Title: Conditional Bounds for Small Prime Solutions of Linear Equations
Authors: Kwok-Kwong CHOI, Ming-Chit LIU and Kai-Man TSANG
Address: Department of Mathematics, University of Hong Kong, Pokfulam Road, Hong Kong

ABSTRACT: Let $a_1, a_2, a_3$ be non-zero integers with $\gcd(a_1, a_2, a_3) = 1$ and let $b$ be an arbitrary integer satisfying $\gcd(b, a_i, a_j) = 1$ for $i \neq j$ and $b \equiv a_1 + a_2 + a_3 \pmod{2}$. In a previous paper [3] which completely settled a problem of A. Baker, the 2nd and 3rd authors proved that if $a_1, a_2, a_3$ are not all of the same sign, then the equation $a_1p_1 + a_2p_2 + a_3p_3 = b$ has a solution in primes $p_j$ satisfying

$$\max_{1 \leq j \leq 3} p_j \leq 3|b| + (3 \max_{1 \leq j \leq 3} |a_j|)^A$$

where $A > 0$ is an absolute constant. In this paper, under the generalized Riemann hypothesis, the authors obtain a much more precise bound for the solutions $p_j$. In particular they obtain $A < 4 + \varepsilon$ for some $\varepsilon > 0$. In connection with Linnik’s constant they also prove that if $\ell, q$ are coprime positive integers and $\ell$ is odd, then there is a prime $p \ll q^2 \log^{10} q$ of the form $p = \ell + (p' + p'')q$ where $p'$ and $p''$ are also primes.

1980 Mathematics Subject Classification: Primary-11D04, 11D85
Secondary-11P55, 11P32

Key words and phrases: Small prime solutions, Vinogradov’s type equation, Linnik’s constant, circle method.
CONDITIONAL BOUNDS FOR SMALL
PRIME SOLUTIONS OF LINEAR EQUATIONS

Kwok-Kwong CHOI, Ming-Chit LIU and Kai-Man TSANG

Let \( a_1, a_2, a_3 \) be non-zero integers with \( \gcd(a_1, a_2, a_3) = 1 \) and let \( b \) be an arbitrary integer satisfying \( \gcd(b, a_i, a_j) = 1 \) for \( i \neq j \) and \( b \equiv a_1 + a_2 + a_3 \pmod{2} \). In a previous paper [3] which completely settled a problem of A. Baker, the 2nd and 3rd authors proved that if \( a_1, a_2, a_3 \) are not all of the same sign, then the equation \( a_1p_1 + a_2p_2 + a_3p_3 = b \) has a solution in primes \( p_j \) satisfying

\[
\max_{1 \leq j \leq 3} p_j \leq 3|b| + (3 \max_{1 \leq j \leq 3} |a_j|)^A
\]

where \( A > 0 \) is an absolute constant. In this paper, under the Generalized Riemann Hypothesis, the authors obtain a more precise bound for the solutions \( p_j \). In particular they obtain \( A < 4 + \varepsilon \) for some \( \varepsilon > 0 \). An immediate consequence of the main result is that the Linnik’s courtant is less than or equal to 2.

1. Introduction

In previous papers [3], [4], [5] the second and third authors completely settled a problem of A. Baker [1, Lemma 6] (see also the introduction in [3]) and studied the solubility and insolubility of some additive equations in prime variables. In particular, they considered [3] Vinogradov’s type of equations

\[
a_1p_1 + a_2p_2 + a_3p_3 = b
\]

in prime variables \( p_1, p_2, p_3 \). Here \( a_1, a_2, a_3 \) are non-zero integral coefficients such that

\[
(a_1, a_2, a_3) = 1
\]

and \( b \) is an arbitrary integer satisfying the conditions:
(1.3) \[ (b, a_i, a_j) = 1 \quad \text{for} \quad 1 \leq i < j \leq 3 , \]
(1.4) \[ b \equiv a_1 + a_2 + a_3 \pmod{2} . \]

Here and in the sequel, for integers \( n_1, \cdots, n_s \) not all equal to zero, \( (n_1, \cdots, n_s) \) denotes their greatest common divisor. In [3], the second and third authors proved

**Theorem LT.** Subject to the conditions (1.2)-(1.4), there exist effective absolute constants \( A_1, A_2 > 0 \) such that

(i) if \( a_1, a_2, a_3 \) are all positive, then equation (1.1) is soluble in primes \( p_1, p_2, p_3 \) whenever

(1.5) \[ b \geq (3 \max\{a_1, a_2, a_3\})^{A_1} ; \]

(ii) if \( a_1, a_2, a_3 \) are not all of the same sign, then equation (1.1) has a prime solution \( p_1, p_2, p_3 \) satisfying

(1.6) \[ \max\{p_1, p_2, p_3\} \leq 3|b| + (3\max\{|a_1|, |a_2|, |a_3|\})^{A_2} . \]

This theorem includes many interesting special cases. For instance, when \( a_1 = a_2 = a_3 = 1 \) and \( b \) is a positive odd integer, then Theorem LT(i) is the classical three primes theorem of Vinogradov. Another interesting example is that, for any pair of coprime positive integers \( \ell \) and \( q, \ell \leq q \), if we take in Theorem LT(ii) \( a_1 = 1, a_2 = -q, a_3 = q \) and \( b = \ell \) or \( \ell + q \) according as \( \ell \) is odd or even, then there is a prime \( p_1 \) in the arithmetic progression \( \ell + kq, k = 0, 1, \cdots \) such that \( p_1 \ll q^{A_2} \). If \( L \) denotes the infimum of the c's such that every such arithmetic progression contains a prime \( p \ll q^c \), the so-called *Linnik's constant*, this example also shows that \( A_2 \geq L \). Analogous example, namely, \( a_1 = a_2 = q, a_3 = q + 1 \) and \( b = \ell + kq \) for some suitable \( k \) so that (1.3) to (1.5) hold, shows that \( A_1 \geq L + 1 \).

So the bounds given in (1.5) and (1.6) are of the right order of infinity. However, the upper bounds we can assign to \( A_1 \) and \( A_2 \) are still far too large. Recently, the first author has shown that \( A_1, A_2 < 4191 \). In this paper, we shall replace (1.5) and (1.6) by much more precise estimates under the assumption of the Generalized Riemann Hypothesis (GRH). We shall prove

**Theorem 1.** Assuming the GRH, we can replace the bounds in (1.5) and (1.6) respectively by

(1.7) \[ b \gg f(a_1, a_2, a_3) \]
and
\[
\max_{1 \leq j \leq 3} \{ |a_j| p_j \} \ll |b| + f(a_1, a_2, a_3)
\]
where
\[
f(a_1, a_2, a_3) := \frac{|a_1 a_2 a_3|}{(a_1, a_2)(a_1, a_3)(a_2, a_3)} \left\{ \frac{|a_1 a_2|}{(a_1, a_3)(a_2, a_3)} + (a_1, a_3) + (a_2, a_3) \right\} \log^{10}(3 \max_{1 \leq j \leq 3} |a_j|).
\]
In particular, \(f(a_1, a_2, a_3) \ll (a_1 a_2)^2 |a_3| \log^{10}(3 \max_{1 \leq j \leq 3} |a_j|)\) and the \(A_1, A_2\) in Theorem LT can be taken respectively as \(5 + \varepsilon\) and \(4 + \varepsilon\) for any \(\varepsilon > 0\).

**Remarks.**

(I) To appreciate the precision of the above bounds, let us consider, say, the estimate (1.8) in the situation where \(a_1, a_2\) are bounded and \(a_3\) varies. Then (1.8) asserts that equation (1.1) has solutions \(p_1, p_2, p_3\) in which \(p_3 \ll |a_3|^{-1} b + \log^{10} |a_3|\), a function which grows much slower than \(|a_3|\). Such information on the location of the solutions \(p_1, p_2, p_3\) is not obtainable from the type of results like (1.6) even when the best possible value of \(A_2(\geq 1)\) is obtained.

(II) Let \(1 \leq \ell \leq q, (\ell, q) = 1\) and consider the equation
\[
p - q p' - q p'' = \ell \quad \text{or} \quad \ell + q
\]
according as \(\ell\) is odd or even. Our Theorem 1 (the bound in (1.8)) ensures that, under the GRH there is always a prime \(p\) in the arithmetic progression \(\ell + kq\), \(k = 0, 1, 2, \ldots\), such that \(p \ll q^2 \log^{10} q\). (*) Furthermore, \(k\) can be specified as a sum of two primes if \(\ell\) is odd or of the form \(p' + p'' + 1\) if \(\ell\) is even.

