TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 322, Number 1, November 1990

UNUSUALLY LARGE GAPS BETWEEN CONSECUTIVE PRIMES

HELMUT MAIER AND CARL POMERANCE

ABSTRACT. Let $G(x)$ denote the largest gap between consecutive primes below x. In a series of papers from 1935 to 1963, Erdös, Rankin, and Schönhage showed that

$$G(x) \geq (c + o(1)) \log x \log\log x \log\log\log\log x (\log\log\log x)^{-2},$$

where $c = e^{\gamma}$ and γ is Euler's constant. Here, this result is shown with $c = c_0 e^{\gamma}$ where $c_0 = 1.31256\ldots$ is the solution of the equation $4/c_0 - e^{-4/c_0} = 3$. The principal new tool used is a result of independent interest, namely, a mean value theorem for generalized twin primes lying in a residue class with a large modulus.

1. INTRODUCTION

Let $G(x)$ denote the largest gap between consecutive primes below x. More precisely, for $x \geq 2$, $G(x) := \max_{p \leq x}(p' - p)$, where p, p' are consecutive primes.

Cramér [2] conjectured that $\limsup G(x)/\log^2 x = 1$, while Shanks [15] made the stronger conjecture that $G(x) \sim \log^2 x$, but we are still a long way from proving these statements. Concerning upper bounds, the best that is known is a very recent of Lou and Yao [8]: $G(x) \ll x^{7/13+\varepsilon}$ for every $\varepsilon > 0$.

Since the prime number theorem immediately gives $G(x) \geq (1 + o(1)) \log x$, one might think that establishing the lower bound implicit in Shanks' conjecture is not too hard. However, the best that is known is

$$G(x) \geq (e^{\gamma} + o(1)) \log x \log\log x \log\log\log\log x (\log\log\log x)^{-2}, \tag{1.1}$$

where γ is Euler's constant. The result (1.1) is due to Rankin [13] in 1963. Erdös [3] had already obtained (1.1) without the $\log\log\log\log x$ factor and with an inexplicit constant factor in 1935. Rankin [12] obtained (1.1) with the constant $1/3$ in 1938, while Schönhage [14] in 1963 proved (1.1) with the constant $e^{\gamma}/2$. Known now as the Erdös-Rankin problem, this paper is concerned with improving (1.1).

All of the cited lower bound attacks on $G(x)$ have done so via the Jacobsthal function $j(n)$, the maximal gap between consecutive integers coprime to n.

Received by the editors November 21, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11N05.
Both authors were supported in part by NSF grants.

0002-9947/90 $1.00 + $.25 per page

Thus if $J(x) := \max_{n \le x} j(n)$, then it is easy to see that for $x \ge 7$,

$$G(x) \ge J(x). \tag{1.2}$$

Thus (1.1) is shown by proving the same inequality for $J(x)$.

From sieve methods it is easy to show that $J(x) \ll (\log x)^K$ for some K. The best that is known along these lines is $J(x) \ll \log^2 x$, a result of Iwaniec [6].

In this paper we show that if $c_0 = 1.31256\ldots$ is the solution of the equation

$$4/c_0 - e^{-4/c_0} = 3, \tag{1.3}$$

then

$$J(x) \ge (c_0 e^{\gamma} + o(1)) \log x \log\log x \log\log\log\log x (\log\log\log x)^{-2}, \tag{1.4}$$

and so, via (1.2), we have the same lower bound for $G(x)$.

It is disappointing that we are only able to improve on the constant factor in (1.1). However, unlike the earlier improvements on the constant factor, which essentially just used sharper analytic tools in the basic argument, the proof of (1.4) involves a new idea. This idea, if combined with a strong form of the prime k-tuples conjecture, supports the assertion

$$J(x) \ge \log x (\log\log x)^{2+o(1)}. \tag{1.5}$$

In fact; we conjecture that equality holds in (1.5). This, of course, would not contradict Cramér's conjecture, since presumably much is lost in the inequality (1.2).

The prime k-tuples conjecture is itself a generalization of the still unproved twin prime conjecture. However, there has been progress on problems of this type of a statistical nature. For example, Montgomery and Vaughan [10], using a variant of the Hardy-Littlewood circle method, have shown the existence of a positive constant $\delta > 0$ such that the number of even numbers up to x that are not the sum of 2 primes is at most $x^{1-\delta}$. Of course, the still unproved conjecture of Goldbach is that every even number exceeding 2 is the sum of 2 primes. The method of Montgomery and Vaughan would also show that the number of even numbers up to x that are not the difference of 2 primes below $2x$ is at most $x^{1-\delta}$.

The principal technical difficulty in this paper is the establishment of a similar result where the primes are restricted to an arithmetic progression. Specifically, if $T(x, n, l, M)$ denotes the number of primes $p \le x$ with $p \equiv l \bmod M$ and $p + n$ prime, then we show there is some absolute constant $c_1 > 0$ such that

$$\sum_{\substack{n \le x \\ n \equiv 0 \bmod 2}} \sum_{M \le x^{c_1}} \max_{l \ (l, M) = (n+l, M) = 1} \left| T(x, n, l, M) - \frac{\alpha_0 T(x, n)}{\varphi(M)} \prod_{\substack{p \mid Mn \\ p > 2}} \frac{p-1}{p-2} \right| \ll_E x^2 (\log x)^{-E} \tag{1.6}$$

for any E, where p denotes a prime, α_0 is the twin prime constant

$$\alpha_0 := 2\prod_{p>2}\frac{p(p-2)}{(p-1)^2} = 1.3203\ldots \tag{1.7}$$

and

$$T(x, n) := \sum_{1<k\le x}\frac{1}{\log k \log(k+n)}.$$

It should be pointed out that Lavrik [7] already achieved a result similar to (1.6) but with a much smaller range of the moduli M, too small for our purposes. Our proof follows the general outline of the argument in Montgomery and Vaughan [10]. In one respect our task is simpler—we do not need to treat a possible exceptional character corresponding to a Siegel zero with any special finesse, using only Siegel's theorem. However, in other respects our argument is considerably more involved than that of [10].

The paper is organized as follows. In §2 we outline the basic argument. §3 presents a slightly different version of (1.6) and a key consequence. In §4 we show how these theorems are used to prove our main result (1.4). §5 cleans up some details from §2. The remainder of the paper, §6–12, is used to establish the results described in §3.

Concerning notation, the letter p shall always denote a prime. The letters q and r (without a subscript) also represent primes through §5, after which they represent natural numbers.

2. The basic argument

The prime factors of an integer n are said to *sieve out* a set S if there is a residue class $a_p \bmod p$ for each prime $p|n$ such that each $s \in S$ satisfies at least one of the congruences $s \equiv a_p \bmod p$. Let $j'(n)$ denote the largest integer such that the prime factors of n sieve out $\{1, 2, \ldots, j'(n)\}$. From the Chinese Remainder Theorem one easily gets that $j'(n) = j(n) - 1$. With a change of notation from the introduction, our principal result (1.4) follows from the following theorem. Let $P(x)$ denote the product of the primes up to x.

Theorem 2.1. *With c_0 given by (1.3), we have*

$$j'(P(x)) \ge (c_0 e^{\gamma} + o(1))x \log x \log\log\log x (\log\log x)^{-2}.$$

Indeed, using the prime number theorem in the form $\log P(x) \sim x$, Theorem 2.1 immediately implies (1.4).

We now introduce some notation. Let $1 < c' < c_0$ be arbitrarily close to c_0, but fixed. Let c'', ε be fixed so that

$$c'' = \frac{c'}{1-\varepsilon} < c_0, \qquad 0 < \varepsilon < \frac{1}{2}.$$

Let

$$U := c' e^{\gamma} x \log x \log\log\log x (\log\log x)^{-2},$$
$$z := x/\log\log x,$$
$$y := \exp\{(1-\varepsilon)\log x \log\log\log x/\log\log x\}.$$

To prove Theorem 2.1 it will be sufficient to show that for x sufficiently large, the prime factors of $P(x)$ sieve out the integers in $[1, U]$. We show this by choosing

$$a_p = 0 \quad \text{for every prime } p \in (y, z],$$
$$a_p = 1 \quad \text{for every prime } p \le y,$$

and a_p "optimally" for every prime $p \in (z, x]$. It is in this last interval that our argument parts company from previous attacks.

We shall call the deletion of the integers in $[1, U]$ that are $0 \bmod p$ for some $p \in (y, z]$, the first sieving, and we shall call the set of remaining integers in $[1, U]$, the first residual set. Similarly, we call the deletion of the integers from the first residual set that are $1 \bmod p$ for some $p \le y$, the second sieving, and we shall call the set of remaining integers the second residual set. The heart of our argument will be with the third sieving, or the removal of the integers from the second residual set which are $a_p \bmod p$ for some $p \in (z, x]$. We must prove that the a_p can be so chosen that for x large enough, this third sieving can sieve out the second residual set.

The first residual set is evidently the disjoint union $\mathbf{R}_{(1)} \cup \mathbf{R}_{(2)}$, where $\mathbf{R}_{(1)}$ is the set of integers in $[1, U]$ divisible by some prime $p > z$ and $\mathbf{R}_{(2)}$ is the set of integers in $[1, U]$ divisible by no prime exceeding y.

Let $\mathbf{R}$ be the members of the second residual set that are in $\mathbf{R}_{(1)}$ and let $\mathbf{R}'$ be the members of the second residual set that are in $\mathbf{R}_{(2)}$. Thus

$$\mathbf{R} = \bigcup_{m \le U/z} \mathbf{R}_m,$$

where

$$\mathbf{R}_m := \{mp : z < p \le U/m, (mp - 1, P(y)) = 1\}, \tag{2.1}$$

and

$$\mathbf{R}' := \{n \le U : p|n \Rightarrow p \le y, q|n-1 \Rightarrow q > y\}. \tag{2.2}$$

The estimation of $|\mathbf{R}|$ and $|\mathbf{R}'|$, where $|\ |$ denotes cardinality, is somewhat more difficult than in Rankin [13], but can be handled by standard sieve arguments. In §5 we will show

$$|\mathbf{R}| \sim \frac{c'}{1-\varepsilon}\frac{x}{\log x} = c''\frac{x}{\log x}, \tag{2.3}$$

$$|\mathbf{R}'| \ll \frac{x}{(\log x)^{1+\varepsilon}}. \tag{2.4}$$

To complete the proof we must show that the primes in $[z, x]$ can sieve out $\mathbf{R} \cup \mathbf{R}'$. The traditional argument is to use each prime in $(z, x]$ to delete a single member of $\mathbf{R} \cup \mathbf{R}'$. Since there are $(1 + o(1))x/\log x$ primes in $(z, x]$, if we had chosen $c_0 = 1$ so that $c'' < 1$, then (2.3) and (2.4) show that this strategy will succeed. What we will show below is that for a certain positive proportion of the primes in $(z, x]$, we can remove two members of $\mathbf{R} \cup \mathbf{R}'$ and so we may choose c_0 somewhat larger than 1.

If $\mathbf{R} \cup \mathbf{R}'$ can be viewed as a random set of residues mod q for each prime $q \in (z, x]$ and these are "independent events" for the different values of q, then we would expect to be able to remove $(\log x)^{1+o(1)}$ members of $\mathbf{R} \cup \mathbf{R}'$ for a positive proportion of these q's. If such an argument could be made rigorous we would have a proof of (1.5).

However, the set $\mathbf{R} \cup \mathbf{R}'$ is not random. For a fixed prime $q \in (z, x]$, we do not and cannot show there are even *two* members of $\mathbf{R} \cup \mathbf{R}'$ that are congruent mod q. In fact, we cannot even show there are two members of the first residual set $\mathbf{R}_{(1)} \cup \mathbf{R}_{(2)}$ that are congruent mod q (for a fixed q not too close to the lower end of $(z, x]$). What we do show is of a statistical nature: for most primes $q \in (z, x]$ there are many pairs of members of $\mathbf{R}$ that are congruent mod q.

To show that for most primes q there are many pairs of members of $\mathbf{R}_{(1)}$ that are congruent mod q is standard and follows from the same arguments that show the exceptional set in Goldbach's conjecture is small. What is needed now though is that a fair number of these pairs (in fact, the expected number) survive the second sieving. This can be accomplished by standard sieve techniques once one knows that there are the proper number of congruent pairs mod q (for most q) that also satisfy a side congruence with a relatively large modulus. These results are the new tools we apply to the Erdös-Rankin problem and are properly described in the next section.

