u_2^2 \cdot \left( \frac{u_1^2 + u_2^2}{2} \right) \mod 4^k + \left( 2 \frac{u_2^2}{u_1^2} \mod u_1^2 u_2^2 - 1 \right) 4^k \cdot \left( \frac{u_2}{u_1} \right) \mod u_1^2 u_2^2 \cdot 4^k u_1^2 u_2^2.
\]
Modulo 1, this congruence implies the equality
\[
\begin{align*}
\frac{t_0}{4^k u_1^2 u_2^2} &= \frac{\xi_1^2 \xi_2^2}{4^k} + \frac{4^k (2 \xi_1^2 u_2^2 - 1)}{u_1^2 u_2^2} \mod 1, \\
&= \kappa - \frac{1}{4^k u_1^2 u_2^2} + 2 \frac{4^k u_2^2}{u_1^2} u_1^2 u_2^2 \mod 1,
\end{align*}
\]
(50)
with
\[
\kappa := \frac{(\xi + 1) \xi_1^2 \xi_2^2}{4^k}.
\]
In the proof of (50), we used Bézout’s relation
\[
\frac{1}{ab} = \frac{a}{b} + \frac{b}{a} \mod 1,
\]
for coprime integers \(a\) and \(b\) and the fact that \(u_i \equiv \xi_i \mod 4^k\) (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
\[
\sum_{t \equiv t_0 \mod 4^k u_1^2 u_2^2, Y_2(2^k u_1 u_2) \leq t \leq Y_3(2^k u_1 u_2)} 1 = \frac{Y_3(2^k u_1 u_2) - Y_2(2^k u_1 u_2)}{4^k u_1^2 u_2^2} + O(1),
\]
(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 \(L(x, U)\), so we gain in efficiency by introducing a smooth function which plays the role of a lower bound of the characteristic function \(1_{[Y_2, Y_3]}\) 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 \(C^\infty\)-function \(g : \mathbb{R} \to \mathbb{R}\), which has the two properties
\[
0 \leq g \leq 1_{[-1/2,1/2]},
\]
and
\[
\int_{-\infty}^{\infty} g(y) dy = 1 - \delta.
\]

It is well known that the Fourier coefficients \(\hat{g}(u)\), defined by
\[
\hat{g}(u) := \int_{-\infty}^{\infty} g(y) e(-uy) dy,
\]
go to 0 very quickly as \(u \to \infty\), since, for every \(n \geq 0\) we have
\[
\hat{g}(u) = O_n(|u|^{-n}),
\]
(52)
uniformly for \(|u| \geq 1\).

Let \(m_0 \in \mathbb{R}\) and \(L_0 > 0\). The function
\[
f_{m_0, L_0}(y) := g\left(\frac{y - m_0}{L_0}\right),
\]
will appear as a good approximation from below of the characteristic function of the interval \( m_0 - \frac{\delta}{2}, m_0 + \frac{\delta}{2} \). 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

\[
\sum_{m \equiv a \mod q} f(m) = \frac{L_0}{q} \sum_h e\left(h \cdot \frac{a - m_0}{q}\right) \hat{g}\left(h \cdot \frac{L_0}{q}\right).
\]

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

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

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

\[
\sum_{t \geq 1} \left| Y_3 - Y_2 \right|^{2k u_1 u_2} \sum_h e\left(h \cdot \frac{1}{4^k u_1^2 u_2^2} + 2 \frac{t}{4^k u_1^2 u_2^2} - \frac{Y_2 + Y_3}{2 \cdot 4^k u_1^2 u_2^2}\right) \hat{g}\left(h \cdot \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}\right).
\]

For \( h = 0 \) we recognize the main term

\[
\text{MT}(u_1, u_2) := (1 - \delta) \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}.
\]

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

\[
H = H(U) := U_1 U_2 x^{-\frac{1}{2} + \varepsilon}.
\]

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

\[
\left| \hat{g}\left(h \cdot \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}\right) \right| \leq \left( \frac{|h| \cdot u_1 u_2 x^{2k u_1 u_2}}{2^k u_1^2 u_2^2}\right)^{-n} \leq \left( \frac{|h|}{H} x^{\varepsilon}\right)^{-2} (x^{\varepsilon})^{-(n-2)},
\]

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

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

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

\[
Y_2 = Y_2(2^k u_1 u_2, \alpha) \quad \text{and} \quad Y_3 = Y_3(2^k u_1 u_2),
\]

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

\[
\sum_{t \geq 1} \leq \text{MT}(u_1, u_2)
\]

\[
+ \int_{-\infty}^{\infty} \sum_{1 \leq |h| \leq H} G(h, y, u_1, u_2) e(h y) e\left(2h \frac{t}{u_1^2}\right) dy + O(x^{-10}).
\]

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

\[
L(x, U) \geq (1 - \delta) \text{EMT}(x, U) + \text{Err}(x, U) + O(1),
\]

Preliminary version – November 25, 2010
ON THE SIZE OF THE FUNDAMENTAL SOLUTION OF PELL EQUATION

We want to know under which conditions, we have the trivial bound is consequence of (14) and (16), we have dependence on $U_{\text{Err}}(x)$ (see (59)). In the notation, it is useless to specify the value of $\xi$. We now simplify $\text{Err}(x)$ where the error term is (59)

$$\text{Err}(x) := \int_{-\infty}^{\infty} \sum_{1 \leq |h| \leq H} e(h\kappa) \sum_{u_1 \sim \xi_1, \ u_2 \sim \xi_2} G(h, y, u_1, u_2) \epsilon \left( 2h \frac{4k \pi^2}{u_1^2} \right) dy. $$

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

$$ \frac{\partial^{\varepsilon_1 + \varepsilon_2}}{\partial \varepsilon_1 \partial \varepsilon_2} G(h, y, u_1, u_2) \ll x^{\frac{1}{2} + \varepsilon} U_1^{-1} U_2^{-1} \left( x^{\varepsilon y} U_1^{-1} \right)^{\varepsilon_1} \left( x^{\varepsilon y} U_2^{-1} \right)^{\varepsilon_2}, $$

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

$$ \text{Err}(x, U) \ll \frac{x^{\frac{1}{2} + \varepsilon} U_1 U_2}{U_1 U_2} \sum_{1 \leq |h| \leq H} e(h\kappa) \sum_{u_1 \sim \xi_1, \ u_2 \sim \xi_2} e \left( 2h \frac{4k \pi^2}{u_1^2} \right). $$