We shall reduce our Theorem 1 to the following system of 4 linear equations:
\[
\alpha_1 n_1 + \alpha_2 n_2 + \alpha_3 n_3 = \kappa, \quad r_j n_j - u_j = p_j \quad (j = 1, 2, 3),
\]
where \(n_1, n_2, n_3\) vary over the natural numbers and \(p_1, p_2, p_3\) are prime variables. Suppose \(\alpha_1, \alpha_2, \alpha_3\) are pairwise coprime non-zero integers and \(r_j, u_j\) \((j = 1, 2, 3)\) are integers such that
\[
0 \leq u_j < r_j, \quad (r_j, u_j) = (r_j, \alpha_j) = 1.
\]
Further, let \(\kappa\) be any integer such that
\[
r_1 r_2 r_3(\alpha_1 (u_1 + 1) + \alpha_2 (u_2 + 1) + \alpha_3 (u_3 + 1) - \kappa) \quad \text{is even}.
\]

(*) It has been conjectured that the bound for \(p\) may be \(q \log^2 q\). Our estimate here is only slightly weaker than the well-known bound \(q^2 \log^2 q\) obtained directly under the GRH.
We have

**Theorem 2.** (i) If $\alpha_1, \alpha_2, \alpha_3$ are all positive, then the system (1.9) is soluble whenever

\[
\kappa \gg \alpha_1 \alpha_2 \alpha_3 (r_1 + r_2 + \alpha_1 \alpha_2 r_3^2) \log^{10} (3 \max_{1 \leq j \leq 3} |\alpha_j r_j|);
\]

(ii) if $\alpha_1, \alpha_2, \alpha_3$ are not all of the same sign, then the system (1.9) has a solution which satisfies

\[
\max_{1 \leq j \leq 3} \{ |\alpha_j| n_j \} \ll |\kappa| + |\alpha_1 \alpha_2 \alpha_3|(r_1 + r_2 + |\alpha_1 \alpha_2| r_3^2) \log^{10} (3 \max_{1 \leq j \leq 3} |\alpha_j r_j|).
\]

To recover Theorem 1, we take in Theorem 2 $r_1 = (a_2, a_3), r_2 = (a_1, a_3)$ and $r_3 = (a_1, a_2)$. Since $(a_1, a_2, a_3) = 1$, we have $r_2 r_3 = (a_1 a_2 a_3) |a_1$. Take $\alpha_1 = a_1 (r_2 r_3)^{-1}$ and similarly $\alpha_2 = a_2 (r_1 r_3)^{-1}, \alpha_3 = a_3 (r_1 r_2)^{-1}$. Then clearly, $\alpha_1, \alpha_2, \alpha_3$ are pairwise coprime and $(r_j, \alpha_j) = 1$ for $j = 1, 2, 3$. Equation (1.1) implies $p_j \equiv a_j^{-1} b \pmod{r_j}$, so we let $u_j \equiv -a_j^{-1} b \pmod{r_j}, 0 \leq u_j < r_j$ for $j = 1, 2, 3$. Condition (1.3) then ensures that $(r_j, u_j) = 1$. Also, we see that $a_1 u_1 + a_2 u_2 + a_3 u_3 \equiv -b \pmod{k}$ holds for $k = r_1 r_2 r_3$, since it holds for $k = r_1, r_2, r_3$ which are pairwise coprime. Finally, take $\kappa = (a_1 u_1 + a_2 u_2 + a_3 u_3 + b)(r_1 r_2 r_3)^{-1}$, then

\[
r_1 r_2 r_3 \left( \sum_{j=1}^{3} \alpha_j (u_j + 1) - \kappa \right) = \sum_{j=1}^{3} a_j (r_j - 1)(u_j + 1) + a_1 + a_2 + a_3 - b
\]

and condition (1.11) is clearly equivalent to (1.4). The primes $p_1, p_2, p_3$ in (1.9) satisfy the equation $a_1 p_1 + a_2 p_2 + a_3 p_3 = b$. Since $b = r_1 r_2 r_3 \kappa - (a_1 u_1 + a_2 u_2 + a_3 u_3) \leq r_1 r_2 r_3 \kappa$ for $a_1, a_2, a_3 > 0$, hypothesis (1.12) is now a consequence of hypothesis (1.7) and the first part of Theorem 1 follows from Theorem 2(i). When $a_1, a_2, a_3$ are not all of the same sign, we have $|a_j| p_j \leq r_1 r_2 r_3 |\alpha_j| n_j$ and $r_1 r_2 r_3 |\kappa| \leq |b| + 3 \max_{1 \leq j \leq 3} \{|a_j| r_j\} = |b| + 3 r_1 r_2 r_3 \max_{1 \leq j \leq 3} |\alpha_j|$. Whence (1.8) follows from (1.13).

Like Theorem LT, the proof of our Theorem 2 is also built on the circle method. While the techniques we developed in [3] have successful applications in some other related problems (see [4], [5]), they are not efficient in giving good upper bounds to $A_1$ and $A_2$. Our aim in this present article is to obtain the sharpest possible estimates in (1.5) and (1.6) under the GRH. To achieve this, we have to modify much of the previous arguments in [3] by injecting new techniques and ideas.
One novel idea is a further averaging of some error terms over the major arcs. This consideration leads to the following mean value result (see Lemma 2(ii) below)

\[
\sum_{\chi^2 \equiv \chi (\bmod q) \neq 0, r} \sum_{h=1}^q |C_\chi(nh,q,r,u)C_{\chi'}(-nh,q,r,u)| = q\phi(rq)^2
\]

involving the generalised Gaussian sums \( C_\chi(m,q,r,u) \) defined in (2.8). It is remarkable that we actually obtain an exact evaluation for the above sum on the left side.

In addition, the major arcs in our arguments are also very specialized and delicate.

2. Notation and some preliminary lemmas

We shall use the standard arithmetic functions, \( \mu(n) \)-the Möbius function, \( \Lambda(n) \)-the von Mangoldt function and \( \phi(n) \)-the Euler totient function. The symbol \( p \) always denotes a prime. By \( p^\sigma \| n \), we shall mean \( p^\sigma | n \), \( p^\sigma + 1 \nmid n \). We write, as usual, \( e(x) = e^{2\pi ix} \) and \( e_q(x) = e(x/q) \). The constants implied in the symbols \( \ll \), \( \gg \) and \( O \) are effectively computable.

Let \( \alpha_j, r_j, u_j \ (j = 1, 2, 3) \) and \( \kappa \) be as given in (1.9)-(1.11). We assume, without loss of generality, that \( \alpha_3 \geq 1 \). Let \( N \geq N_0(\varepsilon) \) be a large parameter which satisfies

\[
N \log^{-10} N \geq \varepsilon^{-4} |\alpha_1\alpha_2\alpha_3| (r_1 + r_2 + |\alpha_1\alpha_2| r_3^2)
\]

for a sufficiently small \( \varepsilon > 0 \). Furthermore, we assume that

\[
N = 2\kappa/3, \quad \text{in case (i) of Theorem 2} ,
\]

\[
N \geq |\kappa|/12, \quad \text{in case (ii) of Theorem 2} .
\]

Let

\[
\lambda(n) := \begin{cases} 
\log p, & \text{if } n = p, \text{ a prime} , \\
0, & \text{otherwise} ,
\end{cases}
\]

and define for \( j = 1, 2, 3 \) the generating functions

\[
S_j(x) := \sum_{N_j' < n \leq N_j} \lambda(r_jn - u_j)e(\alpha_jnx)
\]

where

\[
N_j := c_j N |\alpha_j|^{-1}, \quad N_j' := c_j' N |\alpha_j|^{-1}
\]
and the constants $c_j > c'_j > 0$ are being determined in §3 (following (3.2)). Set

$$\tau := N_3^{-1/2} \log N$$

and define

$$I(N) := \int_{\tau/\alpha_3}^{1+\tau/\alpha_3} e(-\kappa x)S_1(x)S_2(x)S_3(x)dx .$$

