Université de Montréal

Strings of congruent primes in short intervals

par

Tristan Freiberg

Département de mathématiques et de statistique

Faculté des arts et des sciences

Thèse présentée à la Faculté des études supérieures

en vue de l'obtention du grade de

Philosophiæ Doctor (Ph.D.)

en mathématiques

Orientation mathématiques fondamentales

novembre, 2010

Université de Montréal

Faculté des études supérieures

Cette thèse intitulée :

Strings of congruent primes in short intervals

présentée par :

Tristan Freiberg

a été évaluée par un jury composé des personnes suivantes :

Iosif Polterovich	président-rapporteur
Andrew Granville	directeur de recherche
Paul Gauthier	membre du jury
Daniel Goldston	examinateur externe
Iosif Polterovich	représentant du doyen de la FES

Thèse acceptée le :

17 Novembre 2010

CONTENTS

ABSTRACT

Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be the sequence of all primes, and let $q \geqslant 3$ and a be coprime integers. Recently, and very remarkably, Daniel Shiu proved an old conjecture of Sarvadaman Chowla, which asserts that there are infinitely many pairs of consecutive primes p_n, p_{n+1} for which $p_n \equiv p_{n+1} \equiv a \bmod q$. Now fix a number $\epsilon > 0$, arbitrarily small. In their recent groundbreaking work, Daniel Goldston, Jànos Pintz and Cem Yıldırım proved that there are arbitrarily large x for which the short interval $(x, x + \epsilon \log x]$ contains at least two primes congruent to $a \bmod q$. Given a pair of primes $\equiv a \bmod q$ in such an interval, there might be a prime in-between them that is not $\equiv a \bmod q$. One can deduce that *either* there are arbitrarily large x for which $(x, x + \epsilon \log x]$ contains a prime pair $p_n \equiv p_{n+1} \equiv a \bmod q$, *or* that there are arbitrarily large x for which the $(x, x+\epsilon \log x]$ contains a triple of consecutive primes p_n, p_{n+1}, p_{n+2}. Both statements are believed to be true, but one can only deduce that one of them is true, and one does not know which one, from the result of Goldston-Pintz-Yıldırım.

In Part I of this thesis, we prove that the first of these alternatives is true, thus obtaining a new proof of Chowla's conjecture. The proof combines some of Shiu's ideas with those of Goldston-Pintz-Yıldırım, and so this result may be regarded as an application of their method. We then establish lower bounds for the number of prime pairs $p_n \equiv p_{n+1} \equiv a \bmod q$ with $p_{n+1} - p_n < \epsilon \log p_n$ and

$p_{n+1} \leqslant Y$. Assuming a certain unproven hypothesis concerning what is referred to as the 'level of distribution', θ, of the primes, Goldston-Pintz-Yıldırım were able to prove that $p_{n+1} - p_n \ll_\theta 1$ for infinitely many n. On the same hypothesis, we prove that there are infinitely many prime pairs $p_n \equiv p_{n+1} \equiv a \bmod q$ with $p_{n+1} - p_n \ll_{q,\theta} 1$. This conditional result is also proved in a quantitative form.

In Part II we apply the techniques of Goldston-Pintz-Yıldırım to prove another result, namely that there are infinitely many pairs of distinct primes p, p' such that $(p-1)(p'-1)$ is a perfect square. This is, in a sense, an 'approximation' to the old conjecture that there are infinitely many primes p such that $p-1$ is a perfect square. In fact we obtain a lower bound for the number of integers n, up to Y, such that $n = \ell_1 \cdots \ell_r$, the ℓ_i distinct primes, and $(\ell_1 - 1) \cdots (\ell_r - 1)$ is a perfect rth power, for any given $r \geqslant 2$. We likewise obtain a lower bound for the number of such $n \leqslant Y$ for which $(\ell_1 + 1) \cdots (\ell_r + 1)$ is a perfect rth power. Finally, given a finite set A of nonzero integers, we obtain a lower bound for the number of $n \leqslant Y$ for which $\prod_{p|n}(p+a)$ is a perfect rth power, simultaneously for every $a \in A$.

