A BINARY QUADRATIC TITCHMARSH DIVISOR PROBLEM

JUNXIAN LI

ABSTRACT. We consider a binary quadratic variant of the Titchmarsh divisor problem and give an asymptotic formula for $\sum_{p^2+q^2\le N}\tau(p^2+q^2+1)$, where p,q are primes.

1. INTRODUCTION

Let $\tau(n)=\sum_{d|n}1$ be the divisor function. The Titchmarsh divisor problem is concerned with finding an asymptotic formula for the average

$$\sum_{p\le x}\tau(p-1), \tag{1}$$

where p belongs to the set of primes. Under the Generalized Riemann Hypothesis (GRH), Titchmarsh [16] proved that

$$\sum_{p\le x}\tau(p-1)=\frac{\zeta(2)\zeta(3)}{\zeta(6)}x+O\left(\frac{x\log\log x}{\log x}\right). \tag{2}$$

Linnik [14] proved (2) unconditionally using his dispersion method. Later, Halberstam [9] gave a short proof using the Bombieri-Vinogradov theorem on primes in arithmetic progressions. Bombieri, Friedlander and Iwaniec [1] as well as Fouvry [6] improved (2) to

$$\sum_{p\le x}\tau(p-1)=\frac{\zeta(2)\zeta(3)}{\zeta(6)}x+c\,\mathrm{Li}(x)+O\left(\frac{x}{(\log x)^A}\right), \tag{3}$$

for some constant c and any A, where $\mathrm{Li}(x)=\int_2^x\frac{1}{\log t}dt$. Most recently, Drappeau [4] gave a power saving in the error in (3) under GRH. For primes in arithmetic progressions, Felix [5] established a formula for

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\tau\left(\frac{p-a}{k}\right)=c_{k,a}x+O_k\left(\frac{x}{\log x}\right), \tag{4}$$

for some constant $c_{k,a}$. A quadratic analogue of the Titchmarsh problem was considered by Xi [17], where he obtained the correct order of magnitude given by

$$x\ll\sum_{p\le x}\tau(p^2+1)\ll x. \tag{5}$$

2010 *Mathematics Subject Classification.* 11L20, 11N37, 11N36, 11L07 .

Key words and phrases. Divisor sums, Primes.

In this paper, we obtain an asymptotic formula for

$$\sum_{p^2+q^2\le N}\tau(p^2+q^2+1).$$

Theorem 1.1 *For N large enough, we have*

$$\sum_{p^2+q^2\le N}\tau(p^2+q^2+1)=\frac{\pi}{4}\prod_{p>2}\left(1-\frac{1+3p\left(\frac{-1}{p}\right)}{(p-1)^2p}\right)\frac{N}{\log N}\left(1+O\left(\frac{(\log\log N)^2}{\log N}\right)\right), \tag{6}$$

where p,q belong to the set of primes.

A related question is the Hardy-Littlewood problem concerning asymptotic formulas for

$$\sum_{p\le N}r(N-p)\text{ or }\sum_{p\le N}r(p-a), \tag{7}$$

where $r(n)$ is the number of ways of writing n as the sum of two squares. This was solved in the works of Hooley [10] under GRH. Unconditional proofs were given by Linnik [13] and Bredihin [2] using the "dispersion method". More recently, Friedlander and Iwaniec gave a shorter proof in [7]. Greaves [8] considered the number of solutions to $N=p^2+q^2+x^2+y^2$ and gave the lower bound with the right order of magnitude. Later Plaksin [15] obtained an asymptotic formula of the number of solutions to $N=p^2+q^2+x^2+y^2$.

Let us fix some notation: We use the relation $a\sim A$ to denote $A\le a\le 2A$. The arithmetic function $\omega(n)$ denotes the number of distinct prime divisors of n. For a prime p and natural numbers α and n, we write $p^\alpha\|n$ if $p^\alpha\mid n$ but $p^{\alpha+1}\nmid n$. The letters p and q denote primes, the expression $e(x)$ denotes $\exp(2\pi ix)$, and (a,b,c) denotes $\gcd(a,b,c)$. Finally, for an odd integer d, let

$$d^*=\left(\frac{-1}{d}\right)d=\begin{cases}d, & d\equiv 1\,(\mathrm{mod}\,4),\\ -d, & d\equiv 3\,(\mathrm{mod}\,4).\end{cases}$$

2. Outline of the proof

Lemma 2.1

$$\tau(n)=2\sum_{\substack{d|n\\ d\le\sqrt{n}}}1-\mathbb{1}(n=\square), \tag{8}$$

where $\mathbb{1}(n=\square)$ vanishes unless n is a square, in which case it is 1.

Lemma 2.2 *Let $r(n)$ be the number of representations of n as a sum of two squares. Then*

$$r(n)=4\sum_{d|n}\chi(d),$$

where χ is the non-principal character modulo 4, and thus

$$r(n) \ll \tau(n) \ll n^{\epsilon}.$$

Let $Z = \sqrt{N+1}(\log N)^{-A}$, for some sufficently large constant A to be chosen later. From Lemma 2.1 and 2.2, we have

$$\begin{aligned}
\sum_{p^2+q^2\le N} \tau(p^2+q^2+1) &= 2\sum_{p^2+q^2\le N}\ \sum_{\substack{p^2+q^2+1\equiv 0 \,(\mathrm{mod}\, d)\\ d\le\sqrt{p^2+q^2+1}}} (1 - s(p^2+q^2+1)) \\
&= 2\sum_{p^2+q^2\le N}\ \sum_{\substack{p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)\\ d\le\sqrt{p^2+q^2+1}}} 1 + O(\sum_{p^2+q^2\le N}\ \sum_{p^2+q^2+1=\square} 1) \\
&= 2\sum_{d\le\sqrt{N+1}}\ \sum_{\substack{d^2-1\le p^2+q^2\le N\\ p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)}} 1 + O(\sum_{n\le\sqrt{N}} r(n^2-1)) \\
&= 2\sum_{d\le\sqrt{N+1}}\ \sum_{\substack{d^2-1\le p^2+q^2\le N\\ p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)}} 1 + O(N^{1/2+\epsilon}) \\
&= 2\sum_{d\le Z}\ \sum_{\substack{d^2-1\le p^2+q^2\le N\\ p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)}} 1 + 2\sum_{Z<d\le\sqrt{N+1}}\ \sum_{\substack{d^2-1\le p^2+q^2\le N\\ p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)}} 1 + O(N^{1/2+\epsilon}) \\
&:= M_1 + M_2 + O\left(N^{1/2+\epsilon}\right),
\end{aligned}$$

where

$$M_1 = 2\sum_{d\le Z}\ \sum_{\substack{d^2-1\le p^2+q^2\le N\\ p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)}} 1, \tag{9}$$

$$M_2 = 2\sum_{Z<d\le\sqrt{N+1}}\ \sum_{\substack{d^2-1\le p^2+q^2\le N\\ p^2+q^2\equiv -1 \,(\mathrm{mod}\, d)}} 1. \tag{10}$$

We show that M_1 gives the main term in Section 3 and Section 4, and that M_2 contributes to the error term in Section 5 and Section 6. Estimates for M_1 are similar to the main term estimate of Plaksin [15]. Assuming some preliminary results in Section 3, we obtain an asymptotic formula for M_1 in Section 4. Now we are left to prove an upper bound for M_2. Plaksin used Hooley's method, as well as Linnik's dispersion method to study distribution of $u^2+v^2 \le N$ in arithmetic progressions with difference d for $d \le N^{3/4-\epsilon}$. Instead, we use upper bound sieve weights and separate p and q by introducing a smooth function. After applying the Possion summation formula, we are left with the problem of bounding an exponential sum of the form

$$E(e_1,e_2,h_1,h_2,d) = \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1}} e\left(\frac{uh_1+vh_2}{d}\right).$$

We assume an upper bound for $E(e_1,e_2,h_1,h_2,d)$ in Section 5 and prove the bound in Section 6.

3. Preliminaries

Let $\pi(x) = \#\{p \le x\}$ and $\pi(x,d,u) = \#\{p \le x : p \equiv u \pmod d\}$.

Lemma 3.1 (Barban-Davenport-Halberstam) *For any fixed $C > 0$, any $x(\log x)^{-C} \le Q \le x$, we have*

$$\sum_{d \le Q} \sum_{\substack{u=1 \\ (u,d)=1}}^{d} \left(\pi(x,d,u) - \frac{\pi(x)}{\phi(d)}\right)^2 \ll_C xQ\log x$$

Proof. This can be found in Chap 29 of Davenport [3]. □

Lemma 3.2 *Let d be a fixed odd integer. For any fixed u, the number of solutions v to the equation*

$$u^2 + v^2 + 1 \equiv 0 \pmod d$$

is bounded by $\tau(d)$.

