

## Numbers representable by five prime squares with primes in an arithmetic progression

by

YONGHUI WANG (Beijing)

**1. Introduction.** A classical result in additive number theory is the five prime squares theorem proved by L. K. Hua: the diophantine equation

$$(1.1) \quad N = p_1^2 + p_2^2 + p_3^2 + p_4^2 + p_5^2$$

is solvable for large odd  $N$  satisfying  $N \equiv 5 \pmod{24}$ .

This theorem can be regarded as a nonlinear extension of the Goldbach ternary theorem (Goldbach–Vinogradov Theorem), it also gives a deep insight into the Lagrange four square theorem. In this paper we study the equation (1.1) with prime variables in an arithmetic progression, i.e. the prime variables satisfy  $p_i \equiv b_i \pmod{d}$ ,  $i = 1, \dots, 5$ , and  $\mathbf{b} = (b_1, \dots, b_5) \in \mathcal{B}(N, d)$ , where

$$(1.2) \quad \mathcal{B}(N, d) = \{\mathbf{b} \in \mathbb{N}^5 : 1 \leq b_i \leq d, (b_i, d) = 1, b_1^2 + \dots + b_5^2 \equiv N \pmod{\sigma(d)d}\},$$

with  $\sigma(d) = 1, 4, 2$  for  $2 \nmid d$ ,  $2 \parallel d$  and  $4 \mid d$  respectively. We will use this notation in the rest of the paper.

Our main result is

**THEOREM.** *There exists an effective positive constant  $\delta$  such that the diophantine equation*

$$(1.3) \quad \begin{cases} N = p_1^2 + p_2^2 + p_3^2 + p_4^2 + p_5^2, \\ p_i \equiv b_i \pmod{d}, \quad i = 1, \dots, 5, \end{cases}$$

*with prime variables is solvable for all positive integers  $d \leq N^\delta$  provided  $N \equiv 5 \pmod{24}$  is a large odd integer with  $\mathcal{B}(N, d)$  nonempty.*

It should be mentioned that this result implies the famous Linnik theorem on the least prime in an arithmetic progression.

---

1991 *Mathematics Subject Classification*: Primary 11P55, 11P32, 11L07, 11L05.

In the corresponding linear case, i.e. for the Goldbach ternary theorem with prime variables in an arithmetic progression, M. C. Liu and Tao Zhan [7] proved that there exists an effective positive constant  $\delta > 0$  such that, for all positive integers  $d \leq N^\delta$ , the diophantine equation

$$\begin{cases} N = p_1 + p_2 + p_3, \\ p_i \equiv b_j \pmod{d}, \quad j = 1, 2, 3, \end{cases}$$

where  $(b_j, d) = 1$ ,  $\sum_{j=1}^3 b_j \equiv N \pmod{d}$ , is solvable for large odd  $N$ .

Their result improved the work of Rademacher, Ayoub and Zulauf, the previous results holding only for a fixed positive integer  $d$  or  $d \leq (\log N)^C$ .

Hua's method with minor modifications actually gives that the equation (1.3) is solvable for large  $N$  with the set (1.2) nonempty and  $d \ll \log^A N$ , but it fails when we want to enlarge the scope of  $d$  to  $d \leq N^\delta$ , where  $\delta$  is an absolute positive constant.

The difficulty lies in two respects. First, in the case of  $d \leq N^\delta$ , we cannot use the Siegel–Walfisz theorem as usual to estimate the major arcs. Second, the restriction to an arithmetic progression requires finding a way to deal with exponential sums and Gauss sums over an arithmetic progression.

The second difficulty was overcome by Jianya Liu and Tao Zhan in [4, Lemma 2]. By using multiplicativity ingeniously, they transform the exponential sum over an arithmetic progression to the usual exponential sum with Dirichlet characters and Gauss sums. The starting point of this paper is a similar result for the quadratic case, i.e. Lemma 3.2. But we use a different method to deal with the first difficulty.

In 1975, Montgomery and Vaughan [8] diminished the exceptional set of the Goldbach problem from  $O(x \log^{-A} x)$  to  $O(x^{1-\delta})$ . Their difficulty also was wider major arcs and the fact that the Siegel–Walfisz theorem could not be used. They solved it by using the Deuring–Heilbronn phenomenon and Gallagher's theorem. But if we use their method for our quadratic problem, we will face too many cases and need to do lots of calculation. This is also the reason why we do not apply the method of M. C. Liu and Tao Zhan [7]. Hence we shall apply a modification of the method by Liu and Tsang [6]. The point is that we only need to estimate the singular series and singular integral separately and only once. But as we are concerned with the quadratic case and the restriction to an arithmetic progression, we have to work harder from the beginning to estimate the complicated singular series (Lemma 4.8).

## 2. Notations and the minor arcs. Define

$$(2.1) \quad d := N^\delta, \quad Q := N^{21\delta}, \quad T := N^{\sqrt{\delta}}, \quad L := N/50, \quad \tau := N^{-1}T^{1/4},$$

where  $\delta$  is a small computable positive constant. Then  $Q < T < L < N$ . We

write

$$(2.2) \quad L_2 = L^{1/2} \quad \text{and} \quad N_2 = N^{1/2}.$$

In the following,  $\varepsilon > 0$  is a comparable very small constant, and the implied constants in the symbols  $O$  and  $\ll$  are computable, positive and depend at most on  $\delta, \varepsilon$ . We write  $e(y)$  for  $e^{2\pi iy}$  and  $e_q(y)$  for  $e(y/q)$ .

For any  $a, q$  such that  $(a, q) = 1, 1 \leq a \leq q \leq Q$ , let

$$\mathbf{m}(a, q) := \left[ \frac{a - \tau}{q}, \frac{a + \tau}{q} \right].$$

We can easily see that these intervals are mutually disjoint and all lie in  $[\tau, 1 + \tau]$ . We call the union of these  $\mathbf{m}(a, q)$  the *major arcs*  $\mathcal{M}$  and  $[\tau, 1 + \tau] \setminus \mathcal{M}$  the *minor arcs*  $\mathcal{M}'$ .

Define

$$(2.3) \quad S_i(\alpha) := S(\alpha, d, b_i) := \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d}}} \Lambda(n) e(\alpha n^2),$$

$$(2.4) \quad R(N) := \int_{\tau}^{1+\tau} \prod_{i=1}^5 S_i(\alpha) e(-N\alpha) d\alpha.$$

Then the Theorem holds if  $R(N) > 0$ . By interval dissection we get

$$(2.5) \quad R(N) = \left\{ \int_{\mathcal{M}} + \int_{\mathcal{M}'} \right\} \prod_{i=1}^5 S_i(\alpha) e(-N\alpha) d\alpha =: R_1(N) + R_2(N),$$

say. The integral over the minor arcs contributes the error term  $R_2(N)$ . We now estimate it by the following lemma from [11].

LEMMA 2.1. *For  $\alpha$  satisfying  $|\alpha - a/q| \leq 1/q^2, (a, q) = 1$  and  $h = (q, d)$ , we have*

$$(2.6) \quad S_i(\alpha) \ll \frac{N_2^{1+\varepsilon} h}{dq^{1/2}} + \frac{N_2^{11/14}}{d^{1/2}} + \frac{N_2^{6/7} h^{3/4}}{d^{3/4} q^{1/4}} + \left( \frac{q^{1/2}}{h^{1/2}} + \frac{q^{1/4}}{h^{1/4}} N_2^{1/7} \right) N^\varepsilon.$$

For any  $\alpha \in \mathcal{M}'$ , by Dirichlet's lemma we see that there exist  $q, a$  satisfying  $Q \leq q \leq \tau^{-1}, (a, q) = 1, 1 \leq a \leq q$  such that  $|\alpha - a/q| \leq \tau/q \leq 1/q^2$ . Notice that  $d = N^\delta, Q = N^{21\delta}$  and  $\delta$  is sufficiently small. We have

COROLLARY 2.2. *For any  $\alpha \in \mathcal{M}'$ , we have*

$$S_i(\alpha) \ll N^{1/2} Q^{-1/2}$$

*provided  $N \geq N_0(\delta)$ .*

LEMMA 2.3. *We have*

$$R_2(N) \ll N^{3/2} Q^{-1/2} d^{-2} \log^{4+c} N$$

whenever  $N \geq N_1(\delta, c)$ .

Proof. By Corollary 2.2 for  $S_5(\alpha)$ , we have

$$R_2(N) \ll N^{1/2} Q^{-1/2} \int_{\tau}^{1+\tau} \left| \prod_{i=1}^4 S_i(\alpha) \right| d\alpha \ll N^{1/2} Q^{-1/2} \sum_{i=1}^4 \int_{\tau}^{1+\tau} |S_i(\alpha)|^4 d\alpha.$$

Clearly, the inner integral is equal to

$$\begin{aligned} \sum_{\substack{n_j \leq N_2 \\ n_1^2 + n_2^2 = n_3^2 + n_4^2 \\ n_j \equiv b_i \pmod{d}}} \Lambda(n_1) \Lambda(n_2) \Lambda(n_3) \Lambda(n_4) &\leq \log^4 N \sum_{\substack{n_j \leq N_2 \\ n_1^2 + n_2^2 = n_3^2 + n_4^2 \\ n_j \equiv b_i \pmod{d}}} 1 \\ &= \log^4 N \int_0^1 \left| \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d}}} e(\alpha n) \right|^4 d\alpha. \end{aligned}$$

Following the arguments in Hua’s lemma [9], it is seen that there is a constant  $c$  such that

$$\int_0^1 \left| \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d}}} e(\alpha n) \right|^4 d\alpha \ll \frac{N}{d^2} \log^c N,$$

whence our lemma follows.

From (2.5), to obtain our Theorem it remains to find a lower bound for  $R_1(N)$  such that  $R_1(N) > |R_2(N)|$ .

**3. Notations and the major arcs.** We shall use  $\chi \pmod{q}$  and  $\chi_0 \pmod{q}$  to denote a Dirichlet character and the principal character modulo  $q$  respectively. It is known ([1], Chapter 14) that there exists a small  $c_1$  such that there is at most one primitive character  $\tilde{\chi}$  to a modulus  $\tilde{r} \leq T$  for which the corresponding  $L$ -function  $L(s, \tilde{\chi})$  has a zero in the region  $\sigma > 1 - c_1(\log T)^{-1}$ ,  $|t| \leq T$ ; and if there is such an exceptional character, it is quadratic and the corresponding zero  $\tilde{\beta}$ , called the *exceptional zero*, is real, simple and unique. Furthermore we have

$$(3.1) \quad c_2(\tilde{r}^{1/2} \log^2 \tilde{r})^{-1} \leq 1 - \tilde{\beta} \leq c_1/\log T.$$

We write  $\sum_{a=1}^{q'}$  or  $\sum_{(a,q)=1}$  for a sum over integers  $a$  satisfying  $1 \leq a \leq q$  and  $(a, q) = 1$ . For any character  $\chi \pmod{dq/h}$ ,  $h = (d, q)$  define

$$\begin{aligned}
 S(\chi, y) &:= S(\chi, y, d, q) := \sum_{L_2 \leq n \leq N_2} \chi(n) \Lambda(n) e(n^2 y), \\
 I(y) &:= \int_{L_2}^{N_2} e(x^2 y) dx, \\
 \tilde{I}(y) &:= \int_{L_2}^{N_2} x^{\tilde{\beta}-1} e(x^2 y) dx, \\
 I(\chi, y) &:= \sum'_{\gamma \leq T} \int_{L_2}^{N_2} x^{\varrho-1} e(x^2 y) dx,
 \end{aligned}
 \tag{3.2}$$

where  $\Lambda(n)$  is the von Mangoldt function and  $\sum'_{\gamma \leq T}$  denotes the summation over all zeros  $\varrho = \beta + i\gamma$  of the function  $L(s, \chi)$  lying in the region  $1/2 \leq \beta \leq 1 - c_1(\log T)^{-1}$ ,  $|\gamma| \leq T$  (hence excluding  $\tilde{\beta}$ , if it exists). By ([1], p. 120) we can easily deduce that

LEMMA 3.1. *For any real  $y$  and any  $\chi \pmod{dq/h}$  with  $dq/h \leq T$ , we have*

$$S(\chi, y) = \delta'_\chi I(y) - \delta_\chi \tilde{I}(y) - I(\chi, y) + O((1 + |y|N)N_2 T^{-1} \log^2 N),$$

where

$$\begin{aligned}
 \delta'_\chi &= \begin{cases} 1 & \text{if } \chi = \chi_0 \pmod{dq/h}, \\ 0 & \text{otherwise;} \end{cases} \\
 \delta_\chi &= \begin{cases} 1 & \text{if } \chi = \tilde{\chi}\chi_0 \pmod{dq/h}, \\ 0 & \text{otherwise.} \end{cases}
 \end{aligned}$$

We next transform the exponential sum  $S_i(\alpha)$  into character sums or integrals of the above forms. To do this we need some more notations.