Key words: applications of sieve methods; primes in short intervals; primes in progressions.

RÉSUMÉ

Soit $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ la suite des nombres premiers, et soient $q \geqslant 3$ et a des entiers premiers entre eux. Récemment, Daniel Shiu a démontré une ancienne conjecture de Sarvadaman Chowla. Ce dernier a conjecturé qu'il existe une infinité de couples p_n, p_{n+1} de premiers consécutifs tels que $p_n \equiv p_{n+1} \equiv a \bmod q$. Fixons $\epsilon > 0$. Une récente percée majeure, de Daniel Goldston, Jànos Pintz et Cem Yıldırım, a été de démontrer qu'il existe une suite de nombres réels x tendant vers l'infini, tels que l'intervalle $(x, x + \epsilon \log x]$ contienne au moins deux nombres premiers $\equiv a \bmod q$. Étant donné un couple de nombres premiers $\equiv a \bmod q$ dans un tel intervalle, il pourrait exister un nombre premier compris entre les deux qui n'est pas $\equiv a \bmod q$. On peut déduire que soit il existe une suite de réels x tendant vers l'infini, telle que $(x, x+\epsilon \log x]$ contienne un triplet p_n, p_{n+1}, p_{n+2} de nombres premiers consécutifs, soit il existe une suite de réels x, tendant vers l'infini telle que l'intervalle $(x, x+\epsilon \log x]$ contienne un couple p_n, p_{n+1} de nombres premiers tel que $p_n \equiv p_{n+1} \equiv a \bmod q$. On pense que les deux énoncés sont vrais, toutefois on peut seulement déduire que l'un d'entre eux est vrai, sans savoir lequel.

Dans la première partie de cette thèse, nous démontrons que le deuxième énoncé est vrai, ce qui fournit une nouvelle démonstration de la conjecture de Chowla. La preuve combine des idées de Shiu et de Goldston-Pintz-Yıldırım, donc on peut considérer que ce résultat est une application de leurs mt́hodes.

Ensuite, nous fournirons des bornes inférieures pour le nombre de couples p_n, p_{n+1} tels que $p_n \equiv p_{n+1} \equiv a \bmod q$, $p_{n+1} - p_n < \epsilon \log p_n$, avec $p_{n+1} \leqslant Y$.

Sous l'hypothèse que θ, le « niveau de distribution » des nombres premiers, est plus grand que $1/2$, Goldston-Pintz-Yıldırım ont réussi à démontrer que $p_{n+1} - p_n \ll_\theta 1$ pour une infinité de couples p_n, p_{n+1}. Sous la meme hypothèse, nous démontrerons que $p_{n+1} - p_n \ll_{q,\theta} 1$ et $p_n \equiv p_{n+1} \equiv a \bmod q$ pour une infinité de couples p_n, p_{n+1}, et nous prouverons également un résultat quantitatif.

Dans la deuxième partie, nous allons utiliser les techniques de Goldston-Pintz-Yıldırım pour démontrer qu'il existe une infinité de couples de nombres premiers p, p' tels que $(p-1)(p'-1)$ est une carré parfait. Ce resultat est une version approximative d'une ancienne conjecture qui stipule qu'il existe une infinité de nombres premiers p tels que $p-1$ est une carré parfait. En effet, nous démontrerons une borne inférieure sur le nombre d'entiers naturels $n \leqslant Y$ tels que $n = \ell_1 \cdots \ell_r$, avec $\ell_1, \ldots, \ell_r$ des premiers distincts, et tels que $(\ell_1 - 1) \cdots (\ell_r - 1)$ est une puissance r-ième, avec $r \geqslant 2$ quelconque. Également, nous démontrerons une borne inférieure sur le nombre d'entiers naturels $n = \ell_1 \cdots \ell_r \leqslant Y$ tels que $(\ell_1 + 1) \cdots (\ell_r + 1)$ est une puissance r-ième. Finalement, étant donné A un ensemble fini d'entiers non-nuls, nous démontrerons une borne inférieure sur le nombre d'entiers naturels $n \leqslant Y$ tels que $\prod_{p|n}(p+a)$ est une puissance r-ième, simultanément pour chaque $a \in A$.

