PRIME VALUES OF $a^2 + p^4$ (DRAFT)

D.R. HEATH-BROWN AND XIANNAN LI

Abstract.

1. Introduction

Many remarkably difficult conjectures in prime number theory take the form that there are infinitely many primes in some set of natural numbers S. In many interesting examples, we even have conjectured asymptotic formulas for the number of primes in S. Thus, we think that there are infinitely many primes of the form $p+2$, a^2+1, a^2+b^6, and so on.[1]

The generality of our belief is in stark contrast with the paucity of examples for which we can prove our conjectures. In this paper, we are interested in the problem of finding primes in sequences which occur as the special values of a polynomial in two variables. For polynomials in one variable, only the linear case is understood, from the work of Dirichlet.

A classical result is that there are infinitely many primes of the form a^2+b^2. Indeed, by a result of Fermat, primes of that form are essentially the same as primes of the form $4a+1$, so that this reduces to a special case of Dirichlet's theorem on primes in arithmetic progressions. Let us define the exponential density of the sequence of values of the polynomial $P(a,b)$ to be

$$\inf_{\lambda} \#\{P(a,b) \le x\} \ll x^{\lambda}. \tag{1}$$

Then the density of the sequence defined by a^2+b^2 is 1, the same as the set of all natural numbers.

It is much more challenging to prove a similar result when the sequence given by $P(a,b)$ has density less than 1. The first result in this direction was the breakthrough of Friedlander and Iwaniec [4] on the prime values of a^2+b^4, which was followed by the result of Heath-Brown [8] on primes values of a^3+2b^3. It is worth mentioning that the density of the sequence is not the only measure of difficulty, as no results are available for prime values of a^2+b^3 due to its lack of structure.

Aside from generalizations of Heath-Brown's result to more general cubic polynomials by Heath-Brown and Moroz [9], the theorems of Friedlander and Iwaniec [4] and Heath-Brown [8] remain the only results of this type. In this paper, we add the following example on prime values of a^2+p^4.

Theorem 1.

$$\#\{a^2+p^4 \le x : a>0 \text{ and } a^2+p^4 \text{ is prime}\} = \omega \frac{4Jx^{3/4}}{\log^2 x}\left(1+O_\epsilon\left(\frac{1}{(\log x)^{1-\epsilon}}\right)\right), \tag{2}$$

2010 *Mathematics Subject Classification.* Primary: 11M06, Secondary: 11M26.

[1]Everywhere in the paper, p shall always denote a prime.

where

$$J = \int_0^1 \sqrt{1-t^4}\,dt, \tag{3}$$

and

$$\omega = \prod_p \left(1 - \frac{\chi_4(p)}{p-1}\right), \tag{4}$$

for χ_4 the non-principal character modulo 4.

Remark 1. *The reader may check that the number of elements $a^2 + p^4 \le x$ is well approximated by $\frac{4Jx^{3/4}}{\log x}$.*

A little extra book-keeping would allow us to exchange $\frac{1}{(\log x)^{1-\epsilon}}$ for $\frac{\log\log x}{\log x}$. Our method also applies to more general sequences $a^2 + y^4$ where y is restricted to a set Y which is regularly distributed and is not too sparse.

As in the works [4] and [8], the proof rests on establishing a level of distribution for the sequence, and the estimation of special bilinear sums. The first appears in classical sieve theory, and simply asks for good estimates for the remainder term in counting numbers of the form a^2+p^4 divisible by a given integer d, averaged over d. The bilinear sums estimate is the ingredient which allows us to overcome the parity barrier, and as in previous works is the most significant part of the proof.

One ingredient used in Friedlander and Iwaniec's work on prime values of $a^2 + b^4$ is the regularity of the distribution of the squares of integers, which allows them to use a delicate harmonic analysis argument to extract certain main terms in their bilinear sum, and prove that the error terms are small on average (see Sections 4-9 in [4]). This is the portion of their work which overcomes the sparsity of their sequence.

This regularity does not exist in the case of squares of primes, and we need to develop a method which applies for more general sequences. In particular, we prove a result about the distribution of sequences in arithmetic progressions, which is similar in spirit to a general form of the Barban-Davenport-Heilbronn theorem. In our case, for $a^2 + p^4 \le x$, we have $p \le x^{1/4}$, while the modulus appearing in our bilinear sum can be as large as $x^{1/2-\delta}$. We thus need an equidistribution result which holds when the modulus goes up to nearly the square of the length of the sum, in contrast to the Barban-Davenport-Heilbronn theorem. Since this result is of independent interest, we first illustrate our result in the case of primes below.

Corollary 1. *For $(a,q) = 1$, let*

$$S(x;a,q) = \sum_{\substack{m,n\le x \\ n\equiv am \bmod q}} \Lambda(m)\Lambda(n). \tag{5}$$

Then for any $A > 0$, there exists $B = B(A)$ such that

$$\sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} \left| S(x;a,q) - \frac{x^2}{\phi(q)} \right|^2 \ll \frac{x^4}{\log^A x} \tag{6}$$

for $Q \le x^2(\log x)^{-B}$.

For our application, we will require a more general result which applies for sequences satisfying the Siegel-Walfisz condition, which is essentially saying that the sequence is equidistributed for small moduli (see Remark 5 for the precise definition). This is known in the case $c(n)=\Lambda(n)$ by the Siegel-Walfisz Theorem so Corollary 1 follows immediately from Corollary 2 below.

Corollary 2. *Let $c(n)$ be an arithmetic function supported on $n\le x$ satisfying the Siegel-Walfisz condition. For $(a,q)=1$, let*

$$S(x;a,q)=\sum_{\substack{m,n\le x\\ n\equiv am \bmod q}} c(m)c(n), \tag{7}$$

and let

$$S(x;q)=\sum_{d|q}\frac{1}{\phi(q/d)}\left(\sum_{\substack{n\le x\\ (n,q/d)=1}} c(dn)\right)^2. \tag{8}$$

Then for any $A>0$, there exists $B=B(A)$ such that for $Q\le x^2(\log x)^{-B}$

$$\sum_{q\le Q}\ \sideset{}{^*}\sum_{a \bmod q} |S(x;a,q)-S(x;q)|^2 \ll \frac{x^2}{\log^A x}\|c_\tau\|^4, \tag{9}$$

where $\|c_\tau\|^2=\sum_n |c(n)|^2\tau(n)^2$.

Corollary 2 follows from the more technical Theorem 2 stated in Section 8 which applies to general sequences not necessarily satisfying the Siegel-Walfisz condition.

After using Corollary 2 to extract main terms in our bilinear sum, we still need to estimate the sum of these main terms. In Friedlander and Iwaniec's treatment, this is estimated directly, and actually forms the bulk of their work (see Sections 10-26 in [4]). The estimation requires a tour de force treatment of sums of the Mobius function twisted by a quadratic symbol to modulus in several ranges, which leads to results of independent interest (see Theorem 2 in [4] on average of spins).

However, we show that if the main goal is to produce an asymptotic for primes, this difficult direct estimation can be avoided entirely by comparison with a simpler sequence. In our case, we compare our a^2+p^4 with the sequence given by a^2+p^2, previously studied by Fouvry and Iwaniec [2]. Essentially, once we have extracted the main terms in our bilinear sums, understanding the bilinear sums for the sequence a^2+p^2 is sufficient for understanding the analogous bilinear sums attached to the much sparser sequence a^2+p^4. Analogously, the sequence a^2+b^4 can be compared to the classical sequence given by a^2+b^2.

For our result, we may also use the sequence a^2+b^2 where b has no small prime factors below $(\log x)^A$, but using the result of Fouvry and Iwaniec is convenient and elegant. We now move to more precise definitions.

Since the number of $n=a^2+p^4\le x$ with $p<x^{1/4}/\log^2 x$ is bounded by

$$\sum_{p<x^{1/4}/\log^2 x}\ \sum_{a\le\sqrt{x-p^4}} 1 \ll \frac{x^{3/4}}{\log^3 x}, \tag{10}$$

we may assume that $p\ge x^{1/4}/\log^2 x$. Fix an interval $I=(X,X(1+\eta)]$ where $x^{1/2}/\log^4 x\le X\le x^{1/2}$ and $\eta=(\log x)^{-1}$. In our treatment of the bilinear sum, we need the two sequences to behave alike even when restricted to small sets, so that it becomes necessary to introduce proper weights. Define the sequences $\mathcal{A} = \{a(n)\}$ and $\mathcal{B} = \{b(n)\}$ by

$$a(n) = \begin{cases} \sum_{\substack{n=a^2+p^4 \\ p^2\in I}} 2p\log p & \text{if } \sqrt{x} < n \le x \text{ and } (a,p)=1 \\ 0 & \text{otherwise,} \end{cases} \tag{11}$$

and

$$b(n) = \begin{cases} \sum_{\substack{n=a^2+p^2 \\ p\in I}} \log p & \text{if } \sqrt{x} < n \le x \text{ and } (a,p)=1 \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

Further, define

$$\pi(\mathcal{A}) = \sum_p a(p), \tag{13}$$

and

$$\pi(\mathcal{B}) = \sum_p b(p). \tag{14}$$

We claim that it suffices to show

Proposition 1. *With notation as above,*

$$\pi(\mathcal{A}) - \pi(B) \ll \frac{\eta x}{(\log x)^{2-\epsilon}}. \tag{15}$$

We verify that our main Theorem follows from Proposition 1 in the next section. Most of this paper will be devoted to proving the Proposition.

2. Setting up the sieve

Let us first verify that Theorem 1 follows from Proposition 1. Note that the condition $(a,p) = 1$ in the definition of $b(n)$ may be removed since

$$\sum_{p\in I} \log p \sum_{\substack{a\le\sqrt{x-p^2} \\ p|a}} 1 \ll x^{1/2+\epsilon}. \tag{16}$$

Then, by the work of Fouvry and Iwaniec [2] and summation by parts, we have that

$$\pi(\mathcal{B}) = \frac{\sigma(1+O(\log^{\epsilon-1} x))}{\log x} \int_I \sqrt{x-t^2}dt, \tag{17}$$

where

$$\sigma = \prod_p \left(1 - \frac{\chi_4(p)}{p-1}\right), \tag{18}$$

for χ_4 the non-principal character mod 4. Thus Proposition 1 gives us that

$$\pi(\mathcal{A}) = \frac{\sigma}{\log x} \int_I \sqrt{x-t^2}dt \left(1 + O\left(\frac{1}{\log^{1-\epsilon} x}\right)\right). \tag{19}$$

Our main result then follows by partial summation, possible since the length of I is short. To be precise, let $I_j = (X_j, X_j(1+\eta)]$ be disjoint intervals for $1 \le j \le m$ such that

$$\cup_j I_j = (Y, x^{1/2}], \tag{20}$$

where $Y \gg \frac{x^{1/2}}{\log^2 x}$. Further, let $\mathcal{A}_j$ be defined as in (11) with $I = I_j$. Recall that $\eta = \frac{1}{\log x}$, and note that the number of elements $a^2 + p^4 \le x$ where $p|a$ with $p \in I$ is bounded by

$$\sum_{p^2 \in I} \frac{\sqrt{x}}{p} \ll x^{1/2+\epsilon}.$$

Hence,

$$\begin{aligned}
(21) \qquad & \#\{a^2 + p^4 \le x : a^2 + p^4 \text{ is prime and } a > 0\} \\
&= \sum_j \frac{1}{\sqrt{X_j} \log X_j} \pi(\mathcal{A}_j) \left(1 + O\left(\frac{1}{\log x}\right)\right) + O(x^{1/2+\epsilon}) \\
&= \frac{\sigma + O\left(\frac{1}{\log^{1-\epsilon} x}\right)}{\log x} \sum_j \int_{I_j} \sqrt{x - t^2} \frac{dt}{\sqrt{t} \log t} + O(x^{1/2+\epsilon}) \\
&= \frac{2\sigma + O\left(\frac{1}{\log^{1-\epsilon} x}\right)}{\log^2 x} \int_Y^{\sqrt{x}} \sqrt{x - t^2} \frac{dt}{\sqrt{t}} + O(x^{1/2+\epsilon}) \\
&= \frac{4\sigma x^{3/4}}{\log^2 x} \int_0^1 \sqrt{1 - t^4} dt \left(1 + O\left(\frac{1}{\log^{1-\epsilon} x}\right)\right). \qquad (22)
\end{aligned}$$

Thus Theorem 1 follows from Proposition 4.

We now fix some basic notation. For $\mathcal{C} = \{c(n)\}$ any sequence supported on $\sqrt{x} < n \le x$, let

$$\pi(\mathcal{C}) = \sum_{p \le x} c(p), \tag{23}$$

$$\mathcal{C}_d = \sum_{d|n} c(n), \tag{24}$$

and

$$R_d(\mathcal{C}) = |\mathcal{C}_d - M_d(\mathcal{C})|, \tag{25}$$

for some $M_d(\mathcal{C})$ depending on d and $\mathcal{C}$.