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

$$ \tilde{U}(H, U_1, U_2, k) := \sum_{1 \leq |h| \leq H} \alpha_h \sum_{u_1 \sim \xi_1} \beta_{u_1} \sum_{U_2 u_2 \sim U_2^*} e \left( h \frac{4k \pi^2}{u_1^2} \right), $$

where

- $H, U_1$ and $U_2 \geq 1, U_2 \leq U_2^* \leq 2U_2$, $k$ is an integer $\geq 0$,
- $\alpha_h$ is some complex coefficient, satisfying $|\alpha_h| \leq 1$ and $h \equiv h' \mod 2 \cdot 4^k \Rightarrow \alpha_h = \alpha_{h'}$,
- $\beta_{u_1}$ is some complex coefficient, satisfying $|\beta_{u_1}| \leq 1$ and $2 \mid u_1 \Rightarrow \beta_{u_1} = 0$,
- the $^\dagger$-symbol means that the summation over $u_2$ is restricted to some fixed congruence class $u_2 \equiv \xi_2 \mod 4^k$ with $\xi_2$ odd if $k \geq 1$, or $u_2 \equiv 1 \mod 2$ if $k = 0$ (see (59)). In the notation, it is useless to specify the value of $\xi_2$ 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 $\tilde{U}(H, U_1, U_2, k) \ll H U_1 U_2$.

We want to know under which conditions, we have

$$ \tilde{U}(H, U_1, U_2, k) \ll U_1 U_2 x^{-\varepsilon}, $$

for $H$ as in (55). When (62) is satisfied, we deduce from (60) the inequality $\text{Err}(x, U) \ll x^{\frac{1}{2} - \varepsilon}$, which shows that $\text{Err}(x, U)$ 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 \( \sum_{u_2 \sim v_2} e(h\overline{u_2^2}/u_2^2) \), 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

\[
\Sigma(h; n^2, k) := \begin{cases} 
\sum_{m \equiv \overline{1} \mod 4^k n^2 \ (m,n) = 1} e\left(h \frac{m^2}{n^2}\right), & \text{if } k \geq 1, \\
\sum_{m \equiv \overline{1} \mod 2^k n^2 \ (m,n) = 1} e\left(h \frac{m^2}{n^2}\right), & \text{if } k = 0.
\end{cases}
\]

The \( \overline{} \)–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

\[
\Sigma(h; n^2) := \sum_{m \equiv \overline{1} \mod n^2 \ (m,n) = 1} e\left(h \frac{m^2}{n^2}\right).
\]

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

\[
\Sigma(h; n^2) = \sum_{m \equiv \overline{1} \mod n^2 \ (m,n) = 1} e\left(h \frac{m^2}{n^2}\right),
\]

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

\[
G(h; n) := \sum_{m \mod n} e\left(h \frac{m^2}{n}\right).
\]

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

\[
G(h; n_1 n_2) = G(hn_2; n_1) G(hn_1; n_2) \text{ when } \langle n_1, n_2 \rangle = 1.
\]

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

\[
G(h; n_1^2 n_2^2) = G(h; n_1^2) G(h; n_2^2).
\]

Preliminary version – November 25, 2010
For \( (2h, n) = 1 \), we also have

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

and finally

\[ G(h; p^\ell) = (h, p^\ell) G\left( \frac{h}{(h, p^\ell)}; \frac{p^\ell}{(h, p^\ell)} \right). \]

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

\[ \Sigma(h; n^2) = \prod_{i=1}^k \Sigma(h; p_i^{2\alpha_i}), \]

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

\[ \Sigma(h; p^{2\ell}) = G(h; p^{2\ell}) - \sum_{m=1}^{p^{2\ell}-1} e\left( \frac{h(pm^t)^2}{p^{2\ell}} \right), \]

which is

\[ \Sigma(h; p^{2\ell}) = G(h; p^{2\ell}) - pG(h; p^{2\ell-2}). \]

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 \( p^t \mid h \). This implies that \( (h, p^{2\ell}) = p^t \) or \( p^{2\ell} \). By (64) and (66), we have the equalities

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

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

\[ \Sigma(h; p^{2\ell}) = \begin{cases} 
0 & \text{for } t \leq 2\ell - 2, \\
p^{2\ell-1} \left( \frac{hp^{-t}}{p} \right) G(1; p) - p^{2\ell-1} & \text{for } t = 2\ell - 1, \\
p^{2\ell-1} (p - 1) & \text{for } t \geq 2\ell.
\end{cases} \]
To use (65), we recall the definition of the kernel \( \kappa(n) \) of an integer \( n \geq 1 \)

\[
\kappa(n) := \prod_{p \mid n} p,
\]

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

\[
\gamma(m; n) = \prod_{p \mid n, 2^\ell \mid m} \left( p^{2^\ell - 1} \left( \frac{mp - 2^{\ell+1}}{p} \right) G(1; p) - p^{2^\ell - 1} \right) \prod_{p \mid n, 2^\ell \mid m} p^{2^\ell - 1}(p - 1).
\]

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

\[(70) \quad \gamma(m; n) = \gamma(a^2m; n).\]

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

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

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

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

\[
\Sigma(I, h; n^2, k) := \sum_{m \in I, \, (m, n) = 1}^{\|} e\left( \frac{h m^2}{n^2} \right) = \sum_{u \in I}^{\|} e\left( \frac{h u^2}{n^2} \right),
\]

where \( I \) 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 \{\( m \in I \), \( m \) satisfies \( \| \)\} under the form

\[
\frac{1}{4^k n^2} \sum_{\ell = 1}^{4^k n^2} \sum_{u \in I}^{\|} e\left( \frac{\ell (m - u)}{4^k n^2} \right).
\]

This gives the equality

\[
\Sigma(I, h; n^2, k) = \frac{1}{4^k n^2} \sum_{\ell = 1}^{4^k n^2} \sum_{u \in I}^{\|} e\left( -\ell \frac{u}{4^k n^2} \right) \mathcal{G}(4^k h, \ell; 4^k n^2),
\]

with

\[
\mathcal{G}(h, \ell; n^2) := \sum_{m \equiv 0 \mod n^2, (m, n) = 1} e\left( \frac{h m^2 + \ell m}{n^2} \right).
\]

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

\[
|\Sigma(I, h; n^2, k)| \leq |\Sigma(4^k h; 4^k n^2)| + O\left( \sum_{\ell = 1}^{(4^k n^2)^{1/2}} \frac{1}{\ell} |\mathcal{G}(4^k h, \ell; 4^k n^2)| \right).
\]

Preliminary version – November 25, 2010
Write $\mathcal{S}(h, \ell; n^2)$ under the form

$$\mathcal{S}(h, \ell; n^2) := \sum_{m \mod n^2 \atop (m, n) = 1} e\left( \frac{hm^2 + \ell m}{n^2} \right).$$