3. Generalized twin primes in arithmetic progressions

Fix some arbitrary, positive numbers A, B. For a given large number N, let x_1, x_2 satisfy

$$\frac{N}{(\log N)^A} \leq x_1 < x_2 \leq N, \qquad x_2 - x_1 \geq \frac{N}{(\log N)^B}.$$

If n is a positive integer, let

$$\mathbf{T}(n) = \{x_1 < p \leq x_2 - n : p + n \text{ is prime}\},$$

where, as usual, p denotes a prime. Further, if l, M are positive integers, let

$$\mathbf{T}(n, l, M) = \{p \in \mathbf{T}(n) : p \equiv l \bmod M\}.$$

Thus we will only be interested in $\mathbf{T}(n, l, M)$ when

$$n \equiv 0 \mod 2, \quad (l, M) = (n + l, M) = 1. \tag{3.1}$$

Let $T(n, l, M) = |\mathbf{T}(n, l, M)|$ and let

$$T(n) = \sum_{x_1 < k \le x_2 - n} \frac{1}{\log k \log(k+n)}.$$

A heuristic argument suggests that when (3.1) holds,

$$T(n, l, M) \approx \frac{\alpha_0 T(n)}{\varphi(M)} \prod_{\substack{p \mid Mn \\ p>2}} \frac{p-1}{p-2}$$

where α_0 is given by (1.7). Thus define $R(n, l, M)$ by the equation

$$T(n, l, M) = \frac{\alpha_0 T(n)}{\varphi(M)} \prod_{\substack{p \mid Mn \\ p>2}} \frac{p-1}{p-2} + R(n, l, M),$$

and let

$$R(n, M) = \max_l |R(n, l, M)|,$$

where l satisfies (3.1). Let $Z = N^{c_1}$, where c_1 is a certain absolute, positive constant, which will be specified in §9. The major tool that we shall employ is the following result.

Theorem 3.1. *For any $E > 0$ we have*

$$\sum_{\substack{n \le N \\ n \equiv 0 \bmod 2}} \sum_{M \le Z} R(n, M) \ll_{A,B,E} N^2 (\log N)^{-E}.$$

Let Y satisfy $1.5 \le Y \le Z^{1/2}$ and let $\tau = (\log Z^{1/2})/(\log Y)$. Let

$$\mathbf{S}(n, m) = \{p \in \mathbf{T}(n) : ((mp-1)(mp'-1), P(Y)) = 1, \text{ where } p' = p + n\},$$
$$S(n, m) = |\mathbf{S}(n, m)|,$$

where recall that $P(t)$ is the product of the primes up to t.

In §12 we shall use sieve methods and Theorem 3.1 to prove the following result.

Theorem 3.2. *Let $D > 0$, $E > 0$ be arbitrary, but fixed. Then for all even $n \le N$, but for at most $O(N(\log N)^{-D})$ exceptions, we have*

(3.2)

$$S(n, m) = \alpha_0 T(n) \left(\prod_{\substack{p \mid (n,m) \\ p>2}} \frac{p-1}{p-2} \right) \left(\prod_{p \mid (nm)^2 - 1} \frac{p-3}{p-2} \right) \left(\prod_{\substack{p \nmid (nm)^3 - nm \\ p \le Y}} \frac{p-4}{p-2} \right)$$
$$\cdot (1 + O((e\tau)^{-\tau} + (\log N)^{-E} + Y^{-1} \log N)),$$

for every positive integer $m \le N$, $m \equiv 0 \bmod 2$. The O constants depend only on the choice of A, B, D, E.

We shall be primarily interested in the special case $n = kq$, where k is small and q is prime. Let A', $B' > 0$ be arbitrary, but fixed, and let x_1', x_2' satisfy

$$\frac{N}{(\log N)^{A'}} \le x_1' < x_2' \le N, \quad x_2' - x_1' \ge \frac{N}{(\log N)^{B'}}. \tag{3.3}$$

If m is an even integer, p is a prime with $x_1 < p \le x_2$, and k is an even integer, let

$$S'(m, p, k) = |\{q \text{ prime: } x_1' < q \le x_2', p \in \mathbf{S}(kq, m)\}|.$$

Also let

$$T'(p, k) = \sum_{x_1' < u \le x_2'} \frac{1}{\log u \log(p + ku)}.$$

We have the following result.

Theorem 3.3. *Let $D, E, F > 0$ be arbitrary, but fixed. Then for all primes p with $x_1 < p \le x_2$, but for at most $O(N(\log N)^{-D})$ exceptions, we have (where r denotes a prime)*

$$S'(m, p, k) = \alpha_0 T'(p, k) \left(\prod_{\substack{r \mid k \\ r > 2}} \frac{r-1}{r-2} \right) \left(\prod_{\substack{r \nmid km \\ r \le Y}} \frac{r-3}{r-2} \right)$$
$$\cdot (1 + O((e\tau)^{-\tau} + (\log N)^{-E} + Y^{-1} \log N))$$

for all integers m, k with $1 < m \le N$, $1 < |k| \le (\log N)^F$, $m \equiv k \equiv 0 \bmod 2$ and $(mp - 1, P(Y)) = 1$. The implied constants depend only on A', B', D, E, F.

The proof of Theorem 3.3 follows the same lines as that of Theorem 3.2 in that it is a routine sieve argument based on a deeper result analogous to Theorem 3.1. We shall not present the details since the proof would introduce no new ideas and, in fact, Theorem 3.3 is not crucial for our major result on large gaps between consecutive primes. Indeed, the upper bound sieve immediately gives (for $Y > \log N$)

$$S'(m, p, k) \ll T'(p, k) \left(\prod_{\substack{r \mid k \\ r > 2}} \frac{r-1}{r-2} \right) \left(\prod_{\substack{r \nmid km \\ r \le Y}} \frac{r-3}{r-2} \right)$$
$$\ll \frac{x_2' - x_1'}{\log^2 N \log Y} \cdot \frac{k^2 m}{\varphi(k)\varphi(km)},$$

which would be sufficient for us to show (1.4) for some choice of $c_0 > 1$. To achieve the value of c_0 given by (1.3), we use Theorem 3.3.

4. The third sieving

In this section we show how the primes in $(z, x]$ can be used to sieve out the residual set $\mathbf{R} \cup \mathbf{R}'$ left after the second sieving. The idea is to use a certain

positive proportion of the primes in $(z, x]$ to sieve out two residues each from $\mathbf{R} \cup \mathbf{R}'$.

We begin with an ideal situation, which we show later in this section to be a good approximation to what really exists.

Definition 4.1. Say that a graph G is N-colored if there is a function χ from the edge set of G to $\{1, \dots, N\}$.

We think of $1, \dots, N$ as different colors and $\chi(E)$ as the color of the edge E.

Definition 4.2. Say an N-colored graph G is K-uniform if $K|N$ and there are integers S, T such that

(i) each color in $\{1, \dots, N\}$ is assigned to exactly S edges of G,

(ii) for each $i = 1, \dots, K$ and each vertex V in G, there are exactly T/K edges E coincident at V with color in $((i-1)N/K, iN/K]$.

Thus each vertex of G has valence T.

Theorem 4.1. *Say G is a K-uniform, N-colored graph with cN vertices, where $c \geq 1$. Then there is a set of B mutually noncoincident edges with distinct colors such that*

$$B > \frac{cN}{4}\left(1 - \exp\left(-\frac{4}{c} + \frac{8}{c^2K}\right)\right).$$

Proof. Let S, T be as in Definition 4.2. Let $\mathbf{B}_1$ be the largest collection of mutually noncoincident edges of G with distinct colors in $(0, N/K]$. After $\mathbf{B}_1, \dots, \mathbf{B}_{i-1}$ have been chosen and $i \leq K$, let $\mathbf{B}_i$ be the largest collection of edges of G with distinct colors in $((i-1)N/K, iN/K]$ such that the members of $\mathbf{B}_1 \cup \cdots \cup \mathbf{B}_i$ are mutually noncoincident. Let β_i be such that $|\mathbf{B}_i| = \beta_i N$ and let

$$\beta = \beta_1 + \cdots + \beta_K. \tag{4.1}$$

To prove the theorem it will suffice to show that

$$\beta > \frac{c}{4}\left(1 - \exp\left(-\frac{4}{c} + \frac{8}{c^2K}\right)\right). \tag{4.2}$$

Note that since G has cN vertices, each with valence T, and G has NS edges, it follows that

$$S = \tfrac{1}{2}cT. \tag{4.3}$$

We next show that for $i = 1, \dots, K$ we have

$$(\beta_1 N + \cdots + \beta_i N)\frac{2T}{K} + \beta_i NS \geq \frac{1}{K}NS. \tag{4.4}$$

Indeed, consider the $\frac{1}{K}NS$ edges of G with color in $((i-1)N/K, iN/K]$. Since $\mathbf{B}_i$ is maximal, each of these edges not in $\mathbf{B}_i$ is either coincident with some member of $\mathbf{B}_1 \cup \cdots \cup \mathbf{B}_i$ or is of the same color as some member of $\mathbf{B}_i$. Thus each of these $\frac{1}{K}NS - B_iN$ edges is "blocked" for reason of coincidence

or reason of color. But an edge E in $\mathbf{B}_1 \cup \cdots \cup \mathbf{B}_i$ is coincident at each one of its vertices with either T/K or $T/K - 1$ other edges with color in $((i-1)N/K, iN/K]$ depending on whether $E \in \mathbf{B}_1 \cup \cdots \cup \mathbf{B}_{i-1}$ or $E \in \mathbf{B}_i$. Thus each edge of $\mathbf{B}_1 \cup \cdots \cup \mathbf{B}_i$ blocks for reason of coincidence at most $2T/K$ edges. In addition, each edge of $\mathbf{B}_i$ blocks $S-1$ other edges, which have the same color. Thus we have (4.4).

Using (4.1) and (4.3), from (4.4) we have

$$4\beta - 4\beta_{i+1} - \cdots - 4\beta_K + cK\beta_i \geq c, \qquad i = 1, \ldots, K. \tag{4.5}$$

Using (4.5) with $i = K$ (so that the inequality reads $4\beta + cK\beta_K \geq c$), we have $\beta_K \geq (c - 4\beta)/cK$. By using (4.5) sequentially for $i = K-1, K-2, \ldots,$ we inductively have that

$$\beta_{K-j} \geq \frac{c-4\beta}{cK}\left(\frac{cK+4}{cK}\right)^j, \qquad j = 0, \ldots, K-1.$$

Thus from (4.1),

$$\beta \geq \frac{c-4\beta}{4}\left(\left(\frac{cK+4}{cK}\right)^K - 1\right),$$

so that

$$\beta \geq \frac{c}{4}\left(1 - \left(\frac{cK+4}{cK}\right)^{-K}\right). \tag{4.6}$$

Since $(1 + 1/x)^x > e^{1-1/(2x)}$ for $x > 0$, we have

$$\left(\frac{cK+4}{cK}\right)^K = \left(1 + \frac{4}{cK}\right)^{(cK/4)4/c} > e^{(1-2/cK)4/c},$$

which when put in (4.6) gives (4.2) and the theorem.

In our applications the situation is not as ideal as in Definition 4.2 and Theorem 4.1. We now give versions, Definition 4.2′ and Theorem 4.1′, which we can apply directly to our problem. The proof of Theorem 4.1′, which we omit, may be obtained from the proof of Theorem 4.1 with a few minor modifications.

Definition 4.2′. Let K be a positive integer and let $C > 0$, $\delta \geq 0$ be arbitrary. Say an N-colored graph G with M vertices is (K, C, δ)-uniform if there are numbers S, T, such that

(i) but for at most δN exceptions, each color in $\{1, \ldots, N\}$ is assigned to between $(1-\delta)S$ and $(1+\delta)S$ edges of G,

(ii) if we let $n(V, i)$ denote the number of edges coincident at the vertex V with color in $((i-1)N/K, iN/K]$, then $n(V, i) \leq CT/K$ for each $i = 1, \ldots, K$ and, but for at most δM exceptional vertices V, we have $(1-\delta)T/K \leq n(V, i) \leq (1+\delta)T/K$ for each $i = 1, \ldots, K$.

Note that if $K|N$, then a $(K, C, 0)$-uniform N-colored graph is K-uniform.