We shall prove Proposition 1 by applying the same sieving procedure to both sequences. As mentioned in the Introduction, this requires a level of distribution result and an understanding of certain bilinear forms. We refer the reader to Friedlander and Iwaniec's asymptotic sieve for primes [6], Harman's alternative sieve [7] and Heath-Brown's proof of primes of the form $x^3 + 2y^3$ [8] for several perspectives on this. Here, we develop what we need from scratch along the lines of [8]. For our application, this eases some technical details involving the bilinear sum. We begin by stating a level of distribution result for $\mathcal{A}$ and $\mathcal{B}$.

Proposition 2. *Let*

$$g(d) = \frac{\rho(d)}{d}, \tag{26}$$

where $\rho(d)$ denotes the number of solutions to

$$a^2 + 1 \equiv 0 \bmod d. \tag{27}$$

Now define

$$M_d(\mathcal{C}) = g(d)\int_I \sqrt{x-t^2}dt. \tag{28}$$

Then for any constants $A \geq 0$ and $k \geq 0$, there exists a constant $B = B(A,k)$ such that for $D = \frac{x^{3/4}}{(\log x)^B}$, we have

$$\sum_{d\leq D} \tau^k(d) R_d(\mathcal{C}) \ll \frac{x}{(\log x)^A}, \tag{29}$$

for both $\mathcal{C} = \mathcal{A}$ and $\mathcal{C} = \mathcal{B}$.

For $\mathcal{C} = \mathcal{B}$, the Proposition holds in the larger range $D \leq \frac{x}{(\log x)^B}$, but we do not require this. Proposition 2 is a technical modification of a result of Friedlander and Iwaniec [5] to allow for the weights we need and to include the $\tau(d)^k$ factor. The derivation of Proposition 2 is given in Section 3.

Fix for the rest of the paper $\delta = \frac{(\log\log x)^2}{\log x}$ and[2] $Y = x^{1/3+1/48}$. The following Lemma begins our sieving procedure.

Lemma 1. *For any $x^\delta < Y < x^{1/2-\delta}$ and $\mathcal{C} = \mathcal{A}$ and $\mathcal{C} = \mathcal{B}$, we have that*

$$\pi(\mathcal{C}) = S_1(\mathcal{C}) - S_2(C) - S_3(C) + O\left(\delta\eta \frac{x}{\log x}\right), \tag{30}$$

where

$$S_1(\mathcal{C}) = S(\mathcal{C}, x^\delta) \tag{31}$$

$$S_2(\mathcal{C}) = \sum_{x^\delta \leq p < Y} S(\mathcal{C}_p, p) \tag{32}$$

$$S_3(\mathcal{C}) = \sum_{Y \leq p \leq x^{1/2-\delta}} S(\mathcal{C}_p, p). \tag{33}$$

Proof. By Buchstab's identity, we have

$$\pi(\mathcal{C}) = S(\mathcal{C}, x^{1/2}) = S_1(\mathcal{C}) - S_2(C) - S_3(C) - \sum_{x^{1/2-\delta} < p \leq x^{1/2}} S(\mathcal{C}_p, p). \tag{34}$$

Using Selberg's upper bound sieve, we have that

$$\begin{aligned}\sum_{x^{1/2-\delta}<p\leq x^{1/2}} S(\mathcal{C}_p, p) &\leq \sum_{x^{1/2-\delta}<p\leq x^{1/2}} S(\mathcal{C}_p, x^{1/10}) \\ &\ll \sum_{x^{1/2-\delta}<p\leq x^{1/2}} \frac{\eta x}{p\log x} + \sum_{x^{1/2-\delta}<p\leq x^{1/2}} \sum_{d\leq x^{1/5}} \tau_3(d) R_{dp}(\mathcal{C}) \\ &\ll \frac{\eta\delta x}{\log x} + \frac{x}{\log^A x}, \end{aligned} \tag{35}$$

for any $A \geq 0$ by Proposition 2. □

While $S_1(\mathcal{C})$ may be handled via the Fundamental Lemma, and $S_3(\mathcal{C})$ can be readily written in terms of a bilinear form in the right range, $S_2(\mathcal{C})$ requires more attention.

[2] The 1/48 in the following definition can be replaced with any positive number less than 1/24.

Lemma 2. *With notation as in Lemma 1 and* $n_0 = \frac{\log Y}{\delta \log x} + 1$, *we have*

$$S_2(\mathcal{C}) = \sum_{1 \le n \le n_0} (-1)^{n-1}(T^{(n)}(\mathcal{C}) - U^{(n)}(\mathcal{C})), \tag{36}$$

where

$$T^{(n)}(\mathcal{C}) = \sum_{\substack{x^\delta \le p_n < \ldots < p_1 < Y \\ p_1 \ldots p_n < Y}} S(\mathcal{C}_{p_1 \ldots p_n}, x^\delta), \tag{37}$$

and

$$U^{(n)}(\mathcal{C}) = \sum_{\substack{x^\delta \le p_{n+1} < \ldots < p_1 < Y \\ p_1 \ldots p_n < Y \le p_1 \ldots p_{n+1}}} S(\mathcal{C}_{p_1 \ldots p_{n+1}}, p_{n+1}). \tag{38}$$

Proof. Let

$$V^{(n)}(\mathcal{C}) = \sum_{\substack{x^\delta \le p_n < \ldots < p_1 < Y \\ p_1 \ldots p_n < Y}} S(\mathcal{C}_{p_1 \ldots p_n}, p_n). \tag{39}$$

The proof of (36) follows immediately upon observing that $S_2(\mathcal{C}) = V^{(1)}(\mathcal{C})$ and from the identity

$$V^{(n)}(\mathcal{C}) = T^{(n)}(\mathcal{C}) - U^{(n)}(\mathcal{C}) - V^{(n+1)}(\mathcal{C}). \tag{40}$$

□

By Lemmas 1 and 2, in order to prove Proposition 1, it suffices to prove the following two propositions.

Proposition 3. *Let* Q *be a set of squarefree numbers not exceeding* Y. *Then for any* $A > 0$,

$$\Big|\sum_{q \in Q} S(\mathcal{A}_q, x^\delta) - \sum_{q \in Q} S(\mathcal{B}_q, x^\delta)\Big| \ll_A \frac{x}{\log^A x}. \tag{41}$$

Note that Proposition 3 immediately implies that

$$|S_1(\mathcal{A}) - S_1(\mathcal{B})| \ll_A \frac{x}{\log^A x}. \tag{42}$$

Since $n_0 \asymp 1/\delta \ll \log x$, Proposition 3 also implies that

$$\sum_{1 \le n \le n_0} |T^{(n)}(\mathcal{A}) - T^{(n)}(\mathcal{B})| \ll_A \frac{x}{\log^A x}. \tag{43}$$

The rest of the pieces from the decompositions in Lemmas 1 and 2 are handled below.

Proposition 4. *For any* $A > 0$ *and* $n \ge 3$,

$$|S_3(\mathcal{A}) - S_3(\mathcal{B})| \ll \frac{x}{\log^A x}, \text{ and} \tag{44}$$

$$|U^{(n)}(\mathcal{A}) - U^{(n)}(\mathcal{B})| \ll \frac{x}{\log^A x}. \tag{45}$$

For $n \le 2$,

$$|U^{(n)}(\mathcal{A}) - U^{(n)}(\mathcal{B})| \ll \frac{\delta \eta x}{\log x}. \tag{46}$$

Propositions 2 and 3 are proven in Sections 3 and 4 respectively. We reduce the proof of Proposition 4 to a related statement about bilinear sums in Section 5, which is in turn proven in Sections 6 and 7.

3. Level of distribution

Here, we prove Proposition 2. Let

$$\tilde{I} \subset (\tilde{X}, \tilde{X}(1+\tilde{\eta})] \tag{47}$$

with $\tilde{X} \in I$ satisfying $\tilde{X} \gg \frac{x^{1/2}}{\log^2 x}$ and $\tilde{\eta} = \log^{-\tilde{A}} x$ is a parameter to be determined. Define the sequences $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ by

$$\tilde{a}(n) = \begin{cases} \sum_{\substack{n=a^2+p^4 \\ p^2 \in \tilde{I}}} 1 & \text{if } \sqrt{x} < n \le x \text{ and } n \text{ is squarefree} \\ 0 & \text{otherwise,} \end{cases} \tag{48}$$

and

$$\tilde{b}(n) = \begin{cases} \sum_{\substack{n=a^2+p^2 \\ p \in \tilde{I}}} 1 & \text{if } \sqrt{x} < n \le x \text{ and } n \text{ is squarefree} \\ 0 & \text{otherwise.} \end{cases} \tag{49}$$

Friedlander and Iwaniec's main result in [5] gives that for

$$M_d(\tilde{A}) = g(d) \sum_{p^2 \in \tilde{I}} \frac{p-1}{p} \sqrt{x - p^4}, \tag{50}$$

and

$$M_d(\tilde{B}) = g(d) \sum_{p \in \tilde{I}} \frac{p-1}{p} \sqrt{x - p^4}, \tag{51}$$

and any $A > 0$, there exists $B = B(A)$ such that

$$\sum_{d<D} R_d(\tilde{A}) \ll_A \frac{x^{3/4}}{\log^A x} \tag{52}$$

and

$$\sum_{d<D} R_d(\tilde{B}) \ll_A \frac{x}{\log^A x}, \tag{53}$$

for $D = \frac{x^{3/4}}{\log^B x}$. Let us choose $B = B(A)$ so that $A > 2\tilde{A}$.

For clarity, we first record the following trivial bounds.

Lemma 3. *For $A > 2\tilde{A}$, we have*

$$\sum_{d<D} \tilde{\mathcal{A}}_d \le \sum_{d<D} \left(\tilde{R}_d(\tilde{A}) + M_d(\tilde{A})\right) \ll \frac{x^{3/4}}{\log^A x}, \tag{54}$$

$$\sum_{d<D} \tilde{\mathcal{B}}_d \le \sum_{d<D} \left(\tilde{R}_d(\tilde{B}) + M_d(\tilde{B})\right) \ll \frac{x}{\log^A x}. \tag{55}$$

Proof. We have

$$\sum_{d<D} \tilde{\mathcal{A}}_d \leq \sum_{d<D} \tilde{R}_d(\tilde{A}) + \sqrt{x} \sum_{p^2 \in \tilde{I}} \sum_{d<D} g(d)$$
$$\ll \frac{x^{3/4}}{\log^A x} + \tilde{\eta}\sqrt{x\tilde{X}} \log x,$$

where we have used that $g(d) \ll \frac{\tau(d)}{d}$ where τ is the usual divisor function. The proof for $\tilde{\mathcal{B}}_d$ is similar. □

Now, by construction,

$$a(n) = \sum_{\tilde{I} \in U} \sqrt{\tilde{X}} \log \tilde{X} \tilde{a}(n) \left(1 + O(\tilde{\eta})\right)$$

and

$$b(n) = \sum_{\tilde{I} \in U} \log \tilde{X} \tilde{b}(n) \left(1 + O(\tilde{\eta})\right),$$

where U is a disjoint cover for I consisting of intervals $\tilde{I}$. We ask that each $\tilde{I} \in U$ satisfies (47) and that $\#U \ll 1/\tilde{\eta}$. This is possible simply by setting all of the $\tilde{I}$ to be of the form $(\tilde{X}, \tilde{X}(1+\tilde{\eta})]$ except for the last interval which can be shorter if necessary. Of course, the point of restricting our attention to shorter intervals $\tilde{I}$ was to facilitate a crude summation by parts, an example of which is below.