For positive integers  $d, q$  and  $h(q) := (d, q)$ , i.e. the largest common divisor of  $d, q$ , define positive integers  $\alpha_i, \beta_i, \gamma_i$  according to

$$d = p_1^{\alpha_1} \dots p_s^{\alpha_s} d_0, \quad q = p_1^{\beta_1} \dots p_s^{\beta_s} q_0, \quad (d_0, q_0) = 1,$$

$$h(q) = p_1^{\gamma_1} \dots p_s^{\gamma_s},$$

hence  $\gamma_i = \min(\alpha_i, \beta_i)$ ,  $i = 1, \dots, s$ . Define

$$h_1(q) := p_1^{\delta_1} \dots p_s^{\delta_s}, \quad \delta_i = \begin{cases} \alpha_i & \text{if } \beta_i > \alpha_i, \\ 0 & \text{otherwise,} \end{cases}$$

$$h_2(q) := h(q)/h_1(q).$$

For brevity, we write  $h = h(q)$ ,  $h_1 = h_1(q)$  and  $h_2 = h_2(q)$ . It is easily seen that  $(h_1, h_2) = 1$  and  $(d/h_1, q/h_2) = 1$ .

LEMMA 3.2. For  $\alpha = a/q + \lambda$ , we have

$$(3.8) \quad S_i(\alpha) = \varphi^{-1}(d/h_1)\varphi^{-1}(q/h_2) \\ \times \sum_{\eta \pmod{d/h_1}} \bar{\zeta}(b_i) \sum_{\eta \pmod{q/h_2}} G_i(a, \bar{\eta}, q)S(\zeta\eta, \lambda) + O(\log^2 N),$$

where

$$(3.9) \quad G_i(a, \bar{\eta}, q) := G(h, b_i, a, \bar{\eta}, q) := \sum_{\substack{(c,q)=1 \\ c \equiv b_i \pmod{h}}} e(ac^2/q)\bar{\eta}(c),$$

and  $\eta, \zeta$  are characters modulo  $q/h_2$  and  $d/h_1$  respectively.

Proof. We have

$$\begin{aligned} S_i(\alpha) &= \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d}}} \Lambda(n)e(\alpha n^2) \\ &= \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d} \\ (n,q)=1}} \Lambda(n)e(\alpha n^2) + O\left(\sum_{\substack{p^k \leq N_2 \\ p|q}} \log pe(p^{2k}\alpha)\right) \\ &= \sum_{(c,q)=1} e\left(\frac{ac^2}{q}\right) \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d} \\ n \equiv c \pmod{q}}} \Lambda(n)e(n^2\lambda) + O\left(\log N \sum_{p|q} \log p\right) \\ &= \sum_{\substack{(c,q)=1 \\ c \equiv b_i \pmod{h}}} e\left(\frac{ac^2}{q}\right) \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d} \\ n \equiv c \pmod{q}}} \Lambda(n)e(n^2\lambda) + O(\log^2 N). \end{aligned}$$

The inner sum of the main term is empty unless  $c \equiv b_i \pmod{h}$ , we can therefore add the restriction  $c \equiv b_i \pmod{h}$  to the sum over  $c$ . On the other hand, under the condition  $c \equiv b_i \pmod{h}$ , the congruences

$$n \equiv b_i \pmod{d}, \quad n \equiv c \pmod{q}$$

are equivalent to

$$n \equiv b_i \pmod{d/h_1}, \quad n \equiv c \pmod{q/h_2}.$$

Then

$$S_i(\alpha) = \sum_{\substack{(c,q)=1 \\ c \equiv b_i \pmod{h}}} e\left(\frac{ac^2}{q}\right) \sum_{\substack{n \leq N_2 \\ n \equiv b_i \pmod{d/h_1} \\ n \equiv c \pmod{q/h_2}}} \Lambda(n)e(n^2\lambda) + O(\log^2 N)$$

$$\begin{aligned}
 &= \varphi^{-1}(d/h_1)\varphi^{-1}(q/h_2) \sum_{\substack{(c,q)=1 \\ c \equiv b_i \pmod{h}}} e\left(\frac{ac^2}{q}\right) \\
 &\quad \times \sum_{\zeta \pmod{d/h_1}} \bar{\zeta}(b_i) \sum_{\eta \pmod{q/h_2}} \bar{\eta}(c) \\
 &\quad \times \sum_{n \leq N_2} \zeta\eta(n)\Lambda(n)e(n^2\lambda) + O(\log^2 N).
 \end{aligned}$$

Hence we get the assertion.

By using the above lemmas, we now simplify  $R_1(N)$  as follows.

For any  $\alpha = a/q + \lambda \in \mathbf{m}(a, q)$ , we have  $|\lambda| < \tau/q$  and  $q \leq Q$ . By Lemmas 3.1 and 3.2,

$$\begin{aligned}
 S_i(\alpha) &= \varphi^{-1}(d/h_1)\varphi^{-1}(q/h_2) \left( G_i(a, \bar{\eta}_0, q)I(\lambda) - \delta_q \tilde{\zeta}\zeta_0(b_i)G_i(a, \tilde{\eta}\eta_0, q)\tilde{I}(\lambda) \right. \\
 &\quad \left. - \sum_{\zeta \pmod{d/h_1}} \sum_{\eta \pmod{q/h_2}} \bar{\zeta}(b_i)G_i(a, \bar{\eta}, q)I(\zeta\eta, \lambda) \right) \\
 &\quad + O\left(\varphi^{-1}(q/h_2) \sum_{\eta \pmod{q/h_2}} |G_i(a, \bar{\eta}, q)|(1 + |\lambda|N)N^{1/2}T^{-1} \log^2 N\right) \\
 &\quad + O(\log^2 N),
 \end{aligned}$$

where  $\tilde{\zeta}\zeta_0 \pmod{d/h_1} \tilde{\eta}\eta_0 \pmod{q/h_2} = \tilde{\chi}\chi_0 \pmod{dq/h}$ ,  $\tilde{\zeta}, \tilde{\eta}$  are primitive characters, and

$$(3.10) \quad \delta_q := \begin{cases} 1 & \text{if } \tilde{\chi} \pmod{\tilde{r}} \text{ exists and } \tilde{r} | dq/h, \\ 0 & \text{otherwise.} \end{cases}$$

Since  $|\lambda| \ll \tau/q$  and  $|\lambda|N < T^{1/4}q^{-1}$ , the trivial bound

$$\sum_{\eta \pmod{q/h_2}} |G_i(a, \bar{\eta}, q)| \ll \varphi(q/h_2)\varphi(q)$$

shows that the first  $O$ -term above is

$$\ll \varphi(q)T^{1/4}q^{-1}N_2T^{-1} \log^2 N \leq N_2T^{-3/4} \log^2 N.$$

Hence, for  $\alpha = a/q + \lambda \in \mathbf{m}(a, q)$  we obtain

$$(3.11) \quad S_i(\alpha) = \varphi^{-1}(d/h_1)\varphi^{-1}(q/h_2)H_i(a, q, \lambda) + O(N_2T^{-3/4} \log^2 N)$$

where

$$(3.12) \quad H_i(a, q, \lambda) := G_i(a, \bar{\eta}_0, q)I(\lambda) - \delta_q \tilde{\zeta}\zeta_0(b)G_i(a, \tilde{\eta}\eta_0, q)\tilde{I}(\lambda) - F_i(a, q, \lambda),$$

$$(3.13) \quad F(a, q, \lambda) := \sum_{\zeta \pmod{d/h_1}} \sum_{\eta \pmod{q/h_2}} \bar{\zeta}(b_i)G_i(a, \bar{\eta}, q)I(\zeta\eta, \lambda).$$

To estimate  $H_i(a, q, \lambda)$ , we need the following lemma which can be deduced similarly to Lemma 3.3 of [5].

LEMMA 3.3. Let  $I(\lambda)$ ,  $\tilde{I}(\lambda)$  and  $I(\chi, \lambda)$  be defined as in (3.2).

(a) For any real  $y$ , we have

$$I(y) \ll \min(N_2, L_2^{-1}|y|^{-1}), \quad \tilde{I}(y) \ll \min(N_2^{\tilde{\beta}}, L_2^{\tilde{\beta}-1}|y|^{-1})$$

and

$$I(\chi, y) \ll \begin{cases} N_2 & \text{for any real } y, \\ N_2(L|y|)^{-1/2} & \text{for } |y| > L^{-1}, \\ L_2(L|y|)^{-1} & \text{for } |y| > T/(\pi L). \end{cases}$$

(b) We have

$$\int_{-\infty}^{\infty} |I(y)|^2 dy \ll N_2 L_2^{-1}, \quad \int_{-\infty}^{\infty} |\tilde{I}(y)|^2 dy \ll N_2^{\tilde{\beta}} L_2^{\tilde{\beta}-2}$$

and

$$\int_{-\infty}^{\infty} |I(\chi, y)|^2 dy \ll NL^{-1} \log N.$$

By the trivial estimates for  $I(\lambda)$ ,  $\tilde{I}(\lambda)$  and  $I(\chi, \lambda)$  in Lemma 3.3(a),

$$\varphi^{-1}(d/h_1)\varphi^{-1}(q/h_2)H_i(a, q, \lambda) \ll \varphi(q)N_2.$$

Then

$$\begin{aligned} R_1(N) &= \sum_{q \leq Q} \varphi^{-5}(d/h_1)\varphi^{-5}(q/h_2) \\ &\quad \times \sum_{(a,q)=1}^{\tau/q} \int_{-\tau/q}^{\tau/q} e(-N(a/q + \lambda)) \prod_{i=1}^5 H_i(a, q, \lambda) d\lambda \\ &\quad + O\left( \sum_{q \leq Q} \sum_{(a,q)=1} \frac{\tau}{q} \sum_{k=0}^4 (\varphi(q)N_2)^k (N_2 T^{-3/4} \log^2 N)^{5-k} \right) \\ &= \sum_{q \leq Q} \varphi^{-5}(d/h_1)\varphi^{-5}(q/h_2) \sum_{(a,q)=1} e_q(-Na) \\ &\quad \times \int_{-\tau/q}^{\tau/q} e(-N\lambda) \prod_{i=1}^5 H_i(a, q, \lambda) d\lambda + O(N^{3/2} T^{-1/2} Q^5). \end{aligned}$$

The product  $\prod_{k=1}^5 H_k(a, q, \lambda)$  is a sum of at most  $(\phi(dq/h) + 2)^5$  terms, each



of the form  $\prod_{i=1}^5 E_i$  where  $E_i$  is either  $G_i(q)I(\lambda)$ ,  $-\delta_q \tilde{\zeta}(b_i)G(a, \tilde{\eta}\eta_0, q)\tilde{I}(\lambda)$  or  $-\tilde{\zeta}(b_i)G(a, \tilde{\eta}, q)I(\zeta\eta, \lambda)$ .