Proof. For $d = p$, there are either 0 or 2 solutions for v depending u^2+1 on whether is a square or not. Suppose v is a solution to $v^2+u^2+1 \equiv 0 \pmod{p^k}$. Then the solution to $v'^2+u^2+1 = 0 \pmod{p^{k+1}}$ is given by $v' = p^k t + v$, where t is determined by $2tu + \frac{u^2+v^2+1}{p^k} \equiv 0 \mod p$. Thus for $d = p^k$ there are at most 2 solutions to the equation $u^2+v^2+1 \equiv 0 \pmod{p^k}$. The lemma follows by multiplicativity. □

Lemma 3.3

$$\sum_{p^2+q^2 \le N} 1 = \pi N(\log N)^{-2}\left(1 + O\left(\log\log N(\log N)^{-1}\right)\right).$$

Proof. This is Lemma 11 in [15]. We reproduce it here for convenience. The terms with $p \le Z = \sqrt{N}(\log N)^{-A}$ can be bounded by

$$\sum_{p \le Z} \sum_{q \le \sqrt{N-p^2}} 1 \ll \frac{Z}{\log Z}\frac{\sqrt{N}}{\log N} \ll N(\log N)^{-A}.$$

If $p \ge Z$, then $\log p \gg \log Z = \log\sqrt{N} + O(\log\log N)$. Since $p \le \sqrt{N}$, we have $\log p = \frac{1}{2}\log N(1 + O\left(\frac{\log\log N}{\log N}\right))$, it follows that

$$\begin{aligned}\sum_{p^2+q^2 \le N} 1 &= \sum_{Z \le p \le \sqrt{N}} \sum_{Z \le q \le \sqrt{N-p^2}} 1 + O(N(\log N)^{-A}) \\ &= 2\left(\frac{1}{2}\log N\right)^{-2} \sum_{Z \le p \le \sqrt{N/2}} \log p \log q \left(1 + O\left(\frac{\log\log N}{\log N}\right)\right) + O\left(N(\log N)^{-A}\right).\end{aligned}$$

The conclusion follows from the following calculation

$$\begin{aligned}
&\sum_{Z\le p\le\sqrt{N/2}}\log p\sum_{Z\le q\le\sqrt{N-p^2}}\log q\\
&=\sum_{Z\le p\le\sqrt{N/2}}\log p(\sqrt{N-p^2}-Z)(1+O(\sqrt{N}e^{-\sqrt{\log N}}))\\
&=\sum_{Z\le p\le\sqrt{N/2}}\log p\sqrt{N-p^2}+O\left(Ne^{-\sqrt{\log N}}\right)+O\left(Z\sqrt{N}\right)\\
&=\sum_{2\le p\le\sqrt{N/2}}\log p\sqrt{N-p^2}+O\left(N(\log N)^{-A'}\right)\\
&=\int_0^{\sqrt{N/2}}\sqrt{N-x^2}dx(1+O(e^{-\sqrt{\log Z}}))+O\left(N(\log N)^{-A}\right)\\
&=\frac{\pi}{8}N+O\left(N(\log N)^{-A}\right).
\end{aligned}$$

□

Lemma 3.4 *Let ℓ be an odd prime. Then for $(a,p)=1$,*

$$\sum_{u=0}^{p-1}e\left(\frac{au^2}{\ell}\right)=\left(\frac{a}{\ell}\right)\sqrt{\left(\frac{-1}{\ell}\right)\ell}=\left(\frac{a}{\ell}\right)\sqrt{\ell^*}.$$

Proof. This can be found in Proposition 6.3.1 and Theorem 1 in [11, Chap 5]. □

Let $s(d)$ denote the number of solutions (u,v) to

$$u^2+v^2\equiv -1\,(\mathrm{mod}\,d),(uv,d)=1,1\le u,v\le d. \tag{11}$$

Lemma 3.5 *Let ℓ be an odd prime. Then we have*

$$s(\ell)=\ell-2-3\left(\frac{-1}{\ell}\right),s(\ell^{k+1})=\ell^k s(\ell).$$

and from the multiplicativity of $s(d)$, we have

$$s(d)\le d\prod_{p|d}\left(1+\frac{1}{p}\right).$$

Proof. By orthogonality of the characters, we have

$$\begin{aligned}
s(\ell) &= \frac{1}{\ell}\sum_{a=0}^{\ell-1}\sum_{u=1}^{\ell-1}\sum_{v=1}^{\ell-1} e\left(\frac{a(u^2+v^2+1)}{\ell}\right) \\
&= \frac{(\ell-1)^2}{\ell} + \frac{1}{\ell}\sum_{a=1}^{\ell-1}\left(\sum_{u=1}^{\ell-1} e\left(\frac{au^2}{\ell}\right)\right)^2 e\left(\frac{a}{\ell}\right) \\
&= \frac{(\ell-1)^2}{\ell} + \frac{1}{\ell}\sum_{a=1}^{\ell-1}\left(\left(\frac{a}{\ell}\right)\sqrt{\ell^*}-1\right)^2 e\left(\frac{a}{\ell}\right) \\
&= \frac{(\ell-1)^2}{\ell} + \frac{1}{\ell}\sum_{a=1}^{\ell-1}\left(\ell^* - 2\left(\frac{a}{\ell}\right)\sqrt{\ell^*}+1\right) e\left(\frac{a}{\ell}\right) \\
&= \frac{(\ell-1)^2}{\ell} - \left(\frac{-1}{\ell}\right) - \frac{1}{\ell} - 2\frac{1}{\ell}\sqrt{\ell^*}\sum_{a=1}^{\ell-1}\left(\frac{a}{\ell}\right) e\left(\frac{a}{\ell}\right) \\
&= \ell - 2 - 3\left(\frac{-1}{\ell}\right).
\end{aligned}$$

If (u,v) is a solution to $u^2+v^2+1 = 0 \,(\mathrm{mod}\, \ell^k)$, then $u' = u + t\ell^k$, $1 \le t \le p$ determines $v' = v + m\ell^k$ as $2mv \equiv \frac{-1-u'^2-v^2}{\ell^k} \,(\mathrm{mod}\, \ell)$. Thus $s(\ell^{k+1}) = \ell^k s(\ell)$ and $s(d) \le d\prod_{p|d}(1+\frac{1}{p})$. □

Lemma 3.6

$$\sum_{d\le Z}\frac{s(d)}{\phi(d)^2} = \frac{1}{4}\prod_{p>2}\left(1-\frac{1+3p\left(\frac{-1}{p}\right)}{(p-1)^2 p}\right)\log N\left(1+O\left(\frac{(\log\log N)^2}{\log N}\right)\right).$$

Proof. First note that $s(d)$ is multiplicative and the terms with $p=2$ or $q=2$ can be bounded by $O(\sqrt{N})$. Thus we can assume $2 \nmid d$. From Perron's formula, we have

$$\sum_{d\le x}\frac{s(d)}{\phi(d)^2} = \frac{1}{2\pi i}\int_{\kappa-iT}^{\kappa+iT} f(s)\frac{x^s}{s}ds + R(T),$$

where

$$\begin{aligned}
f(s) &= \sum_{d=1}^{\infty}\frac{s(d)}{\phi(d)^2 d^s}, \\
R(T) &\le \frac{x^\kappa}{T}\sum_{n=1}^{\infty}\frac{s(n)}{\phi(n)^2 n^\kappa|\log x/n|}.
\end{aligned}$$

By applying Lemma 3.5, we obtain

$$\begin{aligned} f(s) = \prod_{p>2}\left(1+\sum_{k=1}^{\infty}\frac{s(p^k)}{\phi(p^k)^2p^{ks}}\right) &= \prod_{p}\left(1+\sum_{k=1}^{\infty}\frac{s(p^k)}{\phi(p^k)^2p^{ks}}\right) \\ &= \prod_{p>2}\left(1+\sum_{k=1}^{\infty}\frac{p-1-1-3\left(\frac{-1}{p}\right)}{p^{k-1}(p-1)^2p^{ks}}\right) \\ &= \prod_{p>2}\left(1+\frac{p-1-1-3\left(\frac{-1}{p}\right)}{(p-1)^2}\frac{p^{-s}}{1-p^{-s-1}}\right) \\ &= \prod_{p>2}\left(1-p^{-s-1}\right)^{-1}\left(1-\frac{1+3p\left(\frac{-1}{p}\right)}{(p-1)^2p^{s+1}}\right) \\ &=: \zeta(1+s)(1-2^{-s-1})G(s). \end{aligned}$$

It can be seen that $G(s)$ is entire for $\Re(s) > -1$ and $f(s)$ converges absolutely when $\Re(s) > 0$. Let $\kappa = c_1/\log x$. Moving the line of integration from $\Re(s) = \kappa$ to $\Re(s) = -c/\log T$, passing the pole of $\zeta(s+1)$ at $s = 0$, we see that

$$\sum_{d\le x}\frac{s(d)}{\phi(d)^2} = \frac{1}{2}\prod_{p>2}\left(1-\frac{1+3p\left(\frac{-1}{p}\right)}{(p-1)^2p}\right)\log x + R(T) + H(T),$$

where

$$R(T) \le \frac{x^2}{T}\sum_{n=1}^{\infty}\frac{s(n)}{\phi(n)^2n^2|\log x/n|}, \tag{12}$$

$$H(T) \le \int_{-c/\log T-iT}^{\kappa-iT} f(s)\frac{x^s}{s}ds + \int_{-c/\log T+iT}^{\kappa+iT} f(s)\frac{x^s}{s}ds. \tag{13}$$

Since $s(n) \le n\prod_{p|n}(1+\frac{1}{p})$, we have that

$$\begin{aligned} R(T) &\ll \frac{x^\kappa}{T} + \frac{x^\kappa}{T}\sum_{\frac{x}{2}\le n\le 2x}\frac{s(n)}{\phi(n)^2n^\kappa}\frac{x}{|n-x|} \\ &\ll \frac{x^\kappa}{T} + \frac{(\log\log x)^2}{T}\log x. \end{aligned}$$

Since $f(s) \ll \log|\Im s|$ when $\Re(s) \ge -c/\log T$, we see that

$$H(T) \ll (\log T)^2\frac{x^\kappa}{T}.$$

We also have

$$\int_{-c/\log T-iT}^{-c/\log T+iT} f(s)\frac{x^s}{s}ds \ll x^{-c/\log T}(\log T)^2.$$