Lemma 4. *We have that*

$$\sum_{\tilde{I} \in U} \sqrt{\tilde{X}} \log \tilde{X} M_d(\tilde{\mathcal{A}}) - M_d(\mathcal{A}) \ll g(d)\tilde{\eta}x \tag{56}$$

and

$$\sum_{\tilde{I} \in U} \log \tilde{X} M_d(\tilde{B}) - M_d(\mathcal{B}) \ll g(d)\tilde{\eta}x. \tag{57}$$

Proof. We have that

$$\sum_{\tilde{I} \in U} \sqrt{\tilde{X}} \log \tilde{X} M_d(\tilde{\mathcal{A}}) = g(d) \sum_{\tilde{I} \in U} \sqrt{\tilde{X}} \log \tilde{X} \sum_{p^2 \in \tilde{I}} \frac{p-1}{p} \sqrt{x - p^4} - M_d(\mathcal{A})$$
$$= g(d) \sum_{\tilde{I} \in U} \sqrt{\tilde{X}} \log \tilde{X} \int_{t^2 \in \tilde{I}} \sqrt{x - t^4} \frac{dt}{\log t} - M_d(\mathcal{A}) + O\left(g(d) \frac{x}{\log^A x}\right),$$

for any $A' > 0$, by the Prime Number Theorem. For $t^2 \in \tilde{I}$, we have that $\sqrt{\tilde{X}} \log \tilde{X} = 2t \log t \left(1 + O(\tilde{\eta})\right)$, so that the sum above is

$$g(d) \sum_{\tilde{I} \in U} \int_{t^2 \in \tilde{I}} 2t\sqrt{x - t^4} dt (1 + O(\tilde{\eta})) - M_d(\mathcal{A}) + O\left(g(d) \frac{x}{\log^A x}\right)$$
$$= g(d) \int_{u \in I} \sqrt{x - u^2} du (1 + O(\tilde{\eta})) - M_d(\mathcal{A}) + O\left(g(d) \frac{x}{\log^{A'} x}\right)$$
$$\ll g(d)\tilde{\eta}|I|\sqrt{x},$$

by taking A' large enough. This suffices since $|I| < \sqrt{x}$. The proof of (57) is similar. □

We now prove an intermediate result.

Lemma 5. *With notation as above,*

$$\sum_{d<D} R_d(\mathcal{C}) \ll \frac{x}{(\log x)^{\tilde{A}-2}} \tag{58}$$

for both $\mathcal{C} = \mathcal{A}$ and $\mathcal{C} = \mathcal{B}$.

Proof. We write the proof for $\mathcal{C} = \mathcal{A}$, the case $\mathcal{C} = \mathcal{B}$ being similar.

$$\begin{aligned}\sum_{d<D} R_d(\mathcal{A}) \le \sum_{d<D} \Bigg(& |\mathcal{A}_d - \sum_{\tilde{I}\in U} 2\tilde{X} \log \tilde{X} \tilde{\mathcal{A}}_d| + \sum_{\tilde{I}\in U} 2\tilde{X}\log \tilde{X} |\tilde{\mathcal{A}}_d - M_d(\tilde{\mathcal{A}})| \\ & + |\sum_{\tilde{I}\in U} 2\tilde{X}\log \tilde{X} M_d(\tilde{\mathcal{A}}) - M_d(\mathcal{A})| \Bigg) \\ & \ll \tilde{\eta} X \log X \sum_{\tilde{I}\in U}\sum_{d<D} |\tilde{\mathcal{A}}_d| + X\log X \sum_{\tilde{I}\in U}\sum_{d<D} R_d(\tilde{A}) + \tilde{\eta} x \sum_{d<D} g(d),\end{aligned}$$

by 4. Since $A > 2A'$, we apply Lemma 3 to the first term and see that the above is bounded by

$$\tilde{\eta}\frac{\log X}{\tilde{\eta}}\frac{x}{\log^A x} + \frac{\log X}{\tilde{\eta}}\frac{x}{\log^A x} + \tilde{\eta} x \log^2 x \ll \frac{x}{(\log x)^{\tilde{A}-2}}. \tag{59}$$

□

We want to prove a version of the above lemma which includes a $\tau(d)^k$ term. In order to develop this, we first state an elementary Lemma.

Lemma 6. *For any $n \ge 1$, there exists a divisor $d|n$ such that $d \le \sqrt{n}$ such that*

$$\tau(n) \le 2\tau(d)^2. \tag{60}$$

Proof. Assume $n > 1$. Let $d|n$ with $d < \sqrt{n}$ be such that $\tau(d)$ is maximal. Write $n = dd'$, and note that $d' > 1$. By maximality, any prime divisor $p|d'$ satisfies $pd > \sqrt{n}$ so that $d'/p \le \sqrt{n}$. Again, by maximality, $\tau(d'/p) \le \tau(d)$. Thus we have that $\tau(n) \le \tau(d)\tau(d'/p)\tau(p) \le 2\tau(d)^2$. □

Now we prove the following trivial bound.

Lemma 7. *Recall that $D = \frac{x^{3/4}}{\log^B x}$. For $\mathcal{C} = \mathcal{A}$ and $\mathcal{C} = \mathcal{B}$, we have*

$$\sum_{d<D} \tau(d)^k \mathcal{C}_d \ll x(\log x)^{2^{2k+3}} \tag{61}$$

Proof. We prove the result for $\mathcal{C} = \mathcal{A}$, the proof for $\mathcal{C} = \mathcal{B}$ being essentially the same. By Lemma 6,

$$\begin{aligned}\sum_{d<D} \tau(d)^k \mathcal{A}_d &\le \sum_n \tau(n)^{k+1} a(n) \\ &\ll \sum_{d\le\sqrt{x}} \tau(d)^{2k+2}\mathcal{A}_d,\end{aligned}$$

by Lemma 6. For $d \le \sqrt{x}$,

$$\begin{aligned}\mathcal{A}_d &\le \sum_{p^2 \in I} p \log p \sum_{\substack{a < \sqrt{x} \\ a^2 \equiv -p^4 \bmod d \\ (a,p)=1}} 1 \\ &\ll g(d)\sqrt{x} \sum_{p^2 \in I} p \log p \\ &\ll g(d) x.\end{aligned}$$

Using the bound $g(d) \le \frac{\tau(d)}{d}$, we have

$$\sum_{d \le \sqrt{x}} \tau(d)^{2k+2} \mathcal{A}_d \ll x \sum_{d \le \sqrt{x}} \frac{\tau(d)^{2k+3}}{d} \ll x (\log x)^{2^{2k+3}}.$$

□

Now, we are ready to prove our version of the result.

Lemma 8. *With notation as above,*

$$\sum_{d<D} \tau(d)^k R_d(\mathcal{C}) \ll \frac{x}{(\log x)^{\tilde{A}/2-1-2^{4k+2}}}, \tag{62}$$

for $\mathcal{C} = \mathcal{A}$ and $\mathcal{C} = \mathcal{B}$.

Proof. By Cauchy-Schwarz, we have

$$\begin{aligned}\sum_{d<D} \tau(d)^k R_d(\mathcal{C}) &\ll \left(\sum_{d<D} \tau(d)^{2k} R_d(\mathcal{C}) \right)^{1/2} \left(\sum_{d<D} R_d(\mathcal{C}) \right)^{1/2} \\ &\ll \left(\sum_{d<D} \tau(d)^{2k} (\mathcal{C}_d + M_d(\mathcal{C})) \right)^{1/2} \left(\sum_{d<D} R_d(\mathcal{C}) \right)^{1/2} \\ &\ll \left(x (\log x)^{2^{4k+3}} \right)^{1/2} \left(\frac{x}{(\log x)^{\tilde{A}-2}} \right)^{1/2},\end{aligned}$$

by Lemma 7, which concludes the proof. □

Since $\tilde{A}$ was arbitrary, this suffices for Proposition 2.

4. Application of the Fundamental Lemma

We now prove Proposition 3. Recall that we are interested in studying

$$\sum_{q \in Q} S(\mathcal{C}_q, x^\delta), \tag{63}$$

for $\mathcal{C} = \mathcal{A}$ or $\mathcal{C} = \mathcal{B}$, $\delta = \frac{(\log \log x)^2}{\log x}$, and Q a set of square-free numbers not exceeding Y. The level of distribution provided by Proposition 2 is sufficient to derive the correct asymptotic for this quantity, with a small error term. To be precise, we apply an upper and lower bound sieve of level of distribution $x^{\frac{1}{4}}$ so that the sifting variable $s = \frac{1}{4\delta}$. For $z \ge 1$, we use the usual notation

$$V(z) = \prod_{p \le z} (1 - g(p)). \tag{64}$$

By the Fundamental Lemma (see e.g. Corollary 6.10 in [4]) and Proposition 2, we have

$$\begin{aligned}\sum_{q\in Q} S(\mathcal{C}_q, x^\delta) &= V(x^\delta)\sum_{q\in Q} g(q)\int_I \sqrt{x-t^2}dt\left(1+O\left(\exp\left(-(4\delta)^{-1}\right)\right)\right)+O\left(\sum_{q\in Q}\sum_{d<x^{1/4}} R_{dq}(\mathcal{C})\right)\\ &= V(x^\delta)\sum_{q\in Q} g(q)\int_I \sqrt{x-t^2}dt\left(1+O\left(\frac{1}{\log^A x}\right)\right)+O\left(\sum_{d<x^{3/4-1/8}}\tau(d)R_d(\mathcal{C})\right)\\ &= V(x^\delta)\sum_{q\in Q} g(q)\int_I \sqrt{x-t^2}dt\left(1+O\left(\frac{1}{\log^A x}\right)\right)+O(x\log^{-A} x)\end{aligned}$$

for any $A>0$. Note that the last line is independent of whether $\mathcal{C}=\mathcal{A}$ or $\mathcal{C}=\mathcal{B}$. Thus

$$\begin{aligned}\sum_{q\in Q} S(\mathcal{A}_q, x^\delta)-\sum_{q\in Q} S(\mathcal{B}_q, x^\delta) &\ll \frac{1}{\log^A x}\int_I\sqrt{x-t^2}dt\sum_{q\in Q} g(q)+x\log^{-A} x\\ &\ll x\log^{-A+2} x,\end{aligned}$$

upon noting that $g(q)\ll \frac{\tau(q)}{q}$.

5. Reduction of Proposition 4 to a bilinear form bound

We first rewrite $U^{(1)}$ and $U^{(2)}$ into a more convenient form.

Lemma 9. *For $\mathcal{C}=\mathcal{A}$ and $\mathcal{C}=\mathcal{B}$, and $U^{(j)}$ as defined in Lemma 2,*

$$U^{(1)}(\mathcal{C}) = \sum_{\substack{x^\delta\le p_2<p_1<Y\\ Y\le p_1p_2\le x^{1/2-\delta}}} S(\mathcal{C}_{p_1p_2}, p_2)+\sum_{\substack{x^\delta\le p_2<p_1<Y\\ p_1p_2\ge x^{1/2+\delta}}} S(\mathcal{C}_{p_1p_2}, p_2)+O\left(\frac{\delta\eta x}{\log x}\right)$$

$$=: U_1^{(1)}(\mathcal{C})+U_2^{(1)}(\mathcal{C})+O\left(\frac{\delta\eta x}{\log x}\right), \tag{65}$$

and

$$U^{(2)}(\mathcal{C}) = \sum_{\substack{x^\delta\le p_3<\ldots<p_1<Y\\ p_1p_2<Y\le p_1p_2p_3\le x^{1/2-\delta}}} S(\mathcal{C}_{p_1p_2p_3}, p_3)+\sum_{\substack{x^\delta\le p_3<\ldots<p_1<Y\\ p_1p_2<Y\le p_1p_2p_3\\ p_1p_2p_3\ge x^{1/2+\delta}}} S(\mathcal{C}_{p_1p_2p_3}, p_3)+O\left(\frac{\delta\eta x}{\log x}\right)$$

$$=: U_1^{(2)}(\mathcal{C})+U_2^{(2)}(\mathcal{C})+O\left(\frac{\delta\eta x}{\log x}\right). \tag{66}$$

Proof. To prove (65), it suffices to show that

$$\sum_{\substack{x^\delta\le p_2<p_1<Y\\ x^{1/2-\delta}<p_1p_2<x^{1/2+\delta}}} S(\mathcal{C}_{p_1p_2}, p_2)\ll\frac{\delta\eta x}{\log x}. \tag{67}$$

In the sum above, $p_2>x^{1/2-\delta}/p_1>x^{1/2-\delta}/Y>x^{1/10}$, so that by Selberg's upper bound sieve, and Proposition 2, the left hand side of (67) is bounded by

$$\begin{aligned}\sum_{\substack{x^\delta\le p_2<p_1<Y\\ x^{1/2-\delta}<p_1p_2<x^{1/2+\delta}}} S(\mathcal{C}_{p_1p_2}, x^{1/10}) &\ll \frac{\eta x}{\log x}\sum_{\substack{x^{1/10}<p_2<p_1<Y\\ x^{1/2-\delta}<p_1p_2<x^{1/2+\delta}}}\frac{1}{p_1p_2}\\ &\ll\frac{\delta\eta x}{\log x}.\end{aligned} \tag{68}$$

Similarly, to prove (66), it suffices to show that

$$\sum_{\substack{x^\delta \le p_3 < p_2 < p_1 < Y \\ p_1 p_2 < Y \\ x^{1/2-\delta} < p_1p_2p_3 < x^{1/2+\delta}}} S(\mathcal{C}_{p_1p_2p_3}, p_3) \ll \frac{\delta \eta x}{\log x}. \tag{69}$$