By comparing the estimates for  $I(\lambda)$ ,  $\tilde{I}(\lambda)$  and  $I(\chi, \lambda)$  in Lemma 3.3(a) with  $|\lambda| > \tau/q > L^{-1}$ , it is easily seen that the weakest one among them is  $N^{1/2}(L|\lambda|)^{-1/2}$ , since  $\tau = N^{-1}T^{1/4}$ ,  $L = N/25$  and  $T = Q^{1/\sqrt{\delta}}$ . Then

$$\int_{R \setminus [-\tau/q, \tau/q]} \prod_{i=1}^5 E_i d\lambda \ll \phi^3(q)|\tau/q|^{-3/2} \int_{-\infty}^{\infty} |E_1 E_2| d\lambda \ll \phi^5(q)|\tau/q|^{-3/2},$$

by Cauchy's inequality and Lemma 3.3(b). Hence

$$\begin{aligned} \sum_{q \leq Q} \phi^{-5} \left( \frac{d}{h_1} \right) \phi^{-5} \left( \frac{q}{h_2} \right) \sum_{(a,q)=1} \int_{R \setminus [-\tau/q, \tau/q]} e(-N\lambda) \prod_{i=1}^5 H_i(a, b, \lambda) d\lambda \\ \ll \sum_{q \leq Q} \phi^{-5} \left( \frac{d}{h_1} \right) \phi^{-5} \left( \frac{q}{h_2} \right) \phi(q) \left( \phi \left( \frac{dq}{h} \right) + 2 \right)^5 \phi^5(q) q^{3/2} N^{3/2} T^{-3/8} \\ \ll Q^9 N^{3/2} T^{-3/8} \ll N^{3/2} Q^{-1}. \end{aligned}$$

Therefore

$$\begin{aligned} (3.14) \quad R_1(N) &= \sum_{q \leq Q} \phi^{-5}(d/h_1) \phi^{-5}(q/h_2) \sum_{(a,q)=1} e_q(-Na) \\ &\quad \times \int_{-\infty}^{\infty} e(-N\lambda) \prod_{i=1}^5 H_i(a, q, \lambda) d\lambda + O(N^{3/2} Q^{-1}). \end{aligned}$$

#### 4. Some lemmas for singular series and singular integrals

LEMMA 4.1. *Let  $\chi \pmod{p^\beta/h_2}$  be any character with  $\beta \geq 0$ , let  $h_2 = h_2(p^\beta)$  be defined as in (3.7), and let  $\alpha$  be such that  $p^\alpha \parallel d$ . We have*

- (a)  $G_i(a, \chi, p^\beta) = 0$  if  $\chi \pmod{p^\beta}$  is primitive and  $p \mid a$ ,  $\beta > \alpha$ .
- (b)  $G_i(a, \chi\eta_0, p^t) = 0$  if  $\eta_0$  is modulo  $p^t/h_2(p^t)$ ,  $p \nmid a$  and  $t \geq \theta + \max\{\theta, \alpha, \beta\}$  where  $\theta = 1 + [1/p]$ .
- (c)  $G_i(a, \chi, p^\beta) \leq 2(2, p)p^{\beta/2}$  if  $p \nmid a$ .

Proof. (a) Let  $a' = a/p$ . For  $1 \leq c \leq p^\beta$ , write  $c = u + vp^{\beta-1}$ . Since  $\beta > \alpha$ ,  $h(p^\beta) = p^\alpha$  and the restriction  $c \equiv b_i \pmod{p^\alpha}$  is equivalent to  $u \equiv b_i \pmod{p^\alpha}$ . Hence

$$\begin{aligned} G_i(a, \chi, p^\beta) &= \sum_{\substack{c=1 \\ c \equiv b_i \pmod{p^\alpha}}}^{p^\beta} e\left(\frac{a'c^2}{p^{\beta-1}}\right)\chi(c) \\ &= \sum_{\substack{u=1 \\ u \equiv b_i \pmod{p^\alpha}}}^{p^{\beta-1}} e\left(\frac{a'u^2}{p^{\beta-1}}\right) \sum_{v=1}^p \chi(u + vp^{\beta-1}) = 0. \end{aligned}$$

For a primitive character  $\chi \pmod{p^\beta}$ , the inner sum over  $v$  is zero.

(b) For  $t > \alpha$ , we see from (3.7) that  $h(p^t) = p^\alpha$ ,  $h_2(p^t) = 1$ , so  $\eta_0$  is modulo  $p^t$ .

For  $1 \leq c \leq p^t$ , write  $c = u + vp^{t-\theta}$ . The restriction  $c \equiv b_i \pmod{p^\alpha}$  is equivalent to  $u \equiv b_i \pmod{p^\alpha}$ , since  $t \geq \theta + \max\{\theta, \alpha, \beta\}$ . Moreover, we have  $c^2 \equiv u^2 + 2uvp^{t-\theta} \pmod{p^t}$ ,  $c \equiv u \pmod{p^\beta}$ . Hence

$$G(a, \chi, p^t) = \sum_{\substack{u=1 \\ u \equiv b_i \pmod{p^\alpha}}}^{p^{t-\theta}} \chi\eta_0(u) e\left(\frac{au^2}{p^t}\right) \sum_{v=1}^{p^\theta} e\left(\frac{2auv}{p^\theta}\right).$$

For each  $u$  coprime with  $p$ , in view of  $p \nmid a$ , the inner sum over  $v$  is zero. Hence (b) is proved.

(c) For  $\beta \leq \alpha$ ,  $|G(a, \chi, p^\beta)| \leq 1$ . For  $\beta > \alpha$ , we have

$$\begin{aligned} G(a, \chi, p^\beta) &= \sum_{\substack{c=1 \\ c \equiv b_i \pmod{p^\alpha}}}^{p^\beta} e\left(\frac{ac^2}{p^\beta}\right)\chi_{p^\beta}(c) \\ &= \varphi^{-1}(p^\alpha) \sum_{\chi_{p^\alpha} \pmod{p^\alpha}} \chi_{p^\alpha}(b_i) \sum_{c=1}^{p^\beta} e\left(\frac{ac^2}{p^\beta}\right)\chi_{p^\alpha}\chi_{p^\beta}(c). \end{aligned}$$

By Exercise 14 in Chapter 6 of [10], the inner sum over  $c$  is less than  $2(2, p)p^{\beta/2}$  for  $p \nmid a$ . Hence we get (c).

We shall use the following sums to form the singular series:

$$(4.1) \quad Z(q) := Z(q; \eta_1, \dots, \eta_5) := \sum_{(a, q)=1} e_q(-Na) \prod_{i=1}^5 G_i(a, \eta_i, q),$$

$$(4.2) \quad Y(q) := Y(q; \eta_1, \dots, \eta_5) := \sum_{a=1}^q e_q(-Na) \prod_{i=1}^5 G_i(a, \eta_i, q),$$

where  $\eta_i$  is modulo  $q/h_2(q)$ . We can also write

$$(4.3) \quad Y(q; \eta_1, \dots, \eta_5) = q \sum_{(q)} \eta_1(c_1) \dots \eta_5(c_5),$$

where  $\sum_{(q)}$  denotes the sum over  $c_1, \dots, c_5$  satisfying

$$(4.4) \quad \begin{aligned} 1 \leq c_1, \dots, c_5 \leq q, \quad c_i &\equiv b_i \pmod{(d, q)}, \\ (c_i, q) &= 1, \quad \sum_{i=1}^5 c_i^2 \equiv N \pmod{q}. \end{aligned}$$

Denote by  $N(q)$  the number of solutions of the above congruence equation. By Hua's work on Tarry's problem [3, p. 162] and M. C. Liu, K. M. Tsang [6, (1.5)], we see that if  $N \equiv 5 \pmod{24}$  and  $N$  satisfies (1.2) then  $N(q) \geq 1$  for all  $q$ . In the case where  $\eta_i$  are all principal characters, we see that

$$(4.5) \quad Y(q; \eta_0, \dots, \eta_0) = qN(q).$$

Furthermore we put

$$(4.6) \quad A(q) := \varphi^{-5}(q(d, q)^\infty/h)Z(q; \eta_0, \dots, \eta_0),$$

where  $(d, q)^\infty$  has the same prime factors of  $(d, q)$ , and  $(d, q)^\infty \parallel d$  which means that if  $p^\alpha \parallel (d, q)^\infty$  then  $p^\alpha \parallel d$ .

LEMMA 4.2. *Both  $Z(q)$  and  $Y(q)$  are multiplicative in the sense that if  $q = q_1 \dots q_t$  with  $(q_i, q_j) = 1$  for  $i \neq j$ , then for each  $i = 1, \dots, 5$ , the decompositions  $\eta_i \pmod{q/h_2(q)} = \prod_{j=1}^t \eta_{ij} \pmod{q_j/h_2(q_j)}$  are unique. We have*

$$Z(q; \eta_1, \dots, \eta_5) = \prod_{j=1}^t Z(q_j; \eta_{1j}, \dots, \eta_{5j})$$

and

$$Y(q; \eta_1, \dots, \eta_5) = \prod_{j=1}^t Y(q_j; \eta_{1j}, \dots, \eta_{5j}).$$

In particular,  $N(q)$  and  $A(q)$  are multiplicative functions of  $q$ .

PROOF. It suffices to consider the case  $t = 2$ , and then use induction. Let  $q = q_1 q_2$  with  $(q_1, q_2) = 1$ . It is easily seen from (3.7) that

$$\begin{aligned} h(q) &= h(q_1)h(q_2), \quad h_i(q) = h_i(q_1)h_i(q_2), \quad (h_i(q_1), h_i(q_2)) = 1, \\ \frac{q}{h_i(q)} &= \frac{q_1}{h_i(q_1)} \cdot \frac{q_2}{h_i(q_2)}, \quad \left( \frac{q_1}{h_i(q_1)}, \frac{q_2}{h_i(q_2)} \right) = 1, \quad i = 1, 2. \end{aligned}$$

Then  $\eta_i \pmod{q/h_2(q)} = \prod_{j=1}^2 \eta_{ij} \pmod{q_j/h_2(q_j)}$  are uniquely determined.