Then plainly,

$$I(N) = \sum_{\alpha_1 n_1 + \alpha_2 n_2 + \alpha_3 n_3 = \kappa} \prod_{j=1}^{3} \lambda(r_j n_j - u_j)$$

$$\ll (\log N)^3 \times \text{card}\{n_1, n_2, n_3 : \sum_{j=1}^{3} \alpha_j n_j = \kappa, \ N_j' < n_j \leq N_j \text{ and } r_j n_j - u_j \text{ is a prime for } j = 1, 2, 3\} .$$

Our objective is to show that $I(N) \gg N^2 \prod_{j=1}^{3} (|\alpha_j|^{-1} r_j \phi(r_j)^{-1})$ whereby, in view of (2.1) and (2.2), our Theorem 2 follows. For convenience, set

$$\Omega := N^2 \prod_{j=1}^{3} (|\alpha_j|^{-1} r_j \phi(r_j)^{-1}) ,$$

$$Q := |\alpha_1 \alpha_2|^{1/2} \log^{3/2} N .$$

We begin by defining $\mathcal{M}$, the major arcs. For coprime positive integers $h$ and $q$ such that $h \leq \alpha_3 q$ and $q \leq Q$, let $m(h, q) := [(h - \tau) (\alpha_3 q)^{-1}, (h + \tau) (\alpha_3 q)^{-1})$. These intervals are pairwise disjoint and are all lying inside $[\tau/\alpha_3, 1 + \tau/\alpha_3)$, since, by (2.6), (2.4) and (2.1), we have $2\tau Q < 1$. The union of these intervals $m(h, q)$ then forms our $\mathcal{M}$ and, as usual, its complement in $[\tau/\alpha_3, 1 + \tau/\alpha_3)$ is the minor arcs $\mathcal{M}'$. Accordingly, we have the decomposition

$$I(N) = \alpha_3^{-1} \sum_{q \leq Q} \sum_{\substack{h=1 \cr (h, q) = 1}}^{\alpha_3 q} \int_{-\tau/q}^{\tau/q} e(-\kappa \alpha_3^{-1} (hq^{-1} + \theta)) \prod_{j=1}^{3} S_j(\alpha_3^{-1} (hq^{-1} + \theta))d\theta$$

$$+ \int_{\mathcal{M}'} e(-\kappa x) \prod_{j=1}^{3} S_j(x)dx := I_1(N) + I_2(N) ,$$

say.

For any integers $m, q, r, u$ such that $r, q \geq 1$ and $(r, u) = 1$, we define

$$C_\chi(m, q, r, u) := \sum_{\ell=1}^{q} \chi(r \ell - u)e_q(\ell m)$$

(2.8)
for any Dirichlet character \( \chi \) (mod \( rq \)). When \( r = 1, u = 0 \), this recovers the usual Gaussian sum \( C_\chi(m) := \sum_{1 \leq \ell \leq q} \chi(\ell)e_q(\ell m) \). When \( \chi = \chi_0 \), the principal character, we write

\[
(2.9) \quad C_0(m, q, r, u) := C_{\chi_0}(m, q, r, u) = \sum_{\substack{\ell = 1 \\ (\ell r - u, q) = 1}}^{q} e_q(\ell m) \quad \text{and} \quad C_q(m) := C_{\chi_0}(m).
\]

**Lemma 1.** (i) If \( q_1, q_2 \) are coprime positive integers, then

\[
C_0(m, q_1 q_2, r, u) = C_0(m \overline{q_2}, q_1, r, u) C_0(m \overline{q_1}, q_2, r, u)
\]

where \( q_1 \overline{q_1} + q_2 \overline{q_2} = 1 \).

(ii) Let \( (h, q) = 1 \). Then \( C_0(mh, q, r, u) = 0 \) if \( (r, q) \nmid m \) and \( C_0(mh, q, r, u) = e_q(\overline{r}(umh))C_q(m) \) if \( (r, q) = 1 \). Here \( r \overline{r} \equiv 1 \) (mod \( q \)).

(iii) Let \( (h, q) = 1 \) and \( j = 1 \) or \( 2 \). If \( (q, \alpha_3 r_j) > 1 \) then \( C_0(\alpha_j h, \alpha_3 q, r_j, u_j) = 0 \).

**Proof.** (i) Write \( \ell = \ell_1 q_2 + \ell_2 q_1, \ell_j = 1, \cdots, q_j \) \((j = 1, 2)\), then the defining sum for \( C_0(m, q_1 q_2, r, u) \) in (2.9) can be rearranged as

\[
\sum_{\substack{\ell_1 = 1 \\ (r q_1 \ell_1 - u, q_1) = 1}}^{q_1} e_{q_1}(\ell_1 m) \sum_{\substack{\ell_2 = 1 \\ (r q_2 \ell_2 - u, q_2) = 1}}^{q_2} e_{q_2}(\ell_2 m) = C_0(m \overline{q_2}, q_1, r, u) C_0(m \overline{q_1}, q_2, r, u).
\]

This proves part (i).

(ii), (iii) First of all, if \( (r, q) = 1 \) then

\[
(2.10) \quad C_0(mh, q, r, u) = \sum_{\substack{\ell = 1 \\ (\ell, q) = 1}}^{q} e_q((\ell + u)\overline{r}mh) = e_q(\overline{r}umh)C_q(\overline{r}mh)
\]

\[
= e_q(\overline{r}umh)C_q(m).
\]

If \( (r, q) \nmid m \), let \( p^\sigma \mid q \) such that \( p \mid r, p^\sigma \nmid m \). By (i), \( C_0(mh, q, r, u) \) has a factor of the form

\[
C_0(mhw, p^\sigma, r, u) = \sum_{\ell = 1}^{p^\sigma} e_{p^\sigma}(\ell mhw)
\]

where \( p \nmid w \). Since \( p^\sigma \nmid mhw \), the last sum vanishes and so does \( C_0(mh, q, r, u) \).

Similarly, we have \( C_0(\alpha_j h, \alpha_3 q, r_j, u_j) = 0 \) if \( (q, r_j) > 1 \) since, by (1.9), \( p \nmid \alpha_j h \) for any \( p \mid (q, r_j) \). Finally, if \( (q, r_j) = 1 \) and \( (q, \alpha_3) > 1 \), let \( p \mid (q, \alpha_3) \). Then \( p \nmid r_j \) and \( p^\sigma \mid \alpha_3 q \) for some \( \sigma \geq 2 \). As above, we consider the factor \( C_0(\alpha_j hw, p^\sigma, r_j, u_j) \) where \( p \nmid w \). However, by (2.10), \(|C_0(\alpha_j hw, p^\sigma, r_j, u_j)| = |C_{p^\sigma}(\alpha_j)| \). Since \( (\alpha_3, \alpha_j) = 1, p \mid \alpha_3 \) and \( \sigma \geq 2 \), we infer from (2.16) below that \( C_{p^\sigma}(\alpha_j) = 0 \), and so does \( C_0(\alpha_j h, \alpha_3 q, r_j, u_j) \). This proves Lemma 1.
The following lemma, especially its part (ii), provides the most crucial estimate we need in our argument in §3.

**Lemma 2.** We have (i) $\sum_{\chi \pmod{q}} |C_\chi(m, q, r, u)| \leq q^{1/2}\phi(q)$ and

(ii) $\sum_{\chi, \chi' \pmod{q}} \sum_{h=1}^q C_\chi(nh, q, r, u)C_{\chi'}(-nh, q, r, u) = q\phi(q)^2$

for any integer $n$ coprime to $r$.

**Proof.** (i) It is quite easy to establish (i). In fact, from (2.8), we have

$$\sum_{\chi \pmod{q}} |C_\chi(m, q, r, u)|^2 = \sum_{\ell_1=1}^q \sum_{\ell_2=1}^q e_q((\ell_1 - \ell_2)m) \sum_{\chi \pmod{q}} \chi(r\ell_1 - u)\chi(r\ell_2 - u)$$

$$= \phi(q) \sum_{\ell=1}^q 1 \ .$$

Hence $\sum_{\chi \pmod{q}} |C_\chi(m, q, r, u)|^2 \leq q\phi(q)$ and the desired inequality follows by applying Cauchy's inequality.

