COMPOSITIO MATHEMATICA

Counting fundamental solutions to the Pell equation with prescribed size

Ping Xi

Counting fundamental solutions to the Pell equation with prescribed size

Ping Xi

Abstract

The cardinality of the set of $D \leqslant x$ for which the fundamental solution of the Pell equation $t^2 - Du^2 = 1$ is less than $D^{1/2+\alpha}$ with $\alpha \in [\frac{1}{2}, 1]$ is studied and certain lower bounds are obtained, improving previous results of Fouvry by introducing the q-analogue of van der Corput method to algebraic exponential sums with smooth moduli.

1. Introduction and main results

Let D be a non-square positive integer. The Pell equation is usually referred to as

$$t^2 - Du^2 = 1, \tag{1.1}$$

to which the solution can be written in the usual form

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

The classical Dirichlet's unit theorem asserts that the set of solutions to (1.1) is non-trivial and has the form

$$\{\eta_D : \eta_D \text{ solution of } (1.1)\} = \{\pm\varepsilon_D^n : n \in \mathbf{Z}\},$$

where ε_D is called the fundamental solution of (1.1) and is given by

$$\varepsilon_D := \inf\{\eta_D : \eta_D > 1\}.$$

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

$$\varepsilon_D > 2\sqrt{D}.$$

We are interested in counting the integers D for which ε_D or η_D is less than a fixed power of D.
    For $\alpha > 0$ and $x \geqslant 2$, define

$$S(x, \alpha) := |\{(\eta_D, D) : 2 \leqslant D \leqslant x, \ D \neq \square, \ \eta_D \leqslant D^{1/2+\alpha}\}|,$$
$$S^{\mathrm{f}}(x, \alpha) := |\{(\varepsilon_D, D) : 2 \leqslant D \leqslant x, \ D \neq \square, \ \varepsilon_D \leqslant D^{1/2+\alpha}\}|.$$

In his pioneer work, Hooley [Hoo84] proved the following theorem.

THEOREM A (Hooley). *Let ε_0 satisfy $0 < \varepsilon_0 < \frac{1}{2}$. As $x \to +\infty$, one has*

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

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

In the same paper, Hooley [Hoo84, p. 110] also made the following conjecture.

CONJECTURE 1.1 (Hooley). *For any given $\alpha > \frac{1}{2}$, we have*

$$S^{\mathrm{f}}(x, \alpha) = \frac{1}{\pi^2} (4\alpha - 1 + C(\alpha) + o(1)) \sqrt{x} \log^2 x,$$

where

$$C(\alpha) = \begin{cases} 0, & \alpha \in \left]\frac{1}{2}, 1\right], \\ \frac{1}{18}(\alpha - 1)^2, & \alpha \in \left]1, \frac{5}{2}\right], \\ \frac{1}{24}(4\alpha - 7), & \alpha \in \left]\frac{5}{2}, +\infty\right[. \end{cases}$$

Fouvry [Fou16] made a first significant step towards Hooley's conjecture in the case $\alpha \in \left]\frac{1}{2}, 1\right]$. In fact, he proved the following theorem.

THEOREM B (Fouvry). *As $x \to +\infty$, one has*

$$S^{\mathrm{f}}(x, \alpha) \geqslant \frac{1}{\pi^2} \left(4\alpha - 1 - 4\left(\alpha - \frac{1}{2}\right)^2 - o(1) \right) \sqrt{x} \log^2 x \tag{1.2}$$

and

$$S(x, \alpha) \geqslant \frac{1}{\pi^2} \left(4\alpha - 1 - 3\left(\alpha - \frac{1}{2}\right)^2 - o(1) \right) \sqrt{x} \log^2 x \tag{1.3}$$

uniformly for $\alpha \in \left[\frac{1}{2}, 1\right]$.

Moreover, Fouvry [Fou16] considered a conjectural estimation for short exponential sums.

CONJECTURE 1.2. *There exists an absolute $\vartheta \in \left[\frac{1}{2}, 1\right[$, such that for any integer $k \geqslant 0$, one has the inequality*

$$\sum_{\substack{N < n \leqslant N_1 \\ m \equiv a \,(\mathrm{mod}\, 4^k), (m,n)=1}} e\left(\frac{h\overline{n}^2}{m^2} \right) \ll_k (h, m^2)^{1/2} N^\vartheta$$

uniformly for any integers a, h, m satisfying $h \neq 0, m \geqslant 1$ and $2 \nmid am$, for any real number N satisfying $m \leqslant N \leqslant m^2$ and $N < N_1 \leqslant 2N$.

Assuming Conjecture 1.2, Fouvry [Fou16] derived the following stronger lower bounds.

THEOREM C (Fouvry). *Assume that Conjecture 1.2 is true for some $\vartheta \in \left[\frac{1}{2}, 1\right[$. As $x \to +\infty$, one has*

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

and

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

uniformly for $\alpha \in \left[\frac{1}{2}, \frac{1}{1+\vartheta}\right]$.

The first inequality coincides with Hooley's Conjecture 1.1 when α is slightly larger than $\frac{1}{2}$. On the other hand, Bourgain [Bou15] considered Conjecture 1.2 itself. In particular, he succeeded in saving a power of $\log N$ in the trivial bound for the sum involved. This allows him to improve the lower bound (1.2) by replacing the term $-4(\alpha - \frac{1}{2})^2$ with the term $O((\alpha - \frac{1}{2})^{2+c})$, where c is some positive constant.

Bourgain's improvement is of interest only if α is quite close to $\frac{1}{2}$ and one should pay much more attention if every parameter is to be made effective. The aim of this paper is to give another improvement to Theorem B towards Conjecture 1.1.

THEOREM 1.1. *Let* $x \to +\infty$. *For any fixed* $\theta \in \,]0, \frac{1}{2}[$, *we have*

$$S^{\mathrm{f}}(x, \alpha) \geqslant \frac{1}{\pi^2}\left\{4\alpha - 1 - 4\left(\alpha - \frac{1}{2}\right)^2 + \frac{1}{6}\rho\left(\frac{1}{\theta}\right)F_\theta(\alpha) - o(1)\right\}\sqrt{x}\log^2 x \qquad (1.4)$$

and

$$S(x, \alpha) \geqslant \frac{1}{\pi^2}\left\{4\alpha - 1 - 3\left(\alpha - \frac{1}{2}\right)^2 + \frac{1}{6}\rho\left(\frac{1}{\theta}\right)F_\theta(\alpha) - o(1)\right\}\sqrt{x}\log^2 x \qquad (1.5)$$

uniformly in $\alpha \in [\frac{1}{2}, 1]$, *where* ρ *is the Dickman function given by* (A.1) *and*

$$F_\theta(\alpha) = \begin{cases} 24\alpha - 4(5 + 2\theta)\alpha^2 - (7 - 2\theta) & \alpha \in [\frac{1}{2}, \frac{6}{11+2\theta}], \\ 864(11 + 2\theta)^{-2} - (7 - 2\theta) & \alpha \in \,]\frac{6}{11+2\theta}, 1]. \end{cases} \qquad (1.6)$$

Fix $\theta \in \,]0, \frac{1}{2}[$. One may check that $F_\theta(\alpha)$ is always positive for $\alpha \in \,]\frac{1}{2}, 1]$ and monotonically increasing in $\alpha \in [\frac{1}{2}, \frac{6}{11+2\theta}]$. In particular, for $\alpha \in \,]\frac{1}{2}, \frac{6}{11}[$, we take $\theta = 3/\alpha - \frac{11}{2}$ such that $\alpha = \frac{6}{11+2\theta}$ and

$$\frac{1}{6}\rho\left(\frac{1}{\theta}\right)F_\theta(\alpha) = \rho\left(\frac{2\alpha}{6 - 11\alpha}\right)\frac{4(\alpha - 1/2)^3 + 6(\alpha - 1/2)^2}{\alpha}.$$

Moreover, $\rho(2\alpha/(6 - 11\alpha))/\alpha > 0.3008$ for $\alpha \in \,]\frac{1}{2}, \frac{35}{69}]$. Hence we may conclude the following consequence.

COROLLARY 1.1. *Let* $x \to +\infty$. *Uniformly for* $\alpha \in \,]\frac{1}{2}, \frac{35}{69}]$, *we have*

$$S^{\mathrm{f}}(x, \alpha) \geqslant \frac{1}{\pi^2}\left\{4\alpha - 1 - \frac{11}{5}\left(\alpha - \frac{1}{2}\right)^2 + \frac{6}{5}\left(\alpha - \frac{1}{2}\right)^3\right\}\sqrt{x}\log^2 x$$

and

$$S(x, \alpha) \geqslant \frac{1}{\pi^2}\left\{4\alpha - 1 - \frac{6}{5}\left(\alpha - \frac{1}{2}\right)^2 + \frac{6}{5}\left(\alpha - \frac{1}{2}\right)^3\right\}\sqrt{x}\log^2 x.$$

The framework of the proof is based on [Fou16]. To make the paper clear, we will present the proof as complete as possible, but also with omitting some details that are not quite essential to understand the underlying ideas.

The key point of proving Theorem 1.1 is a variant of Conjecture 1.2 that can be proved unconditionally. More precisely, if one allows the moduli m^2 to be smooth numbers (integers free of large prime factors), it is possible to prove the existence of ϑ in Conjecture 1.2 as long as N is not too small. The details can be referred to Theorem 3.1 and §4. We will adopt the q-analogue of van der Corput method, which can be at least dated back to Heath-Brown [Hea78] on the proof of Weyl-type subconvex bounds for Dirichlet L-functions to well-factorable moduli.

Instead of the AB-process in [Hea78], we apply the BAB-process by introducing a completion in the initial step. It is expected that one can do better on the exponential sums in Conjecture 1.2 if better factorizations of the moduli are imposed; see [WX16] for instance in the case of squarefree moduli. However, the improvements to Theorem 1.1 would be rather slight, since the density of smooth numbers decays rapidly when the size of their prime factors decreases.

As an extension to Theorem 1.1, one may consider

$$S^{\mathrm{f}}(x; \alpha, \beta) := |\{(\varepsilon_D, D) : 2 \leqslant D \leqslant x, \ D \neq \square, \ D^{1/2+\beta} \leqslant \varepsilon_D \leqslant D^{1/2+\alpha}\}|$$

for $\alpha > \beta \geqslant 0$. Conjecture 1.1 would yield asymptotics for $S(x; \alpha, \beta)$ while α, β are of different prescribed sizes. A weaker statement would assert that, for any $\alpha > \beta \geqslant 0$, there exists a positive constant $c = c(\alpha, \beta)$, such that

$$S^{\mathrm{f}}(x; \alpha, \beta) \geqslant c\sqrt{x} \log^2 x$$

for all large $x > x_0(\alpha, \beta)$. This weaker statement was made unconditionally by Fouvry and Jouve [FJ12] whenever $\beta < \frac{3}{2}$. It is expected that the arguments in this paper can enlarge the admissible range of β.