Taking $T = (\log x)^5$ gives

$$\sum_{d\le Z}\frac{s(d)}{\phi(d)^2} = \frac{1}{4}\prod_{p>2}\left(1-\frac{1+3p\left(\frac{-1}{p}\right)}{(p-1)^2p}\right)\log N\left(1+\frac{(\log\log N)^2}{\log N}\right).$$

□

4. Evaluation of M_1

We first extract the main term in M_1. Note that the terms with p or $q \le Z$ can be bounded by

$$\begin{aligned}\sum_{\substack{p\le Z,q\\ p^2+q^2\le N}}\sum_{\substack{d<Z\\ d\mid p^2+q^2+1}}1 &\ll \Bigg(\sum_{p\le Z,q}1\Bigg)^{1/2}\Bigg(\sum_{p\le Z,q\le\sqrt{N}}\Bigg(\sum_{\substack{d<Z\\ d\mid p^2+q^2+1}}1\Bigg)^2\Bigg)^{1/2}\\ &\ll \pi(Z)^{1/2}\pi(\sqrt{N})^{1/2}\Bigg(\sum_{n\le N+1}\tau^2(n)\sum_{\substack{p^2+q^2+1=n\\ p\le Z,q\le\sqrt{N}}}1\Bigg)^{1/2}\\ &\ll \pi(Z)^{1/2}\pi(\sqrt{N})^{1/2}\Bigg(\sum_{n\le N+1}\tau^2(n)r(n-1)\Bigg)^{1/2}\\ &\ll \pi(Z)^{1/2}\pi(\sqrt{N})^{1/2}\Bigg(\sum_{n\le N+1}\tau^2(n)\tau(n-1)\Bigg)^{1/2}\\ &\ll \pi(Z)^{1/2}\pi(\sqrt{N})^{1/2}\Bigg(\sum_{n\le N+1}\tau^4(n)\sum_{n\le N}\tau^2(n)\Bigg)^{1/4}\\ &\ll \left(Z\sqrt{N}N\log^{10}N\right)^{1/2}\\ &\ll N(\log N)^{-A/2+5}.\end{aligned}$$

Thus with $A' = -A/2+5$, from (9), we have

$$\begin{aligned}M_1 &= 2\sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv-1\ (\mathrm{mod}\ d)\\ u,v\le d}}\sum_{\substack{p\equiv u\ (\mathrm{mod}\ d)\\ q\equiv v\ (\mathrm{mod}\ d)\\ d^2-1\le p^2+q^2\le N}}1\\ &= 2\sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv-1\ (\mathrm{mod}\ d)\\ u,v\le d}}\sum_{\substack{p\equiv u\ (\mathrm{mod}\ d)\\ q\equiv v\ (\mathrm{mod}\ d)\\ p^2+q^2\le N\\ Z<p,Z<q}}1+O\left(N(\log N)^{-A'}\right).\end{aligned}\tag{14}$$

When $d \le Z < p$, we must have $(p,d) = 1$. Thus,

$$\begin{aligned} M_1 &= 2\sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ u,v\le d}}\sum_{\substack{p\equiv u\,(\mathrm{mod}\, d)\\ q\equiv v\,(\mathrm{mod}\, d)\\ p^2+q^2\le N\\ Z<p\\ Z<q}} 1 + O\left(N(\log N)^{-A'}\right)\\ &= 2\sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}}\sum_{\substack{p\equiv u\,(\mathrm{mod}\, d)\\ q\equiv v\,(\mathrm{mod}\, d)\\ p^2+q^2\le N}} 1 + O\left(N(\log N)^{-A'}\right). \end{aligned}$$

Let $\Omega = \sqrt{N}(\log N)^{-5}$. Then, we can cover the region $G := \{(p,q) : p^2+q^2 \le N\}$ with $\ll (\log N)^{10}$ squares of the form $X_i \le p \le X_i + \Omega$ and $Y_j \le q \le Y_j + \Omega$, $i,j \ll (\log N)^5$, and the boundary of G denoted by ∂G can be covered with $\ll (\log N)^5$ squares. The contribution from $(p,q) \in \partial G$ can be bounded by

$$\begin{aligned} \sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}}\sum_{\substack{(p,q)\in\partial G\\ p\equiv u\,(\mathrm{mod}\, d)\\ q\equiv v\,(\mathrm{mod}\, d)}} 1 &\ll \sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1}} (\log N)^5\left(\frac{\Omega}{d}\right)^2\\ &\ll N(\log N)^{-5}\sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}}\frac{1}{d^2}\\ &\ll N(\log N)^{-5}\sum_{2^k\le Z}\frac{2^k}{2^{2k}}\sum_{\substack{d\le Z\\ (d,2)=1}}\frac{\tau(d)\phi(d)}{d^2}\\ &\ll N(\log N)^{-5}\sum_{d\le Z}\frac{\tau(d)}{d}\\ &\ll N(\log N)^{-5}(\log N)^2\\ &\ll N(\log N)^{-3}. \end{aligned} \tag{15}$$

Let $\Delta_x(\Omega, d, u) = \pi(x+\Omega, d, u) - \pi(x, d, u)$, and $E_x(\Omega, d, u) := \Delta_x(\Omega, d, u) - \frac{\Delta_x(\Omega)}{\phi(d)}$, where $\Delta_x(\Omega) = \pi(x+\Omega) - \pi(x)$. For (p, q) inside G, we have

$$\begin{aligned}
&\sum_{d\le Z} \sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}} \sum_{X_i}\sum_{Y_j} \sum_{\substack{X_i\le p\le X_i+\Omega\\ p\equiv u\,(\mathrm{mod}\, d)}} 1 \sum_{\substack{Y_j\le p\le Y_j+\Omega\\ q\equiv v\,(\mathrm{mod}\, d)}} 1\\
&= \sum_{d\le Z} \sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}} \sum_{X_i,Y_j} \left(\frac{\Delta_{X_i}(\Omega)}{\phi(d)} + E_{X_i}(\Omega, d, u)\right)\left(\frac{\Delta_{Y_j}(\Omega)}{\phi(d)} + E_{Y_j}(\Omega, d, v)\right)\\
&= \sum_{d\le Z} \frac{1}{\phi(d)^2} \sum_{\substack{u^2+v^2\equiv -1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}} \sum_{X_i,Y_j} \Delta_{X_i}(\Omega, d, u)\Delta_{Y_j}(\Omega, d, v) + E',
\end{aligned}$$

where

$$E' \ll \sum_{d\le Z} \frac{\Omega}{d} \sum_{\substack{u^2+v^2\equiv\equiv 1 \,(\mathrm{mod}\, d)\\ (uv,d)=1\\ u,v\le d}} \sum_{X_i,Y_j} |E_{X_i}(\Omega, d, u)| + |E_{Y_j}(\Omega, d, v)|,$$

where we have used the fact that $\frac{\Delta_{X_i}(\Omega)}{\phi(d)}, E_{X_i}(\Omega, d, u), \frac{\Delta_{Y_i}(\Omega)}{\phi(d)}, E_{Y_i}(\Omega, d, u) \ll \frac{\Omega}{d}$ since $d \le Z \le \Omega$. For a fixed u, we have that for odd d,

$$\sum_{\substack{v^2\equiv -1-u^2 \,(\mathrm{mod}\, d)\\ v\le d}} 1 \ll \prod_{p|d} 2 \ll 2^{\omega(d)} \ll \tau(d).$$

Consequently,

$$\begin{aligned}
E' &\ll \Omega \sum_{X_i,Y_j} \sum_{k\le \log Z} \sum_{d\le Z} \left(\frac{\tau(d)}{d} \sum_{(u,d)=1} |E_{X_i}(\Omega, d, u)| + \sum_{(v,d)=1} |E_{Y_j}(\Omega, d, v)| \right)\\
&\ll \Omega(\log N)^{11} \max_{X\in\{X_i,Y_j\}} \left(\sum_{d\le Z} \frac{(\tau(d))^2}{d^2} \sum_{d\le Z} \left(\sum_{(u,d)=1} |E_X(\Omega, d, u)| \right)^2 \right)^{1/2}\\
&\ll \Omega(\log N)^{11} \max_{X\in\{X_i,Y_j\}} \left(\sum_{d\le Z} \frac{(\tau(d))^2}{d} \sum_{d\le Z} \sum_{\substack{(u,d)=1\\ u=1}}^{d} |E_X(\Omega, d, u)|^2 \right)^{1/2}. \qquad (16)
\end{aligned}$$

From Lemma 3.1, we have

$$\begin{aligned}&\sum_{d\le x(\log x)^{-C}}\sum_{\substack{u=1\\(u,d)=1}}^{d}\left(\pi(x+\Omega,d,u)-\frac{\pi(x+\Omega)}{\phi(d)}-\pi(x,d,u)+\frac{\pi(x)}{\phi(d)}\right)^2\\&\ll\sum_{d\le x(\log x)^{-C}}\left\{\sum_{\substack{u=1\\(u,d)=1}}^{d}\left(\pi(x+\Omega,d,u)-\frac{\pi(x+\Omega)}{\phi(d)}\right)^2+\left(\pi(x,d,u)-\frac{\pi(x)}{\phi(d)}\right)^2\right\}\\&\ll(x+\Omega)^2(\log(x+\Omega))^{3-C}.\end{aligned}$$