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

$$|\mathcal{S}(4^k h, \ell; 4^k n^2)| \leq 4^k \prod_{i=1}^{t} \mathcal{S}\left(4^k h \left(\frac{n}{p_i^{\alpha_i}}\right)^2, \ell \left(\frac{n}{p_i^{\alpha_i}}\right)^2; p_i^{2\alpha_i}\right).$$

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

$$(75) \quad \mathcal{S}(a, b; p^{2\alpha}) = p^{\alpha - 1} \sum_{s=1}^{p^{\alpha - 1}} \sum_{t=0}^{p^{\alpha - 1}} e\left( \frac{as^2 + bs}{p^{2\alpha}} \right) e\left( \frac{(2as - b\bar{s}^2)t}{p^{\alpha}} \right).$$

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

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

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

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

$$s + p^mt \equiv \bar{s} - p^n t \bar{s}^2 \mod p^m.$$

This lemma simplifies (75) into

$$(76) \quad \mathcal{S}(a, b; p^{2\alpha}) = \sum_{s=1}^{p^{\alpha - 1}} \sum_{t=0}^{p^{\alpha - 1}} e\left( \frac{(2as - b\bar{s}^2)t}{p^{\alpha}} \right).$$

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

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

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

$$|\mathcal{S}(a, b; p^{2\alpha})| \leq 3p^\alpha (a, b, p^\alpha),$$

and by the multiplicativity property (74), we obtain

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

$$|\mathcal{S}(a, b; n^2)| \leq 3^{\omega(n)} n (a, b, n).$$

and

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

Preliminary version – November 25, 2010
As usual \( \omega(n) \) is the number of distinct prime factors of \( n \).

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

(77) \[ |\Sigma(\mathcal{I}, h; n^2, k)| \leq |\Sigma(4^k h; 4^k n^2)| + O(n^{1+\varepsilon}), \]

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

\[ |\Sigma(4^k h; 4^k n^2)| \leq 4^k |\Sigma(h; n^2)| \quad \text{if} \quad 2 \nmid n, \]

simplifies (77) into

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

6.3. The final result. Consider the general exponential sum

(79) \[ \Sigma = \Sigma(Y, Z, h; n^2, k) := \sum_{Y < m < Z \atop (m,n) \leq 1} e\left( \frac{hm^2}{n^2} \right), \]

where the \( \text{^{\dagger}} \)–symbol is always defined in (61), \( n \) is an odd integer. We split the interval of summation in \( [(Z-\lfloor Y \rfloor)/2n^2] \) intervals of length \( L = 4^k n^2 \) when \( k \geq 1 \) and in \( [(Z-\lfloor Y \rfloor)/2n^2] \) intervals of length \( L = 2n^2 \) when \( k = 0 \) (as usual, \( \lfloor y \rfloor \) 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 \( \Sigma \) defined in (79). Then for every positive \( \varepsilon \), for every integer \( k \geq 1 \), the following equality holds

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

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 \( \gamma \), since it contains Jacobi symbols in its definition.

7. Application to \( \bar{\Omega}(H, U_1, U_2, k) \)

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

(80) \[ |\gamma(m; n)| \leq n^2 , \]

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

\[ \Sigma = \frac{Z-Y}{4^k n^2} \gamma(h; n) + O(n^2) \quad \text{if} \; (n^2/\kappa(n)) \mid h. \]
By this remark, by (70) and by the second case of Proposition 1, we directly have the equality

\[
\mathcal{U}(H, U_1, U_2, k) = 4^{-k}(U_2^2 - U_2) \sum_{1 \leq |h| \leq H} \alpha_h \sum_{\nu_1 \sim U_1 \atop \nu_1 \not| h} \beta_{\nu_1} u_1^{-2}(h; \nu_1) + O\left( \sum_{1 \leq |h| \leq H} \sum_{\nu_1 \sim U_1}^{u_1} u_1^3 \right) + O\left( \sum_{1 \leq |h| \leq H} \nu_1 \sim U_1 \sum_{1 \leq |h| \leq H} \nu_1^{1+\varepsilon} \right) \]

(81)

by definition. We trivially have

(82)

\[ E_3(H, U_1) = O(H U_1^{2+\varepsilon}). \]

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

\[ E_2(H, U_1) \ll U_1^2 \sum_{\nu} \sum_{\nu \sim U_1} \sum_{1 \leq |h| \leq H} 1, \]

which is

(83)

\[ E_2(H, U_1) = O(HU_1^{2+\varepsilon}). \]

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

(84)

\[ E_1(H, U_1) = O(H). \]

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

(85)

\[ U_1 \leq x^{1-5\varepsilon} \quad \text{and} \quad U_2 \leq x^{1-9\varepsilon}. \]

By (43), we see that these rather easy investigations give a non trivial lower bound on the function \( L(x, U) \), for some choices of \( (U_1, U_2) \) up to \( U_1 U_2 \leq x^{4-6\varepsilon} \). Thus the trivial bound \( U_1 U_2 = x^{1-\varepsilon} \) is passed.

7.2. A precise upper bound. Our purpose is to loosen the conditions (85) by a deeper study of the \( \gamma \)–function which takes into account the oscillations of the Jacobi symbol. We first elaborate a more practical form of the function \( \gamma \). 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

\[ \gamma(h; u_1) = \nu v_1^2 \prod_{p|h'} \left( \frac{h'v/p}{p} \right) G(1; p) - 1 \prod_{p|h'} (p - 1). \]
and the first step is the equality
\[(86) ~ \gamma(h; u_1) = \nu v_1^2 \varphi((h', \nu)) \prod_{p \mid \nu, p \mid h'} \left( \frac{h' \nu/\delta}{p} \right) G(1; p) - 1 \].