(ii) First, we write $q = q_1q_2$ such that $(r, q_2) = 1$ and every prime factor of $q_1$ appears in $r$. Accordingly, each $\chi \pmod{q}$ is factorizable as $\chi_1 \pmod{q_1}$, $\chi_2 \pmod{q_2}$. Writing $\ell = \ell_1q_1 + \ell_2q_2$, $\ell_j = 1, \cdots, q_j$ ($j = 1, 2$), we find that

$$C_\chi(nh, q, r, u) = \sum_{\ell_1=1}^{q_1} \chi_1(rq_2\ell_1 - u)e_{q_1}(\ell_1nh) \sum_{\ell_2=1}^{q_2} \chi_2(rq_1\ell_2 - u)e_{q_2}(\ell_2nh)$$

$$= C_{\chi_1}(\overline{q_2}nh, q_1, r, u)e_{q_2}(\overline{r}\overline{q_1} unh)C_{\chi_2}(\overline{r}\overline{q_1} nh) \ .$$

Here $q_2\overline{q_2} \equiv 1 \pmod{q_1}$ and $q_1\overline{q_1} \equiv 1 \pmod{q_2}$. Analogously, $\chi' \pmod{q}$ is factorizable as $\chi'_1 \pmod{q_1}, \chi'_2 \pmod{q_2}$ and we have

$$C_\chi(nh, q, r, u)C_{\chi'}(-nh, q, r, u)$$

$$= C_{\chi_1}(\overline{q_2}nh, q_1, r, u)C_{\chi_1'}(-\overline{q_2}nh, q_1, r, u)C_{\chi_2}(\overline{r}\overline{q_1} unh)C_{\chi_2'}(-\overline{r}\overline{q_1} nh) \ .$$

Summing both sides for $h = h_1q_2 + h_2q_1$ such that $h_j = 1, \cdots, q_j$ ($j = 1, 2$), we obtain, after some simplifications,

(2.11) $\sum_{\chi, \chi' \pmod{q}} \sum_{h=1}^q |C_\chi(nh, q, r, u)C_{\chi'}(-nh, q, r, u)|$

$$= \left( \sum_{\chi_1, \chi'_1 \pmod{q_1}} \sum_{h=1}^{q_1} |C_{\chi_1}(nh, q_1, r, u)C_{\chi_1'}(-nh, q_1, r, u)| \right) \times$$

$$\times \left( \sum_{\chi_2, \chi'_2 \pmod{q_2}} \sum_{h=1}^{q_2} |C_{\chi_2}(\overline{r}\overline{q_1} unh)C_{\chi_2'}(-\overline{r}\overline{q_1} nh)| \right) := \sum_1 \sum_2 \ .$$
say. Let us first examine \( \sum_2 \). For any integer \( m \) coprime to \( q_2 \), we have

\[
\sum_{h=1}^{q_2} C_{\chi_2}(nh) C_{\chi'_2}(-nh) = \sum_{h=1}^{q_2} C_{\chi_2}(nmh) C_{\chi'_2}(-nmh)
\]

\[
= \chi_2 \chi'_2(m) \sum_{h=1}^{q_2} C_{\chi_2}(nh) C_{\chi'_2}(-nh) .
\]

The first equality holds because \( h \) and \( mh \) run over the same set of integers modulo \( q_2 \). The second equality follows from the fact that \( C_{\chi_2}(mn) = \overline{\chi_2(m)} \chi_2(n) \). If \( \chi_2 \neq \chi_0 \) then there exists an \( m \) such that \( \chi_2 \chi'_2(m) \neq 1 \) and whence the sum \( \sum_{1 \leq h \leq q_2} \) in (2.12) must vanish. Thus,

\[
\sum_2 = \sum_{\chi_2(\text{mod } q_2)} \sum_{h=1}^{q_2} |C_{\chi_2}(nh)|^2
\]

\[
= \sum_{h=1}^{q_2} \sum_{\chi_2(\text{mod } q_2)} |C_{\chi_2}(nh)|^2 = \sum_{h=1}^{q_2} \phi(q_2) = q_2 \phi(q_2) ,
\]

by the same argument in (i). Next we consider \( \sum_1 \). The inner sum over \( h \) is equal to

\[
\sum_{k=1}^{q_1} \sum_{\ell=1}^{q_1} \chi_1(rk - u) \chi'_1(r\ell - u) \sum_{h=1}^{q_1} e_{q_1}((k - \ell)nh)
\]

\[
= q_1 \sum_{k=1}^{q_1} \sum_{\ell=1}^{q_1} \chi_1(rk - u) \chi'_1(r\ell - u) = q_1 \sum_{\ell=1}^{q_1} \chi_1 \chi'_1(r\ell - u)
\]

since \( (n, r) = 1 \) implies \( (n, q_1) = 1 \). Suppose \( \chi_1 \chi'_1 \) is induced by the primitive character \( \psi \) (mod \( \nu \)) with \( \nu \mid rq_1 \). Since \( r \) and \( rq_1 \) have the same set of prime factors, we have \( (r\ell - u, rq_1) = 1 \) so that \( \chi_1 \chi'_1(r\ell - u) = \psi(r\ell - u) \). Recall the well-known formula \( \psi(s) = C_{\psi}^{-1}(1) \sum_{1 \leq k \leq \nu} \overline{\psi}(k) e_{\nu}(sk) \) for primitive \( \psi \) [2, p.65], we have

\[
\sum_{\ell=1}^{q_1} \chi_1 \chi'_1(r\ell - u) = C_{\psi}^{-1}(1) \sum_{k=1}^{\nu} \overline{\psi}(k) e_{\nu}(-ku) \sum_{\ell=1}^{q_1} e_{\nu}(\ell rk) .
\]

Now \( \overline{\psi}(k) \sum_{1 \leq k \leq q_1} e_{\nu}(\ell rk) \) vanishes if \( \nu \mid rk \) or \( (\nu, k) > 1 \). So the above double sum is non-zero only if \( \nu \mid rk \) for some \( k \) coprime to \( \nu \), that is, only if \( \nu \mid r \). In that case, the sum in (2.15) is equal to \( q_1 \psi(-u) \). Since there are precisely \( \phi(r) \) primitive \( \psi \).
with modulus dividing r, we find from (2.14) that

$$
\sum_{1} = \sum_{\psi \equiv 0 \pmod{r}, \psi \text{ primitive}} \sum_{\chi_{1} \equiv 0 \pmod{r}} |q_{1}^{2}\psi(-u)| = \phi(r)\phi(rq_{1})q_{1}^{2} = q_{1}\phi(rq_{1})^{2}.
$$

Combining this with (2.13) and (2.11), we prove part (ii) of Lemma 2.

**Lemma 3.** For any integers $m, q, \nu$ with $q, \nu \geq 1$, we have

$$
\sum_{h=1}^{\nu q} e_{\nu q}(hm) = \begin{cases} 
0, & \text{if } \nu \nmid m, \\
\nu C_{q}(m/\nu), & \text{if } \nu | m.
\end{cases}
$$

**Proof.** Let $\nu = \nu_{1}\nu_{2}$ such that $(\nu_{2}, q) = 1$ and every prime factor of $\nu_{1}$ appears in $q$. By the same argument in Lemma 1(i), we show that

$$
\sum_{h=1}^{\nu q} e_{\nu q}(hm) = \sum_{h=1}^{\nu_{1}} e_{\nu_{1}\nu_{2}}(hm) = \sum_{\ell=1}^{\nu_{2}} e_{\nu_{2}}(\ell m) \sum_{k=1}^{\nu_{1}} e_{\nu_{1}}(km)
$$

$$
= \left(\sum_{\ell=1}^{\nu_{2}} e_{\nu_{2}}(\ell m)\right) C_{\nu_{1}}(m).
$$

The sum over $\ell$ will vanish if $\nu_{2} \nmid m$. Also, it is well-known that

$$
(2.16) \quad C_{q}(m) = \mu(q/(q, m))\phi(q)\phi(q/(q, m))^{-1}.
$$

Hence $C_{\nu_{1}}(m) = 0$ if there is a prime power $p^{\sigma} \parallel \nu_{1}$ such that $p^{\sigma} \nmid m$. Since $(\nu_{1}, \nu_{2}) = 1$, the first case of the lemma follows readily. The second case is straightforward.

We come now to establish the key for estimating the generating functions $S_{j}(x)$.