Let  $a = a_1 q_2 + a_2 q_1$ . If  $a_1, a_2$  run over reduced residue systems modulo  $q_1, q_2$  respectively, then  $a$  will run over a similar system modulo  $q_1 q_2$ . So

$$(4.7) \quad Z(q_1 q_2) = \sum_{(a, q)=1} e_q(-Na) \prod_{i=1}^5 G_i(a, \eta_i, q_1 q_2)$$

$$\begin{aligned}
 &= \sum_{(a_1, q_1)=1} e_{q_1}(-Na_1) \sum_{(a_2, q_2)=1} e_{q_2}(-Na_2) \\
 &\quad \times \prod_{i=1}^5 G_i(a_1q_2 + a_2q_1, \eta_i, q_1q_2).
 \end{aligned}$$

In the same way, let  $c = c_1q_2 + c_2q_1$ . We see that the restriction  $c \equiv b_i \pmod{h(q)}$  is equivalent to  $c_1q_2 \equiv b_i \pmod{h(q_1)}$  and  $c_2q_1 \equiv b_i \pmod{h(q_2)}$ , so we have

$$\begin{aligned}
 &G_i(a_1q_2 + a_2q_1, \eta_i, q_1q_2) \\
 &= \sum_{\substack{c=1 \\ c \equiv b_i \pmod{h(q)}}}^{q_1q_2} e\left(\frac{(a_1q_2 + a_2q_1)c^2}{q_1q_2}\right) \eta(c) \\
 &= \sum_{\substack{(c_1q_2, q_1)=1 \\ c_1q_2 \equiv b_i \pmod{h(q_1)}}} \sum_{\substack{(c_2q_1, q_2)=1 \\ c_2q_1 \equiv b_i \pmod{h(q_2)}}} e\left(\frac{a_1(c_1q_2)^2}{q_1}\right) \eta_{i1}(c_1q_2) \\
 &\quad \times e\left(\frac{a_2(c_2q_1)^2}{q_2}\right) \eta_{i2}(c_2q_1) \\
 &= G_i(a_1, \eta_{i1}, q_1) G_i(a_2, \eta_{i2}, q_2).
 \end{aligned}$$

Hence the right hand side of (4.7) is equal to  $Z(q_1)Z(q_2)$  as desired. The proof for the multiplicativity of  $Y(q)$  is similar.

LEMMA 4.3. *For any positive integer  $q$ , we have*

$$\varphi^{-5} \left( \frac{dq}{h(q)} \right) Z(q) \ll \frac{h^5(q)}{d^5} q^{-3/2} \mathcal{L}.$$

Proof. Let  $q = \prod_{p|q} p^{\beta_p}$  be the prime factorization of  $q$ . By Lemma 4.1(c) and multiplicativity of  $Z(q)$ , we have

$$|Z(q)| = \prod_{p|q} |Z(p^{\beta_p})| \ll \prod_{p|q} p^{\beta_p} \prod_{i=1}^5 p^{\beta_p/2} \ll q^{7/2}.$$

Hence by  $\varphi(q) \gg q \log \log q$ , we get the assertion.

LEMMA 4.4. *For  $i = 1, \dots, 5$ , let  $\chi_i \pmod{p^{\beta_i}}$  be primitive characters and  $\beta = \max\{\beta_1, \dots, \beta_5\}$ . Define  $\alpha := \alpha(p)$  such that  $p^{\alpha(p)} \parallel d$ . For brevity, write  $Z(p^t) = Z(p^t; \chi_1\chi_0, \dots, \chi_5\chi_0)$ , where  $\chi_0$  is modulo  $p^t$ . Then*

- (a)  $Z(p^\beta) = Y(p^\beta)$  if  $\beta > \alpha$ .
- (b)  $Z(p^t) = 0$  if  $t \geq \theta + \max\{\theta, \beta, \alpha\}$ , where  $\theta = 1 + [2/p]$ .

(c)  $\sum_{v=\beta}^t \varphi^{-5}(p^v)Z(p^v) = \varphi^{-5}(p^t)Y(p^t)$  for  $\beta > \alpha$  or  $\sum_{v=0}^\alpha \varphi^{-5}(p^\alpha)Z(p^v) + \sum_{v=\alpha+1}^t \varphi^{-5}(p^v)Z(p^v) = \varphi^{-5}(p^t)Y(p^t)$  for  $\beta = 0$  and  $t > \alpha$ .

Proof. (a) Lemma 4.1(a) asserts that  $G_i(a, \chi, p^\beta) = 0$  for  $p \nmid a$  and  $\beta > \alpha$ . By comparing (4.1) and (4.2), the sum over  $a$  is empty if  $p \mid a$ , hence (a) is proved.

(b) This follows readily from (4.1) and Lemma 4.1(b).

(c) The sum for  $Z(p^t)$  can be written as  $\sum_{a=1}^{p^v} - \sum_{a=1, p \mid a}^{p^v}$ . The first sum is  $Y(p^\alpha)$ . By setting  $a = pa'$ , we see that the second sum is equal to  $p^5 Y(p^{v-1})$  when  $v \geq \max(\beta + 1, \alpha + 1, 2)$ . Thus we have

$$\varphi^{-5}(p^v)Z(p^v) = \varphi^{-5}(p^v)Y(p^v) - \varphi^{-5}(p^{v-1})Y(p^{v-1}).$$

For  $\beta > \alpha$ , summing both sides for  $v = \beta + 1, \dots, t$  and using (a), we get the first equality. In order to consider the condition  $\beta = 0, t > \alpha$ , we still need to sum over those  $t \leq \alpha$  and prove that this yields  $\varphi^{-5}(p^\alpha)Y(p^\alpha)$ . For  $t \leq \alpha, h(p^t) = p^t, h_2(p^t) = p^t$  we have

$$\begin{aligned} Z(p^t) &= \sum_{(a, p^t)=1} e\left(\frac{-Na}{p^t}\right) \prod_{i=1}^5 \left( \sum_{\substack{(c_i, p^t)=1 \\ c_i \equiv b_i \pmod{p^t}}} e\left(\frac{ac_i^2}{p^t}\right) \right) \\ &= \sum_{(a, p^t)=1} e\left(\frac{a(\sum_{i=1}^5 b_i^2 - N)}{p^t}\right) = \varphi(p^t). \end{aligned}$$

Since, by (1.2),  $\sum b_i^2 \equiv N \pmod{d}$ , we have

$$(4.8) \quad \sum_{v=0}^\alpha \varphi^{-5}(p^\alpha)Z(p^v) = \varphi^{-5}(p^\alpha)p^\alpha,$$

which is equal to  $\varphi^{-5}(p^\alpha)Y(p^\alpha)$ . Hence we get (c).

Taking  $\chi_1 = \dots = \chi_5 = \chi_0$  and  $\beta = 0$  in Lemma 4.4, we obtain

COROLLARY 4.5. Let  $A(q), N(q), \alpha = \alpha(p)$  be defined as in (4.6), (4.5), and Lemma 4.4 respectively. Then

- (a)  $A(p^t) = 0$  for  $p \geq 3, t \geq 1 + \alpha$ , and  $A(2^t) = 0$  for  $t \geq 2 + \max\{2, \alpha\}$ .
- (b)  $p^t \varphi^{-5}(p^t)N(p^t) = p^\alpha \varphi^{-5}(p^\alpha)N(p^\alpha)$  for  $p \geq 3, t \geq \alpha$ .
- (c)  $2^t \varphi^{-5}(2^t)N(2^t) = 2^{\alpha'} \varphi^{-5}(2^{\alpha'})N(2^{\alpha'})$  for  $t \geq \alpha', \alpha' = 1 + \max\{2, \alpha\}$ .

In view of the above corollary, we now define

$$(4.9) \quad \begin{aligned} s(p) &:= \sum_{0 \leq t < \theta + \max\{\theta, \alpha(p)\}} A(p^t) \\ &= \varphi^{-5}(\sigma(p^{\alpha(p)})p^{\alpha(p)})N(\sigma(p^{\alpha(p)})p^{\alpha(p)})\sigma(p^{\alpha(p)})p^{\alpha(p)}, \end{aligned}$$

where  $\sigma(q)$  is defined in (1.2). We now simplify  $s(p)$ .

LEMMA 4.6. (a)  $s(p) = \varphi^{-5}(p^\alpha)p^\alpha$  if  $p \neq 2$ ,  $\alpha = \alpha(p) \geq 1$ .

$$(b) s(2) = \begin{cases} 2^3 & \text{if } \alpha(2) = 1, \\ \varphi^{-5}(2^{\alpha(2)})2^{\alpha(2)+1} & \text{if } \alpha(2) \geq 2, \end{cases}$$

hence we can also write  $s(2) = \varphi^{-5}(2^\alpha)2^\alpha \sigma(d)$ .

(c)  $s(p) = 1 + A(p)$  if  $p \neq 2, p \nmid d$ ,  $s(2) = 1 + A(2) + A(2^2) + A(2^3)$  if  $2 \nmid d$ .

PROOF. (a) Use a similar argument to Lemma 4.4(c), (4.8).

(b) By a similar argument, we have  $A(2^t) = \varphi^{-5}(2^\alpha)\varphi(2^t)$  for  $t \leq \alpha$ .

If  $\alpha = 1$ , it remains to consider  $t = 2, 3$ . Since  $\sum_{(a,p^t)=1} = \sum_{a=1}^{p^t} - \sum_{a=1, p|a}^{p^t}$ , we have

$$\begin{aligned} A(2^t) &= \varphi^{-5}(2^t) \sum_{(a,2^t)=1} e\left(\frac{-Na}{2^t}\right) \prod_{i=1}^5 \left( \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2}}}^{2^t} e\left(\frac{ac_i^2}{2^t}\right) \right) \\ &= \varphi^{-5}(2^t) \left( \sum_{a=1}^{2^t} \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2}}}^{2^t} e\left(\frac{a(\sum_{i=1}^5 c_i^2 - N)}{2^t}\right) \right. \\ &\quad \left. - \sum_{a'=1}^{2^{t-1}} \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2}}}^{2^t} e\left(\frac{a'(\sum_{i=1}^5 c_i^2 - N)}{2^{t-1}}\right) \right) \\ &= \varphi^{-5}(2^t)(2^t N(2^t) - 2^{t-1} 2^5 N(2^{t-1})) \\ &= \varphi^{-5}(2^t)2^t N(2^t) - \varphi^{-5}(2^{t-1})2^{t-1} N(2^{t-1}) \end{aligned}$$

where  $N(2^t)$  is the number of solutions of the following congruence equation:

$$1 \leq c_i \leq 2^t, \quad (c_i, 2) = 1, \quad \begin{cases} c_1^2 + \dots + c_5^2 \equiv N \pmod{2^t}, \\ c_i \equiv b_i \pmod{2}. \end{cases}$$

By an easy calculation, we see that  $N(2^3) = 2^{10}$ ,  $N(2) = 1$ . Then

$$\begin{aligned} s(2) &= 1 + A(2) + A(2^2) + A(2^3) \\ &= 1 + 1 - \varphi^{-5}(2)2N(2) + \varphi^{-5}(2^3)2^3 N(2^3) = 2^3. \end{aligned}$$

If  $\alpha > 1$ , it remains to consider  $t = \alpha + 1$ . We have

$$\begin{aligned} A(2^{\alpha+1}) &= \varphi^{-5}(2^{\alpha+1}) \sum_{(a,2^{\alpha+1})=1} e\left(\frac{-Na}{2^{\alpha+1}}\right) \prod_{i=1}^5 \left( \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2^\alpha}}}^{2^{\alpha+1}} e\left(\frac{ac_i^2}{2^{\alpha+1}}\right) \right) \\ &= \varphi^{-5}(2^{\alpha+1}) \left( \sum_{a=1}^{2^{\alpha+1}} \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2^\alpha}}}^{2^{\alpha+1}} e\left(\frac{a(\sum_{i=1}^5 c_i^2 - N)}{2^{\alpha+1}}\right) \right) \end{aligned}$$

$$\begin{aligned}
 & - \sum_{a'=1}^{2^\alpha} e\left(\frac{-Na'}{2^\alpha}\right) \prod_{i=1}^5 \left( \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2^\alpha}}}^{2^{\alpha+1}} e\left(\frac{a'c_i^2}{2^\alpha}\right) \right) \\
 & = \varphi^{-5}(2^{\alpha+1})2^{\alpha+1}N(2^{\alpha+1}) - \varphi^{-5}(2^\alpha)2^\alpha,
 \end{aligned}$$

where  $N(2^{\alpha+1})$  is the number of solutions of the following congruence equation:

$$1 \leq c_i \leq 2^{\alpha+1}, \quad (c_i, 2) = 1, \quad \begin{cases} c_1^2 + \dots + c_5^2 \equiv N \pmod{2^{\alpha+1}}, \\ c_i \equiv b_i \pmod{2^\alpha}. \end{cases}$$

Obviously  $N(2^{\alpha+1}) = 2^5$ . Then

$$\begin{aligned}
 s(2) & = \varphi^{-5}(2^\alpha) + A(2) + \dots + A(2^\alpha) + A(2^{\alpha+1}) \\
 & = \varphi^{-5}(2^{\alpha+1})2^{\alpha+1}N(2^{\alpha+1}) = \varphi^{-5}(2^\alpha)2^{\alpha+1}.
 \end{aligned}$$

Part (c) follows immediately from (4.9) and Corollary 4.5.