Theorem 4.1′. *Let $C > 0$, $\eta > 0$ be arbitrary. There is a number $K(C, \eta)$ such that for each integer $K \geq K(C, \eta)$ there is some $\delta = \delta(C, \eta, K) > 0$ with the property that each (K, C, δ)-uniform, N-colored graph with cN vertices, where $c \geq 1$, has a set of B mutually noncoincident edges with distinct colors, where*

$$B > (1-\eta)\frac{cN}{4}\left(1-\exp\left(-\frac{4}{c}\right)\right).$$

It remains to be seen what such a result has to do with large gaps between consecutive primes. In the next section we will show (Theorem 5.1) that with $\mathbf{R}_m$ defined by (2.1), then uniformly for

$$1 \leq m \leq \frac{\log x}{(\log\log x)^4}, \tag{4.7}$$

we have

$$|\mathbf{R}_m| = \frac{U}{m\log x}\left(\prod_{\substack{r\leq y\\ r\nmid m}}\frac{r-2}{r-1}\right)(1+O(\exp(-(\log\log x)^{1/2}))), \tag{4.8}$$

where r denotes a prime. Define

$$r_m = \frac{\alpha_0}{m\log\log x}\prod_{\substack{r\mid m\\ r>2}}\frac{r-1}{r-2}$$

for m even and $r_m = 0$ for m odd. Then a simple calculation from (4.8) shows that if m satisfies (4.7), then

$$|\mathbf{R}_m| = c'' r_m \frac{x}{\log x}(1+O(\exp(-(\log\log x)^{1/2}))). \tag{4.9}$$

We shall define a graph whose vertex set is $\mathbf{R}_m$. To describe the edges, first let

$$k_0 := \prod_{r<\log\log\log x} r,$$

so that for x large we have $k_0 < (\log\log x)^{1+\varepsilon}$. Let $\mathbf{Q}_m$ denote the set of primes q in the interval

$$\left(\left(1-\sum_{j=1}^{m} r_j\right)x, \left(1-\sum_{j=1}^{m-1} r_j\right)x\right].$$

Note that this interval has length $r_m x$ and that the union of these invervals for m satisfying (4.7) is

$$\left(\left(1-\sum_{j\leq \log x/(\log\log x)^4} r_j\right)x, x\right] \subset (z', x] \subset (z, x]$$

for large x, where (cf. (5.2))

$$z' := (4-\varepsilon)\frac{x \log\log\log x}{\log\log x}.$$

Thus the various $\mathbf{Q}_m$ are disjoint sets of primes in $(z', x]$ with

$$|\mathbf{Q}_m| = r_m \frac{x}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right). \tag{4.10}$$

Let $\mathbf{G}_m$ be the graph with vertex set $\mathbf{R}_m$ and such that mp, $mp' \in \mathbf{R}_m$ are connected by an edge if and only if $|p' - p| = k_0 q$ for some prime $q \in \mathbf{Q}_m$. Define the "color" of an edge by the prime q, so that $\mathbf{G}_m$ is a $|\mathbf{Q}_m|$-colored graph.

In the notation of §3, if $x_1 = z$, $x_2 = U/m$, then the set of edges of $\mathbf{G}_m$ with color q corresponds to $\mathbf{S}(k_0 q, m)$. Thus from Theorem 3.2 with $N = x\log x$, $Y = y$, but for $O(x/(\log x)^2)$ exceptional primes $q \in \mathbf{Q}_m$, the number of edges of $\mathbf{G}_m$ with color q is $s(m, q)(1 + O((\log x)^{-c_1/4}))$, where

$$s(m, q) := \frac{\alpha_0}{(\log x)^2}\left(\frac{U}{m} - k_0 q - z\right)\left(\prod_{\substack{r \mid (k_0 q, m) \\ r>2}} \frac{r-1}{r-2}\right)$$

$$\cdot \left(\prod_{r \mid (k_0 qm)^2 - 1} \frac{r-3}{r-2}\right)\left(\prod_{\substack{r \nmid (k_0 qm)^3 - k_0 qm \\ r \le y}} \frac{r-4}{r-2}\right).$$

We wish to show that for most primes $q \in \mathbf{Q}_m$, $s(m, q)$ does not depend very strongly on q. To accomplish this, recall the definition of k_0. If we define

$$f(q) = \sum_{r \mid (k_0 qm)^2 - 1} \frac{1}{r},$$

we have

$$\begin{aligned}
\sum_{q \in \mathbf{Q}_m} f(q) &= \sum_r \frac{1}{r} \sum_{\substack{q \in \mathbf{Q}_m \\ r \mid (k_0 qm)^2 - 1}} 1 \\
&= \sum_{r \le (\log x)^2} \frac{1}{r} \sum_{\substack{q \in \mathbf{Q}_m \\ r \mid (k_0 qm)^2 - 1}} 1 + \sum_{r > (\log x)^2} \frac{1}{r} \sum_{\substack{q \in \mathbf{Q}_m \\ r \mid (k_0 qm)^2 - 1}} 1 \\
&\ll \sum_{\substack{r \le (\log x)^2 \\ r > \log\log\log x}} \frac{|\mathbf{Q}_m|}{r(r-1)} + \sum_{r > (\log x)^2} \frac{r_m x}{r^2} \\
&= o\left(\frac{|\mathbf{Q}_m|}{\log\log\log x}\right).
\end{aligned}$$

It thus follows that but for $o(|\mathbf{Q}_m|)$ values of $q \in \mathbf{Q}_m$, we have

$$s(m, q) = S(m)\left(1 + o\left(\frac{1}{\log\log\log x}\right)\right),$$

where

$$S(m) := \frac{\alpha_0}{(\log x)^2}\left(\frac{U}{m} - z\right)\left(\prod_{\substack{r|(k_0, m)\\ r>2}} \frac{r-1}{r-2}\right)\left(\prod_{\substack{r\nmid k_0 m\\ r\le y}} \frac{r-4}{r-2}\right).$$

Let $\mathbf{Q}'_m$ be the set of primes q such that the number of edges of $\mathbf{G}_m$ of color q lies in the interval

$$\left[S(m)\left(1 - \frac{1}{\log\log\log x}\right), S(m)\left(1 + \frac{1}{\log\log\log x}\right)\right].$$

Thus $|\mathbf{Q}'_m| \sim |\mathbf{Q}_m|$. Also note that for any $q \in \mathbf{Q}_m$, the number of edges of $\mathbf{G}_m$ of color q is $O(S(m))$.

For a given $mp \in \mathbf{R}_m$, the number of edges of $\mathbf{G}_m$ that contain mp is exactly, in the notation of §3,

$$S'(m, p, k_0) + S'(m, p, -k_0), \tag{4.11}$$

where x'_1, x'_2 are the end points of the interval defining $\mathbf{Q}_m$. To make sure that $m(p \pm k_0 q)$ are in the interval $(mz, U]$, we restrict this discussion of the valency of mp to those $mp \in \mathbf{R}_m$ with

$$mz + mx(\log\log x)^2 \le mp \le U - mx(\log\log x)^2. \tag{4.12}$$

Thus from Theorem 3.3 and (4.11) but for $O(x/(\log x)^3)$ values of $mp \in \mathbf{R}_m$ that satisfy (4.12), there are $S'(m)(1+O((\log x)^{-c_1/4}))$ edges of $\mathbf{G}_m$ that contain mp, where

$$S'(m) := \frac{2\alpha_0 r_m x}{\log^2 x}\left(\prod_{\substack{r|k_0\\ r>2}} \frac{r-1}{r-2}\right)\left(\prod_{\substack{r\nmid k_0 m\\ r\le y}} \frac{r-3}{r-2}\right).$$

Further if K is an arbitrary, fixed natural number, then but for $O(x/(\log x)^3)$ values of $mp \in \mathbf{R}_m$ that satisfy (4.12), there are

$$\frac{1}{K} S'(m)(1 + O((\log x)^{-c_1/4}))$$

edges of $\mathbf{G}_m$ that contain mp with color in

$$\left(\left(1 + \frac{(i-1)}{K} r_m - \sum_{j=1}^{m} r_j\right)x, \left(1 + \frac{i}{K} r_m - \sum_{j=1}^{m-1} r_j\right)x\right] \tag{4.13}$$

for each $i = 1, \ldots, K$. Also note that even if $mp \in \mathbf{R}_m$ does not satisfy (4.12) or is one of the $O(x/(\log x)^3)$ exceptions, then we still have that the number of edges of $\mathbf{G}_m$ that contain mp and have color in (4.13) is $O(\frac{1}{K} S'(m))$.

Thus, while the graph $\mathbf{G}_m$ may not be a K-uniform, $|\mathbf{Q}_m|$-colored graph, it is "approximately" K-uniform. That is, but for $o(|\mathbf{Q}_m|)$ colors, each color appears on $(1+o(1))S(m)$ edges and any exceptional color appears on $O(S(m))$ edges. In addition, for all but $o(|\mathbf{R}_m|)$ vertices, the number of edges containing it with color in any particular one of K equal subintervals of colors is $(1+o(1))\frac{1}{K}S'(m)$ and any exceptional vertex is contained on $O(\frac{1}{K}S'(m))$ edges with colors in that subinterval.

Thus there is some absolute constant $C > 0$ such that for any positive integer K and any $\delta > 0$, the graph $\mathbf{G}_m$ is (K, C, δ)-uniform for all m satisfying (4.7), provided x is sufficiently large depending on the choice of K and δ. It thus follows from (4.9), (4.10), and Theorem 4.1′ that for any $\eta > 0$, for all integers m satisfying (4.7) and for all sufficiently large x depending on the choice of η, $\mathbf{G}_m$ contains at least

$$B_m := \frac{(1-\eta)c''r_m x}{4\log x}(1-e^{-4/c''}) \tag{4.14}$$

mutually noncoincident edges. Since $c'' < c_0$, it follows that

$$1+\frac{c''}{4}(1-e^{-4/c''}) > c'',$$

so that there is some $\eta > 0$ such that

$$(1-\eta)\left(1+\frac{c''}{4}(1-e^{-4/c''})\right) > c''. \tag{4.15}$$

This is the value of η chosen in (4.14).

The third sieving begins by using at least B_m primes in $\mathbf{Q}_m$ to sieve out at least $2B_m$ members of $\mathbf{R}_m$ as guaranteed above. Since by (4.10) we may assume $|\mathbf{Q}_m| \geq (1-\eta)r_m x/\log x$, if we use the remaining primes in $\mathbf{Q}_m$ to sieve out just one member of $\mathbf{R}_m$, then we can cover at least

$$\begin{aligned}|\mathbf{Q}_m| - B_m + 2B_m &= |\mathbf{Q}_m| + B_m \\ &\geq \frac{(1-\eta)r_m x}{\log x}\left(1+\frac{c''}{4}(1-e^{-4/c''})\right)\end{aligned}$$

numbers. But by (4.15) and (4.9), we thus can completely sieve out $\mathbf{R}_m$ with the primes in $\mathbf{Q}_m$.

We still must sieve out those $\mathbf{R}_m$ with $m > \log x/(\log\log x)^4$ and all of $\mathbf{R}'$. From Theorem 5.1 it follows that

$$\sum_{m>\log x/(\log\log x)^4} |\mathbf{R}_m| \sim 3\frac{x\log\log\log x}{\log x\log\log x}$$

(where, of course, $m \leq U/z$). Also from Theorem 5.3 we have $|\mathbf{R}'| \ll x/(\log x)^{1+\varepsilon}$. However, the remaining primes with which we have left to sieve are the primes in $(z, z']$ and there are

$$\sim (4-\varepsilon)\frac{x\log\log\log x}{\log x\log\log x}$$

primes in this interval. Thus we may complete the sieving.

5. The second residual set

In this section we prove the estimates for $|\mathbf{R}|$ and $|\mathbf{R}'|$ in (2.3) and (2.4), where $\mathbf{R}$, $\mathbf{R}'$ are defined in §2.

Theorem 5.1. *With U, z, y as defined in §2, then uniformly for integers*

$$1 \le m \le \frac{U}{z}\left(1 - \frac{1}{\log x}\right),$$

we have (where r denotes a prime and $\mathbf{R}_m$ is defined in (2.1))

$$|\mathbf{R}_m| = \frac{U}{m \log x}\left(\prod_{\substack{r \le y \\ r \nmid m}} \frac{r-2}{r-1}\right)(1 + O(\exp(-(\log\log x)^{1/2}))).$$

Proof. This result follows immediately from Theorem 2.6′ in Halberstam and Richert [5].

Theorem 5.2. *With $\mathbf{R}$ defined in §2, we have*

$$|\mathbf{R}| \sim \frac{c'}{1-\varepsilon}\frac{x}{\log x}.$$

Proof. Let $w = (U/z)(1 - 1/\log x)$. First note that

$$\sum_{w < m \le U/z} |\mathbf{R}_m| \ll \sum_{w < m \le U/z} \frac{U}{m \log x} \ll \frac{U}{\log^2 x} = o\left(\frac{x}{\log x}\right).$$

Thus from Theorem 5.1 we have

$$\begin{aligned} |\mathbf{R}| &= \sum_{\substack{m \le w \\ 2 \mid m}} |\mathbf{R}_m| + o\left(\frac{x}{\log x}\right) \\ &= (1 + o(1))\frac{U}{\log x} \sum_{\substack{m \le w \\ 2 \mid m}} \frac{1}{m} \prod_{\substack{r \le y \\ r \nmid m}} \frac{r-2}{r-1} + o\left(\frac{x}{\log x}\right) \qquad (5.1) \\ &= (1 + o(1))\frac{U}{\log x}\left(\prod_{2 < r \le y} \frac{r-2}{r-1}\right) \sum_{\substack{m \le w \\ 2 \mid m}} \frac{1}{m} \prod_{\substack{r \mid m \\ r > 2}} \frac{r-1}{r-2} + o\left(\frac{x}{\log x}\right). \end{aligned}$$

Now

$$\prod_{2 < r \le y} \frac{r-2}{r-1} = 2\left(\prod_{r \le y} \frac{r-1}{r}\right)\left(\prod_{2 < r \le y} \frac{r-2}{r-1} \cdot \frac{r}{r-1}\right) \sim \frac{\alpha_0}{e^{\gamma} \log y}$$

by Mertens' theorem. Also, by standard arguments,

$$\sum_{\substack{m \le w \\ 2 \mid m}} \frac{1}{m} \prod_{\substack{r \mid m \\ r > 2}} \frac{r-1}{r-2} \sim \frac{1}{\alpha_0} \log w. \qquad (5.2)$$

Putting these estimates into (5.1) we have

$$|\mathbf{R}| = (1+o(1))\frac{U\log w}{e^{\gamma}\log y\log x} + o\left(\frac{x}{\log x}\right),$$

which was to be proved.