**Lemma 4.** Let $h, q, r, u$ be integers such that $(r, u) = 1$, $0 \leq u < r$, $1 \leq q$ and $r, q \leq Z^{10}$. Let $Z \ll Y < Z$ and

$$
W(\theta) := \sum_{Y < n \leq Z} \lambda(n - u)e(n(h^{-1}q + \theta))
$$

Then under the GRH, we have

(i) $W(\theta) = r\phi(rq)^{-1}C_{0}(h, q, r, u) \int_{Y}^{Z} c(t\theta)dt + O((r\theta Z)^{1/2}((Z|\theta|)^{1/2} + \log Z) \log Z)$ for $|\theta| \ll r \log^{-2} Z$,

(ii) $W(0) = r\phi(rq)^{-1}(Z - Y)C_{0}(h, q, r, u) + \phi(rq)^{-1} \sum_{\chi \equiv 0 \pmod{r}} C_{\chi}(h, q, r, u)\Phi_{\chi} + O(\log Z)$, where $\Phi_{\chi}$ does not depend on $h$ and it satisfies
\[ (2.17) \quad \Phi_X \ll (rZ)^{1/2} \log^2 Z. \]

**Proof.** Since \( \lambda(n) = 0 \) if \( n \) is not a prime, we see that
\[ W(\theta) = \sum_{Y < n \leq Z} \sum_{(rn-u,q)=1} \lambda(rn-u)e(n(hq^{-1} + \theta)) + O(\log q). \]

Using the orthogonality relation of the characters \( \chi \pmod{rq} \), we group the numbers \( rn-u \) according to \( n \equiv \ell \pmod{q} \). This leads to
\[ \sum_{rY-u < m \leq rZ-u} \lambda(m)\chi(m)e_r((m+u)\theta) + O(\log Z) \]
\[ = \phi(q)^{-1}e_r(u\theta) \sum_{\chi \pmod{rq}} \left( \sum_{\ell=1}^{q} \chi(\ell-u)e_q(\ell h) \right) \times \]
\[ \sum_{rY-u < m \leq rZ-u} \lambda(m)\chi(m)e_r(m\theta) + O(\log Z) \]
\[ = \phi(q)^{-1}e_r(u\theta) \sum_{\chi \pmod{rq}} C_{\chi}(h, q, r, u) H_{\chi}(\theta) + O(\log Z), \]
where \( H_{\chi}(\theta) := \sum_{rY-u < m \leq rZ-u} \lambda(m)\chi(m)e_r(m\theta). \)

It is well-known that [2, Chapter 19], for \( t \geq T \geq 2 \),
\[ (2.19) \quad \psi(t, \chi) := \sum_{n \leq t} \Lambda(n)\chi(n) = \delta_{\chi} t - \sum_{|\gamma| \leq T} t^\rho \rho^{-1} + O(tT^{-1} \log^2 (rqt)). \]

Here \( \rho = \beta + i\gamma \) are the non-trivial zeros of the \( L \)-function \( L(s, \chi) \) and \( \delta_{\chi} = 1 \) or 0 according as \( \chi \) equals to the principal character or not. Set \( T := rY-u \). Since \( \lambda(n) \) and \( \Lambda(n) \) differ only at \( n = p^\sigma \), \( \sigma \geq 2 \), we find that
\[ (2.20) \quad H_{\chi}(\theta) = \sum_{rY-u < m \leq rZ-u} \Lambda(m)\chi(m)e_r(m\theta) + O((rZ)^{1/2}) \]
\[ = \int_{T}^{rZ-u} e_r(t\theta) d\psi(t, \chi) + O((rZ)^{1/2}) \]
\[ = \delta_{\chi} \left[ \int_{T}^{rZ-u} e_r(t\theta) dt - \sum_{|\gamma| \leq T} \int_{T}^{rZ-u} t^{\beta-1+i\gamma} e_r(t\theta) dt \right] + O((1 + |\theta|Z) \log^2 Z + (rZ)^{1/2}). \]
Now
\[ \int_T^{rZ^{-u}} t^{\beta - 1 + i\gamma} e_r(t\theta) dt = r^{\beta + i\gamma} \int_{Y^{-u}r}^{Z^{-u}r-1} t^{\beta - 1 + i\gamma} e(t\theta) dt. \]

As shown in Lemma 3.2 of [3], the integral on the right side is
\[ Z^\beta |\gamma|^{-1}, \quad \text{if } |\theta| \leq |\gamma|(4\pi Z)^{-1}, \]
\[ Z^\beta |\gamma|^{-1/2}, \quad \text{if } |\gamma|(4\pi Z)^{-1} < |\theta| \leq |\gamma|(\pi Y)^{-1}, \]
\[ Z^{\beta - 1} |\theta|^{-1}, \quad \text{if } |\gamma|(\pi Y)^{-1} < |\theta|. \]

Under the GRH, \( \beta = 1/2 \). Hence, for \( Y|\theta| \geq 2 \), we have
\[ \sum_{|\gamma| \leq T} \int_T^{rZ^{-u}} t^{\beta - 1 + i\gamma} e_r(t\theta) dt \]
\[ \ll r^{1/2} \left( \sum_{|\gamma| < \pi Y|\theta|} Z^{-1/2} |\gamma|^{-1} + \sum_{\pi Y|\theta| < |\gamma| \leq 4\pi Z|\theta|} Z^{1/2} |\gamma|^{-1/2} + \sum_{4\pi Z|\theta| < |\gamma| \leq T} Z^{1/2} |\gamma|^{-1} \right) \]
\[ \ll r^{1/2} (Y Z^{-1/2} \log Z + Z^{1/2} (Y|\theta|)^{-1/2} Z|\theta| \log Z + Z^{1/2} \log^2 Z) \]
\[ \ll (rZ)^{1/2} ((Z|\theta|)^{1/2} + \log Z) \log Z, \]
by using the well-known zero counting formula:
\[ \sum_{|\gamma| \leq t} 1 = \frac{t}{\pi} \log(\frac{rt}{2\pi}) + O(t \log rq) \quad \text{for } t \geq 2. \]

For the case \( Y|\theta| < 2 \), the same estimate still holds, by using the first case in (2.21) and the trivial estimate \( \int_T^{rZ^{-u}} t^{-1/2 + i\gamma} e_r(t\theta) dt \ll (rZ)^{1/2} \). Applying these in (2.20), we have
\[ H_{\chi}(\theta) = r e_r(-u\theta) \delta_{\chi} \int_Y^Z e(t\theta) dt + O((rZ)^{1/2} ((Z|\theta|)^{1/2} + \log Z) \log Z). \]

Substitution in (2.18) then yields
\[ W(\theta) = r\phi(rq)^{-1} C_0(h, q, r, u) \int_Y^Z e(t\theta) dt + O(\log Z) \]
\[ + O(\phi(rq)^{-1} \sum_{\chi \pmod{qr}} |C_{\chi}(h, q, r, u)|(rZ)^{1/2} ((Z|\theta|)^{1/2} + \log Z) \log Z). \]

Finally, we estimate the sum in the last \( O \)-term by Lemma 2(i). This proves part (i).

When \( \theta = 0 \), we take \( \Phi_{\chi} = H_{\chi}(0) - \delta_{\chi} r(Z - Y) \), which is independent of \( h \).

By (2.19) (with \( T = rY - u \)) and the GRH,
\[ \Phi_\chi = \sum_{rZ - u < m \leq Z - u} \Lambda(m)\chi(m) + O((rZ)^{1/2}) - \delta_\chi r(Z - Y) \]
\[ = \sum_{|\gamma| \leq T} \{ (rY - u)^\rho - (rZ - u)^\rho \} \rho^{-1} + O((rZ)^{1/2}) \]
\[ \ll (rZ)^{1/2} \sum_{|\gamma| \leq T} \frac{1}{Z} + i|\gamma|^{-1} \ll (rZ)^{1/2} \log^2 Z. \]

Part (ii) now follows from (2.18). This completes the proof of Lemma 4.