Combining this with the fact that $\max_{i,j}\{X_i,Y_j\}\le\sqrt{N}$, we see that (16) becomes

$$\begin{aligned}E'&\ll\Omega(\log N)^{11}\left(\sum_{d\le Z}\frac{(\tau(d))^2}{d}\sum_{d\le Z}\sum_{\substack{u=1\\(u,d)=1}}^{d}\left(\pi(\sqrt{N}+\Omega,d,u)-\frac{\pi(\sqrt{N}+\Omega)}{\phi(d)}\right)^2\right)^{1/2}\\&\ll\sqrt{N}(\log N)^{-5}(\log N)^{11}(\log N)^2\sqrt{N}(\log N)^{2-A/2}\\&\ll N(\log N)^{10-A/2}.\end{aligned}\tag{17}$$

Therefore, combining (15) and (17), we have

$$\begin{aligned}M_1&=\sum_{d\le Z}\sum_{\substack{u^2+v^2\equiv-1\,(\mathrm{mod}\,d)\\(uv,d)=1\\u,v\le d}}\sum_{X_i,Y_j}\frac{\Delta_{X_i}(\Omega)}{\phi(d)}\frac{\Delta_{Y_j}(\Omega)}{\phi(d)}+O(N(\log N)^{-3})\\&=\sum_{d\le Z}\frac{1}{\phi(d)^2}\sum_{\substack{u^2+v^2\equiv-1\,(\mathrm{mod}\,d)\\(uv,d)=1\\u,v\le d}}\sum_{X_i,Y_j}\Delta_{X_i}(\Omega)\Delta_{Y_j}(\Omega)+O(N(\log N)^{-3})\\&=\sum_{d\le Z}\frac{1}{\phi(d)^2}\sum_{\substack{u^2+v^2\equiv-1\,(\mathrm{mod}\,d)\\(uv,d)=1\\u,v\le d}}\left(\sum_{p^2+q^2\le N}1+O\left((\log N)^5\left(\frac{\Omega}{d}\right)^2\right)\right)+O(N(\log N)^{-3})\\&=\sum_{d\le Z}\frac{s(d)}{\phi(d)^2}\sum_{p^2+q^2\le N}1+O\left(\sum_{d\le Z}\frac{r(d)}{\phi(d)^2}\frac{N(\log N)^{-5}}{d^2}\right)+O(N(\log N)^{-3})\\&=\sum_{d\le Z}\frac{s(d)}{\phi(d)^2}\sum_{p^2+q^2\le N}1+O\left(N(\log N)^{-3}\right),\end{aligned}$$

where $s(d)$ is defined in (11). Applying Lemma 3.3 and Lemma 3.6, we have

$$M_1=\frac{\pi}{4}\prod_{p>2}\left(1-\frac{1+3p\left(\frac{-1}{p}\right)}{(p-1)^2p}\right)\frac{N}{\log N}\left(1+O\left(\frac{(\log\log N)^2}{\log N}\right)\right).\tag{18}$$

5. Estimation of M_2

Recall from (10) that M_2 is defined by

$$M_2 = 2 \sum_{Z<d\leq\sqrt{N+1}} \sum_{\substack{d^2-1\leq p^2+q^2\leq N \\ p^2+q^2\equiv -1 \pmod d}} 1.$$

Similarly to M_1, the terms in M_2 with $p<Z$ can be bounded by

$$\begin{aligned}
\sum_{\substack{p\leq Z,q \\ p^2+q^2\leq N}} \sum_{\substack{Z<d\leq\sqrt{N+1} \\ d|p^2+q^2+1}} 1 &\ll \left(\sum_{p\leq Z,q} 1\right)^{1/2} \left(\sum_{p\leq Z, q\leq\sqrt{N}} \left(\sum_{\substack{Z<d\leq\sqrt{N+1} \\ d|p^2+q^2+1}} 1\right)^2\right)^{1/2} \\
&\ll \pi(Z)^{1/2}\pi(\sqrt{N})^{1/2} \left(\sum_{n\leq N+1} (\tau(n))^2 \sum_{\substack{p^2+q^2+1=n \\ p\leq Z, q\leq\sqrt{N}}} 1\right)^{1/2} \\
&\ll N(\log N)^{-A} \left(\sum_{n\leq N+1} (\tau(n))^2 r(n-1)\right)^{1/2} \\
&\ll N(\log N)^{-A} \left(\sum_{n\leq N+1} (\tau(n))^2 \tau(n-1)\right)^{1/2} \\
&\ll N(\log N)^{-A} \left(\sum_{n\leq N} (\tau(n))^4 \sum_{n\leq N+1} (\tau(n-1))^2\right)^{1/4} \\
&\ll N(\log N)^{-A/2+5}.
\end{aligned}$$

The terms in M_2 with $p \mid d$ can be bounded by

$$\begin{aligned}
&\ll \sum_{Z<d\leq\sqrt{N+1}} \sum_{p|d} \sum_{\substack{q\leq\sqrt{N} \\ q^2\equiv -1+p^2 \pmod d}} 1 \\
&\ll \sum_{2^k\leq\sqrt{N+1}} \sum_{\substack{Z\leq d\leq\sqrt{N+1} \\ 2\nmid d}} \sum_{p|d} \frac{\sqrt{N}}{d}\tau(d) \\
&\ll \sqrt{N}(\log N) \sum_{Z\leq d\leq\sqrt{N}} \frac{\tau(d)^2}{d} \\
&\ll \sqrt{N}(\log N)^5.
\end{aligned}$$

Thus,

$$M_2 \ll \sum_{Z \le d \le \sqrt{N+1}} \sum_{\substack{p^2+q^2 \le N \\ p^2+q^2 \equiv -1 \pmod d \\ (pq,d)=1 \\ p \ge Z, q \ge Z}} 1 + O(N(\log N)^{-A/2+5}). \tag{19}$$

In order to give an upper bound for M_2, we use upper bound sieve weights to detect the primality of p and q. First we recall the fundamental lemma of sieve theory.

Lemma 5.1 (Fundamental lemma of sieve theory) *Let $y > 1$ and $s \ge 1$. There exists a set of numbers (λ_d) such that*

(1) $\lambda_1 = 1$
(2) $|\lambda_d| \le 1$ *if* $1 < d < y$.
(3) $\lambda_d = 0$ *if* $d \ge y$.

and for any integer $n > 1$, $0 \le \sum_{d|n} \lambda_d$. Moreover, for any multiplicative function $g(d)$ with $0 \le g(d) < 1$ and satisfying the dimension condition

$$\prod_{w \le p \le z} (1 - g(p))^{-1} \le \left(\frac{\log z}{\log w}\right)^{\kappa} \left(1 + \frac{K}{\log w}\right) \tag{20}$$

for all $2 \le w < z \le y$, we have

$$\sum_{d|P(z)} \lambda_d g(d) = \prod_{p<z} (1 - g(p)) \left(1 + O\left(e^{-s} \frac{K}{\log z}\right)\right),$$

where $P(z) = \prod_{p<z} p$ and $s = \log y / \log z$, the implied constant only depends on κ.

Proof. See Lemma 6 in Chapter 6 of [12]. □

Let $\theta(m) = \sum_{\substack{e|n \\ e \le E}} \lambda_e$, $E = N^{\delta}$, for some $0 < \delta < 1/2$. Let

$$S = \sum_{Z \le d \le \sqrt{N+1}} \sum_{\substack{m^2+n^2 \le N \\ m^2+n^2 \equiv -1 \pmod d \\ (mn,d)=1}} \theta(m)\theta(n) f(m) f(n), \tag{21}$$

where f is a smooth function which is 1 on $[\frac{Z}{2}, 2\sqrt{N}]$. Since $\theta(p) \ge 1$ when $p > E$, thus $M_2 \ll S$. From (19), it is enough to obtain an upper bound for S. Suppose further that f is bounded by 1 elsewhere satisfying

$$f^{(n)}(x) \ll Z^{-n} \tag{22}$$

for all $n \ge 1$ and x.

Lemma 5.2 (Poisson Summation formula) *Let $f : \mathbb{R} \to \mathbb{C}$ be a Schwartz function, i.e. f is smooth and $|f(x)| \ll (1 + |x|)^{-n}$ as $x \to \infty$ for all n. Then*

$$\sum_{n=-\infty}^{\infty} f(t + nm) = \sum_{k=-\infty}^{\infty} \frac{1}{m} \hat{f}\left(\frac{k}{m}\right) e^{2\pi i \frac{kt}{m}},$$

where $\hat{f}(k) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i k x} dx$.