In the sum above, $p_3 > x^{1/2-2\delta}/Y > x^{1/10}$, so by Selberg's upper bound sieve, and Proposition 2, the quantity on the left hand side of (69) is bounded by

$$\begin{aligned}\sum_{\substack{x^\delta \le p_3 < p_2 < p_1 < Y \\ p_1 p_2 < Y \\ x^{1/2-\delta} < p_1p_2p_3 < x^{1/2+\delta}}} S(\mathcal{C}_{p_1p_2p_3}, x^{1/10}) &\ll \frac{\eta x}{\log x} \sum_{\substack{x^{1/10} < p_3 < p_2 < p_1 < Y \\ x^{1/2-\delta} < p_1p_2p_3 < x^{1/2+\delta}}} \frac{1}{p_1p_2p_3} \\ &\ll \frac{\delta\eta x}{\log x}. \end{aligned} \tag{70}$$

□

For $n \ge 3$, in the sum in $U^{(n)}(\mathcal{C})$, we have

$$Y \le p_1 ... p_{n+1} < (p_1...p_n)^{\frac{n+1}{n}} \le Y^{4/3} < x^{1/2-\delta}. \tag{71}$$

Similarly, we have the same range $Y \le p_1...p_{n+1} < x^{1/2-\delta}$ for $S_3(\mathcal{C})$, $U_1^{(1)}(\mathcal{C})$, and $U_1^{(2)}(\mathcal{C})$. Indeed, for notational convenience, let $l(n)$ denote the least prime divisor of n. Then $S_3(\mathcal{C})$, $U_1^{(1)}(\mathcal{C})$, $U_1^{(2)}(\mathcal{C})$ and $U^{(n)}(\mathcal{C})$ for $n \ge 3$ are all of the form

$$\sum_{q \in Q} S(\mathcal{C}_q, l(q)), \tag{72}$$

where Q is a subset of

$$\tilde{Q} = \{Y \le q < x^{1/2-\delta} : q \text{ is squarefree}\}. \tag{73}$$

Moreover, the sum $S_3(\mathcal{C}) + U_1^{(1)}(\mathcal{C}) + U_1^{(2)}(\mathcal{C}) + \sum_{3 \le n \le n_0} U^{(n)}(\mathcal{C})$ is also of the form (72).

The exception to this are $U_2^{(1)}(\mathcal{C})$ and $U_2^{(2)}(\mathcal{C})$ which can still be written in the form (72) but where for $U_2^{(1)}$

$$Q = \{p_1p_2 \ge x^{1/2+\delta} : x^\delta \le p_2 < p_1 < Y\}, \tag{74}$$

and for $U_2^{(2)}(\mathcal{C})$

$$Q = \{p_1p_2p_3 \ge x^{1/2+\delta} : x^\delta \le p_3 < p_2 < p_1 < Y \text{ and } p_1p_2 < Y \le p_1p_2p_3\}. \tag{75}$$

We would like to ease the dependence of these sums on $l(q)$, for which we prove the following Lemma.

Lemma 10. *Let $J = [V, V^{(1+\kappa)})$. Then with Q any set of squarefree numbers,*

$$\sum_{\substack{q \in Q \\ l(q) \in J}} |S(\mathcal{C}_q, l(q)) - S(\mathcal{C}_q, V)| \ll \kappa^2 x + \frac{x}{\log^A x}, \tag{76}$$

for any $A > 0$.

Proof. We have that

$$\begin{aligned}\sum_{\substack{q\in Q\\ l(q)\in J}} |S(\mathcal{C}_q, l(q)) - S(\mathcal{C}_q, V)| &\le \sum_{\substack{p_1,p_2\in J\\ p_1\neq p_2}} \sum_{\substack{q\in Q\\ p_1p_2|q}} \mathcal{C}_q \\ &\le \sum_{p_1,p_2\in J} \sum_{n} c(p_1p_2n) \\ &\ll \sum_{p_1,p_2\in J} (M_{p_1p_2}(\mathcal{C}) + R_{p_1p_2}(\mathcal{C})) \\ &\le \sum_{p_1,p_2\in J} \frac{x}{p_1p_2} + O\left(\frac{x}{\log^A x}\right),\end{aligned}$$

for any $A > 0$ by Proposition 2. Noting that

$$\sum_{p_1,p_2\in J} \frac{x}{p_1p_2} \ll \kappa^2 x \tag{77}$$

completes the proof. □

Now, let

$$J(m) = [x^{(\kappa+1)^m\delta}, x^{(\kappa+1)^{m+1}\delta}), \tag{78}$$

and let $M \ll (\kappa\delta)^{-1}$ be such that $x^{\delta(\kappa+1)^M} > Y$. Recalling $\delta = \frac{(\log\log x)^2}{\log x}$, by Lemma 10 we have

$$\sum_{q\in Q} S(\mathcal{C}_q, l(q)) - \sum_{m\le M} \sum_{\substack{q\in Q\\ l(q)\in J(m)}} S(\mathcal{C}_q, x^{(\kappa+1)^m\delta}) \ll \kappa x \log x. \tag{79}$$

Picking $\kappa = (\log x)^{-A-1}$ makes this error bounded by $x(\log x)^{-A}$.

Thus, it suffices to show that for fixed m and Q of the form given in (73), (74) or (75) that

$$\sum_{\substack{q\in Q\\ l(q)\in J(m)}} \left|S(\mathcal{A}_q, x^{(\kappa+1)^m\delta}) - S(\mathcal{B}_q, x^{(\kappa+1)^m\delta})\right| \ll_A \frac{x}{\log^A x}, \tag{80}$$

for any $A > 0$.

Now, we may write

$$\sum_{\substack{q\in Q\\ l(q)\in J(m)}} S(\mathcal{C}_q, x^{(\kappa+1)^m\delta}) = \sum_{q\in Q}\sum_{t} \gamma_q\lambda_t c(qt), \tag{81}$$

where γ_q is the indicator function of $q \in Q$ with $l(q) \in J(m)$ while λ_t is the indicator function of numbers t without any prime factors below $x^{(\kappa+1)^m\delta}$.

Recall that $Y = x^{1/3+1/48}$ so that $x/Y^2 = x^{1/4+1/24}$. In the case where Q is of the form (73), $q \in Q$ satisfies

$$x^{1/4+\epsilon} < Y \le q < x^{1/2-\delta}. \tag{82}$$

When Q is of the form given in (74) and (75), λ_t is supported on

$$x^{1/4+\epsilon} < x/2Y^2 \le t \le x^{1/2-\delta}. \tag{83}$$

Hence, (80) and therefore Proposition 4 follows from the Proposition below.

Proposition 5. *Suppose $x^{1/4+\epsilon} \leq N \leq x^{1/2-\delta}$. Then, for any coefficients α_n and β_m satisfying $|\alpha_n| \leq 1$ and $|\beta_m| \leq 1$,*

$$\sum_{N<n\leq 2N} \sum_{\substack{m<x/N \\ (m,n)=1}} \beta_n \alpha_m \big(a(mn) - b(mn)\big) \ll_A \frac{x}{\log^A x}, \tag{84}$$

for any $A > 0$.

6. The bilinear form over Gaussian integers

Our purpose is to prove Proposition 5. The form $a^2 + p^4$ is a special value of the norm form of the Gaussian integers, and we now take advantage of that structure.

For $w, z \in \mathbb{Z}[i]$, let $N(w)$ denote the usual Gaussian norm and

$$S_1(z, w) = \sum_{\substack{p^2 \in I \\ \Re \bar{w} z = p^2}} 2p \log p, \tag{85}$$

and

$$S_2(z, w) = \sum_{\substack{p \in I \\ \Re \bar{w} z = p}} \log p. \tag{86}$$

Note that both sums are either empty or contain only one term. We would now like to convert the sum over m and n present in Proposition 5 to a sum over Gaussian integers. We shall call $\gamma \in \mathbb{Z}[i]$ primitive if γ is not divisible by any integer prime.

Lemma 11. *Let $\gamma \in \mathbb{Z}[i]$ be primitive, and m be a positive integer such that $m|N(\gamma)$. Then there exists exactly four choices for $\lambda \in \mathbb{Z}[i]$ such that $\lambda|\gamma$ and $N(\lambda) = m$.*

Proof. Write the prime factorization of m as

$$m = q_1 ... q_r, \tag{87}$$

for integer primes q_k and where repetition is allowed.

By primitivity of γ any prime divisors q of m cannot be inert in $\mathbb{Z}[i]$ and so satisfy $q = \pi\bar{\pi}$ for some prime π in the Gaussian integers. Suppose without loss of generality that for each $q_k = \pi_k \bar{\pi}_k$ that $\pi_k|\gamma$. Then

$$\lambda := \prod_{k=1}^{r} \pi_k \tag{88}$$

satisfies $\lambda|\gamma$ and $N(\lambda) = m$.

Suppose that $\lambda' \in \mathbb{Z}[i]$ also satisfy $\lambda'|\gamma$ and $N(\lambda') = m = N(\lambda)$. To check that there are exactly 4 choices for λ, we want to show that λ and λ' are associates or λ and $\bar{\lambda}'$ are associates. Since

$$\lambda\bar{\lambda} = \lambda'\bar{\lambda}', \tag{89}$$

we see that for any Gaussian integer prime $\pi|\lambda$, either $\pi|\lambda'$ or $\pi|\bar{\lambda}'$. Let us assume without loss of generality that $\pi_1|\lambda'$. It suffices to show that $\pi_k|\lambda'$ for all k. But

$$\pi_k \nmid \lambda' \Rightarrow \pi_k|\bar{\lambda}' \Rightarrow \bar{\pi}_k|\lambda'.$$

Thus if the above holds, we have $\pi_k\bar{\pi}_k|\gamma$, a contradiction to the primitivity of γ. $\square$

By Lemma 11,

$$a(mn) = \frac{1}{4} \sum_{N(w)=m} \sum_{N(z)=n} S_1(z,w), \tag{90}$$

and

$$b(mn) = \frac{1}{4} \sum_{N(w)=m} \sum_{N(z)=n} S_2(z,w). \tag{91}$$

We let $\beta_z = \beta_{N(z)}$ and $\alpha_w = \alpha_{N(w)}$. It now suffices to show that

$$\sum_z \sum_w \beta_z \alpha_w \left(S_1(z,w) - S_2(z,w)\right) \ll_A \frac{x}{\log^A x}, \tag{92}$$

for any $A > 0$, and for coefficients β_z and α_w satisfying $|\beta_z| \leq 1$ and $|\alpha_w| \leq 1$. Further, β_z is supported on primitive z satisfying $N \leq N(z) < 2N$ and α_w is supported on primitive w such that $N(w) \leq M := x/N$. For the rest of this section, fix $A > 0$.

Let $\theta(z) = \arg z \in [0, 2\pi)$ and

$$\mathcal{R} = \mathcal{R}(A) = \{z \in \mathbb{Z}[i] : N \leq N(z) < 2N, |\theta(z) - k\pi/2| \leq (\log x)^{-A} \text{ for } k \in \mathbb{Z}\}. \tag{93}$$

We first note that we may discard the part of the sum (92) with $z \in \mathcal{R}$. For this, write

$$\begin{aligned} z &= x + iy \\ w &= u + iv. \end{aligned}$$

Lemma 12. *Suppose that both z and*

$$q := \operatorname{Re} \bar{w}z = ux + vy \tag{94}$$

are fixed. Then the number of possible w is

$$\ll \frac{\sqrt{M}}{\sqrt{N}}. \tag{95}$$

Proof. We have either $x \gg \sqrt{N}$ or $y \gg \sqrt{N}$. We deal with the case $x \gg \sqrt{N}$, the other case being similar. Since z is primitive, $(x,y) = 1$ so we may write

$$v \equiv \bar{y}q \pmod{x}. \tag{96}$$

Thus, there are $\ll \sqrt{\frac{M}{N}}$ choices for v. Once v is fixed, u is uniquely determined by (94). □

Lemma 13.

$$\sum_{z \in \mathcal{R}} \sum_w \beta_z \alpha_w S_j(z,w) \ll x(\log x)^{-A} \tag{97}$$

for $j = 1, 2$.