Notation and convention

As usual, $e(x) = e^{2\pi i x}$, φ denotes the Euler function and $\omega(q)$ counts the number of distinct prime factors of q. The variable p is reserved for prime numbers. Denote by $q^\flat$ and $q^\sharp$ the squarefree and squarefull parts of q, respectively; namely,

$$q^\flat = \prod_{p\|q} p, \quad q^\sharp = \prod_{p^\nu\|q, \nu \geqslant 2} p^\nu.$$

For a real number x, denote by $[x]$ its integral part and $\|x\| = \min_{n \in \mathbf{Z}} |x - n|$. From time to time, we use (m, n) to denote the greatest common divisor of m, n, and also to denote a tuple given by two coordinates; these will not cause confusions as one will see later. The symbol $*$ in summation reminds us to sum over primitive elements such that poles of the summand are avoided. For a function $f \in L^1(\mathbf{R})$, its Fourier transform is defined as

$$\widehat{f}(y) := \int_{\mathbf{R}} f(x) e(-yx) \, dx.$$

We use ε to denote a very small positive number, which might be different at each occurrence; we also write $X^\varepsilon \log X \ll X^\varepsilon$. The convention $n \sim N$ means $N < n \leqslant 2N$.

2. Fundamental transformations: after Hooley and Fouvry

We first make some fundamental transformations following the arguments of Hooley and Fouvry. For some conclusions, we omit the proof and the detailed arguments can be found in [Hoo84] and [Fou16].

2.1 An initial transformation
First, we write

$$S(x, \alpha) = \sum_{\substack{\square \neq D \leqslant x \\ t^2 - Du^2 = 1 \\ 1 < t + u\sqrt{D} \leqslant D^{1/2+\alpha}}} \sum_{t \geqslant 1} \sum_{u \geqslant 1} 1 = \sum_{1 \leqslant u \leqslant X_\alpha} \sum_{\substack{Y_2(u,\alpha) \leqslant t \leqslant Y_3(u) \\ Du^2 = t^2 - 1}} 1, \tag{2.1}$$

where

$$X_\alpha := \tfrac{1}{2}(x^\alpha - x^{-1-\alpha}); \tag{2.2}$$

$$Y_3(u) := \sqrt{xu^2 + 1}; \tag{2.3}$$

$$Y_2(u, \alpha) := \sqrt{Y_1(u, \alpha)u^2 + 1}. \tag{2.4}$$

Here, $Y_1(u, \alpha)$ is a function in u, implicitly defined by the equation

$$u = \tfrac{1}{2}(Y_1(u, \alpha)^\alpha - Y_1(u, \alpha)^{-1-\alpha}).$$

We have the following asymptotic characterization for $Y_2(u, \alpha)$. The proof can be found in [Fou16, Lemma 2.1] and the subsequent remark.

LEMMA 2.1. *Let $\alpha > 0$. The function $u \mapsto Y_2(u, \alpha)$ is of $\mathscr{C}^\infty$-class and satisfies the inequalities*

$$2^{1/2\alpha}u^{1+1/2\alpha} < Y_2(u, \alpha) < (2^{1/2\alpha} + o(1))u^{1+1/2\alpha} \tag{2.5}$$

and

$$\frac{d}{du}Y_2(u, \alpha) = O(u^{1/2\alpha}) \tag{2.6}$$

as $u \to +\infty$.

2.2 A first dissection of $S(x, \alpha)$

We truncate the u-sum in (2.1) at $X_{1/2}$, and the contributions from $u \leqslant X_{1/2}$ and $u > X_{1/2}$ are respectively denoted by $A(x, \alpha)$ and $B(x, \alpha)$. Therefore,

$$S(x, \alpha) = A(x, \alpha) + B(x, \alpha). \tag{2.7}$$

Accordingly, we may define $A^{\mathrm{f}}(x, \alpha)$ and $B^{\mathrm{f}}(x, \alpha)$ by introducing the extra restriction $t + u\sqrt{D} = \varepsilon_D$ to the equation $t^2 - Du^2 = 1$.

As stated by Fouvry [Fou16, Formula (4.5)], we have the following.

LEMMA 2.2. *Let $\alpha \in [\tfrac{1}{2}, 1]$. As $x \to +\infty$, we have*

$$A(x, \alpha) = \left(\frac{1}{\pi^2} + o(1)\right)\sqrt{x}\log^2 x. \tag{2.8}$$

Our task thus reduces to proving a lower bound for $B(x, \alpha)$. Put $\mathcal{R}(u) := \{\Omega \pmod{u^2} : \Omega^2 \equiv 1 \pmod{u^2}\}$. We then have

$$B(x, \alpha) = \sum_{X_{1/2} < u \leqslant X_\alpha} \sum_{\Omega \in \mathcal{R}(u)} \sum_{\substack{Y_2(u,\alpha) \leqslant t \leqslant Y_3(u) \\ t \equiv \Omega \pmod{u^2}}} 1. \tag{2.9}$$

Put $\gamma(u) = |\mathcal{R}(u)|$. Thus $u \mapsto \gamma(u)$ is multiplicative and satisfies

$$\begin{cases} \gamma(2) = 2, \gamma(2^k) = 4 & \text{for } k \geqslant 2, \\ \gamma(p^\ell) = 2 & \text{for } p \geqslant 3, \ell \geqslant 1. \end{cases} \tag{2.10}$$

2.3 Analysis of $\mathcal{R}(u)$

For $u \geqslant 1$, write $u = 2^k u_0$, where u_0 is an odd integer. The choice of (k, u_0) is unique for each $u \geqslant 1$. The Chinese remainder theorem implies

$$\Omega^2 \equiv 1 \pmod{u^2} \Longleftrightarrow \begin{cases} \Omega^2 \equiv 1 \pmod{u_0^2}, \\ \Omega^2 \equiv 1 \pmod{4^k}. \end{cases} \tag{2.11}$$

In this way, one can establish a bijection between $\mathcal{R}(u)$ and $\mathcal{R}(2^k) \times \mathcal{R}(u_0)$. Starting from (2.9), we decompose $B(x, \alpha)$ by

$$B(x, \alpha) = \sum_{k \geqslant 0} \sum_{\xi \in \mathcal{R}(2^k)} B(x, \alpha; \xi, k), \tag{2.12}$$

where

$$B(x, \alpha; \xi, k) = \sum_{\substack{2^{-k} X_{1/2} < u \leqslant 2^{-k} X_\alpha \\ 2 \nmid u}} \sum_{\Omega \in \mathcal{R}(u)} \sum_{\substack{Y_2(2^k u, \alpha) \leqslant t \leqslant Y_3(2^k u) \\ t \equiv \Omega \pmod{u^2} \\ t \equiv \xi \pmod{4^k}}} 1.$$

The task will be evaluating $B(x, \alpha; \xi, k)$ for all $k \geqslant 0$ and $\xi \in \mathcal{R}(2^k)$. This would require the following description of $\mathcal{R}(u)$ that allows us to create one more variable. This is Lemma 4.1 in [Fou16].

LEMMA 2.3. *Let u be a positive odd integer. Then there is a bijection Φ between the set of coprime decompositions of u*

$$\mathcal{D}(u) := \{(u_1, u_2) : u_1 u_2 = u, \ (u_1, u_2) = 1, \ u_1, u_2 \geqslant 1\}$$

and the set of roots of congruence

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

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

$$\Phi(u_1, u_2) \equiv -\overline{u}_1^2 u_1^2 + \overline{u}_2^2 u_2^2 \pmod{u^2}. \tag{2.13}$$

Here $\overline{u}_1 u_1 \equiv 1 \,(\mathrm{mod}\, u_2)$ and $\overline{u}_2 u_2 \equiv 1 \,(\mathrm{mod}\, u_1)$.

With the help of Lemma 2.3, we may rewrite $B(x, \alpha; k, \xi)$ as

$$B(x, \alpha; \xi, k) = \sum_{\substack{2^{-k} X_{1/2} < u_1 u_2 \leqslant 2^{-k} X_\alpha \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum_{\substack{Y_2(2^k u_1 u_2, \alpha) \leqslant t \leqslant Y_3(2^k u_1 u_2) \\ t \equiv \Phi(u_1, u_2) \,(\mathrm{mod}\, u_1^2 u_2^2) \\ t \equiv \xi \,(\mathrm{mod}\, 4^k)}} 1$$

$$=: B^>(x, \alpha; \xi, k) + B^<(x, \alpha; \xi, k),$$

where $B^>(x, \alpha; \xi, k)$ and $B^<(x, \alpha; \xi, k)$ correspond to the restrictions $u_1 > u_2$ and $u_1 < u_2$, respectively. Since the treatments of $B^>(x, \alpha; \xi, k)$ and $B^<(x, \alpha; \xi, k)$ are similar, it suffices to study $B^<(x, \alpha; \xi, k)$ as presented in the next section.

We close this section with the trivial equality

$$S(x, \alpha) = S^{\mathrm{f}}(x, \alpha) + S\left(x, \frac{\alpha}{2} - \frac{1}{4}\right), \quad \frac{1}{2} < \alpha \leqslant 1, \tag{2.14}$$

which is a consequence of the equivalence

$$\varepsilon_D^2 \leqslant D^{1/2+\alpha} \Longleftrightarrow \varepsilon_D \leqslant D^{1/2+(\alpha/2-1/4)}.$$

This allows us to transfer between $S^{\mathrm{f}}(x, \alpha)$ and $S(x, \alpha)$.