Proof. See equation (4.24) in Chapter 4 of [12]. □

We have

$$\hat{f}(\lambda) = \int_{\mathbb{R}} f(x)e(-\lambda x)dx \ll \sqrt{N}. \tag{23}$$

Also, from (22),

$$\hat{f}\left(\frac{h_1}{e_1 d}\right) \ll \left(\frac{e_1 d}{h_1}\right)^j Z^{-j}\sqrt{N}, \text{ for all } j \geq 1. \tag{24}$$

Applying Lemma 5.2, we have

$$\begin{aligned}
S &= \sum_{e_1,e_2\leq E} \lambda_{e_1}\lambda_{e_2} \sum_{\substack{Z\leq d\leq\sqrt{N+1}\\(e_1e_2,d)=1}} \sum_{\substack{e_1^2m^2+e_2^2n^2\equiv -1 \,(\mathrm{mod}\, d)\\(mn,d)=1}} f(e_1m)f(e_2n)\\
&= \sum_{e_1,e_2\leq E} \lambda_{e_1}\lambda_{e_2} \sum_{\substack{Z\leq d\leq\sqrt{N+1}\\(e_1e_2,d)=1}} \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1 \,(\mathrm{mod}\, d)\\(uv,d)=1\\u,v\leq d}} \sum_{m\equiv u \,(\mathrm{mod}\, d)} f(e_1m) \sum_{n\equiv v \,(\mathrm{mod}\, d)} f(e_2n)\\
&= \sum_{e_1,e_2\leq E} \lambda_{e_1}\lambda_{e_2} \sum_{\substack{Z\leq d\leq\sqrt{N+1}\\(e_1e_2,d)=1}} \frac{1}{d^2} \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1 \,(\mathrm{mod}\, d)\\(uv,d)=1}} \frac{1}{e_1e_2} \sum_{h_1}\sum_{h_2} e\left(\frac{uh_1+vh_2}{d}\right)\hat{f}\left(\frac{h_1}{e_1d}\right)\hat{f}\left(\frac{h_2}{e_2d}\right).
\end{aligned}$$

The terms with $h_1 = h_2 = 0$ give a contribution of

$$\begin{aligned}
&\sum_{e_1\leq E}\sum_{e_2\leq E} \lambda_{e_1}\lambda_{e_2} \sum_{\substack{Z\leq d\leq\sqrt{N+1}\\(e_1e_2,d)=1}} \frac{1}{d^2e_1e_2} \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1 \,(\mathrm{mod}\, d)\\(uv,d)=1}} \hat{f}(0)\hat{f}(0)\\
&= \sum_{e_1,e_2\leq E} \frac{\lambda_{e_1}\lambda_{e_2}}{e_1e_2} \sum_{\substack{Z\leq d\leq\sqrt{N+1}\\(e_1e_2,d)=1}} \frac{r(d)}{d^2}(\hat{f}(0))^2\\
&= (\hat{f}(0))^2 \sum_{Z\leq d\leq\sqrt{N+1}} \frac{r(d)}{d^2} \sum_{\substack{e_1,e_2\leq E\\(e_1e_2,d)=1}} \frac{\lambda_{e_1}\lambda_{e_2}}{e_1e_2}\\
&= (\hat{f}(0))^2 \sum_{Z\leq d\leq\sqrt{N+1}} \frac{r(d)}{d^2} \left(\sum_{\substack{e\leq E\\(e,d)=1}} \frac{\lambda_e}{e}\right)^2.
\end{aligned} \tag{25}$$

Applying Lemma 5.1 with $z = y = E$, we have

$$\begin{aligned}\sum_{\substack{e_1 \le E \\ (e_1,d)=1}} \frac{\lambda_{e_1}}{e_1} &\ll \prod_{\substack{p \le E \\ (p,d)=1}} \left(1 - \frac{1}{p}\right) \\ &\ll \prod_{p \le E} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \mid d \\ p \le E}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \prod_{p \le E} \left(1 - \frac{1}{p}\right) \prod_{p \mid d} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \prod_{p \le E} \left(1 - \frac{1}{p}\right) \frac{d}{\phi(d)}.\end{aligned}$$

From Lemma 3.6, we see that

$$\sum_{Z \le d \le \sqrt{N+1}} \frac{s(d)}{\phi(d)^2} = \frac{1}{2} \prod_{p>2} \left(1 + \frac{1 + 3p\left(\frac{-1}{p}\right)}{(p-1)^2 p}\right) \log \frac{\sqrt{N+1}}{Z}(1 + o(1)).$$

Since $E = N^\delta$, $Z = \frac{\sqrt{N}}{(\log N)^A}$, we see that (25) is bounded from above by

$$\begin{aligned}\hat{f}(0)\hat{f}(0) \sum_{Z \le d \le \sqrt{N+1}} \frac{s(d)}{d^2} \prod_{p \le E} \left(1 - \frac{1}{p}\right)^2 \frac{d^2}{\phi(d)^2} &\ll \frac{(\hat{f}(0))^2}{(\log E)^2} \log \frac{\sqrt{N+1}}{Z} \\ &\ll N \frac{\log\log N}{(\log N)^2}.\end{aligned}$$

By breaking e_1, e_2 and d into dyadic ranges , we need to consider

$$\sum_{e_1 \sim E_1, e_2 \sim E_2} \lambda_{e_1} \lambda_{e_2} \sum_{\substack{d \sim D \\ (e_1 e_2, d)=1}} \frac{1}{d^2} \sum_{\substack{e_1^2 u^2 + e_2^2 v^2 \equiv -1 \pmod{d} \\ (uv,d)=1}} \frac{1}{e_1 e_2} \sum_{h_1} \sum_{h_2} e\left(\frac{uh_1 + vh_2}{d}\right) \hat{f}\left(\frac{h_1}{e_1 d}\right) \hat{f}\left(\frac{h_2}{e_2 d}\right), \tag{26}$$

where $E_1, E_2 \le E$, $(h_1, h_2) \ne (0, 0)$, and $Z \le D \le \sqrt{N+1}$. Since $E, D \ll N$, the number of E_1, E_2 and D is bounded by $N^{o(1)}$. Applying (24) with $j = n$ for $\hat{f}\left(\frac{h_1}{e_1 d}\right)$

and $j=2$ for $\hat{f}\left(\frac{h_2}{e_2 d}\right)$, we see that the contribution from $|h_1| \geq \frac{DE_1N^\epsilon}{\sqrt{N}}$ is bounded by

$$\begin{aligned}
&\sum_{e_1\sim E_1, e_2\sim E_2} \lambda_{e_1}\lambda_{e_2} \sum_{\substack{d\sim D\\(e_1e_2,d)=1}} \frac{1}{d^2} \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1 \,(\mathrm{mod}\, d)\\(uv,d)=1}} \frac{1}{e_1e_2} \sum_{|h_1|\geq \frac{DE_1N^\epsilon}{\sqrt{N}}} \sum_{h_2} \hat{f}\left(\frac{h_1}{e_1d}\right)\hat{f}\left(\frac{h_2}{e_2d}\right)\\
&\ll \sum_{e_1\sim E_1, e_2\sim E_2} \frac{1}{e_1e_2} \sum_{d\sim D} \frac{r(d)}{d^2} \sum_{|h_1|\geq \frac{DE_1N^\epsilon}{\sqrt{N}}} \left(\frac{e_1d}{h_1}\right)^n \left(\sum_{h_2\neq 0}\left(\frac{e_2d}{h_2}\right)^2 + \hat{f}(0)\right)\\
&\ll N^\epsilon (E_1D)^n \left(\frac{\sqrt{N}}{E_1DN^\epsilon}\right)^{n-1} Z^{-n}\sqrt{N}\left((E_2D)^2Z^{-2}\sqrt{N}+\sqrt{N}\right)\\
&\ll N^\epsilon E_1E_2^2D^3N^{-\epsilon n/2-1/2} + N^\epsilon E_1 D N^{-\epsilon n/2+1/2}\\
&\ll N^{-\delta},
\end{aligned}$$

by taking n sufficiently large. The terms with $|h_2| \geq \frac{DE_2N^\epsilon}{\sqrt{N}}$ can be bounded $N^{-\delta}$ in the same way. Thus it remains to consider the case $0\leq h_1 \leq \frac{DE_1N^\epsilon}{\sqrt{N}}$, $0 \leq h_2 \leq \frac{DE_2N^\epsilon}{\sqrt{N}}$ and $(h_1,h_2)\neq(0,0)$. Denote

$$E(e_1,e_2,h_1,h_2,d) = \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1 \,(\mathrm{mod}\, d)\\(uv,d)=1}} e\left(\frac{uh_1+vh_2}{d}\right). \tag{27}$$

We use the following lemma to complete the estimates for M_2, and the proof of Lemma 5.3 is given in Section 6.

Lemma 5.3 *If $(h_1,h_2)\neq(0,0)$, then*

$$E(e_1,e_2,h_1,h_2,d) \ll C^{\omega(d)}\sqrt{(h_1,h_2,d)d},$$

where $C>0$ is an absolute constant.

Applying Lemma 5.3 to (26), we have

$$\sum_{e_1\sim E_1, e_2\sim E_2}\lambda_{e_1}\lambda_{e_2}\sum_{\substack{d\sim D\\(e_1e_2,d)=1}}\frac{1}{d^2}\frac{1}{e_1e_2}\sum_{|h_1|\le\frac{DE_1N^\epsilon}{\sqrt{N}}}\sum_{\substack{|h_2|\le\frac{DE_2N^\epsilon}{\sqrt{N}}\\(h_1,h_2)\neq(0,0)}}\hat{f}\left(\frac{h_1}{e_1d}\right)\hat{f}\left(\frac{h_2}{e_2d}\right)E(e_1,e_2,h_1,h_2,d)$$

$$\ll N\sum_{e_1\sim E_1}\sum_{e_2\sim E_2}\frac{1}{e_1e_2}\sum_{\substack{d\sim D\\(e_1e_2,d)=1}}\frac{1}{d^2}\sum_{|h_1|\frac{\le DE_1N^\epsilon}{\sqrt{N}}}\sum_{|h_2|\le\frac{DE_2N^\epsilon}{\sqrt{N}}}C^{\omega(d)}\sqrt{(h_1,h_2,d)d}$$

$$\ll N^{1+\epsilon}\sum_{g\le D}\frac{C^{\omega(g)}}{g^2}\sum_{d\sim D/g}\frac{1}{d^2}\sum_{|h_1|\le\frac{DE_1N^\epsilon}{\sqrt{N}g}}\sum_{|h_2|\le\frac{DE_2N^\epsilon}{\sqrt{N}g}}C^{\omega(d)}\sqrt{ggd}$$

$$\ll N^{1+\epsilon}\sum_{g\le D}\frac{C^{\omega(g)}}{g}\frac{g}{D}\frac{DE_1N^\epsilon}{\sqrt{N}g}\frac{DE_2N^\epsilon}{\sqrt{N}g}\max_{d\sim D}C^{\omega(d)}\sqrt{d}$$

$$\ll\sum_{g\le D}\frac{\tau(g)^{\log C/\log 2}}{g}DE_1E_2N^\epsilon\max_{d\sim D}\tau(d)^{\log C/\log 2}\sqrt{d}$$

$$\ll D^{3/2+\epsilon}E_1E_2N^\epsilon.$$

Choosing $E\ll N^{1/8-\delta_0}$, we find that $S\ll N^{1-\delta'}$ for some $\delta'>0$.