Theorem 5.3. *With* $\mathbf{R}'$ *defined in* §2, *we have*

$$|\mathbf{R}'| \ll \frac{x}{(\log x)^{1+\varepsilon}}.$$

Proof. Suppose $n \in \mathbf{R}'$ and $n > x/(\log x)^{1+\varepsilon}$. Further suppose n is divisible by a prime factor $p > y^{1/2}$. Note that the number of $n \in \mathbf{R}'$ that do not satisfy both of these conditions is at most (from de Bruijn [1])

$$\frac{x}{(\log x)^{1+\varepsilon}} + \psi(U, y^{1/2}) = \frac{(1+o(1))x}{(\log x)^{1+\varepsilon}},$$

where $\psi(s, t)$ is the number of integers $n \le s$ with $P^+(n) \le t$ and where $P^+(n)$ denotes the largest prime factor of n. Thus we may consider only values of $n \in \mathbf{R}'$ of the form mp where p is prime, $y^{1/2} < p \le y$,

$$\frac{x}{y(\log x)^{1+\varepsilon}} < m \le \frac{U}{y^{1/2}}, \qquad P^+(m) \le y. \tag{5.3}$$

For each m satisfying (5.3) we ask how many primes $p \le U/m$ there are, such that $(mp-1, P(y)) = 1$. From Theorem 4.2 in [5] this count is

$$\ll \frac{U/m}{\log(U/m)\log y} \prod_{\substack{r\mid m \\ r \text{ prime}}} \frac{r}{r-1} \ll \frac{U\log\log x}{m\log^2 y},$$

since $\log(U/m) \gg \log y$. Furthermore, from de Bruijn [1], $\sum 1/m$ where m satisfies (5.3) is $(\log x)^{-\varepsilon(1-\varepsilon)^{-1}+o(1)}$. Thus

$$\begin{aligned}|\mathbf{R}'| &\ll U\log\log x(\log x)^{-\varepsilon-\varepsilon^2}(\log y)^{-2} + x(\log x)^{-1-\varepsilon} \\ &\ll x(\log x)^{-1-\varepsilon},\end{aligned}$$

which was to be proved.

6. Proof of Theorem 3.1—application of the circle method

We apply the circle method of Hardy and Littlewood in a manner that resembles that of Montgomery and Vaughan [10] in many respects. As usual, let

$$e(t) = e^{2\pi i t}, \quad e_k(t) = e(t/k).$$

Set (recalling the notation of §3) for any real number α

$$S_{l,M}(\alpha) = \sum_{\substack{x_1 < p \le x_2 \\ p \equiv l \bmod M}} e(p\alpha), \quad S(\alpha) = S_{0,1}(\alpha) = \sum_{x_1 < p \le x_2} e(p\alpha). \tag{6.1}$$

Then by orthogonality,

$$T(n, l, M) = \int_0^1 S_{l,M}(\alpha)\overline{S(\alpha)}e(n\alpha)\,d\alpha. \tag{6.2}$$

To dissect the unit interval we now put

$$P = Z^3 = N^{3c_1}, \quad Q = NZ^{-3} = N^{1-3c_1}. \tag{6.3}$$

For $1 \le a \le q \le P$ with $(a, q) = 1$, let

$$\mathbf{M}(q, a) = \left[\frac{a}{q} - \frac{1}{qQ}, \frac{a}{q} + \frac{1}{qQ}\right],$$

a so-called major arc. Let $\mathbf{M}$ be the union of the major arcs and let $\boldsymbol{m}$ be the set of those α with $Q^{-1} < \alpha < 1 + Q^{-1}$, $\alpha \notin \mathbf{M}$. We refer to the connected components of $\boldsymbol{m}$ as the minor arcs.

We now set

$$T(n, l, M) = T_1(n, l, M) + T_2(n, l, M), \tag{6.4}$$

where

$$\begin{aligned} T_1(n, l, M) &= \int_{\boldsymbol{m}} S_{l,M}(\alpha)\overline{S(\alpha)}e(n\alpha)\,d\alpha, \\ T_2(n, l, M) &= \int_{\boldsymbol{m}} S_{l,M}(\alpha)\overline{S(\alpha)}e(n\alpha)\,d\alpha. \end{aligned} \tag{6.5}$$

It turns out that the minor arc contributions can be considered part of the error term. Using Bessel's inequality we have (where $T_2(n, l, M)$ is given by (6.5))

$$\begin{aligned} \sum_{\substack{n \le N \\ n \equiv 0 \bmod 2}} |T_2(n, l, M)|^2 &\le \int_{\boldsymbol{m}} |S_{l,M}(\alpha)|^2 |S(\alpha)|^2\,d\alpha \\ &\le \left(\max_{\alpha \in \boldsymbol{m}} |S(\alpha)|\right)^2 \int_0^1 |S_{l,M}(\alpha)|^2\,d\alpha \\ &\le \left(\max_{\alpha \in \boldsymbol{m}} |S(\alpha)|\right)^2 \sum_{\substack{x_1 < p \le x_2 \\ p \equiv l \bmod M}} 1 \\ &\le \left(\max_{\alpha \in \boldsymbol{m}} |S(\alpha)|\right)^2 N/M. \end{aligned} \tag{6.6}$$

To complete the estimate we apply Vinogradov's fundamental lemma in the following form.

Lemma 6.1. *Suppose* $1 \le y \le x^{1/4}$, $1 \le q \le x/y$, *and* $(a, q) = 1$. *Then for any real number* α *we have*

$$\left|\sum_{p \le x} e(p\alpha)\right| \ll \left(1 + x\left|\alpha - \frac{a}{q}\right|\right) \frac{x}{\sqrt{y}} \log^{16} x.$$

This result follows immediately from Theorem 16.1 in Montgomery [9] by a partial summation to remove the Λ-factor and a second partial summation (as in the proof of Corollary 16.2 in [9]) to pass from a/q to α.

By Dirichlet's approximation theorem, for any α there are integers a, q with $1 \le q \le Q$, $(a, q) = 1$ and $|\alpha - a/q| \le 1/qQ$. If $\alpha \in \boldsymbol{m}$, then we may assume also that $q > P$. Thus

$$|\alpha - a/q| \le 1/qQ < 1/PQ = 1/N,$$

so that from Lemma 6.1 applied to $x = x_2$ and $y = x_2/Q$ and again to $x = x_1$, $y = x_1/Q$ we get

$$|S(\alpha)| \ll \sqrt{Qx_2}\log^{16} x_2 \le NP^{-1/2}\log^{16} N.$$

Using this estimate in (6.6) we have

$$\begin{aligned}
&\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}} \sum_{M\le Z} |T_2(n, l, M)| \\
&\le \sum_{M\le Z} \left(\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}} |T_2(n, l, M)|^2 \right)^{1/2} \left(\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}} 1 \right)^{1/2} \qquad (6.7)\\
&\ll \sum_{M\le Z} (N^3 M^{-1} P^{-1} \log^{32} N)^{1/2} N^{1/2} \\
&\ll N^2 Z^{1/2} P^{-1/2} \log^{16} N = N^2 Z^{-1} \log^{16} N.
\end{aligned}$$

This estimate shows the minor arcs contribute a negligible amount in Theorem 3.1.

7. The major arcs

We introduce the following notation. For any Dirichlet character χ and real number α we set

$$S(\chi, \alpha) = \sum_{x_1 < p \le x_2} \chi(p) e(p\alpha). \qquad (7.1)$$

For positive integers $M \le Z$ and q let $d = d(M, q) = (M, q)$, $D = D(M, q) = [M, q]$. If M, q are given, let l, r, a be integers, with $(a, q) = 1$, $al \equiv r \bmod d$. Let $c = c(l, r, a)$ be defined $\bmod D$ such that

$$c \equiv l \bmod M, \quad ca \equiv r \bmod q. \qquad (7.2)$$

For any character $\chi \bmod D$ and any integers a, l with $(a, q) = 1$, $(l, d) = 1$, we define

$$\rho_{a,l}(\chi) = \sum_{\substack{r \bmod q\\ (r,q)=1\\ r\equiv al \bmod d}} e(r/q)\overline{\chi}(c(l, r, a)). \qquad (7.3)$$

We now evaluate the exponential sums $S_{l,M}(\alpha)$ for $\alpha = a/q + \eta$ where $1 \le a \le q \le P$ and $(a, q) = 1$. We have for l, M satisfying (3.1) and sufficiently large N,

$$
\begin{aligned}
S_{l,M}(\alpha) &= \sum_{\substack{x_1 < p \le x_2 \\ p \equiv l \bmod M}} e(pa/q)e(p\eta) \\
&= \sum_{\substack{s \bmod q \\ (s,q)=1 \\ s \equiv l \bmod d}} e(sa/q) \sum_{\substack{x_1 < p \le x_2 \\ p \equiv l \bmod M \\ p \equiv s \bmod q}} e(p\eta) \\
&= \sum_{\substack{r \bmod q \\ (r,q)=1 \\ r \equiv al \bmod d}} e(r/q) \sum_{\substack{x_1 < p \le x_2 \\ p \equiv c(l,r,a) \bmod D}} e(p\eta) \qquad (7.4) \\
&= \sum_{\substack{r \bmod q \\ (r,q)=1 \\ r \equiv al \bmod d}} e(r/q)\varphi(D)^{-1} \sum_{\chi \bmod D} \overline{\chi}(c(l,r,a)) \sum_{x_1 < p \le x_2} \chi(p)e(p\eta) \\
&= \varphi(D)^{-1} \sum_{\substack{r \bmod q \\ (r,q)=1 \\ r \equiv al \bmod d}} e(r/q) \sum_{\chi \bmod D} \overline{\chi}(c(l,r,a))S(\chi, \eta).
\end{aligned}
$$

We now define $V(\eta)$, $W(\chi, \eta)$ by

$$V(\eta) = \sum_{x_1 < m \le x_2} e(m\eta)/\log m,$$

$$S(\chi_0, \eta) = V(\eta) + W(\chi_0, \eta) \quad (\chi_0 \text{ is a principal character}),$$

$$S(\chi, \eta) = W(\chi, \eta) \qquad (\chi \ne \chi_0).$$

Using this notation and (7.3), in (7.4) we have

(7.5)

$$S_{l,M}(a/q + \eta) = \varphi(D)^{-1}V(\eta) \sum_{\substack{r \bmod q \\ (r,q)=1 \\ r \equiv al \bmod d}} e(r/q) + \varphi(D)^{-1} \sum_{\chi \bmod D} \rho_{a,l}(\chi)W(\chi, \eta).$$

The first sum in (7.5) may be evaluated as follows. Let b_1 be the largest divisor of q that is coprime to d and let $b = q/d$. Thus we always have $b_1 | b$. Let $b_1' \bmod d$ be defined by $b_1 b_1' \equiv 1 \bmod d$. Thus

$$
\begin{aligned}
\sum_{\substack{r \bmod q \\ (r,q)=1 \\ r \equiv al \bmod d}} e(r/q) &= \sum_{\substack{s \bmod b \\ (s, b_1)=1}} e_q(alb_1b_1' + sd) \\
&= e_q(alb_1b_1') \sum_{\substack{s \bmod b \\ (s, b_1)=1}} e_b(s) \\
&= \begin{cases} \mu(b)e_d(alb_1'), & \text{if } b_1 = b, \\ 0, & \text{if } b_1 \ne b, \end{cases} \\
&= \mu(b^2/b_1)e_d(alb_1').
\end{aligned}
$$

Putting this computation into (7.5), we have

(7.6)
$$S_{l,M}(a/q+\eta) = \varphi(D)^{-1}V(\eta)\mu(b^2/b_1)e_d(alb_1') + \varphi(D)^{-1}\sum_{\chi \bmod D}\rho_{a,l}(\chi)W(\chi,\eta).$$

By specialization to the case $M = 1$, we have $d = 1$, $b = b_1 = q$, $D = q$, so that

$$S(a/q+\eta) = \frac{\mu(q)}{\varphi(q)}V(\eta) + \frac{1}{\varphi(q)}\sum_{\chi \bmod q}\chi(a)\tau(\overline{\chi})W(\chi,\eta), \tag{7.7}$$

where $\tau(\chi)$ is the Gaussian sum $\tau(\chi) = \sum_{h \bmod q}\chi(h)e_q(h)$.