2384

COUNTING FUNDAMENTAL SOLUTIONS TO THE PELL EQUATION

3. Lower bound for $B(x,\alpha)$

In order to conclude the lower bound for $B(x,\alpha)$, we now start the study of $B^<(x,\alpha;\xi,k)$. Recall that

$$B^<(x,\alpha;\xi,k) = \sum\sum_{\substack{2^{-k}X_{1/2}<u_1u_2\leqslant 2^{-k}X_\alpha \\ u_1<u_2 \\ (2,u_1u_2)=(u_1,u_2)=1}} \sum_{\substack{Y_2(2^ku_1u_2,\alpha)\leqslant t\leqslant Y_3(2^ku_1u_2) \\ t\equiv\Phi(u_1,u_2)\,(\mathrm{mod}\,u_1^2u_2^2) \\ t\equiv\xi\,(\mathrm{mod}\,4^k)}} 1.$$

We would like to drop the multiplicative constraints $2^{-k}X_{1/2} < u_1u_2 \leqslant 2^{-k}X_\alpha$ and sum over u_1, u_2 separately. To do so, we may introduce the following inequality

$$B^<(x,\alpha;\xi,k) \geqslant \sum_{\mathbf{U}}\sum_{\xi_1}\sum_{\xi_2} B(x,\alpha;\mathbf{U},\xi,\xi_1,\xi_2,k), \tag{3.1}$$

where we have the following.
- The summation is over all $\mathbf{U} = (U_1, U_2)$ satisfying

$$U_1 < U_2, \quad X_{1/2} < 2^k U_1 U_2 \leqslant \frac{X_\alpha}{8},$$

  and U_1, U_2 being powers of 2.
- The summation is over all $\xi_1, \xi_2\,(\mathrm{mod}\,4^k)$ satisfying $(\xi_1\xi_2, 4^k) = 1$.
- We have defined

$$B(x,\alpha;\mathbf{U},\xi,\xi_1,\xi_2,k) := \sum\sum_{\substack{u_1\sim U_1,u_2\sim U_2 \\ u_1\equiv\xi_1,u_2\equiv\xi_2\,(\mathrm{mod}\,4^k) \\ (2,u_1u_2)=(u_1,u_2)=1}} \sum_{\substack{Y_2(2^ku_1u_2,\alpha)\leqslant t\leqslant Y_3(2^ku_1u_2) \\ t\equiv\Phi(u_1,u_2)\,(\mathrm{mod}\,u_1^2u_2^2) \\ t\equiv\xi\,(\mathrm{mod}\,4^k)}} 1.$$

Of course the condition $(2, u_1u_2) = 1$ can be dropped when $k \geqslant 1$. The parameter α is supposed to be fixed and the congruence conditions modulo 4^k are harmless. So to shorten the notation, we write $B(x,\mathbf{U}) := B(x,\alpha;\mathbf{U},\xi,\xi_1,\xi_2,k)$. Finally we shall not make precise the dependence on k of some O-symbols, since we shall work with a finite number of values of k. The case $k = 0$ is typical and really reflects the difficulties of the method.

3.1 Reduction to exponential sums: after Fouvry
The congruence condition $t \equiv \Phi(u_1, u_2)\,(\mathrm{mod}\,u_1^2u_2^2)$ implies that $t \equiv -1\,(\mathrm{mod}\,u_2^2)$, i.e., $t = -1+\ell u_2^2$ for some $\ell \in \mathbf{Z}$. Since $Y_2(2^ku_1u_2,\alpha) \leqslant t \leqslant Y_3(2^ku_1u_2)$, then there is no such t if u_2 is too large, for instance when

$$u_2^2 > \sqrt{4^k x u_1^2 u_2^2 + 1} + 1.$$

Hence we can suppose

$$U_2 \leqslant 2^{k+2}\sqrt{x}U_1, \tag{3.2}$$

otherwise $B(x,\mathbf{U}) = 0$.

Since u_1u_2 is odd, we deduce from (2.13) the equivalence

$$t \equiv \Phi(u_1,u_2)\,(\mathrm{mod}\,u_1^2u_2^2),\ t\equiv\xi\,(\mathrm{mod}\,4^k) \Longleftrightarrow t\equiv t_0\,(\mathrm{mod}\,4^ku_1^2u_2^2)$$

2385

with

$$t_0 \equiv \xi u_1^2 u_2^2 \cdot \overline{(u_1^2 u_2^2)} + (2u_2^2 \overline{u_2^2} - 1)4^k \overline{4^k} \,(\mathrm{mod}\, 4^k u_1^2 u_2^2),$$

where $u_1^2 u_2^2 \cdot \overline{(u_1^2 u_2^2)} \equiv 1 \,(\mathrm{mod}\, 4^k)$, $u_2^2 \overline{u_2^2} \equiv 1 \,(\mathrm{mod}\, u_1^2)$ and $4^k \overline{4^k} \equiv 1 \,(\mathrm{mod}\, u_1^2 u_2^2)$. It follows that

$$\frac{t_0}{4^k u_1^2 u_2^2} \equiv \kappa - \frac{1}{4^k u_1^2 u_2^2} + 2\frac{\overline{4^k u_2^2}}{u_1^2} \,(\mathrm{mod}\, 1)$$

with $\kappa := (\xi + 1)\overline{\xi_1^2 \xi_2^2}/4^k$. The three terms on the right-hand side have completely different structures: the first one is constant, the second one changes very slowly when u_1 and u_2 vary, the third one oscillates a lot when u_2 varies with u_1 fixed.

For each fixed k, we rewrite the sum $B(x, \mathbf{U})$ as

$$B(x, \mathbf{U}) = B(x, \alpha; \mathbf{U}, \xi, \xi_1, \xi_2, k) = \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum_{\substack{Y_2 \leqslant t \leqslant Y_3 \\ t \equiv t_0 \,(\mathrm{mod}\, 4^k u_1^2 u_2^2)}} 1,$$

where $Y_2 := Y_2(2^k u_1 u_2, \alpha)$ and $Y_3 := Y_3(2^k u_1 u_2)$. As in [Fou16], we smooth the t-sum via the following lemma.

LEMMA 3.1. *For every $\delta > 0$ there exists a smooth function $g : \mathbf{R} \to \mathbf{R}$ which has the two properties*

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

and

$$\int_{\mathbf{R}} g(y)\, dy = 1 - \delta.$$

Let g be a smooth function given as in Lemma 3.1. Hence

$$B(x, \mathbf{U}) \geqslant \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum_{\substack{t \in \mathbf{Z} \\ t \equiv t_0 \,(\mathrm{mod}\, 4^k u_1^2 u_2^2)}} g\left(\frac{t - (Y_2 + Y_3)/2}{Y_3 - Y_2}\right). \tag{3.3}$$

By Poisson summation, the t-sum becomes

$$\frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} \sum_{h \in \mathbf{Z}} \widehat{g}\left(\frac{h(Y_3 - Y_2)}{4^k u_1^2 u_2^2}\right) e\left(h\kappa + 2h\frac{\overline{4^k u_2^2}}{u_1^2} - \frac{h(2 + Y_2 + Y_3)}{2 \cdot 4^k u_1^2 u_2^2}\right).$$

From integration by parts, we have $\widehat{g}(y) \ll (1 + |y|)^{-A}$ for any $A \geqslant 0$. Note that

$$\frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} \asymp \frac{\sqrt{x}}{U_1 U_2}.$$

The above sum over h can be truncated to $0 \leqslant |h| \leqslant H$ with $H = U_1 U_2 x^{-1/2+\varepsilon}$, and the remaining contribution is at most $O(x^{-2017})$. Therefore,

$$B(x, \mathbf{U}) \geqslant \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} \sum_{0 \leqslant |h| \leqslant H} \widehat{g}\left(\frac{h(Y_3 - Y_2)}{4^k u_1^2 u_2^2}\right)$$

$$\times e\left(h\kappa + 2h\frac{\overline{4^k u_2^2}}{u_1^2} - \frac{h(2 + Y_2 + Y_3)}{2 \cdot 4^k u_1^2 u_2^2}\right) + O(x^{-1949})$$

$$= B_1(x, \mathbf{U}) + B_2(x, \mathbf{U}) + O(x^{-1949}),$$

where $B_1(x, \mathbf{U})$ and $B_2(x, \mathbf{U})$ are used to denote contributions from $h = 0$ and $h \neq 0$, respectively.
First,

$$B_1(x, \mathbf{U}) = (1 - \delta) \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2},$$

which is $\asymp \sqrt{x}$. It is also desirable to show that

$$B_2(x, \mathbf{U}) \ll x^{1/2 - \varepsilon_0} \tag{3.4}$$

for some $\varepsilon_0 > 0$. By standard tools from analysis (see [Fou16] for details), it suffices to prove that

$$\sum_{\substack{h \leqslant H \\ h \equiv h_0 \,(\mathrm{mod}\, 4^k)}} \sum_{\substack{u_1 \in]U_1, U_1^*] \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum_{u_2 \in]U_2, U_2^*]} e\left(2h\frac{\overline{4^k u_2^2}}{u_1^2}\right) \ll U_1 U_2 x^{-\varepsilon_0}, \tag{3.5}$$

where $U_j < U_j^* \leqslant 2U_j$, $j = 1, 2$. After transforming the u_2-sum to a complete sum $T(\cdot, u_1^2)$, where

$$T(h, q) = \sum_{x \,(\mathrm{mod}\, q)}^* e\left(\frac{h\overline{x^2}}{q}\right) = \sum_{x \,(\mathrm{mod}\, q)}^* e\left(\frac{hx^2}{q}\right),$$

Fouvry [Fou16] evaluated $T(\cdot, u_1^2)$ in terms of classical Gauss sums and Jacobi symbols. He then arrived at a bilinear form involving Jacobi symbols, for which a celebrated estimate due to Heath-Brown [Hea95] was applied. Amongst some other delicate arguments, Fouvry was able to prove (3.4) under the conditions

$$U_1 \leqslant x^{1/4 - 5\varepsilon_0}, \quad U_2 \leqslant U_1 x^{1/2 - 5\varepsilon_0}, \tag{3.6}$$

in which case he obtained the lower bound

$$B(x, \mathbf{U}) \geqslant (1 - \delta) \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1}} \sum \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} + O(x^{1/2 - \varepsilon_0}). \tag{3.7}$$

To obtain a better lower bound for $B(x, \alpha)$ and thus for $S(x, \alpha)$, it is natural to expect that (3.4) and (3.7) can hold in larger ranges of U_1, U_2. However, it seems rather difficult when U_1 is quite close to U_2 since the u_2-sum is too short in the sense of the Pólya–Vinogradov barrier. In fact, Bourgain [Bou15] managed to control the left-hand side in (3.5), but with a saving of a small power of $\log x$ rather than that of x. This allows him to improve upon Fouvry when α is rather close to $\frac{1}{2}$ in Theorem B.

2387

In our subsequent argument, we will specialize u_1 with special structures in the original sum (3.3) before Poisson summation. More precisely, we will consider those u_1 consisting of only small prime factors, so that u_1 has good factorizations, which enable us to control the exponential sums in (3.5) even though U_1 is quite close to U_2.

3.2 Lower bound of $B(x, \mathbf{U})$: smooth approach

A positive integer n is said to be y-smooth (or friable) if all prime factors of n do not exceed y. Let $\theta \in \,]0, \frac{1}{2}[$ be a fixed number. If n is n^θ-smooth, the inclusion–exclusion principle yields the existence of the divisor $d \mid n$ such that $n^{\theta_0} \leqslant d \leqslant n^{\theta_0+\theta}$ for any $\theta_0 \in [0, 1-\theta]$.