6. Proof of Lemma 5.3

6.1. Quadratic Gauss Sums and Twisted Kloosterman Sums.

6.1.1. *Quadratic Gauss Sum.* Let a,b,d be natural numbers. The quadratic Gauss sum is defined by

$$S(a,b,d):=\sum_{n\,(\mathrm{mod}\,d)}e\left(\frac{an^2+bn}{d}\right). \tag{28}$$

Lemma 6.1 *We have the following properties of $S(a,b,d)$.*

(1) *If $(c,d)=1$, then $S(a,b,cd)=S(ac,b,d)S(ad,b,c)$.*
(2) *If $(a,d)>1$, then $S(a,b,d)=0$ except when $(a,d)\mid b$, then*

$$S(a,b,d)=(a,d)S\left(\frac{a}{(a,d)},\frac{b}{(a,d)},\frac{d}{(a,d)}\right). \tag{29}$$

(3) *For $(a,p)=1$ and $p>2$,*

$$S(a,b,p^\alpha)=\sum_{n\,(\mathrm{mod}\,p^\alpha)}e\left(\frac{an^2+bn}{p^\alpha}\right)=\left(\frac{a}{p^\alpha}\right)S(1,0,p^\alpha)e\left(-\frac{\overline{4a}b^2}{p^\alpha}\right) \tag{30}$$

(4)

$$S(1,0,p^\alpha)=pS(1,0,p^{\alpha-2}),\alpha>2 \tag{31}$$

$$S(1,0,p^2)=p. \tag{32}$$

(5)

$$S(1,0,d)=\sqrt{d^*} \tag{33}$$

Proof. See Chapter 3 of [12]. □

6.1.2. *Kloosterman Sums.* Let a,b,m be natural numbers. The Kloosterman sum is defined by

$$K(a,b;m)=\sum_{\substack{(x,m)=1\\ x\,(\mathrm{mod}\,m)}} e\left(\frac{ax+b\overline{x}}{m}\right), \tag{34}$$

where $\overline{x}$ is the inverse of x modulo m.

Lemma 6.2 *Let $K(a,b;m)$ be defined as above. Then*

$$|K(a,b;m)|\leq \tau(m)\sqrt{(a,b,m)}\sqrt{m}.$$

Proof. See corollary 11.12 in chapter 11 of [12]. □

6.1.3. *Salié sums.* Let m,n,d be natural numbers. The Saleé sum is defined by

$$T(m,n;d):=\sum_{x\,(\mathrm{mod}\,d)}\left(\frac{x}{d}\right)e\left(\frac{m\bar{x}+nx}{d}\right),$$

where $\left(\frac{\cdot}{d}\right)$ is the Jacobi-Legendre symbol.

Lemma 6.3 *Suppose $(d,2mn)=1$, Then $T(m,n,d)$ vanishes unless there exists an a with $a^2\equiv mn\,(\mathrm{mod}\,p^\beta)$. Given a, all the solutions to $x^2\equiv mn\,(\mathrm{mod}\,d)$ can be written explicitly as $x=(r\bar{r}-s\bar{s})a$, where r,s run over the factorizations of $rs=d$ with $(r,s)=1$.*

$$T(m,n;d)=\sqrt{d^*}\left(\frac{n}{d}\right)\sum_{\substack{rs=d\\ (r,s)=1}} e\left(2a\left(\frac{\bar{r}}{s}-\frac{\bar{s}}{r}\right)\right).$$

Proof. See equation (12.43) in Chapter 12 of [12]. □

As a corollary of Lemma 6.3, we see that

Corollary 6.4 *Let $T(m,n;d)$ be as above. Then,*

$$T(m,n;d)\ll\sqrt{d}2^{\omega(d)}.$$

Lemma 6.5 *Let ℓ be a prime and $k\geq 1$ be an integer. Then,*

$$\sum_{\substack{(a,\ell)=1\\ a\,(\mathrm{mod}\,\ell^k)}} e\left(\frac{a}{\ell^k}\right)=\begin{cases}-1, & k=1,\\ 0, & k\geq 2.\end{cases}$$

Proof.

$$\sum_{\substack{(a,\ell)=1\\ a\,(\mathrm{mod}\,\ell^k)}} e\left(\frac{a}{\ell^k}\right) = \sum_{a\,(\mathrm{mod}\,\ell^k)} e\left(\frac{a}{\ell^k}\right) - \sum_{a\,(\mathrm{mod}\,\ell^{k-1})} e\left(\frac{a}{\ell^{k-1}}\right) = \begin{cases} -1, & k=1,\\ 0, & k\geq 2.\end{cases}$$

□

Now we are ready to prove Lemma 5.3.

Proof of Lemma 5.3. We rewrite (27) as

$$\begin{aligned} E(e_1,e_2,h_1,h_2,d) &= \sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1\,(\mathrm{mod}\,d)\\ (uv,d)=1}} e\left(\frac{uh_1+vh_2}{d}\right)\\ &= \frac{1}{d}\sum_{a\,(\mathrm{mod}\,d)}\sum_{\substack{u\,(\mathrm{mod}\,d)\\(u,d)=1}}\sum_{\substack{v\,(\mathrm{mod}\,d)\\(v,d)=1}} e\left(\frac{uh_1+vh_2}{d}\right) e\left(\frac{a(e_1^2u^2+e_2^2v^2+1)}{d}\right)\\ &= \frac{1}{d}\sum_{a\,(\mathrm{mod}\,d)} e\left(\frac{a}{d}\right)\sum_{\substack{u\,(\mathrm{mod}\,d)\\(u,d)=1}} e\left(\frac{ae_1^2u^2+uh_1}{d}\right)\sum_{\substack{v\,(\mathrm{mod}\,d)\\(v,d)=1}} e\left(\frac{ae_2^2v^2+vh_2}{d}\right). \end{aligned}$$

From the Chinese remainder theorem, it is enough to consider $E(e_1,e_2,h_1,h_2,\ell^\alpha)$ for primes ℓ. For $(e_1e_2,\ell)=1$, we have

$$\begin{aligned} &E(e_1,e_2,h_1,h_2,\ell^\alpha)\\ &= \frac{1}{\ell^\alpha}\sum_{a\,(\mathrm{mod}\,\ell^\alpha)}\sum_{(uv,\ell)=1} e\left(\frac{h_1\overline{e_1}u+h_2\overline{e_2}v}{\ell^\alpha}\right) e\left(\frac{au^2+av^2+a}{\ell^\alpha}\right)\\ &= \frac{1}{\ell^\alpha}\sum_{k=1}^{\alpha}\sum_{a=\ell^k} e\left(\frac{\ell^{\alpha-k}a}{\ell^\alpha}\right)\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^\alpha}\right)\sum_{\substack{(v,\ell)=1\\ v\,(\mathrm{mod}\,\ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}av^2+h_2\overline{e_2}v}{\ell^\alpha}\right)\\ &+ \frac{1}{\ell^\alpha}\sum_{k=1}^{\alpha}\sum_{\substack{(a,\ell)=1\\ a\,(\mathrm{mod}\,\ell^k)}} e\left(\frac{\ell^{\alpha-k}a}{\ell^\alpha}\right)\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^\alpha}\right)\sum_{\substack{(v,\ell)=1\\ v\,(\mathrm{mod}\,\ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}av^2+h_2\overline{e_2}v}{\ell^\alpha}\right). \end{aligned} \tag{35}$$

From Lemma 6.5, we see that

$$\frac{1}{\ell^\alpha}\sum_{k=1}^{\alpha}\sum_{a=\ell^k} e\left(\frac{\ell^{\alpha-k}a}{\ell^\alpha}\right)\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^\alpha}\right)\sum_{\substack{(v,\ell)=1\\ v\,(\mathrm{mod}\,\ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}av^2+h_2\overline{e_2}v}{\ell^\alpha}\right) = \frac{1}{\ell^\alpha}.$$

For $(a,\ell)=1$, $\ell^{\alpha-k+1}\mid h_1$, from (29), (30), and (31), after writing $h_1=\ell^{\alpha-k+1}h_1'$, we have that if $k\geq 3$,

$$\begin{aligned}
&\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^{\alpha})}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)\\
&=\sum_{u\,(\mathrm{mod}\,\ell^{\alpha})} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)-\sum_{u\,(\mathrm{mod}\,\ell^{\alpha-1})} e\left(\frac{\ell^{\alpha-k+1}au^2+h_1\overline{e_1}u}{\ell^{\alpha-1}}\right)\\
&=\ell^{\alpha-k}\sum_{u\,(\mathrm{mod}\,\ell^{k})} e\left(\frac{au^2+h_1'\ell\overline{e_1}u}{\ell^{k}}\right)-\ell^{\alpha-k+1}\sum_{u\,(\mathrm{mod}\,\ell^{k-2})} e\left(\frac{au^2+h_1'\overline{e_1}u}{\ell^{k-2}}\right)\\
&=\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right)e\left(\frac{-\overline{4ae_1^2}h_1'^2\ell^2}{\ell^k}\right)S(1,0,\ell^k)-\ell^{\alpha-k+1}\left(\frac{a}{\ell^{k-2}}\right)e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell^{k-2}}\right)S(1,0,\ell^{k-2})\\
&=0. \qquad (36)
\end{aligned}$$