We now obtain from (6.5), (7.6), and (7.7)

(7.8)
$$\begin{aligned} T_1(n,l,M) &= \int_{\mathfrak{m}} S_{l,M}(\alpha)\overline{S(\alpha)}e(n\alpha)\,d\alpha \\ &= \sum_{q\le P}\sum_{\substack{a \bmod q \\ (a,q)=1}}\int_{-1/qQ}^{1/qQ} S_{l,M}(a/q+\eta)\overline{S(a/q+\eta)}e(n(a/q+\eta))\,d\eta \\ &= T_1^*(n,l,M) + R_1(n,l,M) + R_2(n,l,M) + R_3(n,l,M), \end{aligned}$$

where

$$T_1^*(n,l,M) := \sum_{q\le P}\frac{\mu(q)\mu(b(q)^2/b_1(q))}{\varphi(D(q))\varphi(q)} \cdot \sum_{\substack{a \bmod q \\ (a,q)=1}} e\left(\frac{alb_1'(q)}{d(q)} + \frac{an}{q}\right)\int_{-1/qQ}^{1/qQ}|V(\eta)|^2 e(n\eta)\,d\eta, \tag{7.9}$$

(7.10)
$$R_1(n,l,M) := \sum_{q\le P}\frac{\mu(b(q)^2/b_1(q))}{\varphi(D(q))\varphi(q)}\sum_{\chi \bmod q}\sum_{\substack{a \bmod q \\ (a,q)=1}} e\left(\frac{alb_1'(q)}{d(q)} + \frac{an}{q}\right) \cdot \overline{\chi}(a)\overline{\tau(\overline{\chi})}\int_{-1/qQ}^{1/qQ} V(\eta)\overline{W(\chi,\eta)}e(n\eta)\,d\eta,$$

$$R_2(n,l,M) := \sum_{q\le P}\frac{\mu(q)}{\varphi(D(q))\varphi(q)}\sum_{\chi \bmod D(q)}\sum_{\substack{a \bmod q \\ (a,q)=1}} e\left(\frac{an}{q}\right) \cdot \rho_{a,l}(\chi)\int_{-1/qQ}^{1/qQ}\overline{V(\eta)}W(\chi,\eta)e(n\eta)\,d\eta, \tag{7.11}$$

$$R_3(n,l,M) := \sum_{q\le P}\frac{1}{\varphi(D(q))\varphi(q)}\sum_{\substack{\chi_1 \bmod D(q) \\ \chi_2 \bmod q}}\sum_{\substack{a \bmod q \\ (a,q)=1}} e\left(\frac{an}{q}\right) \cdot \rho_{a,l}(\chi_1)\overline{\chi}_2(a)\overline{\tau(\overline{\chi}_2)} \cdot \int_{-1/qQ}^{1/qQ} W(\chi_1,\eta)\overline{W(\chi_2,\eta)}e(n\eta)\,d\eta. \tag{7.12}$$

It turns out that T_1^* may be considered a main term, with R_1, R_2, R_3 being error terms. Let

$$R_i(n, m) = \max_{\substack{l \bmod M \\ (l, M)=(l+n, M)=1}} |R_i(n, l, M)| \quad \text{for } i = 1, 2, 3. \tag{7.13}$$

8. The main term

We record the following easy result (see (5.2) in Montgomery and Vaughan [10]). Note that we have already tacitly evaluated a similar sum in the calculation preceding (7.6).

Lemma 8.1. *If q is squarefree,*

$$c_q(m) := \sum_{\substack{a \bmod q \\ (a, q)=1}} e_q(am) = \mu\left(\frac{q}{(q, m)}\right)\varphi((q, m)).$$

The expression $c_q(m)$ is a Ramanujan sum.

Note that in (7.9) we may assume q is squarefree and so $b_1(q) = b(q)$. From Lemma 8.1 we have

$$\begin{aligned} \sum_{\substack{a \bmod q \\ (a, q)=1}} e\left(\frac{alb'(q)}{d(q)} + \frac{an}{q}\right) &= \sum_{\substack{a \bmod q \\ (a, q)=1}} e_q(a(lb'(q)b(q) + n)) \\ &= c_q(lb'(q)b(q) + n) \\ &= \mu\left(\frac{q}{(q, lb'(q)b(q) + n)}\right)\varphi((q, lb'(q)b(q) + n)). \end{aligned} \tag{8.1}$$

Now from (3.1),

$$\begin{aligned} (q, lb'(q)b(q) + n) &= (b(q), lb'(q)b(q) + n)(d(q), lb'(q)b(q) + n) \\ &= (b(q), n)(d(q), l + n) = (b(q), n), \end{aligned}$$

so that (8.1) and (7.9) imply (using $\varphi(D(q)) = \varphi(M)\varphi(b(q))$ for q squarefree)

$$T_1^*(n, l, M) = \frac{1}{\varphi(M)} \sum_{q \le P} \frac{\mu^2(q)\mu(b(q))\varphi((b(q), n))}{\mu((b(q), n))\varphi(b(q))\varphi(q)} \int_{-1/qQ}^{1/qQ} |V(\eta)|^2 e(n\eta)\, d\eta. \tag{8.2}$$

Since

$$|V(\eta)| \ll \frac{1}{\log N}\left|\sum_{x_1 < m \le x_2} e(m\eta)\right| \ll \frac{1}{|e(\eta) - 1|\log N} \ll \frac{1}{\|\eta\|},$$

where $\| \ \|$ denotes the distance to the nearest integer, we have

$$\int_{1/qQ}^{1-1/qQ} |V(\eta)|^2\, d\eta \ll qQ.$$

Thus

$$\int_{-1/qQ}^{1/qQ} |V(\eta)|^2 e(n\eta)\,d\eta = \int_0^1 |V(\eta)|^2 e(n\eta)\,d\eta + O(qQ)$$
$$= T(n) + O(qQ).$$

Using this in (8.2) we have

$$T_1^*(n, l, M) = \frac{T(n)}{\varphi(M)} \sum_{q\le P} \frac{\mu^2(q)\mu(b(q))\varphi((b(q), n))}{\mu((b(q), n))\varphi(b(q))\varphi(q)} + O\left(\frac{Q}{\varphi(M)} \sum_{q\le P} \frac{\varphi((b(q), n))q}{\varphi(b(q))\varphi(q)}\right). \tag{8.3}$$

The error term in (8.3) is of order

$$\frac{Q\log N}{M} \sum_{q\le P} \frac{(b(q), n)(q, M)}{q} \le \frac{Q\log N}{M} \sum_{\substack{d_1|n \\ d_2|M}} \sum_{\substack{q\le P \\ d_1d_2|q}} \frac{d_1d_2}{q}$$
$$\le \frac{Q\log^2 N}{M}\tau(n)\tau(M) \ll NM^{-1}P^{-1/2}, \tag{8.4}$$

where τ denotes the divisor function. The sum in the main term in (8.3) is

$$\sum_{q=1}^{\infty} \frac{\mu^2(q)\mu(b(q))\varphi((b(q), n))}{\mu((b(q), n))\varphi(b(q))\varphi(q)} + O\left(\sum_{q>P} \frac{\mu^2(q)\varphi((b(q), n))}{\varphi(b(q))\varphi(q)}\right)$$
$$= \prod_{p\nmid Mn}\left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|Mn}\left(1 + \frac{1}{p-1}\right) + O\left(\sum_{q>P} \frac{(b(q), n)(q, M)}{\mu^2(q)\varphi^2(q)}\right)$$
$$= \alpha_0 \prod_{\substack{p|Mn \\ p>2}} \frac{p-1}{p-2} + O\left(\sum_{\substack{d_1|n \\ d_2|M}} \sum_{\substack{q>P \\ d_1d_2|q}} \frac{d_1d_2}{\varphi^2(q)}\right)$$
$$= \alpha_0 \prod_{\substack{p|Mn \\ p>2}} \frac{p-1}{p-2} + O\left(\frac{\tau(n)\tau(M)nM}{P\varphi(n)\varphi(M)}\right).$$

Putting this calculation and (8.4) into (8.3), we get

$$T_1^*(n, l, M) = \frac{\alpha_0 T(n)}{\varphi(M)} \prod_{\substack{p|Mn \\ p>2}} \frac{p-1}{p-2} + O(NM^{-1}P^{-1/2}). \tag{8.5}$$

9. The first major arc error term

In this section we show that for any A, B, $E > 0$,

$$\sum_{M\le Z} R_1(n, M) \ll_{A,B,E} N(\log N)^{-E}, \tag{9.1}$$

where $R_1(n, M)$ is given by (7.13) and (7.10).

Recall from §7 that for a fixed M,

$$D(q) = [M, q], \quad d(q) = (M, q), \quad b(q) = q/d(q),$$

$b_1(q)$ is the largest divisor of q coprime to M and

$$b_1(q)b_1'(q) \equiv 1 \mod d(q).$$

Note that the presence of the factor $\mu(b(q)^2/b_1(q))$ in (7.10) implies we may consider only those q with $b_1(q) = b(q)$. Thus

$$\begin{aligned} R_1(n, l, M) = & \sum_{\substack{q \le P \\ b_1(q)=b(q)}} \frac{\mu(b(q))}{\varphi(D(q))\varphi(q)} \\ & \cdot \sum_{\chi \bmod q} \sum_{\substack{a \bmod q \\ (a,q)=1}} e_q(a(lb'(q)b(q) + n))\overline{\chi}(a)\overline{\tau(\chi)} \\ & \cdot \int_{-1/qQ}^{1/qQ} V(\eta)\overline{W(\chi, \eta)}e(n\eta)\, d\eta \\ = & \sum_{\substack{q \le P \\ b_1(q)=b(q)}} \frac{\mu(b(q))}{\varphi(D(q))\varphi(q)} \sum_{\chi \bmod q} c_{\overline{\chi}}(lb'(q)b(q) + n)\overline{\tau(\chi)} \\ & \cdot \int_{-1/qQ}^{1/qQ} V(\eta)\overline{W(\chi, \eta)}e(n\eta)\, d\eta, \end{aligned} \tag{9.2}$$

where

$$c_\chi(m) := \sum_{a=1}^{q} \chi(a)e_q(am).$$

The following generalization of Lemma 8.1 allows us to evaluate $c_\chi(m)$. This result is Lemma 5.4 in [10].

Lemma 9.1. *Let χ be a character* mod q *induced by a primitive character χ^** mod r. *For any integer m, $c_\chi(m) = 0$, unless $r(q, m) | q$, in which case*

$$c_\chi(m) = \overline{\chi^*}\left(\frac{m}{(q, m)}\right) \frac{\varphi(q)}{\varphi(q/(q, m))} \mu\left(\frac{q}{r(q, m)}\right) \chi^*\left(\frac{q}{r(q, m)}\right) \tau(\chi^*).$$

The case $m = 1$ is of special interest in Lemma 9.1, giving us the following well-known result (see Lemma 5.2 in [10]).

Lemma 9.2. *Let χ be a character* mod q *induced by a primitive character χ^** mod r. *Then $\tau(\chi) = \mu(q/r)\chi^*(q/r)\tau(\chi^*)$.*

Finally we record the following classical result (see [10, Lemma 5.1]).

Lemma 9.3. *If χ is a primitive character* mod r, *then* $|\tau(\chi)| = \sqrt{r}$.

We now apply these lemmas to (9.2). Note that the condition $b_1(q) = b(q)$ implies that $(b(q), d(q)) = 1$, so that (as in §8)

$$\begin{aligned}(q, lb'(q)b(q) + n) &= (b(q), lb'(q)b(q) + n)(d(q), lb'(q)b(q) + n)\\ &= (b(q), n)(d(q), l + n) = (b(q), n),\end{aligned}$$

by (3.1). Thus Lemmas 9.1 and 9.2 imply

$$\begin{aligned}c_{\overline{\chi}}(lb'(q)b(q) + n)\overline{\tau(\overline{\chi})} &= \chi^*\left(\frac{lb'(q)b(q) + n}{(b(q), n)}\right)\frac{\varphi(q)}{\varphi(q/(b(q), n))}\\ &\cdot \mu\left(\frac{q}{r(b(q), n)}\right)\overline{\chi^*}\left(\frac{q}{r(b(q), n)}\right)\mu(q/r)\chi^*(q/r)|\tau(\overline{\chi^*})|^2,\end{aligned}$$

if $r(b(q), n)|q$ and 0 otherwise. Thus from Lemma 9.3,

$$|c_{\overline{\chi}}(lb'(q)b(q) + n)\overline{\tau(\overline{\chi})}| \le q$$

and putting this in (9.2), we obtain

$$\begin{aligned}R_1(n, M) &\le \sum_{q\le P}\frac{q}{\varphi(D(q))\varphi(q)}\sum_{\chi \bmod q}\left|\int_{-1/qQ}^{1/qQ} V(\eta)\overline{W(\chi, \eta)}e(n\eta)d\eta\right|\\ &\le \sum_{q\le P}\frac{q}{\varphi(D(q))\varphi(q)}\sum_{\chi \bmod q}\left(\int_{-1/qQ}^{1/qQ} V(\eta))^2 d\eta\right)^{1/2}\\ &\cdot\left(\int_{-1/qQ}^{1/qQ}|W(\chi, \eta)|^2 d\eta\right)^{1/2}.\end{aligned} \tag{9.3}$$

The first integral on the right of (9.3) may be trivially estimated:

$$\begin{aligned}\left(\int_{-1/qQ}^{1/qQ}|V(\eta)|^2 d\eta\right)^{1/2} &\le \left(\int_0^1 |V(\eta)|^2 d\eta\right)^{1/2}\\ &= \left(\sum_{x_1<m\le x_2} 1/\log^2 m\right)^{1/2} \ll N^{1/2}/\log N.\end{aligned} \tag{9.4}$$

If $\chi \bmod q$ is induced by the primitive character $\chi^* \bmod r$, then $W(\chi, \eta) = W(\chi^*, \eta)$, so that

$$\left(\int_{-1/qQ}^{1/qQ}|W(\chi, \eta)|^2 d\eta\right)^{1/2} \le \left(\int_{-1/Q}^{1/Q}|W(\chi^*, \eta)|^2 d\eta\right)^{1/2} := W(\chi^*). \tag{9.5}$$

Assembling (9.3), (9.4), and (9.5), we have

$$\begin{aligned}\sum_{M\le Z} R_1(n, M) &\ll \frac{N^{1/2}}{\log N}\sum_{M\le Z}\sum_{q\le P}\frac{q}{\varphi([M, q])\varphi(q)}\sum_{\chi \bmod q} W(\chi^*)\\ &\ll N^{1/2}\sum_{M\le Z}\sum_{q\le P}\frac{(q, M)}{qM}\sum_{\chi \bmod q} W(\chi^*) \qquad (9.6)\\ &= N^{1/2}\sum_{r\le P}\sum_{\chi \bmod r}^{*} W(\chi)\sum_{M\le Z}\sum_{k\le P/r}\frac{(kr, M)}{krM},\end{aligned}$$

where $\sum^*$ denotes a sum over primitive characters.