To simplify the notations, we define for any odd squarefree \( \delta \) the function \( G(\delta) \) by
\[(87) ~ G(\delta) := \delta^2 \left( \prod_{p \mid \delta, p \equiv 3 \pmod{4}} i \right) = \prod G(1; p). \]

With these remarks we expand (86) as
\[
\gamma(h; u_1) = \nu v_1^2 \mu(\nu) \varphi((h', \nu)) \mu((h', \nu)) \sum_{\delta \mid \nu} \left( \frac{h'}{\delta} \right) G(\delta) \prod_{p \mid \delta} \left( \frac{\nu/p}{p} \right) \mu(\frac{\nu}{\delta}).
\]

Since \( \nu \) is squarefree, we can simplify the \( \mu \)-factor, and we also notice that if \( \delta \mid \nu \) but \( \delta \nmid \frac{h'}{\nu} \) then we have \( \left( \frac{h'}{\nu} \right) = 0 \). These remarks simplify the above formula into
\[
\gamma(h; u_1) = \nu v_1^2 \mu(\nu) \varphi((h', \nu)) \mu((h', \nu)) \sum_{\delta \mid \nu} \left( \frac{h'}{\delta} \right) G(\delta) \prod_{p \mid \delta} \left( \frac{\nu/p}{p} \right) \mu(\delta).
\]

Then write
\[
\nu := \delta \eta,
\]
and define, for every odd squarefree integer \( a \), the function \( \varpi(a) = \pm 1 \) by the formula
\[
\varpi(a) := \prod_{p \mid a} \left( \frac{a/p}{p} \right),
\]
to rewrite \( \gamma(h; u_1) \) as
\[
\gamma(h; u_1) = \nu v_1^2 \mu(\nu) \varphi((h', \nu)) \mu((h', \nu)) \sum_{\delta \mid \nu \eta=\nu} \left( \frac{h'}{\delta} \right) G(\delta) \left( \frac{\eta}{\delta} \right) \varpi(\delta) \mu(\delta).
\]

From this we deduce the following expression of \( E_1(H, U_1) \) defined in (81)
\[(88) ~ E_1(H, U_1) = \sum_{\nu=1} \nu^{-1} \mu(\nu) \sum_{\nu_1=1}^{\nu^\infty} \beta_{\nu v_1} \sum_{\delta h' v_1^2 \equiv 1 \pmod{U_1}} \alpha_{\delta h' v_1^2} \varphi((h', \nu)) \mu((h', \nu)) \sum_{\delta \eta=\nu} \left( \frac{h'}{\delta} \right) G(\delta) \left( \frac{\eta}{\delta} \right) \varpi(\delta) \mu(\delta).
\]

We can always suppose that \( (h', \delta) = 1 \), otherwise \( \left( \frac{h'}{\delta} \right) = 0 \). This remark gives the equality \( (h', \nu) = (h', \eta) \) and transforms (88) into
\[(89) ~ E_1(H, U_1) = \sum_{\delta} \delta^{-1} \varpi(\delta) G(\delta) \sum_{\eta} \eta^{-1} \mu(\eta) \mu^2(2\delta\eta) \left( \frac{\eta}{\delta} \right) \sum_{\nu_1=1}^{\nu^{\infty}} \beta_{\delta \nu v_1} \sum_{\delta \eta h' v_1^2 \equiv 1 \pmod{U_1}} \alpha_{\delta \eta h' v_1^2} \varphi((\eta, h')) \mu((\eta, h')) \left( \frac{h'}{\delta} \right).
\]

To circumvent the difficulty of the g.c.d.(\( \eta, h' \)), we compose \( \eta \) into
\[
\eta := \eta_1 \eta_2,
\]

Preliminary version – November 25, 2010
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
\[
E_1(H, U_1) = \sum_{\delta} \delta^{-1} \varpi(\delta) G(\delta) \sum_{\eta_1} \eta_1^{-1} \eta_2^{-1} \mu^2(2\delta \eta_1 \eta_2)\mu(\eta_2)\varphi(\eta_1) \left( \frac{\eta_2}{\delta} \right) \sum_{\eta_1(\delta^2 \eta_2 v_1^2) \leq \delta_1 \eta_2} \beta_{\delta \eta_1 \eta_2 v_1} \sum_{1 \leq \lambda \leq H/(\delta^2 \eta_2 v_1^2)} \alpha_{\delta \eta_2^2 \lambda \nu_1^2} \left( \frac{\lambda}{\delta} \right).
\]
We now split the above sum into subsums where the congruence classes modulo \(4^k\) of each of the five variables \(\delta, \eta_1, \eta_2, v_1\) and \(\lambda\) are fixed (this implies that, by hypothesis, the coefficient \(\alpha_{\delta \eta_2^2 \lambda \nu_1^2}\) has a constant value). We also fix the order of magnitude of each variables by imposing
\[
\eta_1 \sim \eta_1 Y_1, \quad \eta_2 \sim \eta_2 Y_2, \quad \delta \sim \Delta, \quad v_1 \sim V_1, \quad \lambda \sim L.
\]
These orders of magnitude are constrained as follows
\[
V_1 Y_1 Y_2 \Delta \sim U_1, \quad L \leq \frac{H}{Y_1^2 Y_2^2 V_1^2 \Delta} \quad (\sim \frac{H}{Y_1 U_1 V_1} := L_0).
\]
This double splitting process gives the inequality
\[
E_1(H, U_1) \ll (HU_1)^{\varepsilon} \mathcal{E}^*(L, V_1, Y_1, Y_2, \Delta),
\]
for some \((L, V_1, Y_1, Y_2, \Delta)\) satisfying (92), and where we define
\[
\mathcal{E}^*(L, V_1, Y_1, Y_2, \Delta) := \sum_{\delta} \delta^{-1} \varpi(\delta) G(\delta) \times \sum_{\eta_1} \eta_1^{-1} \eta_2^{-1} \mu^2(2\delta \eta_1 \eta_2)\mu(\eta_2)\varphi(\eta_1) \left( \frac{\eta_2}{\delta} \right) \sum_{\eta_1(\delta^2 \eta_2 v_1^2) \leq \delta_1 \eta_2} \beta_{\delta \eta_1 \eta_2 v_1} \sum_{1 \leq \lambda \leq H/(\delta^2 \eta_2 v_1^2)} \alpha_{\delta \eta_2^2 \lambda \nu_1^2} \left( \frac{\lambda}{\delta} \right),
\]
where the variables are controlled (91) and where the upper \(\ast\)-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 \(\lambda\) from the variables \(\delta\) and \(v_1\) in the inequality \(\lambda \leq H/(\delta \eta_2^2 \nu_1^2)\), 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)
\[
\frac{1}{2\pi i} \int_{\sigma_0-iT}^{\sigma_0+iT} y^s \frac{ds}{s} = \begin{cases} 1 + O(y^{\sigma_0} T^{-1} \log y)^{-1} & \text{ if } y > 1, \\ O(y^{\sigma_0} T^{-1} \log y)^{-1} & \text{ if } 0 < y < 1, \end{cases}
\]
uniformly for \(T \geq 1\), and \(\sigma_0 > 0\). In our context, we can suppose that \(H\) is of the form \(H = [H] + \frac{1}{2}\), and we fix \(y := H/(\delta \eta_2^2 \lambda \nu_1^2)\). Hence, we always have \(|\log y| \gg H^{-1}\). We choose
\[
T := (HU_1)^{100} \quad \text{and } 0 < \sigma_0 \leq \frac{1}{100}.
\]
This transforms (94) into

\[ E^* = \frac{1}{2\pi i} \int_{\gamma_0} \sum_{\delta} \delta^{-1-s} \varpi(\delta) G(\delta) \sum_{\eta_1} \sum_{\eta_2} \delta^{\ast s} \eta_1^{-1-2s} \eta_2^{-1-s} \times \mu^2(\delta \eta_1 \eta_2) \mu(\eta_2) \varphi(\eta_1) \left( \frac{\eta_2}{\delta} \right) \sum_{\nu_1(\delta \eta_1 \eta_2 v_1)} \sum_{\lambda, \eta_2 = 1}^{\ast} \lambda^{-s} \left( \frac{\lambda}{\delta} \right) Hs^s ds + O(1), \]