Proof. We apply Lemma 12 to get

$$\sum_{z\in\mathcal{R}}\sum_{w}\beta_z\alpha_w S_1(z,w) \ll \sum_{z\in\mathcal{R}}\sum_{p^2\in I} p\log p \sum_{\substack{w\\ \mathrm{Re}\ \bar{w}z=p^2}} 1$$
$$\ll \sqrt{\frac{M}{N}}\sum_{p^2\in I} p\log p\sum_{z\in\mathcal{R}}1$$
$$\ll \sqrt{\frac{M}{N}} N(\log x)^{-A}\sum_{p^2\in I} p\log p$$
$$\ll x(\log x)^{-A}.$$

In $S_2(z,w)$, the sum is simpler and we get

$$\sum_{\substack{z\in\mathcal{R}\\ x\gg\sqrt{N}}}^{x}\sum_{w}\beta_z\alpha_w S_2(z,w) \ll \sqrt{\frac{M}{N}}\sum_{p\in I}\log p\sum_{z\in\mathcal{R}}1$$
$$\ll x(\log x)^{-A}.$$

□

We also restrict the sum over z to satisfy either

$$\theta(z)\in[0,\pi) \tag{98}$$

or

$$\theta(z)\in[\pi,2\pi). \tag{99}$$

The treatment of both regions is exactly the same. In the sequel, let $\sum^{\flat}$ denote a sum over primitive z supported on $N\le N(z)<2N$ and $z\notin\mathcal{R}$ and z satisfies either (98) or (99).

Then Cauchy-Scharwz gives that

$$\left|\sum_{w}\alpha_w\sum_{z}^{\flat}\beta_z(S_1(z,w)-S_2(z,w))\right|^2 \le \sum_{w}|\alpha_w|^2\sum_{w}\left|\sum_{z}^{\flat}\beta_z(S_1(z,w)-S_2(z,w))\right|^2, \tag{100}$$

where we now extend the sum over w over all Gaussian integers w satisfying $N(w)\le x/N$, possible by positivity.

By Lemma 13, it suffices to show that

$$\sum_{z_1,z_2}^{\flat}\beta_{z_1}\overline{\beta_{z_2}}\sum_{w}\left(S_1(z_1,w)-S_2(z_1,w)\right)\left(S_1(z_2,w)-S_2(z_2,w)\right) \ll \frac{xN}{\log^A x}, \tag{101}$$

Lemma 14. *The contribution of the diagonal term $z_1=z_2$ in* (101) *is*

$$\sum_{z}|\beta_z|^2\sum_{w}\left(S_1(z,w)^2-2S_1(z,w)S_2(z,w)+S_2(z,w)^2\right)\ll x^{1-\epsilon}N. \tag{102}$$

Proof. Since it is impossible for $\Re \bar{w}z$ to be both a prime and the square of a prime, $S_1(z,w)S_2(z,w) = 0$. Let us record the trivial bounds

$$\sum_z \sum_w S_1(z,w) \ll \sum_{n \le x} \left(\sum_{\substack{a^2+p^4=n \\ p^2 \in I}} 2p \log p \right) \tau^2(n) \ll x^{1+\epsilon} \tag{103}$$

and similarly

$$\sum_z \sum_w S_2(z,w) \ll x^{1+\epsilon}. \tag{104}$$

Now

$$\begin{aligned} \sum_z \sum_w S_1(z,w)^2 + S_2(z,w)^2 &\ll \sqrt{X} \log X \sum_z \sum_w S_1(z,w) + \log X \sum_z \sum_w S_1(z,w) \\ &\ll x^{5/4+\epsilon}, \end{aligned} \tag{105}$$

by (103) and (104). This suffices since $N > x^{1/4+\epsilon}$. □

Thus, in considering (101), we will assume that $z_1 \neq z_2$. For any pair z_1, z_2, let $\theta = \theta(z_1, z_2) = \arg z_2 - \arg z_1$ denote the angle between z_1 and z_2. Moreover, let $\Delta = \Delta(z_1, z_2) = \operatorname{Im} \bar{z}_1 z_2 = |z_1 z_2| \sin \theta(z_1, z_2)$. Note that z_1 and z_2 being primitive and $z_1 \neq z_2$ implies that $\theta \neq 0$. Further, the restriction of either (98) or (99) implies that $\theta \neq \pi$. Hence $\Delta \neq 0$.

If we write

$$\operatorname{Re} \bar{w} z_i = q_i \tag{106}$$

for $i = 1, 2$, then

$$w = -i\Delta(z_1, z_2)^{-1}(q_1 z_2 - q_2 z_1). \tag{107}$$

Of course, we must have

$$q_1 z_2 \equiv q_2 z_1 \pmod{\Delta}. \tag{108}$$

Let $C(q_1, q_2, z_1, z_2)$ be the statement that q_1, q_2, z_1 and z_2 satisfy (108). From (107) and since $N(w) \le x/N$, we have the additional condition

$$|q_1 z_2 - q_2 z_1| \le |\Delta(z_1, z_2)| \sqrt{\frac{x}{N}}. \tag{109}$$

We would much rather the condition in (109) does not exist. To ease this condition, we dissect our sum in (101) into smaller pieces.

To be precise, for some parameter L to be determined, let

$$\omega = (\log x)^{-L}, \tag{110}$$

and let $I = (X, X(1+\eta)]$ be a disjoint union of intervals J of length $\asymp X\omega$. We need $\ll 1/\omega$ such intervals to cover I.

Further, split the sum over z_1 and z_2 into regions of the form $\mathcal{U}$, where each $\mathcal{U}$ is contained in a square of side at most $\sqrt{N}\omega$. The number of regions needed is $1/\omega^2$. Now, write $\mathfrak{C}_1(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)$ as the condition that all $(z_1, z_2, q_1, q_2) \in \mathcal{U}_1 \times \mathcal{U}_2 \times J_1 \times J_2$ satisfy (109). Also, let $\mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)$ be the condition that there exists some $(z_1, z_2, q_1, q_2) \in \mathcal{U}_1 \times \mathcal{U}_2 \times J_1 \times J_2$ which satisfies (109), and there exists some $(z_1', z_2', q_1', q_2') \in \mathcal{U}_1 \times \mathcal{U}_2 \times J_1 \times J_2$ which does not satisfy (109).

For brevity, let

$$f(q) = \begin{cases} 2p\log p & \text{if } q = p^2 \\ 0 & \text{otherwise,} \end{cases} \tag{111}$$

and

$$g(q) = \begin{cases} \log p & \text{if } q = p \\ 0 & \text{otherwise.} \end{cases} \tag{112}$$

Set

$$h(q) = f(q) - g(q). \tag{113}$$

For any $J \subset I$, we have by the Prime Number Theorem that

$$\sum_{q \in J} h(q) = O\left(\frac{\sqrt{x}}{\log^C x}\right), \tag{114}$$

for any $C > 0$. This is a result of our choice of weights.

Remark 2. *To ease notation later, we restrict our attention to those z_1, z_2 such that $\Delta(z_1, z_2) > 0$, the case $\Delta(z_1, z_2) < 0$ being exactly the same. Henceforth, this condition shall be included in $\sum^\flat$.*

For $\mathcal{U}_1, \mathcal{U}_2, J_1, J_2$ satisfying $\mathfrak{C}_1(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)$, set

$$T(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) = \sideset{}{^\flat}\sum_{\substack{z_1 \in \mathcal{U}_1 \\ z_2 \in \mathcal{U}_2}} \left| \sum_{\substack{q_1 \in J_1 \\ q_2 \in J_2 \\ C(q_1, q_2, z_1, z_2)}} h(q_1) h(q_2) \right|, \tag{115}$$

and otherwise, set $T(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) = 0$.

Further, let

$$T'(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) = \sideset{}{^\flat}\sum_{\substack{z_1 \in \mathcal{U}_1 \\ z_2 \in \mathcal{U}_2}} \sum_{\substack{q_1 \in J_1 \\ q_2 \in J_2 \\ C(q_1, q_2, z_1, z_2)}} |h(q_1) h(q_2)|. \tag{116}$$

Then (101) reduces to proving that for any constant $C > 0$,

$$\sum_{\substack{\mathcal{U}_1, \mathcal{U}_2, J_1, J_2 \\ \mathfrak{C}_1(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)}} T(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) + \sum_{\substack{\mathcal{U}_1, \mathcal{U}_2, J_1, J_2 \\ \mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)}} |T'(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)| \ll_C \frac{xN}{\log^C x}. \tag{117}$$

Since L may be freely chosen, it suffices to prove the following Proposition.

Proposition 6. *With notation as above, for any constant $C > 0$,*

$$T(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) \ll_C \frac{xN}{\log^C x}. \tag{118}$$

Further,

$$\sum_{\substack{\mathcal{U}_1, \mathcal{U}_2, J_1, J_2 \\ \mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)}} T'(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) \ll \frac{xN}{\log^{L-2} x}. \tag{119}$$

7. Proof of Proposition 6

To prove the Proposition, we want to study sums of the form

$$S = S(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) = \sideset{}{^\flat}\sum_{\substack{z_1 \in \mathcal{U}_1 \\ z_2 \in \mathcal{U}_2}} \sum_{\substack{q_1 \in J_1 \\ q_2 \in J_2 \\ C(q_1, q_2, z_1, z_2)}} h_1(q_1) h_2(q_2). \tag{120}$$

We may assume that x is large enough for $x^\delta > 2(\log x)^9$ to hold as otherwise Proposition 6 is trivial.

We begin by recording the following useful counting Lemma.

Lemma 15. *Fix $D > 0$ and let $x_1, x_2 \geq 1$ with $d_x = (x_1, x_2) = (x_1, D) = (x_2, D)$. We call a pair (y_1, y_2) admissible if $z_j = x_j + iy_j$ satisfies all the conditions present in $\sum^\flat$, $\Delta(z_1, z_2) = D$, and such that $d_y := (y_1, y_2) = (y_1, D) = (y_2, D) \geq d_x$. Let $H(x_1, x_2)$ be the number of admissible pairs (y_1, y_2). Then*

$$H(x_1, x_2) \ll (\log x)^{2A}. \tag{121}$$

Proof. Let $D_x = D/d_x$, $u_i = x_i/d_x$ for $i = 1, 2$ and (y_1, y_2) be an admissible pair. Then $\Delta(z_1, z_2) = D$ gives

$$u_1 y_2 - u_2 y_1 = D_x. \tag{122}$$

Thus,

$$y_2 \equiv \overline{u_1} D_x \pmod{u_2}, \tag{123}$$

so that the number of choices for y_2 is

$$\ll \frac{\sqrt{N}}{d_y u_2} + 1 \ll \frac{\sqrt{N} d_x}{d_y \sqrt{N} (\log x)^{-A}} + 1 \leq \log^A x, \tag{124}$$

where we have used that $z_i \notin \mathcal{R}$ implies that $x_i \gg \sqrt{N}/(\log x)^A$. The same holds for y_2. ☐

Remark 3. *Lemma 15 holds with y_i in place of x_i. That is, for fixed y_1, y_2, we may prove the same bound for the number of admissible pairs (x_1, x_2).*

Now we note that we may essentially assume that $q_1 q_2$ is coprime with $\Delta(z_1, z_2)$ in the sum S in (120).

Lemma 16. *In the sum S in* (120)*, if either $h_i = g$ or $h_2 = g$, then we have $(q_1 q_2, \Delta) = 1$.*

Proof. Indeed, in those sums, either $q_1 = p \in I$ or $q_2 = p \in I$. On the other hand, $p \in I$ implies that $p \geq X > 2N \geq |\Delta(z_1, z_2)|$, so $p \nmid \Delta$. On the other hand, since $N(z_i)$ is squarefree, (108) implies that $(q_1, \Delta) = (q_2, \Delta)$. ☐

Lemma 17. *We have that*

$$\sideset{}{^\flat}\sum_{z_1, z_2} \sum_{\substack{p_1^2, p_2^2 \in I \\ C(p_1^2, p_2^2, z_1, z_2) \\ (p_1 p_2, \Delta) > 1}} 4 p_1 p_2 \log p_1 \log p_2 \ll x. \tag{125}$$

Proof. Suppose $(p_1, \Delta) > 1$ so $p_1 | \Delta$. But the condition $C(p_1^2, p_2^2, z_1, z_2)$ and the primitivity of z_1 implies that $p_1 | p_2$ so $p_1 = p_2$. Since $p_1^2 \geq X > 2N > |\Delta|$, we have from (108) that

$$z_2 \equiv z_1 \pmod{\Delta/p_1}. \tag{126}$$

Write

$$z_i = x_i + iy_i, \tag{127}$$

and let $d_x = (x_1, x_2)$ and $d_y = (y_1, y_2)$. Without loss of generality, assume that $d_x \le d_y$.

Then there are $\ll \sqrt{N}/d_x$ choices for x_1 and once x_1 is fixed, the congruence

$$x_1 \equiv x_2 \pmod{\Delta/p} \tag{128}$$

gives $p\sqrt{N}/\Delta$ choices for x_2. If we further fix $\Delta(z_1, z_2)$, we see by Lemma 15 that the number of choices for (z_1, z_2) is bounded by $\frac{pN}{\Delta d_x}(\log x)^{2A}$ choices.