For $(a,\ell)=1$, $\ell^{\alpha-k+1}\mid h_1$, from (29), (30), and (31), after writing $h_1=\ell^{\alpha-k+1}h_1'$, we have that if $k<3$, then $\ell^{\alpha-1}\mid h_1$. It thus follows that

$$\begin{aligned}
&\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^{\alpha})}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)\\
&=\sum_{u\,(\mathrm{mod}\,\ell^{\alpha})} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)-\sum_{u\,(\mathrm{mod}\,\ell^{\alpha-1})} e\left(\frac{\ell^{\alpha-k+1}au^2+h_1\overline{e_1}u}{\ell^{\alpha-1}}\right)\\
&=\ell^{\alpha-k}\sum_{u\,(\mathrm{mod}\,\ell^{k})} e\left(\frac{au^2+h_1'\ell\overline{e_1}u}{\ell^{k}}\right)-\sum_{u\,(\mathrm{mod}\,\ell^{\alpha-1})} e\left(\frac{h_1\overline{e_1}u}{\ell^{\alpha-1}}\right)\\
&=\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right)e\left(\frac{-\overline{4ae_1^2}h_1'^2\ell^2}{\ell^k}\right)S(1,0,\ell^k)-\ell^{\alpha-1}\\
&=\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right)S(1,0,\ell^k)-\ell^{\alpha-1}. \qquad (37)
\end{aligned}$$

Similarly, for $(a,\ell)=1$, $\ell^{\alpha-k}\mid\mid h_1$, after writing $h_1=\ell^{\alpha-k}h_1'$, we have that if $k\geq 2$, then

$$\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^{\alpha})}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)=\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right)e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell^k}\right)S(1,0,\ell^k), \qquad (38)$$

and if $k=1$, then

$$\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^{\alpha})}} e\left(\frac{\ell^{\alpha-1}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)=\ell^{\alpha-1}\left(\frac{a}{\ell}\right)e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell}\right)S(1,0,\ell)-\ell^{\alpha-1}. \qquad (39)$$

For $(a,\ell)=1$, $\ell^{\alpha-k}\nmid h_1$, we have that if $k\geq 2$,

$$\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^{\alpha})}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)=0. \tag{40}$$

and that if $k=1$,

$$\sum_{\substack{(u,\ell)=1\\ u\,(\mathrm{mod}\,\ell^{\alpha})}} e\left(\frac{\ell^{\alpha-k}au^2+h_1\overline{e_1}u}{\ell^{\alpha}}\right)=-\sum_{u\,(\mathrm{mod}\,\ell^{\alpha-1})} e\left(\frac{h_1\overline{e_1}u}{\ell^{\alpha-1}}\right)=\begin{cases}-1, & \alpha=1,\\ 0, & \alpha\geq 2.\end{cases}. \tag{41}$$

Let $h_1=\ell^t h_1'$ and $h_2=\ell^s h_2'$, where $(h_1'h_2',\ell)=1$. From (40) and (41), we see that only the terms with k satisfying $\alpha-k\leq t$ and $\alpha-k\leq s$ will contribute to the sum (35) unless $\alpha=1$. Without loss of generality, we can assume $t\leq s$. Thus we only need to consider $k\geq\alpha-t\geq\alpha-s$ when $\alpha\geq 2$. From (36), (37) and (38), we see that we can further restrict k such that $k=1,2,\alpha-t$. In the following we consider $\alpha=1$ in Case 0 and $\alpha\geq 2$ in Case 1-Case 6.

Case 0. For prime ℓ, $(e_1e_2,\ell)=1$, we have

$$\begin{aligned}
&\sum_{\substack{e_1^2u^2+e_2^2v^2\equiv -1\,(\mathrm{mod}\,\ell)\\ (uv,\ell)=1}} e\left(\frac{h_1u+h_2v}{\ell}\right)\\
&=\sum_{\substack{u^2+v^2\equiv -1\,(\mathrm{mod}\,\ell)\\ (uv,\ell)=1}} e\left(\frac{h_1\overline{e_1}u+h_2\overline{e_2}v}{\ell}\right)\\
&=\frac{1}{\ell}\sum_{a\mod \ell}\sum_{(uv,\ell)=1} e\left(\frac{h_1\overline{e_1}u+h_2\overline{e_2}v}{\ell}\right)e\left(\frac{a(u^2+v^2+1)}{\ell}\right)\\
&=\frac{1}{\ell}+\frac{1}{\ell}\sum_{(a,\ell)=1}\sum_{(uv,\ell)=1} e\left(\frac{h_1\overline{e_1}u+h_2\overline{e_2}v}{\ell}\right)e\left(\frac{a(u^2+v^2+1)}{\ell}\right)\\
&=\frac{1}{\ell}+\frac{1}{\ell}\sum_{(a,\ell)=1} e\left(\frac{a}{\ell}\right)\sum_{(u,\ell)=1} e\left(\frac{au^2+h_1\overline{e_1}u}{\ell}\right)\sum_{(v,\ell)=1} e\left(\frac{av^2+h_2\overline{e_2}v}{\ell}\right)\\
&=\frac{1}{\ell}+\frac{1}{\ell}\sum_{(a,\ell)=1} e\left(\frac{a}{\ell}\right)\left(\left(\frac{a}{\ell}\right)e\left(\frac{-\overline{4a}\overline{e_1}^2h_1^2}{\ell}\right)\sqrt{\ell^*}-1\right)\left(\left(\frac{a}{\ell}\right)e\left(\frac{-\overline{4a}\overline{e_2}^2h_2^2}{\ell}\right)\sqrt{\ell^*}-1\right)\\
&=\frac{1}{\ell}+\sum_{(a,\ell)=1} e\left(\frac{a-\overline{4ae_1^2}h_1^2-\overline{4ae_2^2}h_2}{\ell}\right)\left(\frac{-1}{\ell}\right)+O\left(\sqrt{\ell}\right)\\
&=O\left(\sqrt{\ell}\right).
\end{aligned} \tag{42}$$

Case 1. If $t < \alpha - 1$, then $\ell^{\alpha-1} \nmid h_1$, thus only terms with $k = \alpha - t \geq 2$ contribute to (35) when $\alpha \geq 2$ by (40) and (41). If $t = s < \alpha - 1$, then we have

$$\begin{aligned}
&E(e_1, e_2, h_1, h_2, \ell^\alpha) \\
&= \frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{k=1,2\alpha-t} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{\ell^{\alpha-k}a}{\ell^\alpha}\right) \sum_{\substack{(u,\ell)=1 \\ u \,(\mathrm{mod}\, \ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}au^2 + h_1\overline{e_1}u}{\ell^\alpha}\right) \sum_{\substack{(v,\ell)=1 \\ v \,(\mathrm{mod}\, \ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}av^2 + h_2\overline{e_2}v}{\ell^\alpha}\right) \\
&= \frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{k=\alpha-t} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{a}{\ell^k}\right) \ell^{\alpha-k} e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell^k}\right) S(1,0,\ell^k)\ell^{\alpha-k} e\left(\frac{-\overline{4ae_2^2}h_2'^2}{\ell^k}\right) S(1,0,\ell^k) \\
&= \frac{1}{\ell^\alpha} + \ell^t \left(\frac{-1}{\ell^{\alpha-t}}\right) \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^{\alpha-t})}} e\left(\frac{a - \bar{a}(\overline{4e_1^2}h_1'^2 + \overline{4e_2^2}h_2'^2)}{\ell^{\alpha-t}}\right) \\
&= O\left(\sqrt{\ell^{\alpha+t}}\right),
\end{aligned}$$

where the last equality follows from Lemma 6.2.

Case 2. If $s \geq \alpha - 1 > t$, then from (36), we see that if $k = \alpha - t \geq 3$ then

$$E(e_1, e_2, h_1, h_2, \ell^\alpha) = 0 = O\left(\sqrt{\ell^{\alpha+t}}\right).$$

Case 3. When $s \geq \alpha - 1 > t, k = \alpha - t = 2$, from (37) we have

$$\begin{aligned}
&E(e_1, e_2, h_1, h_2, \ell^\alpha) \\
&= \frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{k=1,2,\alpha-t} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{\ell^{\alpha-k}a}{\ell^\alpha}\right) \sum_{\substack{(u,\ell)=1 \\ u \,(\mathrm{mod}\, \ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}au^2 + h_1\overline{e_1}u}{\ell^\alpha}\right) \sum_{\substack{(v,\ell)=1 \\ v \,(\mathrm{mod}\, \ell^\alpha)}} e\left(\frac{\ell^{\alpha-k}av^2 + h_2\overline{e_2}v}{\ell^\alpha}\right) \\
&= \frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{k=\alpha-t} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{a}{\ell^k}\right) \ell^{\alpha-k} e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell^k}\right) S(1,0,\ell^k) \left(\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right) S(1,0,\ell^k) - \ell^{\alpha-1}\right) \\
&= \frac{1}{\ell^\alpha} + \ell^t \left(\frac{-1}{\ell^{\alpha-t}}\right) \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^{\alpha-t})}} \left(\frac{a}{\ell^{\alpha-t}}\right) e\left(\frac{a - \bar{a}(\overline{4e_1^2}h_1'^2)}{\ell^{\alpha-t}}\right) - \frac{\ell^{\alpha-k+\alpha-1}}{\ell^\alpha} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{a - \bar{a}(\overline{4e_1^2}h_1'^2)}{\ell^k}\right) S(1,0,\ell^k) \\
&= O\left(\sqrt{\ell^{\alpha+t}}\right),
\end{aligned}$$

where we used Lemma 6.4.