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

\[ E^* = \frac{1}{2\pi i} \int_{\gamma_0} \sum_{\delta} \sum_{\eta_1} \sum_{\eta_2} \delta^{\ast s} \eta_1^{-1-2s} \eta_2^{-1-s} \mu(\eta_2) \varphi(\eta_1) \sum_{\lambda, \eta_2 = 1}^{\ast} \lambda^{-s} A(\delta, \eta_1, \eta_2, s) \left( \frac{\lambda}{\delta} \right) Hs^s ds + O(1), \]

where

\[ A(\delta, \eta_1, \eta_2, s) = \delta^{-1-s} \varpi(\delta) G(\delta) \mu^2(\delta \eta_1 \eta_2) \left( \frac{\eta_2}{\delta} \right) \sum_{\nu_1(\delta \eta_1 \eta_2 v_1)} \sum_{\lambda, \eta_2 = 1}^{\ast} \lambda^{-s} \lambda. \]

Of course, the variables continue to satisfy (91). It is crucial to remark that in (96), the variables \( \delta \) and \( \lambda \) simultaneously appear in the Jacobi symbol \( \left( \frac{\delta}{\lambda} \right) \) 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 \( a_1, \ldots, a_M \) and \( b_1, \ldots, b_N \) be arbitrary complex numbers satisfying \( |a_m|, |b_n| \leq 1 \). Then, we have

\[ \sum_{m \leq M, 2 \nmid m} \sum_{n \leq N} a_m b_n \left( \frac{n}{m} \right) \ll \varepsilon (MN)^{1+\varepsilon} (M^{-\frac{1}{2}} + N^{-\frac{1}{2}}), \]

for every positive \( \varepsilon \).

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

**Lemma 10.** For every positive \( \varepsilon \), one has the inequality

\[ \sum_{n \leq N} 1 \ll \varepsilon N^\varepsilon 2^{\varepsilon(m)}. \]

**Proof.** It is an application of Rankin’s method. For every \( \varepsilon > 0 \), one has the inequalities

\[ \sum_{n \leq N} \left( \frac{N}{n} \right)^\varepsilon = N^\varepsilon \prod_{p | m} \left( 1 + \frac{1}{p^\varepsilon} + \frac{1}{p^{2\varepsilon}} + \cdots \right) \ll N^\varepsilon \prod_{p | m} \left( 1 - \frac{1}{p^\varepsilon} \right)^{-1}. \]

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

\[ A(\delta, \eta_1, \eta_2, s) \ll \Delta^{-\frac{1}{2}} (HU)^\varepsilon, \]

Preliminary version – November 25, 2010
uniformly over s, \( \eta_1 \) and \( \eta_2 \). By Lemma 9 and after an integration over s (with the choice \( \sigma_0 = \varepsilon/10 \)), we get the inequality

\[
\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{L,V_1,Y_1,Y_2,\Delta} \left\{ Y_1 \Delta^{-\frac{1}{2}} \left( L \Delta \left( \Delta^{-\frac{1}{2}} + L^{-\frac{1}{2}} \right) \right) \right\},
\]

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

\[
\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{V_1,Y_1,Y_2,\Delta} \left\{ Y_1 \Delta^{-\frac{1}{2}} \left( L_0 \Delta \left( \Delta^{-\frac{1}{2}} + L_0^{-\frac{1}{2}} \right) \right) \right\}.
\]

Replacing \( L_0 \) by its value, we obtain the inequality

\[
\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{V_1,Y_1,Y_2,\Delta} \left\{ HU_1^{-1}V_1^{-1} + \frac{1}{2}V_1^{-\frac{1}{2}}Y_1^{\frac{1}{2}} \Delta^{-\frac{1}{2}} \right\}.
\]

We now insert the fact that \( V_1Y_1Y_2\Delta \geq U_1 \) in order to simplify the above upper bound as

\[
\mathcal{E}^* \ll (HU_1)^{3\varepsilon} \sup_{V_1,Y_1,Y_2,\Delta} \left\{ HU_1^{-1}V_1^{-1} + \frac{1}{2}V_1^{-\frac{1}{2}}Y_1^{\frac{1}{2}} \right\}
\]

(98)

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

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

\[
\mathcal{U}(H,U_1,U_2,k) \ll_{\varepsilon,k} (HU_1U_2)^{k} (HU_1^{-1}U_2 + \frac{1}{2}U_2 + H^{\frac{1}{2}}),
\]

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

\[
U_2 \leq x^{\frac{1}{2} - 10\varepsilon}U_1 \quad \text{and} \quad U_1 \leq x^{\frac{1}{2} - 10\varepsilon}.
\]

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 \( \alpha \) 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 \( \text{Err}(x,U) \) (controlled by (60)) satisfies the inequality

\[
\text{Err}(x,U) \ll x^{\frac{1}{2} - \varepsilon},
\]

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

\[
L(x,\alpha) \geq 2(1 - \delta) \times \sum_{k=0}^{k_0} \sum_{\xi \in \mathcal{R}(2^k)} \sum_{\xi_1, \xi_2 \mod 4k} \sum_{U_1, U_2} \sum_{\nu_{j} \equiv \xi_{j} \mod 4k} \sum_{(\nu_{1}, \nu_{2})=1} \sum_{(\nu_{1}, \nu_{2})=1} \frac{Y_{3} - Y_{2}}{4^{k}u_{1}u_{2}} - O(x^{\frac{1}{2}}).
\]

Preliminary version – November 25, 2010
holds provided that \( U_1 \) and \( U_2 \) are powers of 2, satisfying the inequalities
\[ \frac{1}{2} x^{\frac{1}{2}} < 2^k U_1 U_2 < \frac{1}{8} x^\alpha, \quad U_1 < U_2, \quad U_2 \leq x^{\frac{1}{2} - \varepsilon} U_1 \quad \text{and} \quad U_1 \leq x^{\frac{1}{2} - \varepsilon}. \]