LEMMA 4.7. *We have:*

- (a)  $A(p) < 30p^{-2}$  for all  $p \nmid d$ .
- (b)  $\prod_p s(p)$  converges absolutely and  $\prod_p s(p) \gg \varphi^{-5}(d)d\sigma(d)$ .
- (c) 
$$\begin{aligned}
 \sum_{\substack{q=1 \\ (q,r)=1}}^{\infty} \varphi^{-5}(dq/h)Z(q; \eta_0, \dots, \eta_0) & = \prod_{\substack{p \nmid r \\ p \nmid d}} s(p) \\
 & = \frac{\sigma(d/(d,r))d/(d,r)}{\varphi^{-5}(d/(d,r))} \prod_{\substack{p \nmid r \\ p \nmid d}} s(p).
 \end{aligned}$$
- (d)  $\sum_{q \geq y} \varphi^{-5}(dq/h)Z(q; \eta_0, \dots, \eta_0) \ll y^{-1}d^{-3} \log^{30}(y+1)$ .

Proof. (a) Since  $p \nmid d$ , we have  $h(p) = 1$ ; let  $g$  be a quadratic nonresidue modulo  $p$ . Then

$$\begin{aligned}
 A(p) & = \varphi^{-5}(p) \sum_{a=1}^{p-1} \left( e\left(\frac{-Na}{p}\right) \prod_{i=1}^5 \left( \sum_{c_i=1}^{p-1} e\left(\frac{ac_i^2}{p}\right) \right) \right) \\
 & = \frac{1}{2} \varphi^{-5}(p) \sum_{a=1}^{p-1} \left( e\left(\frac{-Na^2}{p}\right) \prod_{i=1}^5 C_p(a^2) + e\left(\frac{-Nga^2}{p}\right) \prod_{i=1}^5 C_p(ga^2) \right),
 \end{aligned}$$

where  $C_p(a) = \sum_{c=1}^{p-1} e(ac^2/p)$ . It is well known [1] that

$$C_p(1) = \lambda - 1, \quad \lambda = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{if } p \equiv -1 \pmod{4}. \end{cases}$$

Furthermore  $C_p(1) + C_p(g) = 2 \sum_{c=1}^{p-1} e_p(c) = -2$ , hence  $C_p(g) = -\lambda - 1$ .

Plainly

$$C_p(a) = \begin{cases} C_p(1) & \text{if } a \text{ is a quadratic residue modulo } p, \\ C_p(g) & \text{otherwise.} \end{cases}$$

We get

$$A(p) = \frac{1}{2}\varphi^{-5}(p) \times \begin{cases} (p-1)((\lambda-1)^5 + (-\lambda-1)^5) & \text{if } p \mid N, \\ (\lambda-1)^6 + (-\lambda-1)^6 & \text{if } p \nmid N \text{ and } \left(\frac{N}{p}\right) = 1, \\ (-\lambda-1)(\lambda-1)^5 + (\lambda-1)(-\lambda-1)^5 & \text{if } p \nmid N \text{ and } \left(\frac{N}{p}\right) = -1, \end{cases}$$

$\left(\frac{N}{p}\right)$  being the Legendre symbol. Hence  $|A(p)| < 30p^{-2}$  for  $p \nmid d$ . The 30 comes from explicit computation, but it is unimportant for our application.

(b) By Lemmas 4.6 and 4.7(a), we have

$$\begin{aligned} \prod_p s(p) &= \prod_{p \mid d} s(p) \prod_{p \nmid d} (1 + A(p)) \\ &\gg \varphi^{-5}(2^{\alpha(2)})\sigma(d)2^{\alpha(2)} \prod_{\substack{p^{\alpha(p)} \parallel d \\ p \neq 2}} \varphi^{-5}(p^{\alpha(p)})p^{\alpha(p)} \prod_{p \nmid d} (1 - 30p^{-2}) \\ &\gg \sigma(d)\varphi^{-5}(d)d. \end{aligned}$$

The proof of the convergence is similar.

(c) Let  $q = q'q''$ ,  $(q', q'') = 1$  and  $q' \mid d^\infty$ ,  $(q'', d) = 1$ . By the multiplicativity of  $Z(q)$ , we have

$$\begin{aligned} \sum_{\substack{q=1 \\ (q,r)=1}}^\infty \varphi^{-5}\left(\frac{dq}{h}\right)Z(q) &= \left( \sum_{\substack{q'=1 \\ (q',r)=1 \\ q' \mid d^\infty}}^\infty \varphi^{-5}\left(\frac{dq'}{h}\right)Z(q') \right) \left( \sum_{\substack{q''=1 \\ (q'',r)=1 \\ (q'',d)=1}}^\infty \varphi^{-5}(q'')Z(q'') \right). \end{aligned}$$

Hence by Corollary 4.5, (4.9) and Lemma 4.6, we obtain the result.

(d) Let  $\delta = (\log(y + 1))^{-1}$ . We have

$$\begin{aligned} \sum_{q \geq y} \varphi^{-5}(dq/h)Z(q) &\leq \sum_{q \geq y} |A(q)| \leq y^{-1+\delta} \sum_{q=1}^\infty q^{1-\delta} |A(q)| \\ &\ll y^{-1} \prod_{p \mid d} \left( \sum_{t=0}^{\theta + \max\{\theta, \alpha(p)\}} p^{t(1-\delta)} |A(p^t)| \right) \prod_{p \nmid d} (1 + 30p^{-1-\delta}) \\ &\ll y^{-1} \frac{d}{\varphi^5(d)} \prod_{p \mid d} p^{\alpha(p)} \prod_p (1 - p^{-1-\delta})^{-30} \ll y^{-1} \frac{d^2}{\varphi^5(d)} \delta^{-30} \end{aligned}$$

since  $1 + nx \ll (1 - x)^{-n}$  and  $\zeta(1 + \delta) \sim \delta^{-1}$ .



LEMMA 4.8. For  $r_i \mid dq/h$ ,  $i = 1, \dots, 5$ , let

$$\chi_i \pmod{r_i} = \zeta_i \pmod{(r_i, d/h_1(q))} \eta_i \pmod{(r_i, q/h_2(q))}$$

be all primitive characters, and  $r = [r_1, \dots, r_5]$ .

$$(a) \sum_{\substack{q \leq Q \\ r \mid dq/h}} \left| \varphi^{-5}(qd/h(q)) Z(q; \eta_1 \eta_0, \dots, \eta_5 \eta_0) \prod_{i=1}^5 \zeta_i \zeta_0(b_i) \right| \ll r^{-3/2} \mathcal{L}.$$

(b) Let  $\alpha(p)$  be defined as in Lemma 4.4. Furthermore let  $r_i = r_i^{(1)} r_i^{(2)}$ ,  $(r_i^{(1)}, r_i^{(2)}) = 1$ , be such that if  $p^\beta \parallel r_i^{(1)}$ , then  $\beta > \alpha(p)$ , and if  $p^\beta \parallel r_i^{(2)}$ , then  $\beta \leq \alpha(p)$ . Let  $d = d_1 d_2$ ,  $(d_1, d_2) = 1$ , be such that if  $p^\beta \parallel r$  and  $p \mid d_1$ , then  $\beta \leq \alpha(p)$ , and if  $p^\beta \parallel r$  and  $p \mid d_2$ , then  $\beta > \alpha(p)$ . Let  $r^{(1)} = [r_1^{(1)}, \dots, r_5^{(1)}]$  and  $\chi_i \pmod{r_i} = \chi_i^{(1)} \pmod{r_i^{(1)}} \chi_i^{(2)} \pmod{r_i^{(2)}}$ . We have

$$\begin{aligned} E &:= \sum_{\substack{q \leq Q \\ r \mid dq/h}} \varphi^{-5} \left( \frac{qd}{h(q)} \right) Z(q; \eta_1 \eta_0, \dots, \eta_5 \eta_0) \prod_{i=1}^5 \zeta_i \zeta_0(b_i) \\ &= \prod_{i=1}^5 \chi_i^{(2)}(b_i) \pmod{r_2} \frac{\sigma(d_1) d_1}{\varphi^5(d_1)} \cdot \frac{Y(\sigma(r^{(1)}) r^{(1)})}{\varphi^5(\sigma(r^{(1)}) r^{(1)})} \prod_{\substack{p \nmid d \\ p \nmid r}} s(p) + O(Q^{-1} \mathcal{L}^{31}). \end{aligned}$$

Proof. Part (a) follows immediately from Lemma 4.3. We use the multiplicativity of  $Z(q)$  and  $Y(q)$  to prove (b).

Let  $d = d' d''$ ,  $q = q' q''$  be such that  $(d'', r) = 1$ ,  $(q'', r) = 1$  and  $d' \mid r^\infty$ ,  $q' \mid r^\infty$ , where the notation  $q \mid r^\infty$  means that every prime factor of  $q$  divides  $r$ . For brevity, set  $h'' = h(q'')$ ,  $h' = h(q')$ ,  $h''_i = h_i(q'')$ ,  $h'_i = h_i(q')$ . By (3.7) and  $r_i \mid dq/h$ , we have

$$\eta_i \pmod{(r_i, q/h_2)} = \eta_i \pmod{(r_i, q'/h'_2)}, \quad \zeta_i \pmod{(r_i, d/h_1)} = \zeta_i \pmod{(r_i, d'/h'_1)}.$$

Then by multiplicativity of  $Z(q)$ ,

$$\begin{aligned} (4.10) \quad E &= \sum_{\substack{q' \leq Q, r \mid q' d' / h' \\ q' \mid r^\infty, d' \mid r^\infty}} \varphi^{-5} \left( \frac{q' d'}{h'} \right) Z(q'; \eta_1 \eta_0, \dots, \eta_5 \eta_0) \prod_{i=1}^5 \zeta_i \zeta_0(b_i) \\ &\quad \times \sum_{\substack{q'' \leq Q/q' \\ (q'', r) = 1, (d'', r) = 1}} \varphi^{-5} \left( \frac{q'' d''}{h''} \right) Z(q''; \eta_0, \dots, \eta_0) \\ &=: E_1 E_2, \end{aligned}$$

say. By Lemma 4.7(c), (d), we have

$$(4.11) \quad E_2 = \frac{\sigma(d'')d''}{\varphi^{-5}(d'')} \prod_{\substack{p \nmid r \\ p \nmid d''}} s(p) + O(q'Q^{-1}(d'')^{-3} \log^{30} Q).$$

Hence by Lemmas 4.3 and 4.8(a), and (4.10),

$$(4.12) \quad \begin{aligned} E &= E_1 \frac{\sigma(d'')d''}{\varphi^{-5}(d'')} \prod_{\substack{p \nmid r \\ p \nmid d''}} s(p) + O\left(Q^{-1}(d'')^{-3} \log^{31} Q \sum_{\substack{q' \leq Q \\ r \mid d'q'/h'}} \frac{1}{(q')^{1/2}}\right) \\ &= E_1 \frac{\sigma(d'')d''}{\varphi^{-5}(d'')} \prod_{\substack{p \nmid r \\ p \nmid d''}} s(p) + O(Q^{-1}(d'')^{-3} \tau(d) \log^{31} Q), \end{aligned}$$

since we will see later from the following proof that the number of  $q'$  is less than  $\tau(d)$ , i.e. the divisor function.