The sum over M and k is easily estimated as follows:

$$\begin{aligned}\sum_{M\le Z}\sum_{k\le P/r}\frac{(kr, M)}{krM} &\le \sum_{d_1\mid r}\sum_{d_2\le Z/d_1}\sum_{\substack{k\le P/r\\ d_2\mid k}}\sum_{\substack{M\le Z\\ d_1d_2\mid M}}\frac{d_1d_2}{krM}\\ &\ll \log Z\sum_{d_1\mid r}\sum_{d_2\le Z/d_1}\sum_{\substack{k\le P/r\\ d_2\mid k}}\frac{1}{kr}\\ &\ll \log Z\log(P/r)\sum_{d_1\mid r}\sum_{d_2\le Z/d_1}\frac{1}{d_2r}\\ &\ll \log^2 Z\log(P/r)\sum_{d_1\mid r}1/r \le \frac{\tau(r)}{r}\log^3 N.\end{aligned}$$

Putting this calculation into (9.6) we obtain

$$\sum_{M\le Z} R_1(n, M) \ll N^{1/2}\log^3 N\sum_{r\le P}\sum_{\chi \bmod r}^{*}\frac{\tau(r)}{r}W(\chi). \qquad (9.7)$$

If $1 < r \le P$ and χ is a primitive character mod r, Lemma 4.2 in [10] implies

$$\begin{aligned}W(\chi) &\ll \left(\int_0^N\left|\frac{1}{Q}\sum_{\substack{x<p\le x+Q/2\\ x_1<p\le x_2}}\chi(p)\right|^2 dx\right)^{1/2} \qquad (9.8)\\ &\ll N^{1/2}\max_{0\le x\le N}\frac{1}{Q}\left|\sum_{\substack{x<p\le x+Q/2\\ x_1<p\le x_2}}\chi(p)\right|.\end{aligned}$$

Now by partial summation,

$$\max_{0\le x\le N}\left|\sum_{\substack{x<p\le x+Q/2\\ x_1<p\le x_2}}\chi(p)\right| \ll \frac{1}{\log N}\max_{0\le x\le N}\max_{0<h\le Q/2}\left|\sum_{x}^{x+h}\chi(p)\log p\right|,$$

so that

$$W(\chi)\ll \frac{N^{1/2}}{\log N}\max_{0\le x\le N}\max_{0<h\le Q/2}\frac{1}{h+Q}\left|\sum_{x}^{x+h}\chi(p)\log p\right|, \tag{9.9}$$

since $1/(h+Q) > 1/2Q$. By a similar argument we have for the primitive, principal character χ_0

$$W(\chi_0)\ll \frac{N^{1/2}}{\log N}\max_{0\le x\le N}\max_{0<h\le Q/2}\frac{1}{h+Q}\left|-h+\sum_{x}^{x+h}\log p\right|. \tag{9.10}$$

We now quote a result which we shall use in (9.7) for small values of r.

Lemma 9.4. *There is an absolute constant $c_2>0$ such that for any $E>0$ and any nonprincipal character χ to a modulus not exceeding $(\log x)^E$, we have*

$$\left|\sum_{x}^{x+h}\chi(p)\log p\right| \ll_{E,\varepsilon} h\exp(-(\log x)^{1/4-\varepsilon})$$

for every $\varepsilon>0$ and all h with $x^{1-c_2}<h\le x$. Moreover, for the same range of h we have

$$\sum_{x}^{x+h}\log p = h(1+O_\varepsilon(\exp(-(\log x)^{1/4-\varepsilon}))).$$

This result follows from Satz 8.6.2 and the proof of Satz 9.3.2 in Prachar [11].

Applying Lemma 9.4 with E replaced by $E+4$, we have from (9.9) and (9.10) that

$$\sum_{1\le r\le(\log N)^{E+4}}{\sum_{\chi \bmod r}}^{*} W(\chi)\ll N^{1/2}\exp(-(\log N)^{1/5}) \tag{9.11}$$

provided we choose $c_1<c_2/4$.

We now wish to apply Lemma 4.3 in [10] (which is based on Theorem 7 in Gallagher [4]). To use this result we must impose a second restriction on c_1. Thus for some absolute constant $c_1>0$ we have (9.11) and, using (9.9),

$$\sum_{1<r\le PZ}{\sum_{\substack{\chi \bmod r\\ \chi\ne\tilde{\chi}}}}^{*} W(\chi)\ll N^{1/2}, \tag{9.12}$$

where $\tilde{\chi}$ is the possible exceptional character (with modulus $\tilde{r}$). Note that the range for r in (9.12) is larger than we shall need in (9.7); however, such a long range is needed in the next two sections.

If $\tilde{\chi}$ should exist, then (9.8) trivially implies

$$W(\tilde{\chi}) \ll N^{1/2} \tag{9.13}$$

and Siegel's theorem implies

$$\tilde{r} > (\log N)^{E+4} \tag{9.14}$$

for N sufficiently large.

To complete the proof of (9.1) we use the inequality

$$\tau(r) = r^{o(1)}. \tag{9.15}$$

Thus from (9.7) and (9.11)–(9.15), we have

$$\begin{aligned}\sum_{M\le Z} R_1(n, M) &\ll N\exp(-(\log N)^{1/5}) \\ &\quad + N^{1/2}\log^3 N \sum_{(\log N)^{E+4}<r\le P}\ \sum_{\chi \bmod r}^{*} \frac{\tau(r)}{r} W(\chi) \\ &\ll N\exp(-(\log N)^{1/5}) \\ &\quad + N^{1/2}(\log N)^{-E} \sum_{1<r\le P}\ \sum_{\chi \bmod r}^{*} W(\chi) \\ &\ll N(\log N)^{-E},\end{aligned}$$

which is (9.1).

10. The second major arc error term

In this section we shall show that for any A, B, $E > 0$,

$$\sum_{M\le Z} R_2(n, M) \ll_{A,B,E} N(\log N)^{-E}, \tag{10.1}$$

where $R_2(n, M)$ is given by (7.13) and (7.11).

The following lemma will allow us to estimate the inner sum in (7.11).

Lemma 10.1. *Suppose M, q are natural numbers with q squarefree, $D = [M, q]$, $d = (M, q)$, $b = q/d$, and χ is a character* mod D. *If n, l satisfy* (3.1), *then*

$$\left| \sum_{\substack{a \bmod q \\ (a,q)=1}} \rho_{a,l}(\chi) e_q(an) \right| \le b\tau(b),$$

where $\rho_{a,l}(\chi)$ is defined in (7.3).

Proof. From (7.2), (7.3), and Lemma 8.1, we have

$$\begin{aligned}
&\sum_{\substack{a=1\\(a,q)=1}}^{q} \rho_{a,l}(\chi)e_q(an)\\
&\quad=\sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{t=1\\t\equiv al \bmod d\\(t,q)=1}}^{q} \overline{\chi}(c(l,t,a))e_q(an+t)\\
&\quad=\sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{s\equiv l \bmod M}^{D} \overline{\chi}(s)e_q(a(n+s)) \qquad (10.2)\\
&\quad=\sum_{s\equiv l \bmod M}^{D} \overline{\chi}(s)c_q(n+s)\\
&\quad=\sum_{s\equiv l \bmod M}^{D} \overline{\chi}(s)\varphi((q,n+s))\mu\left(\frac{q}{(q,n+s)}\right).
\end{aligned}$$

Note that for $s \equiv l \bmod M$

$$(q, n+s) = (b, n+s)(d, n+s) = (b, n+s)(d, n+l) = (b, n+s)$$

from (3.1). Thus from (10.2) we have

$$\begin{aligned}
\left|\sum_{\substack{a=1\\(a,q)=1}}^{q} \rho_{a,l}(\chi)e_q(an)\right| &\le \sum_{s\equiv l \bmod M}^{D} (b, n+s)\\
&=\sum_{s=1}^{b}(b,s) \le \sum_{d|b}\sum_{\substack{s=1\\d|s}}^{b} d = \sum_{d|b} b = b\tau(b),
\end{aligned}$$

which proves the lemma.

Using the lemma in (7.11) and the kind of calculation as in (9.3)–(9.5), we have

$$\begin{aligned}
R_2(n,M) &\le \sum_{q\le P}\frac{b(q)\tau(b(q))}{\varphi(D(q))\varphi(q)}\sum_{\chi \bmod D(q)}\left|\int_{-1/qQ}^{1/qQ}\overline{V(\eta)}W(\chi,\eta)e(n\eta)\,d\eta\right|\\
&\ll \frac{N^{1/2}}{\log N}\sum_{q\le P}\frac{b(q)\tau(b(q))}{\varphi(D(q))\varphi(q)}\sum_{\chi \bmod D(q)} W(\chi^*)\\
&\ll N^{1/2}\sum_{q\le P}\frac{\tau(q)}{Mq}\sum_{\chi \bmod D(q)} W(\chi^*),
\end{aligned}$$

where χ^* is the primitive character that induces χ. Thus

$$\begin{aligned}
\sum_{M\le Z} R_2(n,m) &\ll N^{1/2}\sum_{M\le Z}\sum_{q\le P}\frac{\tau(q)}{Mq}\sum_{\chi \bmod D(q)} W(\chi^*)\\
&= N^{1/2}\sum_{D\le PZ}\sum_{\chi \bmod D} W(\chi^*)\sum_{M\le Z}\sum_{\substack{q\le P\\ [M,q]=D}}\frac{\tau(q)}{Mq}\\
&\le N^{1/2}\sum_{r\le PZ}\sum_{\chi \bmod r}^{*} W(\chi)\sum_{u\le PZ/r}\sum_{M\le Z}\sum_{\substack{q\le P\\ [M,q]=ur}}\frac{\tau(q)}{Mq}\\
&\le N^{1/2}\sum_{r\le PZ}\sum_{\chi \bmod r}^{*} W(\chi)\sum_{u\le PZ}\frac{\tau^3(ur)}{ur}\\
&\le N^{1/2}\sum_{r\le PZ}\sum_{\chi \bmod r}^{*}\frac{\tau^3(r)}{r}W(\chi)\sum_{u\le PZ}\frac{\tau^3(u)}{u}\\
&\ll N^{1/2}\log^8 N\sum_{r\le PZ}\sum_{\chi \bmod r}^{*}\frac{\tau^3(r)}{r}W(\chi).
\end{aligned} \tag{10.3}$$

Thus using (9.11)–(9.15) (with $E+4$ replaced by $E+9$) in (10.3), we get (10.1).

11. The third major arc error term

In this section we shall show that for any A, B, $E>0$

$$\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}}\sum_{M\le Z} R_3(n,M) \ll_{A,B,E} N^2(\log N)^{-E}, \tag{11.1}$$

where $R_3(n,M)$ is given in (7.12) and (7.13). This estimate will complete the proof of Theorem 3.1, which is obtained by assembling (6.4), (6.7), (7.8), (8.5), (9.1), (10.1), and (11.1).

We begin with some algebraic manipulations on the inner sum in (7.12).