We now restrict these u_1 in the right-hand side of (3.3) to U_1^θ-smooth numbers and put

$$B^*(x, \mathbf{U}) = \sum\sum_{\substack{u_1 \sim U_1, u_2 \geqslant 1 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} g_1\!\left(\frac{u_2}{U_2}\right) \sum_{\substack{t \in \mathbf{Z} \\ t \equiv t_0 \,(\mathrm{mod}\, 4^k u_1^2 u_2^2)}} g\!\left(\frac{t - (Y_2 + Y_3)/2}{Y_3 - Y_2}\right), \qquad (3.8)$$

where $g_1(y) = g(y - \frac{3}{2})$ with g given as in Lemma 3.1. Following the similar arguments of Fouvry, we may derive that

$$B^*(x, \mathbf{U}) \geqslant B_1^*(x, \mathbf{U}) + B_2^*(x, \mathbf{U}) + O(x^{-1949}),$$

where

$$B_1^*(x, \mathbf{U}) = (1 - \delta) \sum\sum_{\substack{u_1 \sim U_1, u_2 \geqslant 1 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} g_1\!\left(\frac{u_2}{U_2}\right) \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}$$

$$\geqslant (1 - \delta)^2 \sum\sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2},$$

and we expect to show that

$$B_2^*(x, \mathbf{U}) \ll x^{1/2 - \varepsilon_0} \qquad (3.9)$$

for some $\varepsilon_0 > 0$, for which it suffices to prove, for all $U_1^* \in \,]U_1, 2U_1\,]$, that

$$\sum_{\substack{h \leqslant H \\ h \equiv h_0 \,(\mathrm{mod}\, 4^k)}} \sum_{\substack{u_1 \in \,]U_1, U_1^*] \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} \sum_{u_2 \geqslant 1} g_1\!\left(\frac{u_2}{U_2}\right) e\!\left(2h \frac{\overline{4^k u_2^2}}{u_1^2}\right) \ll U_1 U_2 x^{-\varepsilon_0}. \qquad (3.10)$$

We will prove the following.

THEOREM 3.1. *There exists some $\varepsilon_0 \in \,]0, 10^{-2017}[$ such that (3.10) holds, provided that*

$$U_1^{(8+2\theta)/3} U_2 \leqslant x^{1-2\varepsilon_0}, \quad U_2 \leqslant U_1 x^{1/2 - 5\varepsilon_0}. \qquad (3.11)$$
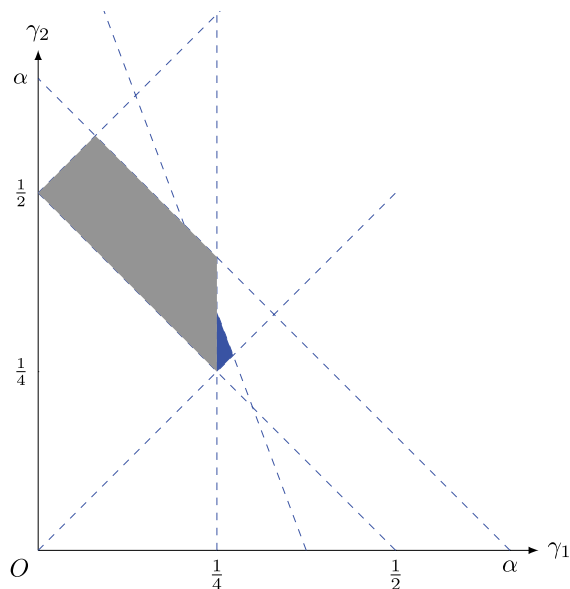
FIGURE 1. Admissible values of (γ_1, γ_2).

Put $U_1 = x^{\gamma_1}$ and $U_2 = x^{\gamma_2}$. In addition to the restrictions $\gamma_2 < \gamma_1 + \frac{1}{2}, \frac{1}{2} < \gamma_1 + \gamma_2 < \alpha$, (3.6) requires $\gamma_1 < \frac{1}{4}$, and we require $\gamma_2 < 1 - \frac{26}{9}\gamma_1$ in the particular case $\theta = \frac{1}{36}$. In Figure 1, the shaded area shows what we can gain more than the previous approach (we are gaining relatively more as α becomes closer to $\frac{1}{2}$).

The proof of Theorem 3.1 will be given in the next section. To see the advantage of our approach, one may consider the particular case $U_1 = U_2$, and our first restriction will reduce to $U_1 \leqslant x^{3/(11+2\theta)-\varepsilon_0}$; however, the stronger restriction $U_1 \leqslant x^{1/4-5\varepsilon_0}$ in (3.6) is required.

Therefore, we may obtain the lower bound

$$B(x, \mathbf{U}) \geqslant (1-\delta)^2 \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2) = (u_1, u_2) = 1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} + O(x^{1/2-\varepsilon_0}) \tag{3.12}$$

subject to the restrictions in (3.11).

3.3 A weakened form of Theorem 1.1

Up to now, we have two lower bounds for $B(x, \mathbf{U})$, i.e., (3.7) and (3.12), subject to the restrictions in (3.6) and (3.11), respectively. In what follows, we will take into account all such admissible tuples $(k, \xi, \xi_1, \xi_2, U_1, U_2)$, for which we appeal to (3.7) if (3.6) is satisfied, and appeal to (3.12) if (3.6) is not satisfied but (3.11) is valid. To this end, we define two sets of tuples

$$\mathscr{U}_1 := \left\{ (U_1, U_2) : U_1 < U_2, \frac{\sqrt{x}}{2} < 2^k U_1 U_2 \leqslant \frac{x^\alpha}{16}, U_1 \leqslant x^{1/4-\eta}, U_2 \leqslant U_1 x^{1/2-\eta} \right\},$$

and

$$\mathscr{U}_2 := \left\{ (U_1, U_2) : U_1 < U_2, \frac{\sqrt{x}}{2} < 2^k U_1 U_2 \leqslant \frac{x^\alpha}{16}, U_1^{(8+2\theta)/3} U_2 \leqslant x^{1-\eta}, U_2 \leqslant U_1 x^{1/2-\eta} \right\} \setminus \mathscr{U}_1,$$

where η is a sufficiently small positive number.

2389

First, we may derive a lower bound for $B^<(x, \alpha; \xi, k)$ by inserting the inequality (3.7) or (3.12) into (3.1). A similar lower bound also holds for $B^>(x, \alpha; \xi, k)$ by symmetry. Therefore, we have

$$
B(x, \alpha) \geqslant 2(1-\delta) \sum_{k=0}^{k_0} \sum_{\xi \in \mathcal{R}(2^k)} \sum_{\mathbf{U} \in \mathscr{U}_1} \sum_{\substack{\xi_1, \xi_2 \,(\mathrm{mod}\, 4^k) \\ 2 \nmid \xi_1 \xi_2}} \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2)=(u_1, u_2)=1}} \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2}
$$
$$
+ 2(1-2\delta) \sum_{k=0}^{k_0} \sum_{\xi \in \mathcal{R}(2^k)} \sum_{\mathbf{U} \in \mathscr{U}_2} \sum_{\substack{\xi_1, \xi_2 \,(\mathrm{mod}\, 4^k) \\ 2 \nmid \xi_1 \xi_2}} \sum_{\substack{u_1 \sim U_1, u_2 \sim U_2 \\ u_1 \equiv \xi_1, u_2 \equiv \xi_2 \,(\mathrm{mod}\, 4^k) \\ (2, u_1 u_2)=(u_1, u_2)=1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{Y_3 - Y_2}{4^k u_1^2 u_2^2} + O(x^{1/2}),
$$

where U_1, U_2 are also restricted to be powers of 2. Recall that

$$
Y_3 - Y_2 = Y_3(2^k u_1 u_2, \alpha) - Y_2(2^k u_1 u_2) = 2^k u_1 u_2 \sqrt{x} + O((2^k u_1 u_2)^{1+1/2\alpha}).
$$

We then obtain the lower bound

$$
B(x, \alpha) \geqslant 2(1-2\delta) \left(\sum_{k=0}^{k_0} \frac{\gamma(2^k)}{2^k} \right) \left\{ \sum_{\substack{(u_1, u_2) \in \mathscr{V}_1 \\ (2, u_1 u_2)=(u_1, u_2)=1}} \frac{1}{u_1 u_2} + \sum_{\substack{(u_1, u_2) \in \mathscr{V}_2 \\ (2, u_1 u_2)=(u_1, u_2)=1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{1}{u_1 u_2} \right\}
$$
$$
+ O(x^{1/2} \log x),
$$

where

$$
\mathscr{V}_1 := \{ (u_1, u_2) : u_1 < u_2, \sqrt{x} < u_1 u_2 \leqslant x^\alpha, u_1 \leqslant x^{1/4-\eta}, \ u_2 \leqslant u_1 x^{1/2-\eta} \},
$$

and

$$
\mathscr{V}_2 := \{ (u_1, u_2) : u_1 < u_2, \sqrt{x} < u_1 u_2 \leqslant x^\alpha, u_1^{(8+2\theta)/3} u_2 \leqslant x^{1-\eta}, u_2 \leqslant u_1 x^{1/2-\eta} \} \backslash \mathscr{V}_1.
$$

Taking $k_0 = k_0(\delta)$ very large, $\eta = \eta(\delta)$ very small, and letting δ tend to zero, we conclude from Lemma A.1 that

$$
B(x, \alpha) \geqslant \frac{1}{\pi^2}((2\alpha-1)(3-2\alpha) - o(1)) \sqrt{x} \log^2 x + B'(x, \alpha) \tag{3.13}
$$

uniformly for $\alpha \in [\frac{1}{2}, 1]$, where

$$
B'(x, \alpha) = 4\sqrt{x} \sum_{\substack{x^{1/4} < u_1 \leqslant x^{\min\{\alpha/2, 3/(11+2\theta)\}} \\ u_1 \text{ is } U_1^\theta\text{-smooth} \\ 2 \nmid u_1}} \frac{\varphi(u_1)}{u_1^2} \log(\sqrt{x} u_1^{-(5+2\theta)/3}).
$$

Note that $B'(x, \alpha)$ is what we have gained more than Fouvry [Fou16]. From Lemma A.3, we arrive at

$$
B'(x, \alpha) = \frac{1}{\pi^2}(F(\alpha, \theta) + o(1)) \sqrt{x} \log^2 x
$$

with

$$
F(\alpha, \theta) = \rho\left(\frac{1}{\theta}\right) \left\{ 4 \min\left\{ \alpha, \frac{6}{11+2\theta} \right\} - \frac{(10+4\theta)}{3} \min\left\{ \alpha, \frac{6}{11+2\theta} \right\}^2 - \frac{(7-2\theta)}{6} \right\}.
$$

One may check that

$$F(\alpha, \theta) = \frac{1}{6}\rho\left(\frac{1}{\theta}\right)F_\theta(\alpha)$$

as given in Theorem 1.1. Combining this asymptotic evaluation for $B'(x, \alpha)$ with (3.13), we may conclude a lower bound for $B(x, \alpha)$, from which and (2.8), (2.7), we get

$$S(x, \alpha) \geqslant \frac{1}{\pi^2}\left\{1 + (2\alpha - 1)(3 - 2\alpha) + \frac{1}{6}\rho\left(\frac{1}{\theta}\right)F_\theta(\alpha) - o(1)\right\}\sqrt{x}\log^2 x \qquad (3.14)$$

uniformly for $\alpha \in [\frac{1}{2}, 1]$.