Let  $q' = m'm''$  with  $(m'', d) = 1$  and  $m' \mid (d')^\infty$ , and let  $r_i = r'_i r''_i$  with  $(r''_i, d) = 1$  and  $r'_i \mid (d')^\infty$ . Obviously  $m' \mid (r, d)^\infty$  and

$$\begin{aligned} \zeta_i \pmod{(r_i, d'/h'_1)} &= \zeta'_i \pmod{(r'_i, d'/h'_1)}, \\ \eta_i \pmod{(r_i, q'/h'_2)} &= \eta'_i \pmod{(r'_i, m'/h_2(m''))} \eta''_i \pmod{(r''_i, m''/h_2(m''))}. \end{aligned}$$

By combining with the multiplicativity of  $Z(q)$ ,

$$(4.13) \quad \begin{aligned} E_1 &= \sum_{\substack{m'' \leq Q \\ r'' \mid m''}} \varphi^{-5}(m'') Z(m''; \eta''_1, \dots, \eta''_5) \\ &\quad \times \sum_{\substack{m' \leq Q/m'' \\ r' \mid m'd'/h'}} \varphi^{-5}\left(\frac{m'd'}{h'}\right) Z(m'; \eta'_1 \eta_0, \dots, \eta'_5 \eta_0) \prod_{i=1}^5 \zeta'_i \zeta_0(b_i) \\ &=: G_1 G_2, \end{aligned}$$

say. By the same argument as in Lemma 3.8, (3.14), of [6], from our Lemma 4.4 we see that

$$G_1 = \varphi^{-5}(\sigma(r'')r'') Y(\sigma(r'')r'') \quad \text{if } \sigma(r'')r'' \leq Q.$$

In fact we can assume  $\sigma(r)r \leq Q$ , otherwise if  $\sigma(r)r > Q$ , by Lemmas 4.3 and 4.8(a) we get

$$\begin{aligned} E_1 &\ll Q^{-3/2} \mathcal{L}, \\ \varphi^{-5}(\sigma(r'')r'') Y(\sigma(r'')r'') G_2 &\ll (r'r'')^{-3/2} \mathcal{L}^2 \ll Q^{-3/2} \mathcal{L}^2. \end{aligned}$$

Then combining with (4.13) we can write

$$(4.14) \quad E_1 = \varphi^{-5}(\sigma(r'')r'')Y(\sigma(r'')r'')G_2 + O(Q^{-3/2}\mathcal{L}^2).$$

Furthermore we can assume  $\sigma(r')r' \leq Q/m''$ . Otherwise if  $\sigma(r')r' > Q/m''$ , then  $G_2 \ll Q^{-3/2}(m'')^{3/2}\mathcal{L}$  by Lemma 4.8(a). By Lemma 4.3 then

$$E_1 \ll \sum_{\substack{m'' \leq Q \\ r'' | m''}} Q^{-3/2}\mathcal{L}^2 \ll Q^{-3/2}\mathcal{L}^2$$

since by a similar proof to that of Lemma 3.8 in [6],  $m'' = ur''$ ,  $u | \sigma(r'')$ . Hence the sum over  $\sigma(r')r' > Q/m''$  will be absorbed in the error term.

Now we simplify  $G_2$  for  $\sigma(r')r' \leq Q/m''$ . It is seen that  $m' | (d')^\infty$ ,  $m' | (r')^\infty$  is in fact  $m' | (r, d)^\infty | (r')^\infty, (d')^\infty$ . Hence we can write

$$d' = p_1^{\alpha_1} \dots p_t^{\alpha_t}, \quad r' = p_1^{\beta_1} \dots p_t^{\beta_t}, \quad m' = p_1^{s_1} \dots p_t^{s_t}$$

where  $p_i^{\alpha_i} \parallel d, p_i^{\beta_i} \parallel r$  and  $\alpha_i, \beta_i > 0$ . The condition  $p_i^{\beta_i} | \frac{p_i^{s_i} p_i^{\alpha_i}}{h(p_i^{s_i})}$  indicates that  $s_i \geq \beta_i$  if  $\beta_i > \alpha_i$ , and  $s_i \geq 0$  if  $\beta_i \leq \alpha_i$ . Hence

$$\zeta'_i \pmod{(r'_i, d'/h_1(m'))} = \prod_{\substack{\beta_j \leq \alpha_j \\ s_j \leq \alpha_j}} \zeta_{ij} \pmod{p_j^{\beta_j}},$$

$$\eta'_i \pmod{(r'_i, m'/h_2(m'))} = \prod_{\substack{\beta_j \leq \alpha_j \\ s_j > \alpha_j}} \eta_{ij} \pmod{p_j^{\beta_j}} \prod_{\beta_j > \alpha_j} \eta_{ij} \pmod{p_j^{\beta_j}}.$$

Let  $\prod_{j=1}^u \chi_{ij} \pmod{p_j^{\beta_j}} = \zeta'_i \eta'_i \pmod{r'_i}$ . Then we have

$$(4.15) \quad \chi_{ij} = \begin{cases} \zeta_{ij} & \text{if } \beta_j \leq \alpha_j, s_j \leq \alpha_j, \\ \eta_{ij} & \text{if } \beta_j \leq \alpha_j, s_j > \alpha_j, \\ \eta_{ij} & \text{if } \beta_j > \alpha_j. \end{cases}$$

Then by Lemmas 4.4 and 4.2, and (4.13),

$$(4.16) \quad G_2 = W_2 \prod_{\substack{p_j \neq 2 \\ \beta_j > \alpha_j}} \varphi^{-5}(p_j^{\beta_j})Y(p_j^{\beta_j}; \chi_{1j}\eta_0, \dots, \chi_{5j}\eta_0) \prod_{\substack{p_j \neq 2 \\ \beta_j \leq \alpha_j}} W_{p_j},$$

where

$$W_{p_j} = \varphi^{-5}(p_j^{\alpha_j}) \left( \sum_{t=0}^{\alpha_j} Z(p_j^t; \eta_0, \dots, \eta_0) \prod_{i=1}^5 \chi_{ij} \zeta_0(b_i) \right),$$

and by Lemma 4.4(b), (c),

$$W_2 = \begin{cases} 1 & \text{if } 2 \nmid (r, d), \\ \varphi^{-5}(2^{\beta_2+1})Y(2^{\beta_2+1}) & \text{if } 2 \mid (r, d), \beta_2 > \alpha_2 > 0, \\ \varphi^{-5}(2) \left( \sum_{t=0}^1 Z(2^t; \eta_0, \dots, \eta_0) \prod_{i=1}^5 \chi_{i2} \zeta_0(b_i) \right) \\ \quad + \sum_{t=2}^3 \varphi^{-5}(2^t) Z(2^t; \chi_{12}\eta_0, \dots, \chi_{52}\eta_0) & \text{if } 2 \mid (r, d), \beta_2 \leq \alpha_2 = 1, \\ \varphi^{-5}(2^\alpha) \left( \sum_{t=0}^\alpha Z(2^t; \eta_0, \dots, \eta_0) \prod_{i=1}^5 \chi_{i2} \zeta_0(b_i) \right) \\ \quad + \varphi^{-5}(2^{\alpha+1}) Z(2^{\alpha+1}; \chi_{12}\eta_0, \dots, \chi_{52}\eta_0) & \text{if } 2 \mid (r, d), \beta_2 \leq \alpha_2, \alpha_2 > 1. \end{cases}$$

We shall estimate  $W_2$  for  $2 \mid (r, d)$ ,  $\beta_2 \leq \alpha_2$  and  $W_{p_j}$  for  $\beta_j \leq \alpha_j$ . By a similar argument to that in Lemma 4.4, (4.8), for  $t \leq \alpha(p)$  and  $(b_i, d) = 1$ ,

$$\prod_{i=1}^5 \zeta_{ij} \zeta_0(b_i) Z(p_j^t) = \prod_{i=1}^5 \chi_{ij}(b_i) \varphi(p^t).$$

Then

$$W_{p_j} = \prod_{i=1}^5 \chi_{ij}(b_i) \varphi^{-5}(p^{\alpha(p)}) p^{\alpha(p)}.$$

And for  $2 \mid (r, d)$ ,

$$\begin{aligned} Z(2^{\alpha_2+1}) &= \sum_{(a, 2^{\alpha_2+1})=1} e\left(-\frac{Na}{2^{\alpha_2+1}}\right) \prod_{i=1}^5 \left( \sum_{\substack{c_i=1 \\ c_i \equiv b_i \pmod{2^{\alpha_2}}} }^{2^{\alpha_2+1}} e\left(\frac{ac_i^2}{2^{\alpha_2+1}}\right) \chi_{i2} \eta_0(c_i) \right) \\ &= Y(2^{\alpha_2+1}) - 2^{\alpha_2} 2^5 \prod_{i=1}^5 \chi_{i2}(b_i) \\ &= (2^{\alpha_2+1} N(2^{\alpha_2+1}) - 2^{\alpha_2+5}) \prod_{i=1}^5 \chi_{i2}(b_i). \end{aligned}$$

Hence, for  $\alpha_2 > 1$ , we see from the proof of Lemma 4.6(b) that  $N(2^{\alpha_2+1}) = 2^5$ , and we have

$$W_2 = \prod_{i=1}^5 \chi_{i2}(b_i) \varphi^{-5}(2^{\alpha_2}) 2^{\alpha_2+1}.$$

If  $\alpha_2 = 1$ , then  $\beta_2 = 1$ , since  $0 < \beta_2 \leq \alpha_2$ , and

$$W_2 = \varphi^{-5}(2) \left( \sum_{t=0}^1 Z(2^t; \eta_0, \dots, \eta_0) \prod_{i=1}^5 \chi_{i2}(b_i) \right)$$

$$\begin{aligned}
 & + \sum_{t=2}^3 \varphi^{-5}(2^t) Z(2^t; \chi_{12}\eta_0, \dots, \chi_{52}\eta_0) \\
 & = \prod_{i=1}^5 \chi_{i2}(b_i) (1 + A(2) + A(2^2) + A(2^3)) \\
 & = 2^3 \prod_{i=1}^5 \chi_{i2}(b_i).
 \end{aligned}$$

The last equality comes from the proof of Lemma 4.6(b). Hence for  $2 \nmid (r, d)$  we obtain

$$(4.17) \quad W_2 = \begin{cases} \prod_{i=1}^5 \chi_{i2}(b_i) \frac{\sigma(2^{\alpha_2}) 2^{\alpha_2}}{\varphi^5(2^{\alpha_2})} & \text{if } \alpha_2 \geq \beta_2, \\ \varphi^{-5}(2^{\beta_2+1}) Y(2^{\beta_2+1}) & \text{if } \alpha_2 < \beta_2. \end{cases}$$

Then by (4.12)–(4.14) and (4.16), we have

$$\begin{aligned}
 (4.18) \quad E & = \prod_{i=1}^5 \chi_i^{(2)}(b_i) \pmod{r_2} \frac{\sigma(d_1) d_1}{\varphi^5(d_1)} \cdot \frac{Y(\sigma(r^{(1)}) r^{(1)})}{\varphi^5(\sigma(r^{(1)}) r^{(1)})} \prod_{\substack{p \nmid d \\ p \nmid r}} s(p) \\
 & + O(Q^{-1} \mathcal{L}^{31}) + O\left(\frac{d''}{\varphi^5(d'')} \prod s(p) Q^{-3/2} \mathcal{L}^2\right) \\
 & = \prod_{i=1}^5 \chi_i^{(2)}(b_i) \pmod{r_2} \frac{\sigma(d_1) d_1}{\varphi^5(d_1)} \cdot \frac{Y(\sigma(r^{(1)}) r^{(1)})}{\varphi^5(\sigma(r^{(1)}) r^{(1)})} \prod_{\substack{p \nmid d \\ p \nmid r}} s(p) \\
 & + O(Q^{-1} \mathcal{L}^{31}).
 \end{aligned}$$

The error term can be obtained from Lemmas 4.4 and 4.8(a).