Thus, the contribution of terms where $p_1|\Delta$ is bounded by

$$\begin{aligned}
\sum_{p\in I} p^2 \log^2 p \sum_{\substack{D\le 2N\\ p|D}} \sideset{}{^\flat}\sum_{\substack{z_1,z_2\\ \Delta(z_1,z_2)=D\\ z_1\equiv z_2 \bmod \Delta/p}} 1 &\ll (\log x)^{2A} \sum_{p\in I} p^2 \log^2 p \sum_{d_x\ge 1} \sum_{\substack{D\le 2N\\ d_x p|D}} \frac{pN}{Dd_x}\\
&\ll (\log x)^{2A} \sum_{p\in I} p^2 \log^2 p \sum_{d_x\ge 1} \frac{N}{d_x^2} \log N\\
&\ll (\log x)^{2A+2} N x^{1/2}\\
&\ll x, \qquad (129)
\end{aligned}$$

since $N \le x^{1/2-\delta}$. □

We begin by noting that we may essentially assume that $(q_1q_2, \Delta(z_1, z_2) = 1$ in the sum S in (120).

If $(q_i, \Delta) = 1$, (108) is equivalent to there existing $a \pmod{\Delta}$ with $(a, \Delta) = 1$ such that

$$\begin{aligned}
q_1 &\equiv aq_2 \pmod{\Delta}\\
az_2 &\equiv z_1 \pmod{\Delta}. \qquad (130)
\end{aligned}$$

By Lemmas 16 and 17, we may rewrite S from (120) as

$$S = \sum_{D\le N} \sideset{}{^*}\sum_{a \bmod D} Y(a, D)Z(a, D) + O(x) \tag{131}$$

where

$$Z(a, D) = \sideset{}{^\flat}\sum_{\substack{z_1,z_2\\ \Delta(z_1,z_2)=D\\ az_2\equiv z_1 (\bmod D)\\ z_1\in\mathcal{U}_1, z_2\in\mathcal{U}_2}} \beta_{z_1}\overline{\beta_{z_2}}, \tag{132}$$

and

$$Y(a, D) = \sum_{\substack{q_1\in J_1, q_2\in J_2\\ q_1\equiv aq_2 \bmod D\\ (q_1q_2,D)=1}} h_1(q_1)h_2(q_2). \tag{133}$$

In the above, we have $(q_1q_2, D) = 1$ whenever either of h_1 or h_2 is g by Lemma 16. If $h_1 = h_2 = f$, we may eliminate terms for which $(q_1q_2, D) > 1$ with an error of $O(x)$ by Lemma 17.

The rewriting of S in (131) separates the sum $Z(a, D)$ containing arbitrary coefficients β_{z_j} from the congruence sum $Y(a, D)$. This key procedure has transformed the sum into the right form for us to extract the main terms from S using Corollary 2. Of course, we also need some understanding of the size of $Z(a, D)$ for which the following second moment bounds suffices.

Lemma 18. *Let*

$$\tilde{Z}(b, D) = \sum^{\flat}_{\substack{z_1, z_2 \\ \Delta(z_1, z_2) = D \\ az_2 \equiv z_1 (\bmod D)}} 1. \tag{134}$$

We have

$$\sum^{*}_{b \bmod D} |\tilde{Z}(b, D)|^2 \ll (\log x)^{4A+3} \frac{N^2}{D}. \tag{135}$$

Proof. For a given pair (z_1, z_2) which appear in the sum for $\tilde{Z}(b, D)$, we once again write $z_j = x_j + iy_j$ for $j = 1, 2$, $d_x = (x_1, x_2)$ and $d_y = (y_1, y_2)$. Let $\tilde{Z}_x(b, D)$ denote the same sum as $\tilde{Z}(b, D)$ with the additional condition that $d_x \leq d_y$, and let $\tilde{Z}_y(b, D)$ denote the rest. Clearly $|\tilde{Z}(b, D)|^2 \leq 2(|\tilde{Z}_x(b, D)|^2 + |\tilde{Z}_y(b, D)|^2)$. By symmetry, it suffices to prove the bound (135) with $\tilde{Z}_x(b, D)$ in place of $\tilde{Z}(b, D)$.

Note that the congruence

$$az_2 \equiv z_1 \bmod D \tag{136}$$

along with the condition that $\Delta(z_1, z_2) = D$ implies that $d_x = (x_j, D)$ and $d_y = (y_j, D)$ for $j = 1, 2$. Then for $H(x_1, x_2)$ as defined in Lemma 15,

$$\begin{aligned}
\sum^{*}_{b \bmod D} |\tilde{Z}_x(b, D)|^2 &\leq \sum^{*}_{b \bmod D} \left| \sum_{x_1 \equiv bx_2 \bmod D} H(x_1, x_2) \right|^2 \\
&\ll (\log x)^{4A} \sum^{*}_{b \bmod D} \sum_{\substack{x_1, x_2, x_1', x_2' \\ x_1 \equiv bx_2 \bmod D \\ x_1' \equiv bx_2' \bmod D}} 1 \\
&= (\log x)^{4A} \sum_{\substack{x_1, x_2, x_1', x_2' \\ x_1 x_2' \equiv x_1' x_2 \bmod D}} d_x.
\end{aligned}$$

In the above, $d_x = (x_1, x_2) = (x_1', x_2')$ is simply the number of $b \bmod D$ such that $x_1 \equiv bx_2 \bmod D$. Given $x_1 x_2'$, the number of choices for the product $x_2 x_1'$ subject to the condition $x_1 x_2' \equiv x_2 x_1' \bmod D$ is bounded by $\frac{N}{D}$. From this, we see that

$$\begin{aligned}
\sum_{\substack{x_1, x_2, x_1', x_2' \\ x_1 x_2' \equiv x_2 x_1' \bmod D}} d_x &\leq \sum_{d_x < \sqrt{2N}} d_x \sum_{\substack{x_1 \leq \sqrt{2N} \\ x_2' \leq \sqrt{2N} \\ d_x | (x_1, x_2')}} \frac{N}{D} \tau(x_1 x_2') \\
&\ll \frac{N^2}{D} (\log N)^3.
\end{aligned}$$

Thus,

$$\sum^{*}_{b \bmod D} |\tilde{Z}_x(b, D)|^2 \ll (\log x)^{4A+3} \frac{N^2}{D}.$$

□

Remark 4. *Note that trivially $|Z(b, D)| \leq \tilde{Z}(b, D)$ so that Lemma 18 applies with $\tilde{Z}(b, D)$ replaced by $Z(b, D)$.*

We also record the following convenient lemma.

Lemma 19.

$$\sum_{\mathfrak{D}\le D<2\mathfrak{D}} \sideset{}{^\flat}\sum_{\substack{z_1,z_2\\ \Delta(z_1,z_2)=D}} 1 = \sideset{}{^\flat}\sum_{\substack{z_1,z_2\\ \mathfrak{D}\le\Delta(z_1,z_2)<2\mathfrak{D}}} 1 \ll \mathfrak{D}N\log\log x. \tag{137}$$

Proof. Again, write

$$z_k = x_k + iy_k \tag{138}$$

for $k\in\{1,2\}$. We may assume without loss of generality that $x_1 \ge 0$. Since $z_1 \notin \mathcal{R}$, we must have $x_1 \gg \frac{\sqrt{N}}{\log^A x}$.

For fixed x_1, x_2, the number of y_1, y_2 with $\Delta(z_1,z_2) = D$ is $\ll \frac{\sqrt{N}}{x_1}(x_1,x_2)$. Thus,

$$\sqrt{N}\sum_{d<2\mathfrak{D}}\sum_{\substack{\mathfrak{D}\le D<2\mathfrak{D}\\ d|D}}\sum_{\substack{\frac{\sqrt{N}}{\log^A x}\ll x_1\ll\sqrt{N}\\ x_2\\ d=(x_1,x_2)}}\frac{d}{x_1} \ll N\mathfrak{D}\log\log x.$$

□

Now let

$$Y(J_1) := \sum_{q\in J_1} h_1(q),$$

$$Y(J_2) := \sum_{q\in J_2} h_2(q), \tag{139}$$

and

$$Y_{h_1,h_2}(D) = Y(D) = \frac{1}{\phi(D)}Y(J_1)Y(J_2). \tag{140}$$

If h_1 or h_2 is g, $Y(d)$ is the expected value of $Y(a,D)$.

If $h_1 = h_2 = f$, note that $p_1^2 \equiv ap_2^2 \bmod D$ implies that $a\equiv b^2 \bmod D$ for some b, and so $p_1 \equiv \sigma b p_2 \bmod D$ for $\sigma^2 = 1 \bmod D$. Here, $Y(a,D) = 0$ if a is a nonresidue mod D so

$$\sideset{}{^*}\sum_{a \bmod D} Y(a,D)Z(a,D) = \frac{1}{R(D)}\sideset{}{^r}\sum_{\sigma}\sum_{b \bmod D} Y_f(\sigma b, D)Z(b^2,D), \tag{141}$$

where

$$Y_f(\sigma b, D) = \sum_{\substack{p_1^2\in J_1\\ p_2^2\in J_2\\ p_1\equiv\sigma b p_2 \bmod D}} f(p_1^2)f(p_2^2) \tag{142}$$

When $h_1 = h_2 = f$, $Y(D)$ is the expected value of $Y_f(\sigma b, D)$ while $R(D)Y(D)$ is the expected value of $Y(a,D)$ when a is a quadratic residue modulo D.

The following proposition makes the above discussion precise.

Proposition 7. *For $h_1 = g$ or $h_2 = g$, let*

$$\mathcal{E}(N) = \sum_{D\le N}\sideset{}{^*}\sum_{a \bmod D}\left(Y(a,D) - Y(D)\right)Z(a,D). \tag{143}$$

Then for any constant $C > 0$,

$$\mathcal{E}(N) \ll_C \frac{xN}{\log^C x}. \tag{144}$$

For $h_1 = h_2 = f$, let

$$\mathcal{E}_f(N) = \sum_{D \le N} \frac{1}{R(D)} \sum_{\sigma}{}^{r} \sum_{b \bmod D}{}^{*} |Y_f(\sigma b, D) - Y(D)||Z(b^2, D)|. \tag{145}$$

Then for any constant $C > 0$,

$$\mathcal{E}_f(N) \ll_C \frac{xN}{\log^C x}. \tag{146}$$

Proof. We first prove the bound (144) for $\mathcal{E}$. We prove the result for $h_1 = g$ and $h_2 = f$. The case $h_1 = h_2 = g$ is easier and the case $h_1 = f$ and $h_2 = g$ is the same. We write

$$\begin{aligned}
\mathcal{E} &= \sum_{D \le N} \sum_{a \bmod D}{}^{*} \sum_{p \in J_1} f(p) \left(Y(a, D) - Y(D) \right) Z(a, D) \\
&= \sum_{D \le N} \sum_{p \in J_1} f(p) \sum_{a \bmod D}{}^{*} \left(\sum_{\substack{q \in J_2 \\ q \equiv a \bmod D}} g(q) - \frac{Y(J_2)}{\phi(D)} \right) Z(a\bar{p}^2, D).
\end{aligned}$$

By Cauchy-Schwarz and Lemma 18, we have that

$$\begin{aligned}
\mathcal{E} &\ll \left(\sum_{D \le N} \sum_{p \in J_1} f(p) \sum_{a \bmod D}{}^{*} \left(\sum_{\substack{q \in J_2 \\ q \equiv a \bmod D}} g(q) - \frac{Y(J_2)}{\phi(D)} \right)^2 \right)^{1/2} \left(Y(J_1) \sum_{D \le N} (\log x)^{4A+2} \frac{N^2}{D} \right)^{1/2} \\
&\ll Y(J_1) N (\log x)^{2A+3} \left(\sum_{D \le N} \sum_{a \bmod D}{}^{*} \left(\sum_{\substack{q \in J_2 \\ q \equiv a \bmod D}} g(q) - \frac{Y(J_2)}{\phi(D)} \right)^2 \right)^{1/2}.
\end{aligned}$$

Now it suffices to show that

$$\sum_{D \le N} \sum_{a \bmod D}{}^{*} \left(\sum_{\substack{q \in J_2 \\ q \equiv a \bmod D}} g(q) - \frac{Y(J_2)}{\phi(D)} \right)^2 \ll_C \frac{x}{\log^C x}, \tag{147}$$

for any $C > 0$. This follows by the Barban-Davenport-Heilbronn theorem (see, e.g. Theorem 9.14 in [4]), and noting that $\sqrt{x} \ge X \ge \sqrt{x}/\log^4 x$ while $N \le x^{1/2-\delta}$.