Lemma 11.1. *Suppose n, l, M satisfy (3.1), q is a natural number, $D=[M,q]$, χ_1 is a character* mod D, *χ_2 is a character* mod q *induced by the primitive character χ_2^** mod r, *and b_2 is the largest divisor of q coprime to Mr. Then with $\rho_{a,l}(\chi_1)$ defined by (7.3) and with*

$$R := \sum_{a=1}^{q}\rho_{a,l}(\chi_1)e_q(an)\overline{\chi}_2(a)\overline{\tau(\overline{\chi}_2)},$$

we have $R=0$, unless q/r is squarefree and coprime to r, in which case we have

$$R = r\sum_{w\mid b_2}\mu(w)w\sum_{\substack{s=1\\ s\equiv l \bmod M\\ s\equiv -n \bmod w}}^{D}\overline{\chi}_1(s)\chi_2^*(n+s).$$

Proof. From Lemma 9.2 we have

$$\overline{\tau(\overline{\chi}_2)} = \mu(q/r)\chi_2^*(q/r)\tau(\overline{\chi_2^*}). \tag{11.2}$$

Thus $R = 0$ unless q/r is squarefree and coprime to r; we now assume q, r satisfy these conditions.

As in the proof of Lemma 10.1 we have (where as usual, $d = (M, q)$)

$$\begin{aligned} R &= \sum_{a=1}^{q} \sum_{\substack{t=1 \\ t\equiv al \bmod d \\ (t,q)=1}}^{D} \overline{\chi}_1(c(l,t,a))e_q(an+t)\overline{\chi}_2(a)\overline{\tau(\overline{\chi}_2)} \\ &= \sum_{a=1}^{q} \sum_{\substack{s=1 \\ s\equiv l \bmod M}}^{D} \overline{\chi}_1(s)e_q(a(n+s))\overline{\chi}_2(a)\overline{\tau(\overline{\chi}_2)} \qquad (11.3) \\ &= \sum_{\substack{s=1 \\ s\equiv l \bmod M}}^{D} \overline{\chi}_1(s)c_{\overline{\chi}_2}(n+s)\overline{\tau(\overline{\chi}_2)}. \end{aligned}$$

We now use Lemma 9.1 for $c_{\overline{\chi}_2}(n+s)$. This expression will be 0 unless $r(q, n+s)|q$. Since q/r is now assumed coprime to r, this condition is equivalent to $(r, n+s) = 1$. But (3.1) and $s \equiv l \bmod M$ imply $(M, n+s) = 1$. Thus we need only consider those s in (11.3) with $(q, n+s) = (b_2, n+s)$, where, recall, b_2 is the largest divisor of q coprime to Mr.

Thus using (11.2) and Lemma 9.1, (11.3) gives

$$\begin{aligned} R = & \sum_{\substack{s=1 \\ s\equiv l \bmod M \\ (q,n+s)=(b_2,n+s)}}^{D} \overline{\chi}_1(s)\chi_2^*\left(\frac{n+s}{(b_2, n+s)}\right)\frac{\varphi(q)}{\varphi(q/(b_2, n+s))} \\ & \cdot \mu\left(\frac{q}{r(b_2, n+s)}\right)\overline{\chi_2^*}\left(\frac{q}{r(b_2, n+s)}\right)\tau(\overline{\chi_2^*})\overline{\tau(\overline{\chi}_2)} \\ = & \sum_{\substack{s=1 \\ s\equiv l \bmod M \\ (q,n+s)=(b_2,n+s)}}^{D} \overline{\chi}_1(s)\chi_2^*\left(\frac{n+s}{(b_2, n+s)}\right) \\ & \cdot \varphi((b_2, n+s))\mu((b_2, n+s))\chi_2^*((b_2, n+s))|\tau(\overline{\chi_2^*})|^2 \\ = & \, r \sum_{\substack{s=1 \\ s\equiv l \bmod M}}^{D} \overline{\chi}_1(s)\chi_2^*(n+s)\varphi((b_2, n+s))\mu((b_2, n+s)). \end{aligned}$$

Note that we may drop the restriction $(q, n+s) = (b_2, n+s)$, since if this fails

then $(r, n+s) > 1$ and $\chi_2^*(n+s) = 0$. Thus

$$R = r\sum_{u|b_2} \sum_{\substack{s=1 \\ s\equiv l \bmod M \\ s\equiv -n \bmod u}}^{D} \sum_{v|(b_2/u,(n+s)/u)} \mu(v)\overline{\chi}_1(s)\chi_2^*(n+s)\varphi(u)\mu(u)$$

$$= r\sum_{u|b_2} \sum_{v|b_2/u} \mu(uv)\varphi(u) \sum_{\substack{s=1 \\ s\equiv l \bmod M \\ s\equiv -n \bmod uv}}^{D} \overline{\chi}_1(s)\chi_2^*(n+s)$$

$$= r\sum_{w|b_2} \mu(w)w \sum_{\substack{s=1 \\ s\equiv l \bmod M \\ s\equiv -n \bmod w}}^{D} \overline{\chi}_1(s)\chi_2^*(n+s),$$

which proves the lemma.

Lemma 11.2. *If n, D, r are natural numbers with $r|D$, χ is a character* mod D, *and ψ is a primitive character* mod r, *then $S := \sum_{s=1}^{D} \chi(s)\psi(n+s)$ is 0 unless the conductor of χ divides r and the conductor of $\chi\psi$ divides $r/(r, n)$ in which case*

$$|S| \le D\sqrt{\frac{(r, n)}{r}}.$$

Proof. Since ψ is primitive, we have

$$\psi(n+s) = \tau(\overline{\psi})^{-1} \sum_{a \bmod r} \overline{\psi}(a)e_r(a(n+s)),$$

so that

$$\begin{aligned} S &= \tau(\overline{\psi})^{-1} \sum_{a \bmod r} \overline{\psi}(a) \sum_{s=1}^{D} \chi(s)e_r(a(n+s)) \\ &= \tau(\overline{\psi})^{-1} \sum_{a \bmod r} \overline{\psi}(a)e_r(an)c_\chi\left(a\frac{D}{r}\right). \end{aligned} \tag{11.4}$$

When $(a, r) = 1$ we have

$$\frac{D}{(D, aD/r)} = \frac{r}{(r, a)} = r, \tag{11.5}$$

so that Lemma 9.1 implies $c_\chi(aD/r) = 0$ unless (where $\mathrm{cond}(\chi)$ denotes the conductor of χ)

$$D_1 := \mathrm{cond}(\chi) | r. \tag{11.6}$$

With this assumption, Lemma 9.1 implies

$$c_\chi\left(a\frac{D}{r}\right) = \overline{\chi^*}(a)\frac{\varphi(D)}{\varphi(r)}\mu\left(\frac{r}{D_1}\right)\chi^*\left(\frac{r}{D_1}\right)\tau(\chi^*),$$

since (11.5) implies

$$\frac{aD/r}{(D, aD/r)} = a.$$

Putting this in (11.4), we have

$$S = \frac{\tau(\chi^*)}{\tau(\overline{\psi})}\frac{\varphi(D)}{\varphi(r)}\mu\left(\frac{r}{D_1}\right)\chi^*\left(\frac{r}{D_1}\right)\sum_{a \bmod r}\overline{\chi^*}(a)\overline{\psi}(a)e_r(an)$$

$$= \frac{\tau(\chi^*)}{\tau(\overline{\psi})}\frac{\varphi(D)}{\varphi(r)}\mu\left(\frac{r}{D_1}\right)\chi^*\left(\frac{r}{D_1}\right)c_{\overline{\chi^*}\overline{\psi}}(n), \tag{11.7}$$

since (11.6) implies $\overline{\chi^*}\overline{\psi}$ is a character mod r.

Let $D_2 = \operatorname{cond}(\chi\psi) = \operatorname{cond}(\overline{\chi^*}\overline{\psi})$. Thus $D_2 | r$ and Lemma 9.1 implies $c_{\overline{\chi^*}\overline{\psi}}(n) = 0$ unless

$$D_2 \Big| \frac{r}{(r, n)}. \tag{11.8}$$

Thus $S = 0$ unless both (11.6) and (11.8) hold, which proves the first assertion of the lemma. Further, with these conditions on D_1 and D_2 holding, Lemma 9.1 implies

$$c_{\overline{\chi^*}\overline{\psi}}(n) = \overline{\sigma}\left(\frac{n}{(r, n)}\right)\frac{\varphi(r)}{\varphi(r/(r, n))}\mu\left(\frac{r}{D_2(r, n)}\right)\sigma\left(\frac{r}{D_2(r, n)}\right)\tau(\sigma),$$

where σ is the primitive character mod D_2 that induces $\overline{\chi^*}\overline{\psi}$. Putting this in (11.7), we have

$$S = \frac{\tau(\chi^*)\tau(\sigma)}{\tau(\overline{\psi})}\frac{\varphi(D)}{\varphi(r/(r, n))}\mu\left(\frac{r}{D_1}\right)\mu\left(\frac{r}{D_2(r, n)}\right)$$
$$\cdot\chi^*\left(\frac{r}{D_1}\right)\sigma\left(\frac{r}{D_2(r, n)}\right)\overline{\sigma}\left(\frac{n}{(r, n)}\right),$$

so that

$$|S| \le \frac{\sqrt{D_1}\sqrt{D_2}}{\sqrt{r}}\cdot\frac{D(r, n)}{r} \le \sqrt{D_2}\frac{D(r, n)}{r} \le D\sqrt{\frac{(r, n)}{r}},$$

using (11.6) and (11.8). This completes the proof of the lemma.

Lemma 11.3. *With R given in Lemma 11.1 and with $M, q \le N$, we have*

$$|R| \ll \frac{D\sqrt{r}}{M}(r, M)\sqrt{(r, n)}\tau(b_2)\log\log N$$
$$\le q\tau(q)\sqrt{r(r, n)}\log\log N.$$

Proof. If $w | b_2$, let $c'(w)$ denote that residue $\bmod Mw$ with

$$c'(w) \equiv l \bmod M, \quad c'(w) \equiv -n \bmod w.$$

Thus

$$\sum_{\substack{s=1\\ s\equiv l \bmod M\\ s\equiv -n \bmod w}}^{D} \overline{\chi}_1(s)\chi_2^*(n+s)$$

$$= \frac{1}{\varphi(Mw)} \sum_{\psi \bmod Mw} \overline{\psi}(c'(w)) \sum_{s=1}^{D} \psi(s)\overline{\chi}_1(s)\chi_2^*(n+s) \tag{11.9}$$

$$= \frac{1}{\varphi(Mw)} \sum_{\substack{\psi \bmod Mw\\ \operatorname{cond}(\psi\chi_1\chi_2)\mid \frac{r}{(r,n)}}} \overline{\psi}(c'(w)) \sum_{s=1}^{D} (\psi\overline{\chi}_1)(s)\chi_2^*(n+s),$$

using Lemma 11.2 to restrict the sum on ψ. Now $(b_2, r) = 1$, so the number of $\psi \bmod Mw$ with $\operatorname{cond}(\psi\chi_1\chi_2)|r/(r, n)$ is

$$\left(Mw, \frac{r}{(r,n)}\right) = \left(M, \frac{r}{(r,n)}\right) \le (r, M).$$

Thus (11.9) and Lemmas 11.1 and 11.2 imply

$$|R| \le r \sum_{w|b_2} w \frac{1}{\varphi(Mw)} (r, M) D \sqrt{\frac{(r,n)}{r}}$$

$$\ll \frac{D\sqrt{r}}{M} (r, M) \sqrt{(r,n)}\tau(b_2) \log\log N,$$

which proves the lemma.