3.4 Concluding Theorem 1.1

To pass from a lower bound of $S(x, \alpha)$ to that of $S^{\mathrm{f}}(x, \alpha)$, it is natural to invoke the identity (2.14) and Theorem A. In fact, one can do a bit better following the arguments of Fouvry [Fou16] and show that the above lower bound (3.14) also hold for $S^{\mathrm{f}}(x, \alpha)$. This will depend on a more elaborate study of the contribution from non-fundamental solutions. In other words, we would like to show that the non-fundamental solutions create negligible contributions to $A(x, \alpha)$ and $B(x, \alpha)$.

The following lemma is borrowed directly from [Fou16, Lemma 9.1].

LEMMA 3.2. *Uniformly for* $\alpha \in [\frac{1}{2}, 1]$ *and* $x \geqslant 2$, *one has*

$$A(x, \alpha) - A^{\mathrm{f}}(x, \alpha) \ll \sqrt{x}\log x.$$

To deal with the contribution of the non-fundamental solutions to $B(x, \alpha)$, we also follow Fouvry. The above arguments which lead to (3.14) are essentially counting the number $\mathscr{N}(x, \alpha; \varepsilon, k_0)$ of 5-tuples of integers (k, t, u_1, u_2, D) satisfying

$$2 \nmid u_1 u_2, \quad (u_1, u_2) = 1, \quad 0 \leqslant k \leqslant k_0, \quad D \leqslant x,$$
$$X_{1/2} \leqslant 2^k u_1 u_2 \leqslant X_\alpha, \quad t + 2^k u_1 u_2 \sqrt{D} \leqslant D^{1/2+\alpha},$$
$$t^2 \equiv 1 \pmod{4^k}, \quad t \equiv 1 \pmod{u_1^2}, \quad t \equiv -1 \pmod{u_2^2},$$

as well as one of the following restrictions:

- $u_1 \leqslant u_2 \leqslant u_1 x^{1/2-\eta}$, $u_1 \leqslant x^{1/4-\eta}$;
- $u_2 \leqslant u_1 \leqslant u_2 x^{1/2-\eta}$, $u_2 \leqslant x^{1/4-\eta}$;
- $u_1 \leqslant u_2 \leqslant u_1 x^{1/2-\eta}$, $u_1^{(8+2\theta)/3} u_2 \leqslant x^{1-\eta}$;
- $u_2 \leqslant u_1 \leqslant u_2 x^{1/2-\eta}$, $u_1 u_2^{(8+2\theta)/3} \leqslant x^{1-\eta}$.

By introducing the extra constraint $t + 2^k u_1 u_2 \sqrt{D} = \varepsilon_D$, we may also define $\mathscr{N}^{\mathrm{f}}(x, \alpha; \varepsilon, k_0)$. In fact, the above arguments yield

$$B(x, \alpha) \geqslant \mathscr{N}(x, \alpha; \varepsilon, k_0), \quad B^{\mathrm{f}}(x, \alpha) \geqslant \mathscr{N}^{\mathrm{f}}(x, \alpha; \varepsilon, k_0), \qquad (3.15)$$

which are true for every positive $\varepsilon > 0$ and for every $k_0 \geqslant 0$. More precisely, we have proved for every δ, $0 < \varepsilon < \varepsilon_0(\delta)$, $k_0 > k_0(\delta)$ and $x > x_0(\delta)$ that

$$\mathscr{N}(x, \alpha; \varepsilon, k_0) \geqslant \frac{1}{\pi^2}\left\{(2\alpha - 1)(3 - 2\alpha) + \frac{1}{6}\rho\left(\frac{1}{\theta}\right)F_\theta(\alpha) - \delta\right\}\sqrt{x}\log^2 x \qquad (3.16)$$

with $\alpha \in [\frac{1}{2}, 1]$.

Following the approach of Fouvry [Fou16], we can state the following without proof.

LEMMA 3.3. *For every $k_0 \geqslant 0$ and every $\varepsilon > 0$, one has*

$$\mathscr{N}(x, \alpha; \varepsilon, k_0) - \mathscr{N}^{\mathrm{f}}(x, \alpha; \varepsilon, k_0) \ll_{\varepsilon, k_0} \sqrt{x} \log x$$

uniformly for $\alpha \in [\frac{1}{2}, 1]$ and $x \geqslant 2$.

We are now ready to complete the proof of Theorem 1.1. In view of (3.15), we may write

$$
\begin{aligned}
S^{\mathrm{f}}(x, \alpha) &= A^{\mathrm{f}}(x, \alpha) + B^{\mathrm{f}}(x, \alpha) \\
&\geqslant A^{\mathrm{f}}(x, \alpha) + \mathscr{N}^{\mathrm{f}}(x, \alpha; \varepsilon, k_0) \\
&= A(x, \alpha) + \mathscr{N}(x, \alpha; \varepsilon, k_0) + \{A^{\mathrm{f}}(x, \alpha) - A(x, \alpha)\} \\
&\quad + \{\mathscr{N}^{\mathrm{f}}(x, \alpha; \varepsilon, k_0) - \mathscr{N}(x, \alpha; \varepsilon, k_0)\},
\end{aligned}
$$

which are true for every $\varepsilon > 0$ and $k_0 \geqslant 0$. From Lemmas 3.2 and 3.3, we obtain

$$S^{\mathrm{f}}(x, \alpha) \geqslant A(x, \alpha) + \mathscr{N}(x, \alpha; \varepsilon, k_0) + O(\sqrt{x} \log x).$$

By (2.8), (3.16), and by choosing $k_0 = k_0(\delta)$ sufficiently large, $\eta = \eta(\delta)$ sufficiently small, and letting δ tend to zero, we find the lower bound (3.14) holds definitely for $S^{\mathrm{f}}(x, \alpha)$. This establishes (1.4).

The lower bounds for $S(x, \alpha)$ in Theorem 1.1 can be deduced from (1.2) by adding the contribution of the non-fundamental solutions, as it is shown by (2.14).

4. Estimate for triple exponential sums

We now prove Theorem 3.1. For the economy of the presentation, we only focus on the case $k = 0$ and define

$$\mathfrak{S}(U_1, U_2, H) := \sum_{h \leqslant H} \sum_{\substack{u_1 \in]U_1, U_1^*] \\ (2, u_1 u_2) = (u_1, u_2) = 1 \\ u_1 \text{ is } U_1^\theta\text{-smooth}}} \sum_{u_2 \geqslant 1} g_1\left(\frac{u_2}{U_2}\right) e\left(\frac{h \overline{u_2^2}}{u_1^2}\right). \tag{4.1}$$

We would like to show that

$$\mathfrak{S}(U_1, U_2, H) \ll U_1 U_2 x^{-\varepsilon_0}, \quad H = U_1 U_2 x^{-1/2 + \varepsilon} \tag{4.2}$$

for some $\varepsilon_0 \in]0, 10^{-2017}[$ while U_1, U_2 fall into the ranges in (3.11).

By Poisson summation, the u_2-sum in (4.1) becomes

$$\sum_{u_2} = \frac{U_2}{2u_1^2} \sum_{r \in \mathbf{Z}} \widehat{g_1}\left(\frac{r U_2}{2u_1^2}\right) \sum_{\substack{z \,(\mathrm{mod}\, 2u_1^2) \\ (z, 2u_1) = 1}} e\left(\frac{h \overline{z^2}}{u_1^2} + \frac{rz}{2u_1^2}\right).$$

From the Chinese remainder theorem, the sum over z can be rewritten as

$$
\begin{aligned}
&\sum_{\substack{z_1 \,(\mathrm{mod}\, u_1^2) \\ (z_1, u_1) = 1}} \sum_{\substack{z_2 \,(\mathrm{mod}\, 2) \\ (z, 2) = 1}} e\left(\frac{h \overline{(2z_1 + u_1^2 z_2)^2}}{u_1^2} + \frac{r(2z_1 + u_1^2 z_2)}{2u_1^2}\right) \\
&= \sum_{\substack{z_1 \,(\mathrm{mod}\, u_1^2) \\ (z_1, u_1) = 1}} \sum_{\substack{z_2 \,(\mathrm{mod}\, 2) \\ (z, 2) = 1}} e\left(\frac{h \overline{(2z_1)^2}}{u_1^2} + \frac{r \overline{z_1}}{u_1^2} + \frac{r z_2}{2}\right) = (-1)^r K(r, \overline{4}h; u_1^2),
\end{aligned}
$$

where K is an analogue of Kloosterman sums:

$$K(m, n; q) = \sum_{x \,(\mathrm{mod}\, q)}^{*} e\left(\frac{mx + n\overline{x}^2}{q}\right).$$

Hence we may conclude that

$$\sum_{u_2} = \frac{U_2}{2u_1^2} \sum_{r \in \mathbf{Z}} (-1)^r \widehat{g_1}\left(\frac{rU_2}{2u_1^2}\right) K(r, \overline{4}h; u_1^2).$$

Note that $K(0, h; q) = T(h, q)$ and if q is odd, we have $T(\overline{4}h, q) = T(h, q)$. According to $r = 0$ and $r \neq 0$, we split $\mathfrak{S}(U_1, U_2, H)$ by

$$\mathfrak{S}(U_1, U_2, H) = \mathfrak{S}_1(U_1, U_2, H) + \mathfrak{S}_2(U_1, U_2, H),$$

where

$$\mathfrak{S}_1(U_1, U_2, H) = \frac{U_2(1 - \delta)}{2} \sum_{h \leqslant H} \sum_{\substack{u_1 \in \,]U_1, U_1^*] \\ 2 \nmid u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{T(h, u_1^2)}{u_1^2}$$

and

$$\mathfrak{S}_2(U_1, U_2, H) = \frac{U_2}{2} \sum_{h \leqslant H} \sum_{\substack{u_1 \in \,]U_1, U_1^*] \\ 2 \nmid u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{1}{u_1^2} \sum_{0 \neq r \in \mathbf{Z}} (-1)^r \widehat{g_1}\left(\frac{rU_2}{2u_1^2}\right) K(r, \overline{4}h; u_1^2).$$

Following the approach of Fouvry, one may express $T(h, u_1^2)$ in terms of Jacobi symbols (see [Fou16, Lemma 6.2]) and then appeal to the bilinear estimate of Heath-Brown [Hea95], getting

$$\mathfrak{S}_1(U_1, U_2, H) \ll (U_1 U_2 H)^\varepsilon (H U_1 U_2^{-1} + H^{1/2} U_1), \tag{4.3}$$

which produces the second restriction in (3.6). Moreover, Fouvry proved that

$$\mathfrak{S}_2(U_1, U_2, H) \ll (U_1 U_2 H)^\varepsilon H U_2^2,$$

which produces the first restriction in (3.6).