We insert (21) under the form
\[ (102) \quad Y_3 - Y_2 = Y_3(2^k u_1 u_2) - Y_2(2^k u_1 u_2, \alpha) = 2^k u_1 u_2 x^{\frac{1}{2}} + O((u_1 u_2)^{1 + \frac{1}{k^2}}). \]

The contribution of the error term in (102) to the right hand side of (101), is handled in (22) and (25) and is in \( O(x^{\frac{1}{2} \log x}) \). Recalling the definition of \( \rho(2^k) = \sharp \mathcal{R}(2^k) \), summing over all possible \( \xi_1 \) and \( \xi_2 \) modulo \( 4^k \), and gluing the intervals \([U_1, 2U_1]\) back together, we get the inequality
\[ (103) \quad L(x, \alpha) \geq 2(1 - 2\delta)(\sum_{k=0}^{k_0} \frac{\rho(2^k)}{2^k}) x^{\frac{1}{2}} \sum_{(u_1, u_2) \neq (u_1, u_2, 2)} \frac{1}{u_1 u_2} - O(x^{\frac{1}{2} \log x}), \]

where the integer variables \( u_1 \) and \( u_2 \) satisfy the inequalities
\[ x^{\frac{1}{2}} < u_1 u_2 < x^\alpha, \quad u_1 \leq u_2, \quad u_2 \leq u_1 x^{\frac{1}{2} - \varepsilon} \quad \text{and} \quad u_1 \leq x^{\frac{1}{2} - \varepsilon}. \]

In the proof of (103), we used the inequalities
\[ \sum_{y \leq u_1 u_2 \leq Ay} \frac{1}{u_1 u_2} \ll A \log 2y \quad \text{and} \quad \sum_{u_1 \leq u_2 \leq Ay} \sum_{u_1 \leq u_2 \leq A u_1} \frac{1}{u_1 u_2} \ll A \log 2y, \]

for any fixed constant \( A \geq 1 \). Appealing to (19), choosing \( k_0 = k_0(\delta) \) very large and \( \varepsilon = \varepsilon(\delta) \) very small and redefining the constant \( \delta \), the inequality (103) is simplified in
\[ (104) \quad L(x, \alpha) \geq 8 x^{\frac{1}{2}} \sum_{(u_1, u_2) \neq (u_1, u_2, 2)} \frac{1}{u_1 u_2} - O(\delta x^{\frac{1}{2} \log^2 x}) - O_\delta(x^{\frac{1}{2} \log x}), \]

where the conditions of summation now are
\[ x^{\frac{1}{2}} < u_1 u_2 < x^\alpha, \quad u_1 \leq u_2, \quad u_2 \leq u_1 x^{\frac{1}{2}} \quad \text{and} \quad u_1 \leq x^{\frac{1}{2}}. \]

The inequality (104) is true for any positive \( \delta \) and the corresponding region of summation can be written as
\[ \{(u_1, u_2) \mid u_1 \leq x^{\frac{1}{2}}, \quad x^{\frac{1}{2}} u_1^{-1} \leq u_2 \leq \min(x^\alpha u_1^{-1}, x^{\frac{1}{2}} u_1), \quad (u_1, u_2) = (u_1 u_2, 2) = 1\}. \]

We now appeal to the classical

**Lemma 11.** For any integer \( m \geq 1 \) and for any \( y \geq 1 \), one has the equality
\[ \sum_{n \leq y \atop (m, n) = 1} \frac{1}{n} = \frac{\varphi(m)}{m} \log y + O\left(1 + \sum_{d \mid m} \frac{\log d}{d}ight). \]

**Proof.** By Möbius’ inversion formula, one may write
\[ \sum_{n \leq y \atop (m, n) = 1} \frac{1}{n} = \sum_{d \mid m} \mu(d) \sum_{n \leq y/d \atop (d, n) = 1} \frac{1}{n}, \]
\[ = \sum_{d \mid m} \frac{\mu(d)}{d} \left(\log(y/d) + O(1)\right). \]


Lemma 11 combined with the inequality
\[
\sum_{u_1 \leq x^4} 1/u_1 \cdot \left(1 + \sum_{d|u_1} \log d/d\right) \ll \log x,
\]
transforms (104) in
\[
L(x, \alpha) \geq 8 x^{3/2} \sum_{u_1 \leq x^{3/4}} \varphi(u_1) \left(\log \min \left(x^{\alpha - \frac{1}{4}}, u_1^2\right)\right)
- O(\delta x^{3/2} \log^2 x) - O_\delta(x^{3/2} \log x).
\]
We now appeal to a classical consequence of the theory of Dirichlet series.

**Lemma 12.** As \(y \to \infty\), one has the asymptotic behaviours
\[
\sum_{n \leq y} \varphi(n)/n^2 \sim \frac{4}{\pi^2} \log y,
\]
and
\[
\sum_{n \leq y} \log n \varphi(n)/n^2 \sim \frac{2}{\pi^2} \log^2 y.
\]

**Proof.** For \(\Re s > 1\), consider the Dirichlet series
\[
F(s) := \sum_{2 \nmid n} \varphi(n)/n^s = \zeta(s) \left(1 - \frac{1}{2^s}\right) \prod_{p \geq 3} \left(1 - \frac{1}{p^{s+1}}\right).
\]
As \(s \to 1\), 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. \(\square\)

Returning to (105), one gets the inequality
\[
L(x, \alpha) \geq 8 x^{3/2} \left\{ \sum_{u_1 \leq x^{3/4}} \frac{\varphi(u_1)}{u_1^2} \log u_1 \right. \\
+ \left(\alpha - \frac{1}{2}\right) \log x \sum_{x^{3/4} < u_1 \leq x^{3/4}} \frac{\varphi(u_1)}{2u_1^2} \right\} - O(\delta x^{3/2} \log^2 x) - O_\delta(x^{3/2} \log x).
\]
The second sum on the right hand side of (108) is empty for \(\alpha \geq 1\). Lemma 12 now leads to the inequality
\[
L(x, \alpha) \geq 8 \left\{ \frac{2}{\pi^2} \left(\frac{\alpha}{2} - \frac{1}{4}\right)^2 + \frac{2}{\pi^2} (\alpha - \frac{1}{2}) \left(\frac{1}{2} - \frac{\alpha}{2}\right) - \delta \right\} x^{3/2} \log^2 x
+ \frac{1}{\pi^2} \left((2\alpha - 1)(3 - 2\alpha) - \delta\right) x^{3/2} \log^2 x,
\]
which holds for every \(\delta > 0\) and \(x > x_0(\delta)\). It remains to take \(\delta\) tending to 0 and insert the above lower bound in (33) and (34) to obtain the following inequality
\[
S(x, \alpha) \geq \frac{1}{\pi^2} (1 + (2\alpha - 1) (3 - 2\alpha) - o(1)) x^{3/2} \log^2 x,
\]