Verifying the hypotheses by means of (2.4), (2.6), (2.3) and (2.1), we obtain from Lemma 4 the following formulas which will be used in the next section:

\[ S_3(\alpha_3^{-1}(hq^{-1} + \theta)) = r_3 \phi(r_3q)^{-1} C_0(h, q, r_3, u_3) \int_{N_3'} e(t\theta)dt \]
\[ + O((r_3qN_3)^{1/2}((N_3|\theta|)^{1/2} + \log N) \log N) \]
for \( q \leq r^{-1}, |\theta| \leq \tau q^{-1}. \)

\[ S_j(h(\alpha_3q)^{-1}) = r_j \phi(r_j\alpha_3q)^{-1} (N_j - N_j') C_0(\alpha_j h, \alpha_3q, r_j, u_j) \]
\[ + O(\phi(r_j\alpha_3q)^{-1} \sum_{\chi(\text{mod } r_j\alpha_3q)} C_\chi(\alpha_j h, \alpha_3q, r_j, u_j) \Phi_\chi + \log N) \]
for \( q \leq Q, j = 1, 2. \) Furthermore, with \( h = \theta = 0, q = 1, \) Lemma 4(i) together with (2.1) gives

\[ S_j(0) \ll N_j r_j \phi(r_j)^{-1} \quad \text{for} \quad j = 1, 2. \]

3. Proof of Theorem 2

We now proceed to prove Theorem 2 by establishing that \( I_1(N) \gg \Omega \) and \( I_2(N) \ll \varepsilon \Omega. \) The constants implied in the symbols \( \ll, \gg \) and \( O \) are independent of \( \varepsilon. \)

Let us consider \( I_2(N) \) first. Take any \( x \in \mathcal{M}'. \) By Dirichlet’s theorem on diophantine approximation, there exist coprime integers \( h \) and \( q \) such that \( 1 \leq q \leq r^{-1} \) and \( \theta := \alpha_3 x - hq^{-1} \) satisfies \( |\theta| < \tau q^{-1}. \) Since \( x \geq \tau / \alpha_3, \) we have \( 1 \leq h. \) If \( q \leq Q, \) then the two facts: \( 2\tau Q < 1 \) and \( \alpha_3 x < \alpha_3 + \tau \) together imply \( h \leq \alpha_3 q \) and hence \( x \in m(h, q) \) for some \( q \leq Q. \) This contradicts that \( x \in \mathcal{M}'. \) Thus, it
must be \(q > Q\). Now, with the help of Lemma 1 (ii), (2.16) and (2.4), we deduce from (2.22) that

\[
S_3(x) = S_3(\alpha_3^{-1}(hq^{-1} + \theta))
\leq r_3\phi(r_3q)^{-1} N_3 + (r_3qN_3)^{1/2} \log^2 N + N_3(r_3q|\theta|)^{1/2} \log N
\leq Q^{-1} N_3 \log \log N + (r_3^{-1} N_3)^{1/2} \log^2 N + N_3(r_3\tau)^{1/2} \log N
\leq Q^{-1} N_3 \log \log N + r_3^{1/2} N_3^{3/4} \log^{3/2} N
\]

for any \(x \in \mathcal{M}'\). Hence

\[
(3.1) \quad I_2(N) = \int_{\mathcal{M}'} e(-\kappa x) \prod_{j=1}^{3} S_j(x) dx
\leq (Q^{-1} N_3 \log \log N + r_3^{1/2} N_3^{3/4} \log^{3/2} N) \int_{\frac{1}{\alpha_3}}^{1+\frac{1}{\alpha_3}} |S_1(x)S_2(x)| dx .
\]

Applying Cauchy’s inequality, the last integral is

\[
\leq \prod_{j=1}^{2} \left( \int_{\frac{1}{\alpha_3}}^{1+\frac{1}{\alpha_3}} |S_j(x)|^2 dx \right)^{1/2} = \prod_{j=1}^{2} \left( \sum_{N_j' < n \leq N_j} \lambda(r_jn - u_j)^2 \right)^{1/2}
\leq (\log N) \prod_{j=1}^{2} S_j(0)^{1/2} \leq (\log N) \prod_{j=1}^{2} (N_j r_j \phi(r_j)^{-1})^{1/2} ,
\]

by (2.24). Hence, from (3.1), (2.6), (2.3), (2.1) and (2.5), we find that \(I_2(N) \ll \varepsilon \Omega\) as desired.

Next, we turn to \(I_1(N)\), the main contribution in (2.7). As above, we substitute \(S_3(\alpha_3^{-1}(hq^{-1} + \theta))\) from (2.22). The \(O\)-term there contributes \(\ll \varepsilon \Omega\) to \(I_1(N)\), as it can be seen by the same argument for \(I_2(N)\) in (3.1). Therefore, we can now write

\[
(3.2) \quad I_1(N) = O(\varepsilon \Omega) +
\]

\[
+ r_3\alpha_3^{-1} \sum_{q \leq Q} \phi(r_3q)^{-1} \sum_{N_j' < n \leq N_j} \prod_{j=1,2} \lambda(r_jn - u_j) \sum_{h=1}^{\alpha_3 q} C_0(h, q, r_3, u_3) \times
\]

\[
\times e^{\alpha_3 q(h(\alpha_1 n_1 + \alpha_2 n_2 - \kappa))} \int_{N_j}^{N_j^3} \int_{-\tau/q}^{\tau/q} e^{(\alpha_3^{-1}(\alpha_1 n_1 + \alpha_2 n_2 + \alpha_3 t - \kappa)\theta)} d\theta dt .
\]

The double integral \(\int_{N_j}^{N_j^3} \int_{-\tau/q}^{\tau/q}\) is equal to \(\pi^{-1} \int_{\xi_1}^{\xi_2} z^{-1} \sin z \, dz\), where

\[
\xi_1 := \frac{2\pi\tau}{\alpha_3 q}(\alpha_1 n_1 + \alpha_2 n_2 + \alpha_3 N_j' - \kappa) , \quad \xi_2 := \frac{2\pi\tau}{\alpha_3 q}(\alpha_1 n_1 + \alpha_2 n_2 + \alpha_3 N_3 - \kappa) .
\]
We now choose the constants $c_j, c'_j$ as follow: In case (i) of Theorem 3, that is, when all $\alpha_1, \alpha_2, \alpha_3$ are positive, we set $c_1 = c_2 = 1/2, c_3 = 5/4$ and $c_j' = 1/4$ for $j = 1, 2, 3$. In case (ii), that is, not both $\alpha_1, \alpha_2$ are positive, say $\alpha_1 < 0$, we take $c_1 = 32, c_1' = 28, c_2 = 2, c_2' = 1, c_3 = 48$ and $c_3' = 12$. In view of (2.2), we find, in both cases, that $\xi_2 \geq \pi \tau N (2\alpha_3q)^{-1}$ and $\xi_1 \leq -\pi \tau N (2\alpha_3q)^{-1}$. Hence

$$\pi^{-1} \int_{\xi_1}^{\xi_2} z^{-1} \sin z \, dz = 1 + O(|\xi_1|^{-1} + \xi_2^{-1}) = 1 + O((\alpha_3q)(\tau N)^{-1}).$$

Let $E_1$ be the contribution of the above $O$-term to $I_1(N)$ in (3.2). Then plainly

$$E_1 \ll r_3(\tau N)^{-1} \sum_{q \leq Q} \phi(r_3q)^{-1} \sum_{N_j' < n_j \leq N_j} \prod_{j=1}^{2} \lambda(r_jn_j - u_j) \times \left| \sum_{\substack{\alpha_3q \in \mathbb{Z} \cap \langle h,q \rangle = 1 \atop h = 1}} C_0(h, q, r_3, u_3)e_{\alpha_3q}(h(\alpha_1n_1 + \alpha_2n_2 - \kappa)) \right| .$$

Denote by $\sum_{(h)}$ the above inner sum over $h$. By Lemma 1(ii) and (2.16) we see that $C_0(h, q, r_3, u_3) = 0$ if $(q, r_3) > 1$ and $C_0(h, q, r_3, u_3) = \mu(q)e_q(hu_3r_3)$ if $(q, r_3) = 1$. Here $r_3r_3 \equiv 1 \pmod{q}$. Thus, for $(q, r_3) = 1$, we have

$$\sum_{(h)} = \mu(q) \sum_{h = 1}^{\alpha_3q} e_{\alpha_3q}(h(\alpha_1n_1 + \alpha_2n_2 + \alpha_3u_3r_3 - \kappa)) .$$