Our task will be proving a stronger estimate for $\mathfrak{S}_2(U_1, U_2, H)$ by virtue of the special structure of u_1. More precisely, we shall prove that

$$\mathfrak{S}_2(U_1, U_2, H) \ll (U_1 U_2 H)^\varepsilon H U_1 U_2^{1/2} (Q + U_1^{1/2} Q^{-1/2}),$$

where Q will be chosen at our demand. This would at least require the following inequality as proved by Fouvry [Fou16]. In fact, Fouvry only considered those q that are perfect squares, and his argument also applies to more general q.

LEMMA 4.1. *Let q be an odd positive integer. Then we have*

$$|K(m, n; q)| \leqslant 3^{\omega(q)} (m, n, q) \sqrt{q}.$$

As an extension to $K(m, n; q)$, we define another exponential sum

$$\mathscr{B}(m, n, \ell, u; q) = \sum_{a \,(\mathrm{mod}\, q)}^{*} e\left(\frac{m\overline{a^2} + n\overline{(a + u)^2} + \ell a}{q}\right), \tag{4.4}$$

where $*$ in summation reminds us to sum over primitive elements, i.e., $(a(a + u), q) = 1$. We will need the following inequality.

LEMMA 4.2. *For each odd $q \geqslant 1$, we have*

$$|\mathscr{B}(m, n, \ell, u; q)|$$
$$\leqslant 3q^{1/2}(\ell, m, n, q^\flat)^{1/2}(\ell, m + n, u, q^\flat)^{1/2}(\ell, m, n, q^\ddagger)(\ell, m + n, u, q^\ddagger) \cdot 18^{\omega(q)} \cdot \Xi(q)^{1/2},$$

where

$$q^\ddagger = \prod_{p^2 \| q} p, \quad \Xi(q) = \prod_{p^\nu \| q, \nu \geqslant 3} p^\nu.$$

The proof of Lemma 4.2 will be given in Appendix B.

We now start to prove Theorem 3.1. Due to the decay of $\widehat{g}_1$, we may truncate the r-sum in $\mathfrak{S}_2(U_1, U_2, H)$ by $R = U_1^{2+\varepsilon}U_2^{-1}$, so that

$$\mathfrak{S}_2(U_1, U_2, H) = \frac{U_2}{2} \sum_{h \leqslant H} \sum_{\substack{u_1 \in]U_1, U_1^*] \\ 2 \nmid u_1 \text{ is } U_1^\theta\text{-smooth}}} \frac{1}{u_1^2} \sum_{1 \leqslant |r| \leqslant R} (-1)^r \widehat{g}_1\left(\frac{rU_2}{2u_1^2}\right) K(r, \overline{4}h; u_1^2)$$
$$+ O((U_1 U_2 H)^{-2017}). \tag{4.5}$$

Our project will be controlling the cancellations while summing over r with $1 \leqslant |r| \leqslant R$. More precisely, we would like to estimate

$$\sum_{1 \leqslant |r| \leqslant R} (-1)^r \widehat{g}_1\left(\frac{rU_2}{2u_1^2}\right) K(r, \overline{4}h; u_1^2).$$

The contributions from negative r and positive r can be treated similarly, it thus suffices to consider

$$\sum_{r \leqslant R} (-1)^r \widehat{g}_1\left(\frac{rU_2}{2u_1^2}\right) K(r, \overline{4}h; u_1^2),$$

which can be rewritten as

$$2 \sum_{r \leqslant R/2} \widehat{g}_1\left(\frac{rU_2}{u_1^2}\right) K(2r, \overline{4}h; u_1^2) - \sum_{r \leqslant R} \widehat{g}_1\left(\frac{rU_2}{2u_1^2}\right) K(r, \overline{4}h; u_1^2).$$

Clearly, $K(2r, \overline{4}h; u_1^2) = K(r, h; u_1^2)$. By partial summation, it suffices to consider

$$\Sigma(R, u_1^2; h) := \sum_{r \leqslant R} K(r, h; u_1^2).$$

For each $u_0 \mid u_1$, we define d, q_1, q_2 by

$$d = (u_0, (u_1/u_0)^\infty), \quad q_1 = (u_0/d)^2, \quad q_2 = u_1^2/q_1.$$

It follows that $u_1^2 = q_1 q_2$ and $(q_1, q_2) = 1$. By virtue of the q-analogue of van der Corput method, we will prove the following.

LEMMA 4.3. *With the above notation, we have*

$$\Sigma(R, u_1^2; h) \ll u_1^\varepsilon R^{1/2}\{u_0 u_1 + u_0 R^{1/2}(u_0, u_1/u_0) + (u_0, (u_1/u_0)^\infty)^{1/2}(h, u_0^2)^{1/2} u_1^{3/2}(u_1^\sharp)^{1/4}/u_0^{1/2}\}.$$

Proof. Lemma 4.3 is a trivial consequence of Lemma 4.1 if $R \leqslant u_0^2$. We now assume $R > u_0^2$. Denote by I_R the characteristic function of the interval $[1, R]$. Thus,

$$\Sigma(R, u_1^2; h) = \sum_{r \in \mathbf{Z}} I_R(r) K(r, h; u_1^2) = \sum_{r \in \mathbf{Z}} I_R(r + u_0^2 \ell) K(r + u_0^2 \ell, h; u_1^2)$$

for any $\ell \in \mathbf{Z}$. From the Chinese remainder theorem, we may write

$$\begin{aligned} K(r + u_0^2 \ell, h; u_1^2) &= K(r + u_0^2 \ell, h\overline{q}_2^3; q_1) K(r + u_0^2 \ell, h\overline{q}_1^3; q_2) \\ &= K(r, h\overline{q}_2^3; q_1) K(r + u_0^2 \ell, h\overline{q}_1^3; q_2), \end{aligned}$$

where we have used the fact that $q_1 \mid u_0^2$.

For $L = [R/u_0^2]$, we sum over ℓ, getting

$$\begin{aligned} \Sigma(R, u_1^2; h) &= \frac{1}{L} \sum_{\ell \leqslant L} \sum_{r \in \mathbf{Z}} I_R(r + u_0^2 \ell) K(r + u_0^2 \ell, h; u_1^2) \\ &\leqslant \frac{1}{L} \sum_{r \in \mathbf{Z}} |K(r, h\overline{q}_2^3; q_1)| \left| \sum_{\ell \leqslant L} I_R(r + u_0^2 \ell) K(r + u_0^2 \ell, h\overline{q}_1^3; q_2) \right|. \end{aligned}$$

From Lemma 4.1 we find

$$\Sigma(R, u_1^2; h) \ll \frac{q^\varepsilon \sqrt{q_1}}{L} \sum_{r \in \mathbf{Z}} (r, h, q_1) \left| \sum_{\ell \leqslant L} I_R(r + u_0^2 \ell) K(r + u_0^2 \ell, h\overline{q}_1^3; q_2) \right|.$$

In view of the support of I_R, the sum over r is in fact restricted to $[-R, R]$. By Cauchy inequality, we derive that

$$\Sigma(R, u_1^2; h)^2 \ll \frac{q^\varepsilon q_1 R}{L^2} \sum_{r \in \mathbf{Z}} \left| \sum_{\ell \leqslant L} I_R(r + u_0^2 \ell) K(r + u_0^2 \ell, h\overline{q}_1^3; q_2) \right|^2.$$

Squaring out and switching summations, we get

$$\Sigma(R, u_1^2; h)^2 \ll \frac{q^\varepsilon q_1 R}{L} \sum_{0 \leqslant |\ell| \leqslant L} \left| \sum_{r \in I_\ell} K(r, h\overline{q}_1^3; q_2) \overline{K(r + u_0^2 \ell, h\overline{q}_1^3; q_2)} \right|, \tag{4.6}$$

where I_ℓ is an interval, depending on ℓ, of length at most R. For $\ell = 0$, we appeal to Lemma 4.1 to estimate the r-sum trivially. For $1 \leqslant |\ell| \leqslant L$, reasonable cancellations in the r-sum are expected. In fact, by completion, we have

$$\sum_{r \in I_\ell} [\cdots] = \sum_{y \,(\mathrm{mod}\, q_2)} I(y, q_2) \widehat{K}(y, q_2; h, q_1, u_0, \ell),$$

where

$$I(y, q_2) = \sum_{r \in I_\ell} e\left(\frac{-yr}{q_2} \right),$$

and

$$\widehat{K}(y, q_2; h, q_1, u_0, \ell) = \frac{1}{q_2} \sum_{x \,(\mathrm{mod}\, q_2)} K(x, h\overline{q}_1^3; q_2) \overline{K(x + u_0^2 \ell, h\overline{q}_1^3; q_2)} e\left(\frac{yx}{q_2} \right).$$

2395

Firstly,

$$I(y, q_2) \ll \min\left\{R, \left\|\frac{y}{q_2}\right\|^{-1}\right\}.$$

Opening each K by definition, the orthogonality of additive characters gives

$$\widehat{K}(y, q_2; h, q_1, u_0, \ell) = e\left(\frac{-u_0^2 \ell y}{q_2}\right) \sum_{a \,(\mathrm{mod}\, q_2)}^{*} e\left(\frac{h\overline{q}_1^3(\overline{a^2} - \overline{(a+y)^2}) - u_0^2 \ell a}{q_2}\right)$$
$$= e\left(\frac{-u_0^2 \ell y}{q_2}\right) \mathscr{B}(h\overline{q}_1^3, -h\overline{q}_1^3, -u_0^2 \ell, y; q_2).$$

For $y = 0$, we have

$$\mathscr{B}(h\overline{q}_1^3, -h\overline{q}_1^3, -u_0^2 \ell, 0; q_2) = \sum_{a \,(\mathrm{mod}\, q_2)}^{*} e\left(\frac{u_0^2 \ell a}{q_2}\right) \ll (u_0^2 \ell, q_2).$$

For $y \neq 0$, we would like to appeal to Lemma 4.2. To do so, we first derive from Lemma 4.2 that (we have $q_2^\flat = 1$ since q_2 is a perfect square)

$$|\mathscr{B}(h\overline{q}_1^3, -h\overline{q}_1^3, -u_0^2 \ell, y; q_2)| \ll q_2^{1/2+\varepsilon}(h, u_0^2 \ell, q_2^\ddagger)(y, u_0^2 \ell, q_2^\ddagger) \cdot \Xi(q_2)^{1/2}.$$