Preliminary version – November 25, 2010
uniformly for $\frac{1}{2} \leq \alpha \leq 1$. To pass from a lower bound of $S(x, \alpha)$ to a lower bound on $S^f(x, \alpha)$ ($\alpha \leq 1$), we have to subtracx the cardinality of the set of $(D, \eta_D)$ where $\eta_D$ is of the shape $\eta_D = \varepsilon_5^D$. So we use (29) and appeal to (7) and (110) to deduce the following lower bound

\begin{equation}
S^f(x, \alpha) \geq \frac{u}{\pi^2} \left(1 + (2\alpha - 1)(\frac{13}{4} - \frac{5\alpha}{2}) - o(1)\right) x^{\frac{1}{2}} \log^2 x,
\end{equation}

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 $S^f(x, \alpha)$.

9. Proof of Theorem 1

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

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

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

\begin{equation}
t + u\sqrt{D} = (t_0 + u_0\sqrt{D})^2 = t_0^2 + u_0^2D + 2t_0u_0\sqrt{D}.
\end{equation}

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 $\varepsilon_5^D$, in particular the fact that the integer $u_2$ associated to $\varepsilon_5^D$ (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 $Z(x, \alpha, \varepsilon, k_0)$ of $5$–uples of integers defined by

\begin{equation}Z(x, \alpha, \varepsilon, k_0) := \left\{ (k, t, u_1, u_2, D); 2 \mid u_1u_2, (u_1, u_2) = 1, 0 \leq k \leq k_0, \right. \nonumber \end{equation}

\begin{equation}D \leq x, X_{1/2} \leq 2^k u_1u_2 \leq X_{\alpha}, t + 2^k u_1u_2\sqrt{D} \leq D^{\frac{1}{2} + \alpha}, \nonumber \end{equation}

\begin{equation}t^2 - 1 \equiv 0 \mod 4^k, t \equiv 1 \mod u_1^2, t \equiv -1 \mod u_2^2, t^2 - 4^k u_1^2u_2^2D = 1, \nonumber \end{equation}

\begin{equation}(u_1 \leq u_2 \leq u_1 x^{\frac{1}{2} - \varepsilon} \text{ and } u_1 \leq x^{\frac{1}{2} - \varepsilon}) \text{ or } (u_2 \leq u_1 \leq u_2 x^{\frac{1}{2} - \varepsilon} \text{ and } u_2 \leq x^{\frac{1}{2} - \varepsilon}) \right\} \text{.} \nonumber \end{equation}

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

\[ t + 2^k u_1u_2\sqrt{D} = \varepsilon_D. \]

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

Preliminary version – November 25, 2010
The arithmetical preparation made in §4 can be summarized in the following inequality
\[(114)\quad L(x, \alpha) \geq Z(x, \alpha, \varepsilon, k_0) \quad \text{and} \quad L^f(x, \alpha) \geq Z^f(x, \alpha, \varepsilon, k_0)\]
which is true for every positive \(\varepsilon\) and for every \(k_0 \geq 0\), (see (38), (39) and (42)).

By (103) and (109), we also have the following lower bound
\[(115)\quad Z(x, \alpha, \varepsilon, k_0) \geq \frac{1}{\pi^2} \left\{ (2\alpha - 1)(3 - 2\alpha) - \delta \right\} x^{\frac{1}{2}} \log^2 x,
\]
which is true for every \(\delta\), 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
\[Z(x, \alpha, \varepsilon, k_0) - Z^f(x, \alpha, \varepsilon, k_0) = O_{\varepsilon, k_0}(x^{\frac{1}{2}} \log x),\]
uniformly for \(\frac{1}{2} \leq \alpha \leq 1\) and \(x \geq 2\).

*Proof.* Let \((k, t, u_1, u_2) \in Z(x, \alpha, \varepsilon, k_0)\) such that
\[(116)\quad t + 2^k u_1 u_2 \sqrt{D} = \varepsilon_D^2 := (t_0 + u_0 \sqrt{D})^2.\]
In particular we have
\[(117)\quad \varepsilon_D \leq D^{\frac{3}{4}}.
\]
The relation (116) is equivalent to the two equalities
\[t = t_0^2 + Du_0^2 \quad \text{and} \quad 2^k u_1 u_2 = t_0 u_0.
\]
So we suppose \(1 \leq k \leq k_0\). By the equality \(t_0^2 - Du_0^2 = 1\), we deduce that
\[
either \left( 2^{k-1} \parallel t_0 \right) \text{and} \left( 2 \not\parallel u_0 \right) \text{or} \left( 2^{k-1} \parallel u_0 \right) \text{and} \left( 2 \not\parallel t_0 \right),
\]
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
\[
\begin{cases}
  t^2 \equiv 1 \mod 4^k, \\
  t \equiv 1 \mod \tilde{u}_0^2, \\
  t \equiv -1 \mod \tilde{t}_0^2.
\end{cases}
\]
Since \((\tilde{t}_0, \tilde{u}_0) = 1\), we recognize the congruences appearing in the definition of \(Z(k, \alpha, \varepsilon, k_0)\). In other words, we proved the equalities
\[(118)\quad \tilde{t}_0 = u_2 \quad \text{and} \quad \tilde{u}_0 = u_1.
\]
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
\[(119)\quad 2^{-k+1} \tilde{u}_1 \sqrt{D} \leq \tilde{u}_2 \leq 2^k \tilde{u}_1 \sqrt{D}.
\]
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 \((\varepsilon_D, D)\) is \(< (x(\log x)^{-2})^{\frac{3}{2}} \log^2 x \ll x^{\frac{1}{2}}(\log x)\).
Now suppose \( x(\log x)^{-2} \leq D \leq x \). In these circumstances, (119) implies that
\[
u_2 \geq 2^{-k_0+1}u_1 x^{\frac{1}{3}}(\log x)^{-1}.
\]
If we choose \( x \geq x_1(k_0, \varepsilon) \), this inequality is incompatible with the inequality \( \nu_2 \leq u_1 x^{\frac{1}{3} - \varepsilon} \) appearing in the definition of \( Z(k, \alpha, \varepsilon, k_0) \).