According to Lemma 3, the last sum vanishes if $\alpha_3 \not|\alpha_1n_1 + \alpha_2n_2 - \kappa$. Otherwise, we have $\sum_{(h)} \ll \alpha_3\phi(q)$. Consequently,

$$E_1 \ll r_3\alpha_3(\tau N \phi(r_3))^{-1} \sum_{q \leq Q} \sum_{n_1}^{n_2} \sum_{\alpha_3|\alpha_1n_1 + \alpha_2n_2 - \kappa} \prod_{j=1}^{2} \lambda(r_jn_j - u_j) \ll r_3\alpha_3(\tau N \phi(r_3))^{-1} Q^2 \sum_{n_1}^{n_2} \lambda(r_1n_1 - u_1) \sum_{\alpha_2n_2 \equiv \kappa - \alpha_1n_1 \pmod{\alpha_3}} \log N \ll r_3\alpha_3(\tau N \phi(r_3))^{-1} Q^2(N_2\alpha_3^{-1}S_1(0) \log N) \ll \varepsilon \Omega ,$$

by (2.4), (2.6), (2.24), (2.3), (2.5) and (2.1). Hence, when (3.3) is substituted in (3.2), we have

$$I_1(N) = O(\varepsilon \Omega) +$$

$$+ r_3\alpha_3^{-1} \sum_{q \leq Q} \phi(r_3q)^{-1} \sum_{\substack{\alpha_3q \in \mathbb{Z} \cap \langle h,q \rangle = 1 \atop h = 1}} C_0(h, q, r_3, u_3)e_{\alpha_3q}(-h\kappa)S_1(h(\alpha_3q)^{-1})S_2(h(\alpha_3q)^{-1}) .$$
The next step is to approximate $S_j(h(\alpha_3 q)^{-1})$ ($j = 1, 2$) by the formula in (2.23). For simplicity, let us rewrite the formula as $S_j = M_j + O(R_j)$ where $M_j$ is the main term and $R_j$ is the remainder. Then we have

$$(3.4) \quad I_1(N) = r_3 \alpha_3^{-1} \sum_{q \leq Q} \phi(r_3 q)^{-1} \sum_{h = 1}^{\alpha_3 q} C_0(h, q, r_3, u_3) e_{\alpha_3 q}(-hk)(M_1 M_2 + O(|M_1 R_2 + |M_2 R_1 + R_1 R_2| + O(\varepsilon \Omega)).$$

The three terms inside the $O$-symbol are to be estimated by similar arguments. Consider, for instance, the term $|M_1| R_2$ and let $E_2$ be its total contribution to the right side of (3.4). Then by Cauchy's inequality, we have

$$(3.5) \quad E_2 \ll r_3 \alpha_3^{-1} \sum_{q \leq Q} \phi(r_3 q)^{-1} \left( \sum_{h = 1}^{\alpha_3 q} |C_0(h, q, r_3, u_3)|^{2} \right)^{1/2} \left( \sum_{h = 1}^{\alpha_3 q} |R_2|^2 \right)^{1/2}.$$

Let $j = 1, 2$. With reference to (2.23), we see that

$$C_0(h, q, r_3, u_3) M_j = r_j \phi(r_j \alpha_3 q)^{-1}(N_j - N_j') C_0(h, q, r_3, u_3) C_0(\alpha_j h, \alpha_3 q, r_j, u_j),$$

and Lemma 1 (ii), (iii) show that this will vanish if $(q, r_j r_3 \alpha_3) > 1$. So we consider only those $q$'s such that $(q, r_j r_3 \alpha_3) = 1$. In this case, applying Lemma 1 (i), (ii), we have

$$|C_0(h, q, r_3, u_3) M_j| \ll r_j \phi(r_j \alpha_3 q)^{-1} N_j |C_q(\alpha_j)| |C_0(\alpha_j h \overline{q}, \alpha_3, r_j, u_j)|$$

where $q \overline{q} \equiv 1 \pmod{\alpha_3}$. Since $|C_q(\alpha_j)| \leq (q, \alpha_j)$, we deduce that

$$\left( \sum_{h = 1}^{\alpha_3 q} |C_0(h, q, r_3, u_3) M_j|^2 \right)^{1/2} \ll r_j \phi(r_j \alpha_3 q)^{-1} N_j (q, \alpha_j) \phi(q)^{1/2} \left( \sum_{h = 1}^{\alpha_3} |C_0(\alpha_j h \overline{q}, \alpha_3, r_j, u_j)|^2 \right)^{1/2}$$

$$= r_j \phi(r_j \alpha_3 q)^{-1} N_j (q, \alpha_j) (\alpha_3 \phi(q))^{1/2} \left( \sum_{\ell = 1}^{\alpha_3} 1 \right)^{1/2}$$

$$\ll r_j \alpha_3 (\phi(r_j) \phi(\alpha_3))^{-1} \phi(q)^{-1/2} (q, \alpha_j) N_j.$$
\[
\sum_{h=1}^{q_3} |R_j|^2 \ll \phi(r_j \alpha_3 q)^{-2} \sum_{h=1}^{q_3} \sum_{\chi \mod r_j \alpha_3} C_{\chi}(\alpha_j h, \alpha_3 q, r_j, u_j) \Phi_{\chi}^2 + \alpha_3 q \log^2 N
\]

\[
= \phi(r_j \alpha_3 q)^{-2} \sum_{\chi, \chi' \mod r_j \alpha_3} \Phi_{\chi} \Phi_{\chi'} \sum_{h=1}^{q_3} C_{\chi'}(\alpha_j h, \alpha_3 q, r_j, u_j) C_{\chi'}(-\alpha_j h, \alpha_3 q, r_j, u_j) + \alpha_3 q \log^2 N.
\]

Invoking (2.17) and then Lemma 2(ii), we see that the last expression is

\[
\ll \phi(r_j \alpha_3 q)^{-2} r_j N_j \alpha_3 q \phi(r_j \alpha_3 q)^2 \log^4 N = \alpha_3 q r_j N_j \log^4 N.
\]

Collecting these estimates into (3.5), we find that

\[
E_2 \ll r_1 r_3 \alpha_3 (\alpha(r_1) \phi(r_3) \phi(\alpha_3))^{-1} N_1 (N_2 r_2 \alpha_3^{-1})^{1/2} \log^2 N (\log \log Q)^{3/2} \sum_{q \leq Q} q^{-1}(q, \alpha_1).
\]

The last sum over \( q \) is

\[
\leq \sum_{k|\alpha_1} k \sum_{q \leq Q} q^{-1} = \sum_{k|\alpha_1} \sum_{q \leq Q} q^{-1} \ll \sum_{k|\alpha_1} \log Q \ll |\alpha_1|^{1/2} \log Q.
\]

Hence, \( E_2 \ll N^{3/2} r_2^{1/2} |\alpha_1 \alpha_2 \alpha_3|^{-1/2} \log^4 N \ll \varepsilon \Omega \), by (2.3), (2.5) and (2.1). The same bound holds for the contributions from \( |M_2| R_1 \) and \( R_1 R_2 \) in (3.4). We therefore have

(3.6) \( I_1(N) = r_3 \alpha_3^{-1} \sum_{q \leq Q} \phi(r_3 q)^{-1} \sum_{h=1}^{q_3} C_0(h, q, u_3) M_1 M_2 e_\alpha q (-h \kappa) + O(\varepsilon \Omega) \)

\[
= (c_1 - c'_1)(c_2 - c'_2) N^2 |\alpha_1 \alpha_2 \alpha_3|^{-1} r_1 r_2 r_3 \sum_{q \leq Q} \{\phi(r_3 q) \phi(r_1 \alpha_3 q) \phi(r_2 \alpha_3 q)\}^{-1} T(q) + O(\varepsilon \Omega)
\]

where

\[
T(q) := \sum_{h=1}^{q_3} C_0(h, q, u_3) C_0(\alpha_1 h, \alpha_3 q, r_1, u_1) C_0(\alpha_2 h, \alpha_3 q, r_2, u_2) e_\alpha q (-h \kappa).
\]