This yields

$$\sum_{r \in I_\ell}[\cdots] \ll R(u_0^2 \ell, q_2) + q_2^{1/2+\varepsilon}(h, u_0^2 \ell, q_2^\ddagger) \cdot \Xi(q_2)^{1/2} \sum_{1 \leqslant |y| \leqslant q_2/2} \min\left\{R, \frac{q_2}{y}\right\}(y, u_0^2 \ell, q_2^\ddagger)$$
$$\ll R(u_0^2 \ell, q_2) + q_2^{3/2+\varepsilon}(h, u_0^2 \ell, q_2^\ddagger) \cdot \Xi(q_2)^{1/2},$$

from which and (4.6) we obtain

$$\Sigma(R, u_1^2; h)^2 \ll \frac{u_1^\varepsilon q_1 R}{L}\big\{Rq_2(h, q_2) + LR(u_0^2, q_2) + Lq_2^{3/2}(h, u_0^2, q_2^\ddagger) \cdot \Xi(q_2)^{1/2}\big\}$$
$$\ll u_1^\varepsilon R\big\{(u_0 u_1)^2 + q_1 R(u_0^2, q_2) + u_1^2 q_2^{1/2}(h, u_0^2) \cdot \Xi(q_2)^{1/2}\big\}.$$

Note that $q_2 = (u_1 d/u_0)^2 = \{u_1(u_0, (u_1/u_0)^\infty)/u_0\}^2$. Thus,

$$\Xi(q_2) = \Xi(\{u_1(u_0, (u_1/u_0)^\infty)/u_0\}^2) = (u_1(u_0, (u_1/u_0)^\infty)/u_0)^\sharp \leqslant u_1^\sharp.$$

We then conclude that

$$\Sigma(R, u_1^2; h)^2 \ll u_1^\varepsilon R\{(u_0 u_1)^2 + u_0^2 R(u_0, u_1/u_0)^2 + (u_0, (u_1/u_0)^\infty)(h, u_0^2)u_1^3(u_1^\sharp)^{1/2}/u_0\},$$

which gives Lemma 4.3 immediately. $\qquad\square$

In view of Lemma 4.3 and the discussions before it, we may derive from (4.5) that

$$\mathfrak{S}_2(U_1, U_2, H) \ll U_1^\varepsilon HQU_2(R^{1/2} + RU_1^{-1}) + \frac{U_1^\varepsilon HU_2 R^{1/2}}{(QU_1)^{1/2}} \sum_{u_1 \sim U_1} \sum_{ab=u_1} (a, b^\infty)^{1/2}((ab)^\sharp)^{1/4},$$

where $U_1^{\theta_0} \leqslant Q \leqslant U_1^{\theta_0+\theta}$. In view of the choice $R = U_1^{2+\varepsilon}U_2^{-1}$, Lemma A.5 yields

$$\mathfrak{S}_2(U_1, U_2, H) \ll U_1^\varepsilon HU_1 U_2^{1/2}\{Q + U_1^{1/2}Q^{-1/2}\},$$

from which and (4.3) we conclude that

$$\mathfrak{S}(U_1, U_2, H) \ll (U_1 U_2 H)^\varepsilon\{HU_1 U_2^{-1} + H^{1/2}U_1 + HU_1 U_2^{1/2}(Q + U_1^{1/2}Q^{-1/2})\}.$$

Choosing $\theta_0 = (1 - 2\theta)/3$, we then have $U_1^{(1-2\theta)/3} \leqslant Q \leqslant U_1^{(1+\theta)/3}$. Recalling the choice of H, we then arrive at the expected estimate (4.2), provided that (3.11) holds.

2396

Appendix A. Mean values of arithmetic functions

A.1 Some basic asymptotics

The first part of the appendix is devoted to state several basic asymptotics.

Recall that $\gamma(u)$ denotes the number of solutions to the congruence equation $x^2 \equiv 1 \pmod{u^2}$. As a multiplicative function, γ satisfies the evaluation (2.10). We are now ready to state the following averages.

LEMMA A.1. *As $N \to +\infty$, we have*

$$\sum_{0 \leqslant n \leqslant N} \frac{\gamma(2^n)}{2^n} = 4 + O(2^{-N}),$$

$$\sum_{\substack{n \leqslant N \\ (n,q)=1}} \frac{1}{n} = \frac{\varphi(q)}{q} \log N + O\left(1 + \sum_{d|q} \frac{\log d}{d}\right),$$

$$\sum_{\substack{n \leqslant N \\ (n,2)=1}} \frac{\varphi(n)}{n^2} \sim \frac{4}{\pi^2} \log N,$$

and

$$\sum_{\substack{n \leqslant N \\ (n,2)=1}} \frac{\varphi(n) \log n}{n^2} \sim \frac{2}{\pi^2} \log^2 N.$$

Proof. The first one can be derived from the evaluations of $\gamma(2^n)$ as given in (2.10). The other three asymptotics can be found in Fouvry [Fou16, Lemma 8.1, Lemma 8.2]. □

A.2 Smooth numbers

Denote by $\mathcal{S}(x,y)$ the set of y-smooth numbers not exceeding x. Write $\Psi(x,y) = |\mathcal{S}(x,y)|$. We now introduce the Dickman function $\rho(u)$ by

$$\begin{cases} \rho(u) = 1, & u \in]0,1], \\ u\rho'(u) + \rho(u-1) = 0, & u \in]1,+\infty[. \end{cases} \tag{A.1}$$

In the first several intervals, we have

$$\rho(u) = 1 - \log u, \quad u \in]1,2],$$
$$\rho(u) = 1 - \log u + \int_2^u \frac{\log(t-1)}{t} \, dt, \quad u \in]2,3],$$
$$\rho(u) = 1 - \log u + \int_2^u \frac{\log(t-1)}{t} \, dt - \int_3^u \frac{dt}{t} \int_2^{t-1} \frac{\log(s-1)}{s} \, ds, \quad u \in]3,4].$$

The following lemma is classical and shows ρ is the density function of smooth numbers.

2397

Lᴇᴍᴍᴀ A.2. *Uniformly for $x \geqslant y \geqslant 2$, we have*

$$\Psi(x, y) = x\rho\left(\frac{\log x}{\log y}\right) + O\left(\frac{x}{\log y}\right).$$

Proof. See [Ten95, p. 367, Theorem 6]. □

Lᴇᴍᴍᴀ A.3. *Let $\theta \in \,]0, 1[$ be fixed. As $N \to +\infty$, we have*

$$\sum_{\substack{2\nmid n \leqslant N \\ n \text{ is } n^\theta\text{-smooth}}} \frac{\varphi(n)}{n^2} \sim \frac{4}{\pi^2}\rho\left(\frac{1}{\theta}\right)\log N,$$

and

$$\sum_{\substack{2\nmid n \leqslant N \\ n \text{ is } n^\theta\text{-smooth}}} \frac{\varphi(n)\log n}{n^2} \sim \frac{2}{\pi^2}\rho\left(\frac{1}{\theta}\right)\log^2 N.$$

Proof. One can refer to [TW03], for instance, for some general theorems on the mean values of multiplicative functions over smooth numbers. In particular, one has

$$\sum_{\substack{2\nmid n \leqslant N \\ n \text{ is } n\theta\text{-smooth}}} \frac{\varphi(n)}{n} = \frac{4}{\pi^2}\rho\left(\frac{1}{\theta}\right)N + O\left(\frac{N}{\log N}\right).$$

The lemma then follows from the partial summation. □

Lᴇᴍᴍᴀ A.4. *For all $q \geqslant 1$, we have*

$$\sum_{n \leqslant x} (n^\sharp)^{1/4}(n, q)^{1/2} \ll x(qx)^\varepsilon.$$

Proof. Note that $n \mapsto (n^\sharp)^{1/4}(n, q)^{1/2}$ is multiplicative. For $\Re s > 1$, we consider the Dirichlet series

$$\mathscr{D}(s) = \sum_{n \geqslant 1} \frac{(n^\sharp)^{1/4}(n, q)^{1/2}}{n^s}.$$

By the Euler product formula, we have

$$\begin{aligned}
\mathscr{D}(s) &= \prod_p \left(\sum_{k \geqslant 0} \frac{((p^k)^\sharp)^{1/4}(p^k, q)^{1/2}}{p^{ks}}\right) \\
&= \prod_p \left(1 + \frac{(p, q)^{1/2}}{p^s} + \sum_{k \geqslant 2} \frac{(p^k, q)^{1/2}}{p^{k(s-1/4)}}\right) \\
&= \prod_{p \nmid q} \left(1 + \frac{1}{p^s} + \sum_{k \geqslant 2} \frac{1}{p^{k(s-1/4)}}\right) \cdot \prod_{p | q} \left(1 + \frac{1}{p^{s-1/2}} + \sum_{k \geqslant 2} \frac{(p^k, q)^{1/2}}{p^{k(s-1/4)}}\right) \\
&= \zeta(s)\mathscr{D}_1(s)\mathscr{D}_2(s, q),
\end{aligned}$$

where $\mathscr{D}_1(s)$ is holomorphic for $\Re s > 3/4$ and

$$\mathscr{D}_2(s, q) = \prod_{p | q} \left(1 + \frac{1}{p^s} + \sum_{k \geqslant 2} \frac{1}{p^{k(s-1/4)}}\right)^{-1} \cdot \left(1 + \frac{1}{p^{s-1/2}} + \sum_{k \geqslant 2} \frac{(p^k, q)^{1/2}}{p^{k(s-1/4)}}\right).$$

The lemma then follows from a routine application of Perron's formula. □

The following inequality is a consequence of Rankin's method, which is a stronger version of [Fou16, Lemma 7.2].