9.1. The final step. We gather the relations (34), (114) to write the following inequality
\[
S^f(x, \alpha) = S^f(x, \frac{1}{2}, \alpha) + L^f(x, \alpha)
\]
\[
\geq S(x, \frac{1}{2}, \alpha) + Z(x, \alpha, k_0) + \left( S^f(x, \frac{1}{2}, \alpha) - S(x, \frac{1}{2}, \alpha) \right)
\]
\[
+ Z^f(x, \alpha, \varepsilon, k_0) - Z(x, \alpha, \varepsilon, k_0),
\]
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 \( \varepsilon \) sufficiently small, in terms of the parameter \( \delta \), we deduce the following inequality
\[
S^f(x, \alpha) \geq 1 - o(1) \frac{\pi}{2} x^{\frac{1}{2}} \log^2 x + \frac{1}{2} \left\{ (2\alpha - 1)(3 - 2\alpha) - \delta \right\} x^{\frac{1}{2}} \log^2 x - O(\delta x^{\frac{1}{2} - \varepsilon} \log x),
\]
which is true for any positive \( \delta \). Letting \( \delta \) 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 \( U \) defined in (61).

**Proposition 3.** Suppose that Conjecture 1, is true for some \( \vartheta_0 \), satisfying \( 0 < \vartheta_0 < 1 \). Then we have the inequality
\[
U(H, U_1, U_2, k) \ll_k H U_1^{\vartheta_0},
\]
uniformly for \( H \geq 1 \) and \( U_1 < U_2 \leq U_1^2 \).

**Proof.** By a direct application of Conjecture 1, we have
\[
U(H, U_1, U_2, k) \ll U_2^{\vartheta_0} \sum_{1 \leq |h| \leq H} \sum_{u_i \sim U_1} (h, u_i^2)^{\frac{1}{2}}.
\]
For \( n \geq 1 \), let \( n^\dagger \) be the integer defined by
\[
n^\dagger := \prod_{p \mid [n]} p^{\frac{1}{[n]}}.
\]
Summing over \( \delta := (h, u_i^2) \), we have
\[
\sum_{1 \leq |h| \leq H} \sum_{u_i \sim U_1} (h, u_i^2)^{\frac{1}{2}} \leq \sum_{\delta \leq 4H U_1^2} \delta^{\frac{1}{2}} \sum_{1 \leq |h| \leq H} \sum_{u_i \sim U_1} \frac{1}{\delta^2} \leq 2HU_1 \sum_{\delta \leq 4H U_1^2} \frac{1}{\delta^2} \ll H U_1.
\]
Inserting this bound in (120), we complete the proof of Proposition 3. \( \square \)
We can now pass to the proof of Theorem 2 itself. We first remark that we have the inequality (62), that is
\[ U(H, U_1, U_2, k) \ll U_1 U_2 x^{-7\varepsilon}, \]
as soon as we have the inequalities
\[ U_1 < U_2 < U_1^2, \text{ and } U_1 U_2^\theta_0 \leq x^{1/2 - 8\varepsilon}. \]
This is a direct consequence of Proposition 3. This implies that, under the assumption of Conjecture 1, the lower bound (104) is improved into
\[ L(x, \alpha) \geq 8 x^{1/2} \sum_{u_1, u_2} \frac{1}{u_1 u_2} - O(\delta x^{1/2} \log^2 x) - O_3(x^{1/2} \log x), \]
where the conditions of summation are
\[ x^{1/2} < u_1 u_2 < x^\alpha \text{ and } \begin{cases} u_1 < u_2, & u_2 \leq u_1 x^{1/2} \text{ and } u_1 \leq x^{1/2}, \\ u_1 < u_2 < u_1^2 \text{ and } u_1 < x^{1/2} u_2^{-0}. \end{cases} \]
If we suppose the inequality
\[ 1/2 \leq \alpha \leq \min \left( \frac{3}{4}, \frac{1}{1 + \theta_0} \right), \]
by drawing a picture in the \((u_1, u_2)\)–plane, we see that the domain of summation (123) is simplified into
\[ x^{1/2} < u_1 u_2 < x^\alpha, \text{ } u_1 < u_2 \text{ and } u_2 \leq u_1 x^{1/2}. \]
After this simplification we can compute the right part of (122). Applying Lemma 11 and following the computation leading to (108), we have
\[ L(x, \alpha) \geq 8 x^{1/2} \left\{ \sum_{u_1 \leq x^{1/4}} \frac{\varphi(u_1)}{u_1^2} \log u_1 + (\alpha - \frac{1}{2}) \log x \right. \sum_{\frac{1}{2} < u_1 < x^{1/4}} \frac{\varphi(u_1)}{u_1^2} \]
\[ \left. + \sum_{x^{1/2} < u_1 < x^{1/4}} \frac{\varphi(u_1)}{u_1^2} \log(x^\alpha u_1^{-2}) \right\} - O(\delta x^{1/2} \log^2 x) - O_3(x^{1/2} \log x). \]
By Lemma 12, we obtain the inequality
\[ L(x, \alpha) \geq 8 x^{1/2} \log^2 x \left\{ \frac{2}{\pi^2} \left( \frac{\alpha}{2} - \frac{1}{4} \right)^2 + \frac{2}{\pi^2} (\alpha - \frac{1}{2}) (\frac{1}{2} - \frac{1}{4}) \right. \]
\[ + \frac{2}{\pi^2} (\frac{1}{2} - \frac{1}{4})^2 + \frac{2}{\pi^2} \left( \frac{\alpha}{2} - \frac{1}{4} \right)^2 - \frac{1}{16} \right\} - O(\delta x^{1/2} \log^2 x) - O_3(x^{1/2} \log x). \]
This gives the inequality
\[ L(x, \alpha) \geq \frac{8}{\pi^2} (\frac{\alpha}{2} - \frac{1}{4}) x^{1/2} \log^2 x - O(\delta x^{1/2} \log^2 x), \]
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
\[
L^f(x, \alpha) \geq \frac{8}{\pi^2} \left( \frac{\alpha}{2} - \frac{1}{4} \right) x^{1/2} \log^2 x - O(\delta x^{1/2} \log^2 x),
\]
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 \( u_1 \leq x^{1/4} - \varepsilon \) and \( u_2 \leq x^{1/4} - \varepsilon \).

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

References


Université Paris-Sud, Laboratoire de Mathématique, UMR 8628, Orsay, F–91405 France, CNRS, Orsay, F–91405, France
E-mail address: Étienne.Fouvry@math.u-psud.fr

Preliminary version – November 25, 2010