The following lemma is actually Lemma 3.9 of [6].

LEMMA 4.9. *For any complex numbers  $\rho_i$  with  $0 < \text{Re } \rho_i \leq 1, i = 1, \dots, 5$ , we have*

$$\begin{aligned}
 (4.19) \quad & \int_{-\infty}^{\infty} e(-N\lambda) \prod_{i=1}^5 \left( \int_{L_2}^{N_2} x^{\rho_i-1} e(\lambda x^2) dx \right) d\lambda \\
 & = N^{3/2} 2^{-5} \int_{\mathcal{D}} \prod_{i=1}^5 (Nx_i)^{(\rho_i-1)/2} x_i^{-1/2} dx_1 \dots dx_4,
 \end{aligned}$$

where

$$(4.20) \quad x_5 := 1 - \sum_{i=1}^4 x_i$$

and

$$(4.21) \quad \mathcal{D} := \{(x_1, \dots, x_4) : L/N \leq x_1, \dots, x_4, x_5 \leq 1\}.$$

Furthermore, we have

$$(4.22) \quad \int_{\mathcal{D}} \left( \prod_{i=1}^5 x_i^{-1/2} \right) dx_1 \dots dx_4 \gg 1.$$

**5. Major arcs and the completion of the proof of Theorem.** We can now complete the proofs of our main results by showing that  $R_1(N)$  dominates the error term in (2.5). From (3.12), we see that the product  $\prod_{i=1}^5 H_i(a, q, \lambda)$  is a sum of  $3^5$  terms which can be classified into three categories:

(C<sub>1</sub>): the term  $\prod_{i=1}^5 G_i(q)I(\lambda)$ , in which  $\zeta_i, \eta_i$  are all principal characters.

(C<sub>2</sub>): the 211 terms each of which has at least one  $F_i(a, q, \lambda)$  as factor.

(C<sub>3</sub>): the 31 remaining terms.

For convenience, we write, for  $i = 1, 2, 3$ ,

$$(5.1) \quad M_i := \sum_{q \leq Q} \varphi^{-5}(dq/h) \sum_{(a,q)=1} e_q(-Na) \times \int_{-\infty}^{\infty} e(-N\lambda) \{\text{sum of the terms in (C}_i)\} d\lambda.$$

In view of (3.14), we have

$$(5.2) \quad R_1(N) = M_1 + M_2 + M_3 + O(N^{3/2}Q^{-1}).$$

For distinct integers  $m_1, m_2, \dots$  taken from the set  $\{1, \dots, 5\}$ , let

$$(5.3) \quad \mathcal{P}(m_1, m_2, \dots) := N^{3/2}2^{-5} \int_{\mathcal{D}} \left( \prod_{i=1}^5 x_i^{-1/2} \right) (Nx_{m_1}Nx_{m_2}\dots)^{(\tilde{\beta}-1)/2} dx_1 \dots dx_4$$

and

$$(5.4) \quad \Delta(m_1, m_2, \dots) := \tilde{\chi}(n_{m_1})\tilde{\chi}(n_{m_2})\dots,$$

where the region  $\mathcal{D}$  is defined in (4.21), and  $\tilde{\chi}$  and  $\tilde{\beta}$  are the exceptional character and exceptional zero respectively. Let

$$(5.5) \quad \mathcal{P}_0 := N^{3/2}2^{-5} \int_{\mathcal{D}} \left( \prod_{i=1}^5 x_i^{-1/2} \right) dx_1 \dots dx_4.$$

Clearly, from (4.21) we have

$$(5.6) \quad |\mathcal{P}(m_1, m_2, \dots)| \leq \mathcal{P}_0 \ll N^{3/2}.$$

LEMMA 5.1. *We have*

$$M_1 = \frac{\sigma(d)d}{\varphi^{-5}(d)} \prod_{p \nmid d} s(p) \mathcal{P}_0 + O(N^{3/2}d^{-3}Q^{-1}\mathcal{L}^{31}).$$

Proof. From (5.1), we see that

$$M_1 = \sum_{q \leq Q} \varphi^{-5}(dq/h) \sum_{(a,q)=1} e_q(-Na) \prod_{i=1}^5 G_i(q) \int_{-\infty}^{\infty} e(-N\lambda) \prod_{i=1}^5 I(\lambda) d\lambda.$$

By (5.5) the above integral is equal to  $\mathcal{P}_0$ . In view of (4.1), the above double sum is  $\sum_{q \leq Q} \varphi^{-5}(dq/h)Z(q)$ . By Lemma 4.7(c), (d), this can be written as

$$\frac{\sigma(d)d}{\varphi^5(d)} \prod_{p \nmid d} s(p) + O\left(\sum_{q > Q} |A(q)|\right) = \prod_{p \nmid d} s(p) + O(Q^{-1}d^{-3}\mathcal{L}^{31}).$$

Our lemma then follows from this and (5.6).

LEMMA 5.2. *If the exceptional zero  $\tilde{\beta}$  exists, and  $\tilde{r}_1, d_1$  are defined as in Lemma 4.8(b), by taking  $r^{(1)} = \tilde{r}_1$ , then*

$$\begin{aligned} \text{(a)} \quad M_3 &= \frac{\sigma(d_1)d_1}{\varphi^{-5}(d_1)} \cdot \frac{\sigma(\tilde{r}_1)\tilde{r}_1}{\varphi^5(\sigma(\tilde{r}_1)\tilde{r}_1)} \prod_{\substack{p \nmid d \\ p \nmid \tilde{r}_1}} s(p) \sum_{(\sigma(\tilde{r}_1)\tilde{r}_1)} \left\{ - \sum_{i=1}^5 \Delta(i)\mathcal{P}(i) \right. \\ &\quad \left. + \sum_{1 \leq i < j \leq 5} \Delta(i, j)\mathcal{P}(i, j) - \dots - \Delta(1, 2, 3, 4, 5)\mathcal{P}(1, 2, 3, 4, 5) \right\} \\ &\quad + O(N^{3/2}Q^{-1}\mathcal{L}^{31}), \\ \text{(b)} \quad M_3 &\ll N^{3/2}\tilde{r}^{-3/2}\mathcal{L}^{31}. \end{aligned}$$

Proof. In view of (3.12), the 31 terms in  $(C_3)$  can be grouped into 5 types according to the number of the factors  $\tilde{\zeta}(b_i)G_i(a, \tilde{\eta}, q)\tilde{I}(\lambda)$  in these terms. A typical term with  $k$  such factors is of the form

$$(-1)^k \delta_q \left( \prod_{i=1}^k \tilde{\zeta}(b_i)G_i(a, \tilde{\eta}, q)\tilde{I}(\lambda) \right) \left( \prod_{i=k+1}^5 G_i(a, \eta_0, q) \right).$$

If  $M_{3k}$  is the contribution to  $M_3$  from such a term, then according to (5.1),

$$\begin{aligned} M_{3k} &= (-1)^k \left( \sum_{\substack{q \leq Q \\ \tilde{r}|q}} \varphi^{-5}\left(\frac{dq}{h}\right) \sum_{(a,q)=1} e_q(-Na) \prod_{i=1}^k \tilde{\zeta}(b_i)G_i(a, \tilde{\eta}, q) \right. \\ &\quad \left. \times \prod_{i=k+1}^5 G_i(a, \eta_0, q) \right) \left( \int_{-\infty}^{\infty} e(-N\lambda)\tilde{I}^k(\lambda)I^{5-k}(\lambda) d\lambda \right) \\ &=: (-1)^k WU, \quad \text{say.} \end{aligned}$$

The integral  $U$ , by (4.19), is equal to  $\mathcal{P}(1, \dots, k)$ . In view of (4.1),  $W$  is the singular series

$$W = \sum_{\substack{q \leq Q \\ \tilde{r}_1 | q}} \varphi^{-5}(dq/h) Z(q; \tilde{\eta}\eta_0, \dots, \tilde{\eta}\eta_0, \eta_0, \dots, \eta_0) \tilde{\zeta}\zeta_0 \cdot \dots \cdot \tilde{\zeta}\zeta_0 \cdot \zeta_0 \cdot \dots \cdot \zeta_0.$$

By Lemma 4.8(b) and  $Y(\sigma\tilde{r}_1) = \sigma\tilde{r}_1 \sum_{(\sigma\tilde{r}_1)} \dots$ , we have

$$M_{3k} = (-1)^k \frac{\sigma(d_1)d_1}{\varphi^{-5}(d_1)} \cdot \frac{\sigma(\tilde{r}_1)\tilde{r}_1}{\varphi^5(\sigma(\tilde{r}_1)\tilde{r}_1)} \prod_{\substack{p|d \\ p|\tilde{r}}} \sum_{(\sigma(\tilde{r}_1)\tilde{r}_1)} \Delta(1, \dots, k) \mathcal{P}(1, \dots, k) + O(N^{3/2}Q^{-1}\mathcal{L}^{31}).$$

Hence we obtain (a) by combining all these contributions.

The bound in (b) can be deduced directly from Lemma 4.3.

Define

$$(5.7) \quad \Omega = \begin{cases} (1 - \tilde{\beta}) \log T & \text{if } \tilde{\beta} \text{ exists,} \\ 1 & \text{otherwise.} \end{cases}$$

In view of Corollary 4.5, Lemma 4.6 and (4.9), we have

$$(5.8) \quad \prod_{\substack{p|d \\ p|r}} s(p) = \sigma(r'')r''\varphi^{-5}(\sigma(r'')r'')N(\sigma(r'')r''),$$

$$(5.9) \quad \frac{\sigma(r'_1)r'_1}{\varphi^5(\sigma(r'_1)r'_1)}N(\sigma(r'_1)r'_1) = \frac{\sigma(d_2)d_2}{\varphi^5(\sigma(d_2)d_2)}N(\sigma(d_2)d_2) = \frac{\sigma(d_2)d_2}{\varphi^5(d_2)},$$

where  $r''r' = r$ ,  $(r', r'') = 1$ ,  $(r'', d) = 1$ ,  $r' | d^\infty$ ;  $r'_1, d_2 | (r, d)$  have the same prime factors and the exponent of each prime factor of  $d_2$  is less than in  $r'_1$ . Hence we can write  $M_1$  in the form

$$M_1 = \frac{\sigma(d_1)d_1}{\varphi^{-5}(d_1)} \cdot \frac{\sigma(\tilde{r}_1)\tilde{r}_1}{\varphi^5(\sigma(\tilde{r}_1)\tilde{r}_1)} \prod_{\substack{p|d \\ p|\tilde{r}}} s(p) \sum_{(\sigma(\tilde{r}_1)\tilde{r}_1)} \mathcal{P}_0 + O(N^{-3/2}d^{-3}Q^{-1}\mathcal{L}^{31}).$$