Using Lemma 11.3 in (7.12), we have

$$R_3(n, M) \ll (\log\log N)^3 \sum_{q\le P} \frac{\tau(q)}{D(q)} \sum_{r|q} \sqrt{r(r,n)}$$

$$\cdot \sum_{\substack{\chi_1 \bmod D(q)\\ \chi_2 \bmod q\\ \operatorname{cond}(\chi_2)=r}} \left| \int_{-1/qQ}^{1/qQ} W(\chi_1, \eta)\overline{W(\chi_2, \eta)} e(n\eta)\, d\eta \right|$$

$$\le (\log\log N)^3 \sum_{q\le P} \frac{\tau(q)}{D(q)} \sum_{r|q} \sqrt{r(r,n)} \sum_{\substack{\chi_1 \bmod D(q)\\ \chi_2 \bmod q\\ \operatorname{cond}(\chi_2)=r}} W(\chi_1^*)W(\chi_2^*),$$

where χ_1^*, χ_2^* are the primitive characters that induce χ_1, χ_2. Thus (11.10)

$$\sum_{M\le Z} R_3(n, M) \ll (\log\log N)^3 \sum_{M\le Z}\sum_{q\le P}\frac{\tau(q)}{[M, q]}\sum_{r|q}\sqrt{r(r, n)}\sum_{s|[M,q]}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2)$$

$$\le (\log\log N)^3 \sum_{D\le PZ}\sum_{M|D}\sum_{\substack{q\\ [M,q]=D}}\frac{\tau(D)}{D}\sum_{\substack{r,s\\ [r,s]|D}}\sqrt{r(r, n)}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2)$$

$$\le (\log\log N)^3 \sum_{D\le PZ}\frac{\tau^3(D)}{D}\sum_{\substack{r,s\\ [r,s]|D}}\sqrt{r(r, n)}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2)$$

$$\le (\log\log N)^3 \sum_{r,s\le PZ}\sum_{t\le PZ/[r,s]}\frac{\tau^3([r, s]t)}{[r, s]t}\sqrt{r(r, n)}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2)$$

$$\ll (\log N)^9 \sum_{r,s\le PZ}\frac{\tau^3([r, s])}{[r, s]}\sqrt{r(r, n)}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2).$$

Now

$$\sum_{n\le N}\sqrt{(r, n)} \le \sum_{d|r}\sqrt{d}\frac{N}{d} \le N\tau(r).$$

Thus from (11.10) we have

$$\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}}^{\cdot}\sum_{M\le Z} R_3(n, M)$$

$$\ll N(\log N)^9 \sum_{r,s\le PZ}\frac{\tau^4(r)\tau^3(s)(r, s)}{r^{1/2}s}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2)$$

$$= N(\log N)^9 \sum_{r,s\le PZ}\frac{\tau^4(r)(r, s)^{1/4}}{r^{1/2}}\cdot\frac{\tau^3(s)(r, s)^{3/4}}{s}\sum_{\substack{\chi_1 \bmod s\\ \chi_2 \bmod r}}^{*} W(\chi_1)W(\chi_2)$$

$$\le N(\log N)^9\left(\sum_{r\le PZ}\frac{\tau^4(r)}{r^{1/4}}\sum_{\chi \bmod r}^{*} W(\chi)\right)^2.$$

We now obtain (11.1) by using in this last estimate (9.11)–(9.15) (with $E+4$ replaced by $2E+19$).

12. Proof of Theorem 3.2

Let $\nu(n)$ denote the number of distinct prime factors of n. We begin with the following simple corollary of Theorem 3.1. The notation is as defined in §3.

Lemma 12.1. *For any $E > 0$ we have*

$$\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}}\sum_{M\le Z} 6^{\nu(M)} R(n, M) \ll_{A,B,E} N^2(\log N)^{-E}.$$

Proof. Using the trivial estimate $R(n, M) \ll N/M$, Theorem 3.1 (with E replaced by $2E + 36$), and the Cauchy-Schwarz inequality, the double sum in the lemma is at most

$$\left(\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}}\sum_{M\le Z} 36^{\nu(M)}R(n, M)\right)^{1/2}\left(\sum_{\substack{n\le N\\ n\equiv 0 \bmod 2}}\sum_{M\le Z} R(n, M)\right)^{1/2}$$
$$\ll_{A,B,E} N^{1/2}\left(\sum_{M\le Z} 36^{\nu(M)}N/M\right)^{1/2} N(\log N)^{-E-18}$$
$$\ll N^2(\log N)^{-E},$$

which is what we wanted to prove.

The proof of Theorem 3.2 will use Theorem 7.1 in Halberstam and Richert [5]. Let

$$\mathbf{A} = \mathbf{A}(n, m) = \{(mp - 1)(mp' - 1): p' = p + n, p \in \mathbf{T}(n)\},$$
$$X = X(n) = \alpha_0 T(n)\prod_{\substack{p\mid n\\ p>2}}\frac{p-1}{p-2}.$$

Let $\omega = \omega_{n,m}$ be the multiplicative function such that

$$\omega(p) = \begin{cases} \dfrac{2p}{p-2}, & \text{if } p \nmid (nm)^3 - nm,\\ \dfrac{p}{p-2}, & \text{if } p\mid (nm)^2 - 1,\\ \dfrac{p}{p-1}, & \text{if } p\mid n \text{ and } p \nmid m,\\ 0, & \text{if } p\mid m, \end{cases}$$

and $\omega(p^a) = 0$ for $a > 1$. Since both sides of (3.2) are 0 if $nm \not\equiv 0 \bmod 3$, we may assume $nm \equiv 0 \bmod 3$ in addition to our usual condition $n \equiv m \equiv 0 \bmod 2$. Thus $0 \le \omega(p)/p \le 2/3$ for every prime p, so that $1 \le 1/(1 - \omega(p)/p) \le 3$. Also, if w, z are any numbers with $2 \le w \le z$, then

$$\sum_{w\le p\le z}\frac{\omega(p)\log p}{p} \le 2\log\frac{z}{w} + O(1).$$

If $d\mid P(Y)$, let $\mathbf{A}_d = \{a \in \mathbf{A}: a \equiv 0 \bmod d\}$, $R_d = |\mathbf{A}_d| - (\omega(d)/d)X$.

Lemma 12.2. *If $d\mid P(Y)$, then $|R_d| \le 2^{\nu(d)}R(n, d) + \nu((nm)^2 - 1)$.*

Proof. We may assume $(d, m) = 1$, for otherwise $\mathbf{A}_d = \varnothing$ and $\omega(d) = 0$, so that $R_d = 0$. Write $d = efg$, where $e = (d, n(nm - 1))$, $f = (d, nm + 1)$. For each natural divisor g_1 of g, let

$$\mathbf{A}_{d,g_1} = \{(mp - 1)(mp' - 1) \in \mathbf{A}_d: mp \equiv 1 \bmod eg_1, mp' \equiv 1 \bmod fg/g_1\}.$$

Also, let

$$\mathbf{A}'_d = \{(mp-1)(mp'-1) \in \mathbf{A}_d : p|(e, nm-1) \text{ or } p'|f\}.$$

We first claim that the sets $\mathbf{A}_{d,g_1}$ and $\mathbf{A}'_d$ give a disjoint partition of $\mathbf{A}_d$. It is easily seen that they are disjoint subsets of $\mathbf{A}_d$. Indeed, since d is squarefree and

$$(mp-1, mp'-1) = (mp-1, n), \tag{12.1}$$

it follows that the various $\mathbf{A}_{d,g_1}$ for $g_1|d$ are disjoint. Moreover, if $p|e$, then clearly $e \nmid mp-1$; if $p'|f$, then $f \nmid mp'-1$.

To see that the sets $\mathbf{A}_{d,g_1}$ and $\mathbf{A}'_d$ cover $\mathbf{A}_d$, let $(mp-1)(mp'-1) \in \mathbf{A}_d$, where $p' = p+n$. We must show that if it is not the case that both $e|mp-1$ and $f|mp'-1$, then either $p|(e, nm-1)$ or $p'|f$. Let q be a prime dividing e. Then either $q|n$ or $q|nm-1$. If $q|n$, then (12.1) implies $q|mp-1$. If $q|nm-1$ and $q \nmid mp-1$, then

$$0 \equiv mp'-1 = mp+mn-1 \equiv mp \bmod q,$$

so $q = p$; that is, $p|(e, nm-1)$. Thus $p \nmid (e, nm-1)$ implies $e|mp-1$. Similarly $p' \nmid f$ implies $f|mp'-1$, for if a prime $q|f$ then $q|nm+1$ and so $mp-1 \equiv mp' \not\equiv 0 \bmod q$ implies $q|mp'-1$.

Next we note that if $l = l(g_1)$ satisfies

$$ml \equiv 1 \bmod eg_1, \quad m(l+n) \equiv 1 \bmod fg/g_1,$$

then $(l, d) = (l+n, d) = 1$ and

$$\mathbf{A}_{d,g_1} = \{(mp-1)(mp'-1) \in \mathbf{A}_d : p \in \mathbf{T}(n, l(g_1), d)\},$$

where $\mathbf{T}(n, l(g_1), d)$ is defined in §3. Thus

$$\begin{aligned} |\mathbf{A}_d| - |\mathbf{A}'_d| &= \sum_{g_1|g} T(n, l(g_1), d) \\ &= \frac{2^{\nu(g)}\alpha_0 T(n)}{\varphi(d)} \prod_{\substack{p|dn \\ p>2}} \frac{p-1}{p-2} + \sum_{g_1|g} R(n, l(g_1), d). \end{aligned} \tag{12.3}$$

Note that since d is squarefree,

$$\begin{aligned} \frac{2^{\nu(g)}}{\varphi(d)} \prod_{\substack{p|dn \\ p>2}} \frac{p-1}{p-2} &= 2^{\nu(g)} \left(\prod_{\substack{p|d \\ p\nmid n}} \frac{1}{p-2} \right) \left(\prod_{p|(d,n)} \frac{1}{p-1} \right) \left(\prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2} \right) \\ &= \frac{\omega(d)}{d} \prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2}. \end{aligned}$$

Thus from (12.3) and the definition of X, we have

$$R_d = \sum_{g_1|g} R(n, l(g_1), d) + |\mathbf{A}'_d|,$$

so that $|R_d| \le 2^{\nu(g)} R(n, d) + |\mathbf{A}'_d|$.

It remains to show that $|\mathbf{A}'_d| \le \nu((nm)^2 - 1)$. But this is immediate from the definition of $\mathbf{A}'_d$. This completes the proof of the lemma.

We now return to the proof of Theorem 3.2 by applying Theorem 7.1 in [5] with $q = 1$, $z = Y$, $\xi = Z^{1/2}$, $\tau = \log \xi / \log Y$. Thus

$$S(n, m) = X\left(\prod_{p \le Y}\left(1 - \frac{\omega(p)}{p}\right)\right)(1 + O((e\tau)^{-\tau})) + \theta \sum_{\substack{d \le Z \\ d \mid P(Y)}} 3^{\nu(d)}|R_d|, \tag{12.4}$$

where $|\theta| \le 1$ and the constant implied by the O-notation is uniformly bounded as n, m vary.

Let $D > 0$ be arbitrary. By Lemma 12.1, the number of even $n \le N$ for which

$$\sum_{M \le Z} 6^{\nu(M)} R(n, M) \le N(\log N)^{-B-E-5} \tag{12.5}$$

fails is $\cdot O(N(\log N)^{-D})$. So suppose $n \le N$, $n \equiv 0 \bmod 2$ and (12.5) holds for n. Then for all $m \le N$ with $m \equiv 0 \bmod 2$ and $nm \equiv 0 \bmod 3$, we have from Lemma 12.2 that

$$\begin{aligned} \sum_{\substack{d \le Z \\ d \mid P(Y)}} 3^{\nu(d)}|R_d| &\le \sum_{\substack{d \le Z \\ d \mid P(Y)}} (6^{\nu(d)} R(n, d) + 3^{\nu(d)} \nu((nm)^2 - 1)) \\ &\le \sum_{d \le Z} 6^{\nu(d)} R(n, d) + \nu((nm)^2 - 1) \sum_{d \le Z} 3^{\nu(d)} \\ &\ll N(\log N)^{-B-E-5} + Z(\log Z)^2 \log N \\ &\ll N(\log N)^{-B-E-5}. \end{aligned} \tag{12.6}$$

Putting (12.6) into (12.4), we have (3.2) for all even $n \le N$, except possibly at most $O(N(\log N)^{-D})$ exceptions, and for all even $m \le N$ with $m \equiv 0 \bmod 2$ and $nm \equiv 0 \bmod 3$. Indeed, the only new errors introduced are the product of $(p-3)/(p-2)$ over primes $p \mid (nm)^2 - 1$ with $p > Y$ and the product of $(p-2)/(p-1)$ over primes $p \mid (n, m)$ with $p > Y$. The error introduced by including these large primes in the products in (3.2) is a factor $1 + O(Y^{-1} \log N)$.

Finally recall that (3.2) holds trivially if $nm \not\equiv 0 \bmod 3$. This concludes the proof of Theorem 3.2.

Acknowledgment. We wish to thank András Sárközy and Joel Spencer for some helpful conversations.

REFERENCES

1. N. G. deBruijn, *On the number of positive integers* $\leq x$ *and free of prime factors* $> y$, Nederl. Akad. Wetensch. Proc. Ser. A **54** (1951), 50–60.
2. H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1936), 396–403.
3. P. Erdös, *On the difference of consecutive primes*, Quart. J. Math. Oxford Ser. **6** (1935), 124–128.
4. P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. **11** (1970), 329–339.
5. H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, 1974.
6. H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. **11** (1978), 225–231.
7. A. F. Lavrik, *The number of k-twin primes lying on an interval of a given length*, Dokl. Akad. Nauk SSSR **136** (1961), 281–283; English transl., Soviet Math. Dokl. **2** (1961), 52–55.
8. S.-t. Lou and Q. Yao, *On gaps between consecutive primes* (to appear).
9. H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Math., vol. 227, Springer-Verlag, Berlin and New York, 1971.
10. H. L. Montgomery and R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.
11. K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, Göttingen, and Heidelberg, 1957.
12. R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc. **13** (1938), 242–247.
13. ———, *The difference between consecutive prime numbers.* V, Proc. Edinburgh Math. Soc. (2) **13** (1962/63), 331–332.
14. A. Schönhage, *Eine Bemerkung zur Konstruktion grosser Primzahllücken*, Arch. Math. **14** (1963), 29–30.
15. D. Shanks, *On maximal gaps between successive primes*, Math. Comp. **18** (1964), 646–651.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602