It is necessary to use Corollary 2 in the bound for $\mathcal{E}_f$. Here, similar to before, it suffices to show

$$\sum_{D \le N} \frac{1}{R(D)} \sum_{\sigma}{}^{r} \sum_{b \bmod D}{}^{*} |Y_f(\sigma b, D) - Y(D)|^2 \ll \frac{x^2}{\log^C x} \tag{148}$$

for any constant C. But the left hand side above is simply

$$\sum_{D \le N} \sum_{b \bmod D}{}^{*} |Y_f(b, D) - Y(D)|^2 \tag{149}$$

and since the primes satisfy the Siegel Walfisz condition, we may apply Corollary 2 to complete the proof. $\square$

By Proposition 7,

$$S = \sum_{D \le N} \sum_{a \bmod D}^{*} Y(D) Z(a, D) + O_C\left(\frac{xN}{\log^C x}\right), \tag{150}$$

for any $C > 0$. On the other hand, by the Prime Number Theorem

$$Y(J_i) = |J_i| + O\left(\frac{\sqrt{x}}{\log^C x}\right) \tag{151}$$

so that

$$Y_{f,f}(D) - Y_{f,g}(D) - Y_{g,f}(D) + Y_{g,g}(D) \ll \frac{1}{\phi(D)} \frac{x}{\log^C x} \tag{152}$$

for any constant $C > 0$. Thus for any $C > 0$,

$$\begin{aligned}
T(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) &\ll \frac{x}{\log^C x} \sum_{D \le N} \frac{1}{\phi(D)} \sum_{a \bmod D}^{*} |Z(a, D)| + \frac{xN}{\log^C x} \\
&\ll \frac{x}{\log^C x} \sum_{D \le N} \frac{1}{\phi(D)} \sum_{\substack{z_1, z_2 \\ \Delta(z_1, z_2) = D}}^{\flat} 1 + \frac{xN}{\log^C x} \\
&\ll \frac{x}{\log^C x} \sum_{\mathfrak{D}}^{d} \frac{\log \log \mathfrak{D}}{\mathfrak{D}} \sum_{\mathfrak{D} \le D < 2\mathfrak{D}} \sum_{\substack{z_1, z_2 \\ \Delta(z_1, z_2) = D}}^{\flat} 1 + \frac{xN}{\log^C x} \\
&\ll \frac{xN}{\log^{C-2} x}.
\end{aligned}$$

for any $C > 0$ by Lemma 19, and where $\sum_{\mathfrak{D}}^{d}$ denotes a dyadic sum over $\mathfrak{D}$ powers of 2 satisfying $\mathfrak{D} \le 2N$. This suffices for the proof of the first assertion of Proposition 6.

For the second assertion, note that it suffices to show that

$$\sum_{\substack{\mathcal{U}_1, \mathcal{U}_2, J_1, J_2 \\ \mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)}} S(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2) \ll \frac{xN}{\log^{L-2} x}, \tag{153}$$

for S as defined in (120) where $\beta_{z_1} = \beta_{z_2} = 1$. Again by (150), it suffices to show that

$$\mathcal{E} := \sum_{\substack{\mathcal{U}_1, \mathcal{U}_2, J_1, J_2 \\ \mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)}} |J_1||J_2| \sum_{D \le N} \frac{1}{\phi(D)} \sum_{a \bmod D}^{*} Y(D) Z(a, D) \ll \frac{xN}{\log^{L-2} x}. \tag{154}$$

We have

$$\mathcal{E} \ll \omega^2 X \sum_{\mathcal{U}_1, \mathcal{U}_2} \sum_{D \le N} \sum_{\substack{J_1, J_2 \\ \mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)}} \frac{1}{\phi(D)} \sum_{\substack{z_1, z_2 \\ \Delta(z_1, z_2) = D \\ z_1 \in \mathcal{U}_1, z_2 \in \mathcal{U}_2}}^{\flat} 1. \tag{155}$$

Lemma 20. *For fixed $\mathcal{U}_1, \mathcal{U}_2$ and D, the number of choices for J_1, J_2 subject to $\mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)$ is $\ll 1/\omega$.*

Proof. Let $X_i = \inf J_i$, and fix $Z_i \in \mathcal{U}_i$. Then $\mathfrak{C}_2(\mathcal{U}_1, \mathcal{U}_2, J_1, J_2)$ implies that there exists $q_i \in J_i$ and $z_i \in \mathcal{U}_i$ such that

$$D\sqrt{\frac{x}{N}} \geq |q_1 z_2 - q_2 z_1| = |X_1 Z_2 - X_2 Z_1| + O(\omega X\sqrt{N}), \tag{156}$$

and that there exists $q_i' \in J_i$ and $z_i' \in \mathcal{U}_i$ such that

$$D\sqrt{\frac{x}{N}} < |q_1' z_2' - q_2' z_1'| = |X_1 Z_2 - X_2 Z_1| + O(\omega X\sqrt{N}). \tag{157}$$

Recall that there are $\asymp \frac{1}{\omega}$ choices for J_1. Now, suppose that J_1 is fixed so that X_1 is fixed. Then the above implies that

$$|X_1 Z_2 - X_2 Z_1| = D\sqrt{\frac{x}{N}} + O(\omega X\sqrt{N}), \tag{158}$$

so that

$$X_2 = X_1 \frac{Z_2}{Z_1} + \frac{D}{Z_1}\sqrt{\frac{x}{N}} + O(\omega X), \tag{159}$$

so that X_2 is fixed in an interval of length $\ll \omega X$. But each J_2 is an interval of length $\asymp \omega X$ so there can only be $O(1)$ choices for J_2. □

By Lemma 20 and (155),

$$\begin{aligned}
\mathcal{E} &\ll \omega X \sum_{\mathcal{U}_1, \mathcal{U}_2} \sum_{D \leq N} \frac{1}{\phi(D)} \sideset{}{^\flat}\sum_{\substack{z_1, z_2 \\ \Delta(z_1,z_2)=D \\ z_1 \in U_1, z_2 \in \mathcal{U}_2}} 1 \\
&\ll \omega X \sum_{D \leq N} \frac{1}{\phi(D)} \sideset{}{^\flat}\sum_{\substack{z_1, z_2 \\ \Delta(z_1,z_2)=D}} 1 \\
&\ll \omega X \sideset{}{^d}\sum_{\mathfrak{D}} \frac{\log\log \mathfrak{D}}{\mathfrak{D}} \sum_{\mathfrak{D} \leq D < 2\mathfrak{D}} \sideset{}{^\flat}\sum_{\substack{z_1, z_2 \\ \Delta(z_1,z_2)=D}} 1 \\
&\ll \omega X N \log^2 x,
\end{aligned} \tag{160}$$

by Lemma 19, and where $\sideset{}{^d}\sum_{\mathfrak{D}}$ denotes a dyadic sum over $\mathfrak{D}$ powers of 2 satisfying $\mathfrak{D} \leq 2N$. This suffices for the second assertion of Proposition 6 and hence for the proof of our main theorem.

8. Distribution of sequences in arithmetic progressions

The purpose of this section is to prove Corollary 2 and the more general Theorem 2 below. Theorem 2 is motivated by the possibility that an interesting arithmetic function can be biased for certain small moduli - that is, the sequences does not satisfy the Siegel-Walfisz condition. In this case, we can still prove a result about the distribution of such a sequence in arithmetic progressions by adjusting the main term.

First, let make precise what we mean by the Siegel-Walfisz condition.

Remark 5. *We say that an arithmetic function $c(n)$ satisfies a Siegel-Walfisz condition if for any constant κ, we have that for any $q < (\log x)^\kappa$, $(a,q) = 1$, and $d, e \geq 1$,*

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q \\ (e,n)=1}} c(dn) = \frac{1}{\phi(q)} \sum_{\substack{n \leq x \\ (n,e)=1}} c(dn) \left(1 + O_\kappa\left((\log x)^{-\kappa}\right)\right). \tag{161}$$

We now fix some notation for the rest of the section: for any arithmetic function $a(n)$ with finite support, we let

$$\|a_\tau\|^2 = \sum_n |a(n)|^2 \tau(n)^2. \tag{162}$$

Roughly speaking $\|a_\tau\|^2$ is an upper bound for $\|a * a\|^{1/2}$. The main result of this section is below.

Theorem 2. *Let $\gamma(n)$ and $\delta(n)$ be arithmetic functions supported on $n \leq N_1$ and $n \leq N_2$ respectively and let $Q_0 \geq 1$. For a character χ, let χ_P be the unique primitive character which induces χ, and let $Q(\chi)$ be the conductor of χ_P. For $(a,q) = 1$, let*

$$\mathcal{E}(a,q) = \sum_{d|q} \mathcal{E}(a,q,d), \tag{163}$$

where

$$\mathcal{E}(a,q,d) = \sum_{\substack{n_1,n_2 \\ n_1 \equiv a n_2 \bmod q/d \\ (n_1 n_2, q/d)=1}} \gamma(dn_1)\delta(dn_2) - \frac{1}{\phi(q/d)} \sum_{n_1,n_2} \gamma(dn_1)\delta(dn_2) \sum_{\substack{\chi \bmod q/d \\ Q(\chi) \leq Q_0}} \chi(n_1)\overline{\chi(an_2)}. \tag{164}$$

Further, let

$$\mathcal{E} = \sum_{q \leq \tilde{Q}} \sideset{}{^*}\sum_{a \bmod q} |\mathcal{E}(a,q)|^2. \tag{165}$$

Then,

$$\mathcal{E} \ll \left(\tilde{Q} + \frac{N_1 N_2}{\sqrt{Q_0}} + \sqrt{\tilde{Q} N_1 N_2}\right) (\log \tilde{Q})^3 \|\gamma_\tau\|^2 \|\delta_\tau\|^2. \tag{166}$$

8.1. **Proof of Corollary 2.** We first prove a convenient Lemma which will be used here and also in the proof of Theorem 2.

Lemma 21. *Let $\gamma(n)$ and $\delta(n)$ be arithmetic functions with finite support, and for any $d \geq 1$, let*

$$b_d(n) = \sum_{n = n_1 n_2} \gamma(dn_1)\delta(dn_2). \tag{167}$$

Then

$$\sum_d \tau(d) \sum_n |b_d(n)|^2 \leq \|\gamma_\tau\|^2 \|\delta_\tau\|^2, \tag{168}$$

with $\|\gamma_\tau\| \|\delta_\tau\|$ as defined in Theorem 2.

Proof. Let

$$\begin{aligned}
f(n) &:= \sum_{n=n_1n_2=u_1u_2} |\gamma(n_1)\delta(n_2)\gamma(u_1)\delta(u_2)| \sum_{d|(n_1,n_2,u_1,u_2)} \tau(d) \\
&\le \frac{1}{2} \sum_{n=n_1n_2=u_1u_2} \left(|\gamma(n_1)\delta(n_2)|^2 + |\gamma(u_1)\delta(u_2)|^2\right) \tau((n_1,n_2,u_1,u_2))^2 \\
&\le \frac{1}{2} \sum_{n=n_1n_2} \sum_{n=u_1u_2} \left(|\gamma(n_1)\delta(n_2)|^2\tau(n_1)\tau(n_2) + |\gamma(u_1)\delta(u_2)|^2\tau(u_1)\tau(u_2)\right) \\
&= \sum_{n=n_1n_2} |\gamma(n_1)\delta(n_2)|^2\tau(n_1)\tau(n_2)\tau(n). \qquad (169)
\end{aligned}$$

Then

$$\sum_d \tau(d) \sum_n |b_d(n)|^2 = \sum_n f(n) \le \|\gamma_\tau\|^2\|\delta_\tau\|^2, \qquad (170)$$

as desired. □

We now deduce Corollary 2 from Theorem 2. We set $Q_0 = (\log x)^{2A+6}$, and assume by (161) that for any $q \le Q_0$

$$\sum_{\substack{n\le x \\ n\equiv a \bmod q \\ (e,n)=1}} c(dn) = \frac{1}{\phi(q)} \sum_{\substack{n\le x \\ (n,e)=1}} c(dn) \left(1 + O_\kappa\left((\log x)^{-\kappa}\right)\right), \qquad (171)$$

for κ to be determined. For $(a,q)=1$, the condition $n_1 \equiv an_2 \pmod q$ implies that $(n_1,q)=(n_2,q)$. Writing $d=(n_1,q)=(n_2,q)$, we have

$$S(x;a,q) = \sum_{d|q} \frac{1}{\phi(q/d)} \sum_{\chi \bmod \frac{q}{d}} \sum_{n_1,n_2} \chi(n_1)\overline{\chi(an_2)}. \qquad (172)$$