Comparing it with the form of  $M_3$  in Lemma 5.2(a), we have

$$(5.10) \quad M_1 + M_3 = \frac{\sigma(d_1)d_1}{\varphi^{-5}(d_1)} \cdot \frac{\sigma(\tilde{r}_1)\tilde{r}_1}{\varphi^5(\sigma(\tilde{r}_1)\tilde{r}_1)} \times \prod_{\substack{p|d \\ p|\tilde{r}}} s(p) N^{3/2} 2^{-5} \sum_{(\sigma(\tilde{r}_1)\tilde{r}_1)} \int_{\mathcal{D}} \left( \sum_{i=1}^5 x_i^{-1/2} \right)$$



$$\begin{aligned} & \times \prod_{i=1}^5 (1 - \tilde{\chi}(c_i)(Nx_i)^{(\tilde{\beta}-1)/2}) dx_1 \dots dx_4 \\ & + O(N^{3/2}Q^{-1}\mathcal{L}^{31}). \end{aligned}$$

It remains to bound the integral, as

$$\prod_{i=1}^5 (1 - \tilde{\chi}(c_i)(Nx_i)^{(\tilde{\beta}-1)/2}) \geq \prod_{i=1}^5 (1 - L^{\tilde{\beta}-1})$$

since  $x_i \geq L/N$  in the region  $\mathcal{D}$ . Hence, we have

$$1 - L^{\tilde{\beta}-1} \geq 1 - \exp(-\frac{1}{2}(1 - \beta) \log N) \geq \min \left\{ \frac{1}{2}, \frac{1}{4}(1 - \tilde{\beta}) \log N \right\} \geq \Omega.$$

Then the main term in (5.10) is

$$\geq \Omega^5 \frac{\sigma(d_1)d_1}{\varphi^{-5}(d_1)} \cdot \frac{\sigma(\tilde{r}_1)\tilde{r}_1}{\varphi^5(\sigma(\tilde{r}_1)\tilde{r}_1)} \prod_{\substack{p \mid d \\ p \nmid \tilde{r}}} s(p) \sum_{(\sigma(\tilde{r}_1)\tilde{r}_1)} \mathcal{P}_0.$$

Hence, by (5.8) and (5.9), we have

LEMMA 5.3.

$$M_1 + M_3 \geq \Omega^5 \frac{\sigma(d)d}{\varphi^{-5}(d)} \prod_{p \mid d} s(p) \mathcal{P}_0 + O(N^{3/2}Q^{-1}\mathcal{L}^{31}).$$

We need to estimate  $M_2$ . By the Deuring–Heilbronn phenomenon, we have

LEMMA 5.4.

$$M_2 \ll \Omega^5 \exp(-c/\sqrt{\delta}) \frac{\sigma(d)d}{\varphi^{-5}(d)} \prod_{p \mid d} s(p) \mathcal{P}_0 + O(N^{3/2}Q^{-1}\mathcal{L}^{31}).$$

Proof. In view of (3.12), each term in  $(C_2)$  must have the form like  $\sum_{\zeta\eta} \bar{\zeta}(b_i)G_i(a, \bar{\eta}, q)I_2(\zeta\eta, \lambda)$  at least once. Indeed, to be specific, we only need to treat a typical term

$$\delta_q \left( \prod_{i=1}^3 \sum_{\zeta\eta} \bar{\zeta}(b_i)G_i(a, \bar{\eta}, q)I_2(\zeta\eta, \lambda) \right) G_4(a, \eta_0, q)I(\lambda)\tilde{\beta}(b_5)G_5(a, \tilde{\eta}, q)\tilde{I}(\lambda)$$

to illustrate the method. Denote the contribution of this term to  $M_2$  by  $X$ . By (5.1),

$$\begin{aligned}
 X &= \sum_{\substack{q \leq Q \\ \tilde{r} | dq/h}} \delta_q \varphi^{-5}(dq/h) \sum_{(a,q)=1} e_q(-Na) G_4(a, \eta_0, q) \tilde{\zeta}(b_5) G_5(a, \tilde{\eta}, q) \\
 &\times \left( \prod_{i=1}^3 \sum_{\zeta \eta} \bar{\zeta}(b_i) G_i(a, \bar{\eta}, q) \right) \sum'_{|\gamma| \leq T} \int_{-\infty}^{\infty} e(-N\lambda) \left( \prod_{i=1}^3 \int_{L_2}^{N_2} x^{\varrho_i-1} e(\lambda x^2) dx \right) \\
 &\times \left( \int_{L_2}^{N_2} e(\lambda x^2) dx \right) \left( \int_{L_2}^{N_2} x^{\tilde{\beta}-1} e(\lambda x^2) dx \right) d\lambda.
 \end{aligned}$$

By (4.19) the integral  $\int_{-\infty}^{\infty} \dots d\lambda$  is

$$N^{3/2} 2^{-5} \int_{\mathcal{D}} \left( \prod_{i=1}^5 x_i^{-1/2} \right) \left( \prod_{i=1}^3 (Nx_i)^{(\varrho_i-1)/2} \right) (Nx_5)^{(\tilde{\beta}-1)/2} dx_1 \dots dx_4.$$

It is well known [1] that each character is induced uniquely by a primitive character, and conversely, for each primitive character  $\chi^* \pmod r$  and each  $q$  divisible by  $r$ , there is a unique character  $\chi \pmod q$  which is induced by  $\chi^*$ . Furthermore, the  $L$ -functions  $L(s, \chi^*)$  and  $L(s, \chi)$  have the same set of nontrivial zeros with positive real parts. Accordingly, we can rearrange the summation for  $X$  as follows:

$$\begin{aligned}
 (5.11) \quad X &= N^{3/2} 2^{-5} \int_{\mathcal{D}} \left( \prod_{i=1}^5 x_i^{-1/2} \right) \\
 &\times (Nx_5)^{(\tilde{\beta}-1)/2} \left( \prod_{i=1}^3 \sum_{r_i \leq dQ} \sum_{\chi_i = \zeta_i \eta_i \pmod{r_i}}^* \sum'_{|\gamma| \leq T} (Nx_i)^{(\varrho_i-1)/2} \right) \\
 &\times \sum_{\substack{q \leq Q \\ r | dq/h}} \varphi^{-5}(dq/h) \sum_{(a,q)=1} G_4(a, \eta_0, q) \tilde{\zeta} \zeta_0(b_5) G_5(a, \tilde{\eta} \eta_0, q) \\
 &\times \left( \prod_{i=1}^3 \bar{\zeta}(b_i) G_i(a, \bar{\eta}, q) \right) dx_1 \dots dx_4,
 \end{aligned}$$

where  $\sum^*$  denotes the summation over all the primitive characters modulo  $r_i$  and  $r = [r_1, r_2, r_3, \tilde{r}]$ . In view of Lemma 4.8, the inner sum  $\sum_{q \leq Q, r | dq/h}$  is equal to

$$\begin{aligned}
 (5.12) \quad \prod_{i=1}^3 \chi_i^{(2)}(b_i) \tilde{\chi}^{(2)}(b_5) \frac{\sigma(d_1) d_1}{\varphi^{-5}(d_1)} \cdot \frac{Y(\sigma(r^{(1)}) r^{(1)})}{\varphi^5(\sigma(r^{(1)}) r^{(1)})} \prod_{p \nmid d, r} s(p) \\
 + O(N^{3/2} Q^{-1} \mathcal{L}^{31}),
 \end{aligned}$$

where  $d_1$  and  $r^{(1)}$  are defined as in Lemma 4.8(b). Since

$$Y(\sigma(\tilde{r}_1) \tilde{r}_1) \leq \sigma(\tilde{r}_1) \tilde{r}_1 N(\sigma(\tilde{r}_1) \tilde{r}_1),$$

combining with (5.8), (5.9), we obtain

$$\left| \sum_{\substack{q \leq Q \\ r|dq/h}} \right| \leq \frac{\sigma(d)d}{\varphi^{-5}(d)} \prod_{p \nmid d} s(p) + O(N^{3/2}Q^{-1}\mathcal{L}^{31}).$$

By the idea of [2], Lemma 6.2 of [6] proved the following form of large sieve: for some suitable  $c$  and for any real  $y \geq N_2$ ,

$$\sum_{q \leq T} \sum_{\chi \pmod{q}}^* \sum'_{|\gamma| \leq T} y^{\beta-1} \ll \Omega^5 \exp(-c/\sqrt{\delta}).$$

Applying these to the multiple sums in (5.11), and combining with (4.21), we prove the lemma.

We can now combine all our estimates to obtain a lower bound for  $R_1(N)$ . There are two cases to be considered.

(1)  $\tilde{r} > Q^{1/13}$  or  $\tilde{\beta}$  does not exist. By Lemmas 5.1, 5.2(b), and 5.4 with a sufficiently small  $\delta$ , we have

$$R_1(N) \geq \frac{1}{2} \cdot \frac{\sigma(d)d}{\varphi^{-5}(d)} \prod_{p \nmid d} s(p) \mathcal{P}_0 + O(N^{3/2}Q^{-3/26}\mathcal{L}^{31}).$$

Then by Lemma 4.7(a), this gives  $I_1(N) \gg N^{3/2}Q^{-1/5}$ ; notice that  $d = Q^{1/21}$ .

(2)  $\tilde{r} \leq Q^{1/13}$ . From Lemmas 5.3 and 5.4, we can deduce that for sufficiently small  $\delta$ ,

$$R_1(N) \geq \frac{1}{2} \Omega^5 \frac{\sigma(d)d}{\varphi^{-5}(d)} \prod_{p \nmid d} s(p) \mathcal{P}_0 + O(N^{3/2}Q^{-1}\mathcal{L}^{31}).$$

Since

$$\Omega \gg (\tilde{r}^{1/2} \log^2 \tilde{r})^{-1} \gg Q^{-1/26} \log^{-2} Q,$$

we get

$$R_1(N) \gg N^{3/2}Q^{-2/5}.$$

Finally, comparing this with Lemma 2.3, both of these two cases give that  $R_1(N) > |R_2(N)|$  for large  $N$ . Hence our Theorem is proved.

**Acknowledgements.** The author is very grateful to his supervisor Zhan Tao for his suggestions and enthusiastic encouragement.

### References

- [1] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, 1980.
- [2] P. X. Gallagher, *A large sieve density estimates near  $\sigma = 1$* , Invent. Math. 11 (1970), 329–339.

- [3] L. K. Hua, *Additive Theory of Prime Numbers*, Transl. Math. Monographs 13, Amer. Math. Soc., 1965.
- [4] J. Y. Liu and T. Zhan, *The ternary Goldbach problem in arithmetic progressions*, Acta Arith. 82 (1997), 197–227.
- [5] M. C. Liu and K. M. Tsang, *Small prime solutions of linear equations*, in: Théorie des Nombres, de Gruyter, 1989, 595–624.
- [6] —, —, *Small prime solutions of some additive equations*, Monatsh. Math. 111 (1991), 147–169.
- [7] M. C. Liu and T. Zhan, *The Goldbach problem with primes in arithmetic progressions*, in: Analytic Number Theory, Y. Motohashi (ed.), London Math. Soc. Lecture Note Ser. 247, Cambridge Univ. Press, 1997, 227–251.
- [8] H. L. Montgomery and R. C. Vaughan, *The exceptional set of Goldbach's problem*, Acta Arith. 27 (1975), 353–370.
- [9] R. C. Vaughan, *The Hardy–Littlewood Method*, Cambridge Univ. Press, 1981.
- [10] I. M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.
- [11] Y. H. Wang, *Some exponential sums over primes in an arithmetic progression*, Shanda Xuebao, to appear (in Chinese).

Department of Mathematics  
The Capital Normal University  
Beijing 100037  
P.R. China  
E-mail: yhwang@mail.cnu.edu.cn

Received on 3.11.1998

(3502)