LEMMA A.5. *For any $\varepsilon > 0$, one has*

$$\sum_{mn \leqslant N} (m, n^\infty)^{1/2}((mn)^\sharp)^{1/4} \ll N^{1+\varepsilon}.$$

Proof. Denote by S the sum in question. First, we have

$$S \ll \sum_{n \leqslant N} \sum_{\substack{d | n^\infty}} d^{1/2} \sum_{\substack{m \leqslant N/n \\ d | m}} ((mn)^\sharp)^{1/4} = \sum_{n \leqslant N} \sum_{\substack{d \leqslant N \\ d | n^\infty}} d^{1/2} \sum_{m \leqslant N/(nd)} ((mnd)^\sharp)^{1/4}.$$

Note that

$$(ab)^\flat = \prod_{p \| ab} p = \prod_{p \| a, p \nmid b} p \cdot \prod_{p \| b, p \nmid a} p = a^\flat \cdot b^\flat \cdot \prod_{p \| a, p | b} \frac{1}{p} \cdot \prod_{p \| b, p | a} \frac{1}{p} \geqslant \frac{a^\flat \cdot b^\flat}{\{(a, b)^\flat\}^2},$$

giving

$$(ab)^\sharp \leqslant a^\sharp \cdot b^\sharp \cdot \{(a, b)^\flat\}^2,$$

from which and Lemma A.4 it follows that

$$S \ll \sum_{n \leqslant N} \sum_{\substack{d \leqslant N \\ d | n^\infty}} d^{1/2}((nd)^\sharp)^{1/4} \sum_{m \leqslant N/(nd)} (m^\sharp)^{1/4}(m, nd)^{1/2}$$

$$\ll N^{1+\varepsilon} \sum_{n \leqslant N} \frac{1}{n} \sum_{\substack{d \leqslant N \\ d | n^\infty}} d^{-1/2}((nd)^\sharp)^{1/4}$$

$$\ll N^{1+\varepsilon} \sum_{n \leqslant N} \frac{(n^\sharp)^{1/4}}{n} \sum_{\substack{d \leqslant N \\ d | n^\infty}} d^{-1/2}(d^\sharp)^{1/4}((n, d)^\flat)^{1/2}.$$

By Rankin's method, the last sum over d is, for any $\varepsilon > 0$,

$$\leqslant N^\varepsilon \sum_{\substack{d \leqslant N \\ d | n^\infty}} d^{-1/2-\varepsilon}(d^\sharp)^{1/4}((n, d)^\flat)^{1/2}$$

$$\leqslant N^\varepsilon \prod_{p | n} \left(1 + \sum_{k \geqslant 1} \frac{((p^k)^\sharp)^{1/4}((n, p^k)^\flat)^{1/2}}{p^{k(1/2+\varepsilon)}}\right)$$

$$= N^\varepsilon \prod_{p | n} \left(1 + \frac{2}{p^\varepsilon} + \sum_{k \geqslant 3} \frac{1}{p^{k(1/4+\varepsilon)-1/2}}\right)$$

$$\ll (nN)^\varepsilon$$

by re-defining ε. We now get

$$S \ll N^{1+\varepsilon} \sum_{n \leqslant N} \frac{(n^\sharp)^{1/4}}{n} \ll N^{1+\varepsilon},$$

where the last step follows from Lemma A.4 together with partial summation and taking $q = 1$ therein. $\square$

Appendix B. Estimate for $\mathscr{B}(m, n, \ell, u; q)$

While invoking the ideas of the q-analogue of the van der Corput method, we have transformed the original algebraic exponential sum $K(m, n, q)$ to a new sum $\mathscr{B}(m, n, \ell, u; q)$ as given by (4.4). This appendix will be devoted to present an estimation for $\mathscr{B}(m, n, \ell, u; q)$ that suits well in our applications to Theorem 1.1. In fact, the job can be done for the general complete exponential sum

$$\Sigma(\lambda, q) := \sum_{a \,(\mathrm{mod}\, q)} e\left(\frac{\lambda(a)}{q}\right).$$

Here $\lambda = \lambda_1 / \lambda_2$ with $\lambda_1, \lambda_2 \in \mathbf{Z}[X]$ and λ_1, λ_2 being coprime in $\mathbf{Z}[X]$. The values of a such that $(\lambda_2(a), q) \neq 1$ are excluded from summation. We define the degree of λ by

$$d = d(\lambda) = \deg(\lambda_1) + \deg(\lambda_2).$$

If

$$\lambda_1(x) = \sum_{0 \leqslant j \leqslant d_1} r_j x^j \in \mathbf{Z}[x], \quad \lambda_2(x) = \sum_{0 \leqslant j \leqslant d_2} t_j x^j \in \mathbf{Z}[x],$$

we then adopt the convention that

$$(\lambda, c)_* = (r_0, r_1, r_2, \ldots, r_{d_1}, c), \tag{B.1}$$
$$(\lambda, c) = (r_1, r_2, \ldots, r_{d_1}, t_1, t_2, \ldots, t_{d_2}, c), \tag{B.2}$$
$$(\lambda', c) = (\lambda_1' \lambda_2 - \lambda_1 \lambda_2', c) \tag{B.3}$$

for all $c \mid q$.

There are many known estimates for complete exponential sums in the literature. In [WX16, Theorem B.1], we obtained the following estimate for $\Sigma(\lambda, q)$.

THEOREM B.1. *Let $d = d(\lambda) \geqslant 1$. For $q \geqslant 1$, we have*

$$|\Sigma(\lambda, q)| \leqslant q^{1/2} (\lambda, q^\flat)^{1/2} (\lambda, q^\flat)_*^{1/2} (\lambda', q^\ddagger) (2d)^{\omega(q)} \cdot \Xi(q)^{1/2},$$

where $q^\ddagger$ and $\Xi(q)$ are given as in Lemma 4.2.

In fact, the case of q being a prime is essentially due to Weil [Wei48], and one can refer to [Bom66] for a complete proof that suits quite well in our situation. Thanks to the Chinese remainder theorem, the evaluation of $\Sigma(\lambda, q)$ can be reduced to the case of prime power moduli $p^\alpha (\alpha \geqslant 2)$, which can usually be treated following an elementary device; see [IK04, § 12.3] for details. This is in fact the line of the proof in [WX16].

The upper bound in Theorem B.1 is complicated at first glance and it even gives a worse bound than the trivial one if λ is a constant function modulo q. However, it provides an essentially optimal bound if we have an extra average over q, since $(\lambda, q^\flat)^{1/2} (\lambda, q^\flat)_*^{1/2} (\lambda', q^\ddagger) \Xi(q)^{1/2}$ does not oscillate too much on average.

Given $m, n, u, \ell \in \mathbf{Z}$, we take

$$\lambda(x) = \frac{m}{x^2} + \frac{n}{(x+u)^2} + \ell x = \frac{\lambda_1(x)}{\lambda_2(x)}$$

with

$$\lambda_1(x) = \ell x^5 + 2\ell u x^4 + \ell u^2 x^3 + (m+n) x^2 + 2mux + mu^2, \quad \lambda_2(x) = x^2 (x+u)^2.$$

Moreover, we have

$$
\begin{aligned}
(\lambda_1'\lambda_2 &- \lambda_1\lambda_2')(x) \\
&= (5\ell x^4 + 8\ell u x^3 + 3\ell u^2 x^2 + 2(m+n)x + 2mu)x^2(x+u)^2 \\
&\quad - (4x^3 + 6ux^2 + 2u^2 x)(\ell x^5 + 2\ell u x^4 + \ell u^2 x^3 + (m+n)x^2 + 2mux + mu^2) \\
&= 5\ell x^8 + 8\ell u x^7 + 3\ell u^2 x^6 + 2(m+n)x^5 + 2mux^4 \\
&\quad + 10\ell u x^7 + 16\ell u^2 x^6 + 6\ell u^3 x^5 + 4(m+n)ux^4 + 4mu^2 x^3 \\
&\quad + 5\ell u^2 x^6 + 8\ell u^3 x^5 + 3\ell u^4 x^4 + 2(m+n)u^2 x^3 + 2mu^3 x^2 \\
&\quad - (4\ell x^8 + 8\ell u x^7 + 4\ell u^2 x^6 + 4(m+n)x^5 + 8mux^4 + 4mu^2 x^3) \\
&\quad - (6\ell u x^7 + 12\ell u^2 x^6 + 6\ell u^3 x^5 + 6(m+n)ux^4 + 12mu^2 x^3 + 6mu^3 x^2) \\
&\quad - (2\ell u^2 x^6 + 4\ell u^3 x^5 + 2\ell u^4 x^4 + 4mu^3 x^2 + 2mu^4 x) \\
&= \ell x^8 + 4\ell u x^7 - 6\ell u^2 x^6 - (2m + 2n - 4\ell u^3)x^5 + (\ell u^4 - 2nu - 8mu)x^4 \\
&\quad + (2n - 10m)u^2 x^3 - 8mu^3 x^2 - 2mu^4 x.
\end{aligned}
$$

Thus, for odd $c \mid q$, we have

$$
\begin{aligned}
(\lambda, c)_* &= (\ell, 2\ell u, \ell u^2, m+n, 2mu, mu^2, c) = (\ell, m+n, mu, c) \leqslant (\ell, m, n, c)(\ell, m+n, u, c), \\
(\lambda, c) &= (\ell, 2\ell u, \ell u^2, m+n, 2mu, 1, 2u, u^2, c) = 1
\end{aligned}
$$

and

$$
\begin{aligned}
(\lambda', c) &= (\ell, 4\ell u, 6\ell u^2, 2m+2n - 4\ell u^3, \ell u^4 - 2nu - 8mu, (2n - 10m)u^2, 8mu^3, 2mu^4, c) \\
&= (\ell, m+n, (4m+n)u, (5m-n)u^2, mu^3, c) \\
&= (\ell, m+n, 3mu, 6mu^2, mu^3, c) \\
&\leqslant 3(\ell, m+n, mu, c) \\
&\leqslant 3(\ell, m, n, c)(\ell, m+n, u, c).
\end{aligned}
$$

Note that $d(\lambda) = \deg(\lambda_1) + \deg(\lambda_2) = 5 + 4 = 9$.

From Theorem B.1, we may conclude the following estimate as given in Lemma 4.2.

THEOREM B.2. *For each odd $q \geqslant 1$, we have*

$$
\begin{aligned}
|\mathscr{B}(m, &n, \ell, u; q)| \\
&\leqslant 3q^{1/2}(\ell, m, n, q^\flat)^{1/2}(\ell, m+n, u, q^\flat)^{1/2}(\ell, m, n, q^\ddagger)(\ell, m+n, u, q^\ddagger) \cdot 18^{\omega(q)} \cdot \Xi(q)^{1/2}.
\end{aligned}
$$

REFERENCES

Bom66   E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), 71–105.

Bou15   J. Bourgain, *A remark on solutions of the Pell equation*, Int. Math. Res. Not. IMRN **2015** (2015), 2841–2855.

Fou16   É. Fouvry, *On the size of the fundamental solution of the Pell equation*, J. Reine Angew. Math. **717** (2016), 1–33.

FJ12   É. Fouvry and F. Jouve, *Fundamental solutions to Pell equation with prescribed size*, Proc. Steklov Inst. Math. **276** (2012), 40–50.

Hea78   D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions*, Invent. Math. **47** (1978), 149–170.

Hea95   D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), 235–275.

Hoo84   C. Hooley, *On the Pellian equation and the class number of indefinite binary quadratic forms*, J. Reine Angew. Math. **353** (1984), 98–131.

IK04   H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53 (American Mathematical Society, Providence, RI, 2004).

Ten95   G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46 (Cambridge University Press, Cambridge, 1995).

TW03   G. Tenenbaum and J. Wu, *Moyennes de certaines fonctions multiplicatives sur les entiers friables*, J. Reine Angew. Math. **564** (2003), 119–166.

Wei48   A. Weil, *On some exponential sums*, Proc. Natl. Acad. Sci. USA **34** (1948), 204–207.

WX16   J. Wu and P. Xi, *Arithmetic exponent pairs for algebraic trace functions and applications*, Preprint (2016), arXiv:1603.07060 [math.NT].

Ping Xi   ping.xi@xjtu.edu.cn

School of Mathematics and Statistics, Xi'an Jiaotong University,
Xi'an 710049, PR China