Then

$$\begin{aligned}
\sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} |S(x;a,q)-S(x;q)|^2 &= \sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} \left| \sum_{d|q} \frac{1}{\phi(q/d)} \sum_{\substack{\chi \bmod \frac{q}{d} \\ \chi \text{ nonprincipal}}} \sum_{n_1,n_2} \chi(n_1)\overline{\chi(an_2)} \right|^2 \\
&= \sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} |\mathcal{E}(a,q) + E(a,q,Q_0)|^2 \\
&\ll \sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} \left(|\mathcal{E}(a,q)|^2 + |E(a,q,Q_0)|^2\right)
\end{aligned}$$

where

$$E(a,q,Q_0) = \sum_{d|q} \frac{1}{\phi(q/d)} \sum_{n_1,n_2} c(dn_1)c(dn_2) \sum_{\substack{\chi \bmod q/d \\ 1<Q(\chi)\le Q_0}} \chi(n_1)\overline{\chi(an_2)} \qquad (173)$$

and $\mathcal{E}(a,q)$ is as defined in Theorem 2 with $\gamma=\delta=c$. Letting $B(A)=2A+6$ and apply Theorem 2 to see that

$$\sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} |S(x;a,q)-S(x;q)|^2 \ll \frac{x^2}{\log^A x}\|c_\tau\|^4 + \sum_{q\le Q} \sideset{}{^*}\sum_{a \bmod q} |E(a,q,Q_0)|^2, \qquad (174)$$

so it suffices to bound the last term. By Cauchy-Schwarz,

$$|\mathcal{E}(a,q,Q_0)|^2 \le \tau(q) Q_0^2 \sum_{q=dM} \frac{1}{\phi(M)^2} \sum_{\substack{\chi \bmod M\\ 1<Q(\chi)\le Q_0}} |C(\chi,d)|^4, \tag{175}$$

where for χ induced by ψ mod M_1, $M = M_1 M_2$,

$$\begin{aligned} C(\chi,d) &= \sum_n c(dn)\chi(n) \\ &= \sum_{b \bmod M_1} \psi(b) \sum_{\substack{n\equiv b \bmod M_1\\ (n,M_2)=1}} c(dn) \\ &= \frac{1}{\phi(M_1)} \sum_{b \bmod M_1} \psi(b) \sum_{(n,M_2)=1} c(dn)(1+O_\kappa((\log x)^{-\kappa}) \\ &\ll (\log x)^{-\kappa} \sum_n |c(dn)|. \end{aligned} \tag{176}$$

Thus

$$\sum_{a \bmod q}{}^{*} |E(a,q,Q_0)|^2 \ll Q_0^4 (\log x)^{-4\kappa} \sum_{q=dM} d\tau(d) \frac{\tau(M)}{\phi(M)} \left(\sum_n |c(dn)|\right)^2, \tag{177}$$

so

$$\begin{aligned} \sum_{q\le Q} \sum_{a \bmod q}{}^{*} |E(a,q,Q_0)|^2 &\ll Q_0^4 (\log x)^{-4\kappa} \sum_{d\le Q} d\tau(d) \left(\sum_n |c(dn)|\right)^4 \sum_{M\le Q/d} \frac{\tau(M)}{\phi(M)} \\ &\ll Q_0^4 (\log x)^{-4\kappa+1} \sum_{d \le Q} d\tau(d) \left(\sum_n b_d(n)\right)^2 \end{aligned} \tag{178}$$

where

$$b_d(n) = \sum_{n=n_1n_2} |c(dn_1)c(dn_2)|. \tag{179}$$

Now by Cauchy-Schwarz and Lemma 21,

$$\begin{aligned} \sum_d d\tau(d) \left(\sum_n b_d(n)\right)^2 &\le x^2 \sum_d \frac{\tau(d)}{d} \sum_n |b_d(n)|^2 \\ &\le x^2 \|c_\tau\|^4. \end{aligned} \tag{180}$$

Putting this into (178) we see that the Corollary follows upon choosing $4\kappa = 1 + 4(2A + 6) + A$.

8.2. **Proof of Theorem 2.**

For clarity, we first isolate the simple Lemma below.

Lemma 22. *Let $a(n)$ be an arithmetic function supported on $n \le N$, and $q \ge 1$. Then*

$$\sum_{\substack{m,n\\ m\equiv n \bmod q}} |a(n)a(m)| \le \left(\frac{N}{q}+1\right) \|a\|^2. \tag{181}$$

Proof. The Lemma follows directly from two applications of Cauchy-Schwarz. To be precise

$$\sum_{\substack{m,n \\ m \equiv n \bmod q}} |a(n)a(m)| \leq \sqrt{\frac{N}{q}+1} \sum_m |a(m)| \left(\sum_{n \equiv m \bmod q} |a(n)|^2 \right)^{1/2}$$
$$\leq \|a\|^{1/2} \sqrt{\frac{N}{q}+1} \left(\sum_m \sum_{n \equiv m \bmod q} |a(n)|^2 \right)^{1/2}$$
$$\leq \left(\frac{N}{q} + 1 \right) \|a\|^2.$$

□

We now prove a consequence of the large sieve which lies at the heart of these types of results.

Proposition 8. *Let $a(n)$ be any arithmetic function supported on $n \leq N$, and for any character χ, let*

(182) $$A(\chi) = \sum_n a(n)\chi(n).$$

Further, let $Q(\chi)$ denote the conductor of the unique primitive character that induces χ. Then

(183)
$$S := \sum_{M \leq \tilde{M}} \frac{\tau(M)}{\phi(M)} \sum_{\substack{\chi \bmod M \\ Q(\chi) > M_0}} |A(\chi)|^2 \ll \left(\tilde{M} + \frac{N \log \tilde{M}}{\sqrt{M_0}} + \sqrt{\tilde{M} N \log \tilde{M}} \right) (\log \tilde{M})^2 \|a\|^2.$$

Proof. We have that

(184) $$S \leq \sqrt{S_1 S_2},$$

where

(185) $$S_1 = \sum_{M \leq \tilde{M}} \frac{1}{\phi(M)} \sum_{\substack{\chi \bmod M \\ Q(\chi) > M_0}} |A(\chi)|^2,$$

and

(186) $$S_2 = \sum_{M \leq \tilde{M}} \frac{\tau(M)^2}{\phi(M)} \sum_{\chi \bmod M} |A(\chi)|^2.$$

Let us first bound S_2. We have

(187) $$S_2 \leq \sum_{M \leq \tilde{M}} \tau(M)^2 \sum_{\substack{m,n \\ m \equiv n \bmod M}} |a(n)a(m)|$$

(188) $$\leq \|a\|^2 \sum_{M \leq \tilde{M}} \tau(M)^2 \left(\frac{N}{M} + 1 \right),$$

by Lemma 22. Thus

(189) $$S_2 \ll (N \log \tilde{M} + \tilde{M}) \|a\|^2 (\log \tilde{M})^4.$$

Now, we bound S_1. For each non-principal character χ mod M, let ψ mod M_1 be the unique primitive character which induces χ, where we may write $M = M_1M_2$ for $M_1 > 1$. Then for any n, $\chi(n) = \psi(n)$ if $(n, M_2) = 1$. Let us write

$$A_{M_2}(\psi) = \sum_{\substack{n \\ (n,q_2)=1}} a(n)\psi(n). \tag{190}$$

We have

$$S_1 \leq \sum_{\substack{M_1M_2 \leq \tilde{M} \\ M_1 \geq M_0}} \frac{1}{\phi(M_2)} \frac{1}{\phi(M_1)} \sideset{}{^*}\sum_{\psi \bmod M_1} |A(M_2)|^2, \tag{191}$$

where $\sideset{}{^*}\sum_{\psi \bmod M_1}$ denotes a sum over all primitive characters modulo M_1. Applying the multiplicative large sieve, we see that

$$\begin{aligned} S_1 &\leq \sum_{M_2 \leq \tilde{M}} \frac{1}{\phi(M_2)} \left(\frac{\tilde{M}}{M_2} + \frac{N}{M_0} \right) \|a\|^2 \\ &\leq \left(\tilde{M} + \frac{N \log \tilde{M}}{M_0} \right) \|a\|^2. \end{aligned} \tag{192}$$

The Proposition follows from (189) and (192). □

We now proceed to the proof of Theorem 2.

Proof. We have

$$\mathcal{E}(a, q) = \sum_{d|q} \frac{1}{\phi(q/d)} \sum_{\substack{\chi \bmod q/d \\ Q(\chi) > Q_0}} G(\chi, d)\overline{D(\chi, d)\chi(a)},$$

where

$$G(\chi, d) = \sum_n \gamma(dn)\chi(n), \tag{193}$$

and

$$D(\chi, d) = \sum_n \delta(dn)\chi(n). \tag{194}$$

By Cauchy-Schwarz,

$$|\mathcal{E}(a, q)|^2 \leq \tau(q) \sum_{q=dM} \frac{1}{\phi(M)^2} \left| \sum_{\substack{\chi \bmod M \\ Q(\chi) > Q_0}} G(\chi, d)\overline{D(\chi, d)\chi(a)} \right|^2. \tag{195}$$

We extend the sum over reduced residue classes a mod q to all a mod q. Thus

$$\begin{aligned}
\mathcal{E} &\le \sum_{q\le\tilde{Q}}\sum_{a \bmod q}|\mathcal{E}(a,q)|^2 \\
&\le \sum_{q\le\tilde{Q}}\tau(q)\sum_{q=dM}\frac{1}{\phi(M)^2}\sum_{a \bmod q}\left|\sum_{\substack{\chi \bmod q/d\\ Q(\chi)>Q_0}}G(\chi,d)\overline{D(\chi,d)\chi(a)}\right|^2 \\
&\le \sum_{d\le\tilde{Q}}d\tau(d)\sum_{M\le\frac{\tilde{Q}}{d}}\frac{\tau(M)}{\phi(M)}\sum_{\substack{\chi \bmod M\\ Q(\chi)>Q_0}}|G(\chi,d)D(\chi,d)|^2 \\
&\le \sum_{d\le\tilde{Q}}d\tau(d)\left(\frac{\tilde{Q}}{d}+\frac{\log\tilde{Q}N_1N_2}{\sqrt{Q_0}d^2}+\sqrt{\frac{\tilde{Q}N_1N_2}{d^3}\log\tilde{Q}}\right)(\log\tilde{Q})^2\|b_d\|^2 \qquad (196)
\end{aligned}$$

where

$$b_d(n)=\sum_{n=n_1n_2}\gamma(dn_1)\delta(dn_2), \qquad (197)$$

and where we have used Proposition 8 with $a(n)=b_d(n)$ supported on $n\le N_1N_2/d^2$.

Now by Lemma 21, $\sum_d\tau(d)\|b_d\|^2\le\|\gamma_\tau\|^2\|\delta_\tau\|^2$, so

$$\mathcal{E}\le\left(\tilde{Q}+\frac{N_1N_2}{\sqrt{Q_0}}+\sqrt{\tilde{Q}N_1N_2}\right)(\log\tilde{Q})^3\|\gamma_\tau\|^2\|\delta_\tau\|^2, \qquad (198)$$

as desired.

□

References

[1] H. Davenport, *Multiplicative Number Theory*, vol.74, Springer-Verlag (GTM), New York, 2000.
[2] E. Fouvry and H. Iwaniec, Gaussian primes. Acta Arith. 79 (1997), no. 3, 249-287.
[3] J. Friedlander and H. Iwaniec, *Opera de cribro.* American Mathematical Society Colloquium Publications, 57. American Mathematical Society, Providence, RI, 2010.
[4] J. Friedlander and H. Iwaniec, The polynomial X^2+Y^4 captures its primes. Ann. of Math. (2) 148 (1998), no. 3, 945 - 1040.
[5] J. Friedlander and H. Iwaniec, Gaussian sequences in arithmetic progressions. Funct. Approx. Comment. Math. 37 (2007), part 1, 149-157.
[6] J. Friedlander and H. Iwaniec, Asymptotic sieve for primes. Ann. of Math. (2) 148 (1998), no. 3, 1041-1065.
[7] G. Harman, *Prime-detecting sieves.* London Mathematical Society Monographs Series, 33. Princeton University Press, Princeton, NJ, 2007.
[8] D.R. Heath-Brown, Primes represented by x^3+2y^3. Acta Math. 186 (2001), no. 1, 1-84.
[9] D.R. Heath-Brown and B.Z. Moroz. On the representation of primes by cubic polynomials in two variables. Proc. London Math. Soc. (3) 88 (2004), no. 2, 289-312.

Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford, UK, OX2 6GG

E-mail address: `Roger.Heath-Brown@maths.ox.ac.uk`

Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford, UK, OX2 6GG

E-mail address: `lix1@maths.ox.ac.uk`