Case 4. If $s > t = \alpha - 1$, then we have

$$
\begin{aligned}
&E(e_1, e_2, h_1, h_2, \ell^\alpha) \\
=&\frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell)}} e\left(\frac{a}{\ell}\right) \left(\ell^{\alpha-1}\left(\frac{a}{\ell}\right) e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell}\right) S(1,0,\ell) - \ell^{\alpha-1}\right)\left(\ell^{\alpha-1}\left(\frac{a}{\ell}\right) S(1,0,\ell) - \ell^{\alpha-1}\right) \\
&+ \frac{1}{\ell^\alpha} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^2)}} e\left(\frac{a}{\ell^2}\right)\left(\ell^{\alpha-2}\left(\frac{a}{\ell}\right) S(1,0,\ell^2) - \ell^{\alpha-1}\right)\left(\ell^{\alpha-2}\left(\frac{a}{\ell}\right) S(1,0,\ell^2) - \ell^{\alpha-1}\right) \\
=&\frac{1}{\ell^\alpha} + \ell^{\alpha-1}\left(\frac{-1}{\ell}\right) \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell)}} e\left(\frac{a - \bar{a}\overline{4e_1^2}h_1'^2}{\ell}\right) + 2\ell^{\alpha-2} \\
&- \ell^{\alpha-2} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell)}} \left(\frac{a}{\ell}\right)\left(e\left(\frac{a - \overline{4e_1^2}h_1'^2\bar{a}}{\ell}\right) + e\left(\frac{a}{\ell}\right)\right) S(1,0,\ell) \\
&- 2\ell^{\alpha-3} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^2)}} e\left(\frac{a}{\ell^2}\right)\left(\frac{a}{\ell}\right) S(1,0,\ell^2) + \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^2)}} e\left(\frac{a}{\ell^2}\right) S(1,0,\ell^2)^2 \ell^{\alpha-4} \\
=&O\left(\sqrt{\ell^{\alpha+t}}\right).
\end{aligned}
$$

Case 5. If $s \geq t \geq \alpha$, then from (37), we have

$$
\begin{aligned}
&E(e_1, e_2, h_1, h_2, \ell^\alpha) \\
&= \frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{k=1}^{2} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{a}{\ell^k}\right)\left(\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right) S(1,0,\ell^k) - \ell^{\alpha-1}\right)\left(\ell^{\alpha-k}\left(\frac{a}{\ell^k}\right) S(1,0,\ell^k) - \ell^{\alpha-1}\right) \\
&= \frac{1}{\ell^\alpha} + \sum_{k=1}^{2} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^k)}} e\left(\frac{a}{\ell^k}\right)\left(\ell^{\alpha-k}\left(\frac{-1}{\ell^k}\right) - 2\ell^{\alpha-k-1} S(1,0,\ell^k)\right) + \ell^{\alpha-2} \\
&= O\left(\ell^{\alpha-1}\right) = O\left(\sqrt{\ell^{2\alpha}}\right).
\end{aligned}
$$

where the last equality follows from Lemma (6.5) for $k \leq 2$.

Case 6. If $s = t = \alpha - 1$, then $k = 1, 2$ contribute to (35). From (39), (37) and Lemma 6.5, Lemma 6.3, we have

$$\begin{aligned}
&E(e_1, e_2, h_1, h_2, \ell^\alpha) \\
&= \frac{1}{\ell^\alpha} + \frac{1}{\ell^\alpha} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell)}} e\left(\frac{a}{\ell}\right) \left(\ell^{\alpha-1}\left(\frac{a}{\ell}\right) e\left(\frac{-\overline{4ae_1^2}h_1'^2}{\ell}\right) S(1,0,\ell) - \ell^{\alpha-1}\right) \\
&\qquad \times \left(\ell^{\alpha-1}\left(\frac{a}{\ell}\right) e\left(\frac{-\overline{4ae_1^2}h_2'^2}{\ell}\right) S(1,0,\ell) - \ell^{\alpha-1}\right) \\
&+ \frac{1}{\ell^\alpha} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^2)}} e\left(\frac{a}{\ell^2}\right) \left(\ell^{\alpha-2}\left(\frac{a}{\ell}\right) S(1,0,\ell^2) - \ell^{\alpha-1}\right)\left(\ell^{\alpha-2}\left(\frac{a}{\ell}\right) S(1,0,\ell^2) - \ell^{\alpha-1}\right) \\
&= \frac{1}{\ell^\alpha} + \ell^{\alpha-1}\left(\frac{-1}{\ell}\right) \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell)}} e\left(\frac{a - \bar{a}(\overline{4e_1^2}h_1'^2 + \overline{4e_2^2}h_2'^2)}{\ell}\right) + 2\ell^{\alpha-2} \\
&\quad - \ell^{\alpha-2} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell)}} \left(\frac{a}{\ell}\right)\left(e\left(\frac{a - \overline{4e_1^2}h_1'^2\bar{a}}{\ell}\right) + e\left(\frac{a - \overline{4e_2^2}h_2'^2\bar{a}}{\ell}\right)\right) S(1,0,\ell) \\
&\quad - 2\ell^{\alpha-3} \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^2)}} e\left(\frac{a}{\ell^2}\right)\left(\frac{a}{\ell}\right) S(1,0,\ell^2) + \sum_{\substack{(a,\ell)=1 \\ a \,(\mathrm{mod}\, \ell^2)}} e\left(\frac{a}{\ell^2}\right) S(1,0,\ell^2)^2 \ell^{\alpha-4} \\
&= O\left(\sqrt{\ell^{\alpha+t}}\right).
\end{aligned}$$

Combining all cases, we see that

$$E(e_1, e_2, h_1, h_2, \ell^\alpha) = O\left(\sqrt{(h_1, h_2, \ell^\alpha)\ell^\alpha}\right), \text{ if } \alpha \geq 2. \tag{43}$$

Combining (42) and (43), we have

$$E(e_1, e_2, h_1, h_2, \ell^\alpha) = O\left(\sqrt{(h_1, h_2, \ell^\alpha)\ell^\alpha}\right), \text{ for all } \alpha \geq 1. \tag{44}$$

For $E(e_1, e_2, h_1, h_2, d)$, by multiplicativity and (44), we have

$$E(e_1, e_2, h_1, h_2, d) = \prod_{\ell^{\alpha_\ell} || d} E(e_1, e_2, h_1, h_2, \ell^{\alpha_\ell}) \ll C^{\omega(d)}\sqrt{(h_1, h_2, d)d},$$

where C is an absolute constant. □

7. Acknowledgement

The author wishes to thank Valentin Blomer for suggesting the problem and for comments on an earlier draft. The author expresses gratitude to Kyle Pratt for helpful discussions and comments.

References

[1] E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. *Acta Math.*, 156(3-4):203–251, 1986.

[2] B. M. Bredihin. Binary additive problems of indeterminate type. II. Analogue of the problem of Hardy and Littlewood. *Izv. Akad. Nauk SSSR Ser. Mat.*, 27:577–612, 1963.

[3] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1980. Revised by Hugh L. Montgomery.

[4] S. Drappeau. Sums of Kloosterman sums in arithmetic progressions, and the error term in the dispersion method. *Proc. Lond. Math. Soc. (3)*, 114(4):684–732, 2017.

[5] A. T. Felix. Generalizing the Titchmarsh divisor problem. *Int. J. Number Theory*, 8(3):613–629, 2012.

[6] É. Fouvry. Sur le problème des diviseurs de Titchmarsh. *J. Reine Angew. Math.*, 357:51–76, 1985.

[7] J. B. Friedlander and H. Iwaniec. On a theorem of Bredihin and Linnik. *arXiv preprint arXiv:1807.06648*, 2018.

[8] G. Greaves. On the representation of a number in the form $x^2 + y^2 + p^2 + q^2$ where p, q are odd primes. *Acta Arith.*, 29(3):257–274, 1976.

[9] H. Halberstam. Footnote to the Titchmarsh-Linnik divisor problem. *Proc. Amer. Math. Soc.*, 18:187–188, 1967.

[10] C. Hooley. On the representation of a number as the sum of two squares and a prime. *Acta Math.*, 97:189–210, 1957.

[11] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[12] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[13] Yu. V. Linnik. An asymptotic formula in an additive problem of Hardy-Littlewood. *Izv. Akad. Nauk SSSR Ser. Mat.*, 24:629–706, 1960.

[14] Yu. V. Linnik. *The dispersion method in binary additive problems*. Translated by S. Schuur. American Mathematical Society, Providence, R.I., 1963.

[15] V. A. Plaksin. Asymptotic formula for the number of solutions of an equation with primes. *Izv. Akad. Nauk SSSR Ser. Mat.*, 45(2):321–397, 463, 1981.

[16] E. C. Titchmarsh. A divisor problem. *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, 54(1):414–429, 1930.

[17] P. Xi. A quadratic analogue of Titchmarsh divisor problem. *J. Number Theory*, 184:192–205, 2018.

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA.

E-mail address: jli135@illinois.edu