Let us first examine \( T(q) \). Using Lemma 1(ii), (iii), we see that the summand in \( T(q) \) will vanish if \( (q, r_1 r_2 r_3 \alpha_3) > 1 \). For those \( q \)'s such that \((q, r_1 r_2 r_3 \alpha_3) = 1\),
we find by Lemma 1 (i), (ii) that

\[
C_0(h, q, r_3, u_3) \prod_{j=1}^{2} C_0(\alpha_j h, \alpha_3 q, r_j, u_j) =
\]

\[
= C_q(1) e_q(\bar{r}_3 u_3 h) \prod_{j=1}^{2} C_q(\alpha_j) e_q(r_j u_j \alpha_j \bar{r}_3 h) C_0(\alpha_j h q, \alpha_3, r_j, u_j)
\]

where \( q \bar{r}_3 \equiv 1 \pmod{\alpha_3} \). If we write \( h = h_1 \alpha_3 + h_2 q \) with \( h_1 = 1, \cdots, q, (h_1, q) = 1 \) and \( h_2 = 1, \cdots, \alpha_3 \), then for \( (q, r_1 r_2 r_3 \alpha_3) = 1 \) we have

\[
T(q) = C_q(1) C_q(\alpha_1) C_q(\alpha_2) \sum_{h=1}^{q} e_q(h_1(\alpha_1 \bar{r}_1 u_1 + \alpha_2 \bar{r}_2 u_2 + \alpha_3 \bar{r}_3 u_3 - \kappa)) \times
\]

\[
\times \sum_{h=1}^{\alpha_3} e_{\alpha_3}(-h_2 \kappa) \prod_{j=1}^{2} C_0(\alpha_j h_2, \alpha_3, r_j, u_j)
\]

\[
= \mu(q) C_q(\alpha_1) C_q(\alpha_2) C_q(\eta) F(\alpha_3),
\]

where \( \eta := \alpha_1 \bar{r}_1 u_1 + \alpha_2 \bar{r}_2 u_2 + \alpha_3 \bar{r}_3 u_3 - \kappa, r_j \bar{r}_j \equiv 1 \pmod{q} \) and

\[
F(n) := \sum_{h=1}^{n} e_n(-h \kappa) \prod_{j=1}^{2} C_0(\alpha_j h, n, r_j, u_j)
\]

for any positive integer \( n \). Substituting this into (3.6), we have

\[
(3.7) \quad I_1(N) = (c_1 - c'_1)(c_2 - c'_2) N^2 |\alpha_1 \alpha_2 \alpha_3|^{-1} r_1 r_2 r_3 \{\phi(r_3) \phi(\alpha_3) \phi(\alpha_2)\}^{-1} \times
\]

\[
\times F(\alpha_3) \sum_{q \leq Q} \mu(q) C_q(\alpha_1) C_q(\alpha_2) C_q(\eta) \phi(q)^{-3} + O(\epsilon \Omega).
\]

Since \( |C_q(\alpha_1) C_q(\alpha_2) C_q(\eta)| \leq \alpha_1 \alpha_2 \phi(q) \), we see that the above sum over \( q \) converges absolutely. Let \( \xi \) be its limit. Then

\[
\xi = \sum_{q=1}^{\infty} \mu(q) C_q(\alpha_1) C_q(\alpha_2) C_q(\eta) \phi(q)^{-3}
\]

\[
= \prod_{p \nmid r_1 r_2 r_3 \alpha_3} (1 - C_p(\alpha_1) C_p(\alpha_2) C_p(\eta) \phi(p)^{-3})
\]

since \( C_q(m) \) is multiplicative in \( q \). For each \( p \nmid r_1 r_2 r_3 \alpha_3 \), let \( \omega(p) \) be the number of the integers \( \alpha_1, \alpha_2, \eta \) which are divisible by \( p \). Then

\[
\xi = \prod_{p \nmid r_1 r_2 r_3 \alpha_3} (1 - (-\phi(p))^{\omega(p)-3}).
\]
Furthermore, $(\alpha_1, \alpha_2) = 1$ shows that $0 \leq \omega(p) \leq 2$. Thus, $1 - (\phi(p))^{\omega(p) - 3} \geq 1 - \phi(p)^{-2} \geq 1 - 3p^{-2}$ for $p \geq 3$. For $p = 2$, the condition (1.11) ensures that $\omega(2) \neq 1$ if $2 \nmid r_1 r_2 r_3 \alpha_3$. Hence $1 - (\phi(2))^{\omega(2) - 3} = 2$ and

$$
(3.8) \quad \xi \geq \prod_{p \nmid 2r_1 r_2 r_3 \alpha_3} (1 - 3p^{-2}) \gg 1.
$$

We turn now to $F(n)$. Similar to Lemma 1(i), we can show that $F(n)$ is multiplicative in $n$. Furthermore, if $p^\sigma \| \alpha_3$ then

$$
F(p^\sigma) = \sum_{\ell_1 = 1}^{p^\sigma} \sum_{\ell_2 = 1}^{p^\sigma} \sum_{h = 1}^{p^\sigma} e_{p^\sigma} (h(\alpha_1 \ell_1 + \alpha_2 \ell_2 - \kappa))
$$

$$
= p^\sigma \times \text{card}\{\ell_1, \ell_2 : 1 \leq \ell_1, \ell_2 \leq p^\sigma, p \nmid r_1 \ell_i - u_j, \alpha_1 \ell_1 + \alpha_2 \ell_2 \equiv \kappa \pmod{p^\sigma}\}.
$$

Since $p|\alpha_3$ and $(\alpha_2, \alpha_3) = 1$, each given $\ell_1$ determines one $\ell_2$ (mod $p^\sigma$) by the congruence $\alpha_1 \ell_1 + \alpha_2 \ell_2 \equiv \kappa$ (mod $p^\sigma$). Hence

$$
F(p^\sigma) = p^\sigma \times \text{card}\{\ell : 1 \leq \ell \leq p^\sigma, p \nmid r_1 \ell - u_1, p \nmid r_2 (\kappa - \alpha_1 \ell) - \alpha_2 u_2\}
$$

$$
= p^{2\sigma - 1} \times \text{card}\{\ell : 1 \leq \ell \leq p, p \nmid r_1 \ell - u_1, p \nmid r_2 (\kappa - \alpha_1 \ell) - \alpha_2 u_2\}
$$

$$
= p^{2\sigma - 1}(p - \nu(p)),
$$

where $\nu(p) = 0$ if $p|(r_1, r_2)$, $\nu(p) = 1$ if $p$ divides exactly one of $r_1, r_2$, and $\nu(p) = 1$ or 2 if $p \nmid r_1 r_2$. The case $\nu(p) = 2$ occurs only if $p \nmid r_1 r_2$ and $\alpha_1 r_2 u_1 + \alpha_2 r_1 u_2 \neq r_1 r_2 \kappa$ (mod $p$). In particular, condition (1.11) ensures that such situation will not occur for $p = 2$, that is, $\nu(2) \leq 1$ if $2|\alpha_3$. Hence

$$
F(\alpha_3) = \prod_{p^\sigma \| \alpha_3} p^{2\sigma - 1}(p - \nu(p)) = \alpha_3^2 \prod_{p \nmid (\alpha_3, r_1, r_2)} p^{(1 - \nu(p))} \prod_{p \nmid \alpha_3} (1 - \nu(p))
$$

$$
> \alpha_3^2 \prod_{p \nmid (\alpha_3, r_1, r_2)} (1 - p^{-1}) \prod_{p \nmid \alpha_3} (1 - 2p^{-1})
$$

$$
> \alpha_3^2 \prod_{p \nmid (\alpha_3, r_1, r_2)} (1 - p^{-1}) \prod_{p \nmid \alpha_3} (1 - p^{-1})^2 = \alpha_3^2 \prod_{p \nmid \alpha_3} (1 - \frac{1}{p}) \prod_{p \nmid \alpha_3} (1 - \frac{1}{p}).
$$

Applying this and (3.8) in (3.7), we conclude that, when $Q$ is sufficiently large
\[ I_1(N) \gg N^2 |\alpha_1 \alpha_2 \alpha_3|^{-1} r_1 r_2 r_3 \{\phi(r_3) \phi(r_1 \alpha_3) \phi(r_2 \alpha_3)\}^{-1} \alpha_3^2 \times \]
\[ \prod_{p|\alpha_3} (1 - p^{-1}) \prod_{p \nmid \alpha_3} (1 - p^{-1}) \xi + O(\varepsilon \Omega) \]
\[ \gg N^2 |\alpha_1 \alpha_2 \alpha_3|^{-1} r_1 r_2 r_3 \{\phi(r_1) \phi(r_2) \phi(r_3)\}^{-1} + O(\varepsilon \Omega) . \]

In view of (2.5) and (2.1), when \( \varepsilon \) is sufficiently small, we have \( I(N) = I_1(N) + O(\varepsilon \Omega) \gg \Omega \), as desired. This completes the proof of Theorem 2.

Acknowledgement

This paper was written while the third author was a Senior Visiting Fellow at the Mathematical Institute of Oxford University. The visit was supported by a Commonwealth Fellowship awarded by The Commonwealth Scholarship Commission in the United Kingdom.

References