Mots clés : applications des méthodes de crible ; nombres premiers dans les intervalles courts ; nombres premiers dans les progressions arithmétiques.

ACKNOWLEDGEMENTS

First of all, I would like to thank Andrew Granville. Without his guidance and encouragement I would never have proved the results in this thesis, and his feedback has improved its quality immensely. My thanks also to Paul Gauthier, Daniel Goldston, and Iosif Polterovich, for carefully reading this thesis, and for their corrections and comments.

I benefited greatly from discussions with Jorge Jiménez Urroz, who helped me understand the work of Goldston, Pintz and Yıldırım. I have also had many fruitful conversations with my colleagues and friends in the département de mathématiques. I thank them all, especially my fellow number theory students: Farzad Aryan, Mohammad Bardestani, Daniel Fiorilli, and Kevin Henriot. I am privileged to have been a member of the number theory community in Montréal.

I am grateful for financial support from the Institut des sciences mathématiques in Montréal. For very generously providing further financial assistance, I am extremely grateful to Mr. Robert Cripps, Professor John Morgan, and the St. John's College Foundation, of St. John's College within the University of Queensland, Australia.

Finally, for their constant support, my most heartfelt thanks go to Lien Do and my family: Anna, Giselle, John, and especially my father and mother, John and Wendy.

1. INTRODUCTION

1.1 Part I: Strings of congruent primes in short intervals

Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be the sequence of all primes. The prime number theorem states that $n \sim p_n / \log p_n$ as $n \to \infty$, and hence

$$\frac{1}{N} \sum_{n=1}^{N} \frac{p_{n+1} - p_n}{\log p_n} \to 1 \quad \text{as} \quad N \to \infty.$$

In this sense, the nth prime gap $p_{n+1} - p_n$ is around $\log p_n$ on average. From this we also deduce that

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} \leqslant 1.$$

In 2005, after decades of partial progress by various authors, Goldston, Pintz and Yıldırım [17, 21] made a spectacular breakthrough by proving the long-standing conjecture that

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

In words, the nth prime gap is infinitely often arbitrarily smaller than average.

Before Goldston-Pintz-Yıldırım, the most important development in this direction had been the work of Bombieri and Davenport [7], in which it is established that $\liminf_{n \to \infty} \, (p_{n+1} - p_n)/\log p_n \leqslant (2 + \sqrt{3})/8 = 0.46650 \ldots$.

Bombieri's work on the large sieve [5] is an essential feature of [7], and of all subsequent improvements of that result, including the work of Goldston-Pintz-Yıldırım. For a comprehensive historical background and survey of results related to this problem, see [20, 21, 31].

In [19] Goldston, Pintz and Yıldırım extended their original argument to primes in arithmetic progressions. Thus if we fix coprime integers $q \geqslant 3$ and a and let $p_1' < p_2' < \cdots$ be the sequence of all primes $\equiv a \bmod q$, as a consequence of [19, Theorem 1] we have

$$\liminf_{n\to\infty} \frac{p_{n+1}' - p_n'}{\log p_n'} = 0.$$

In other words, for any fixed $\epsilon > 0$, we have $p_{n+1}' - p_n' < \epsilon \log p_n'$ for infinitely many n.

Given such a pair p_n', p_{n+1}', there may or may not be a prime in-between them that is not $\equiv a \bmod q$. Hence one can deduce that *either* there are infinitely many pairs of consecutive primes $p_n \equiv p_{n+1} \equiv a \bmod q$ with $p_{n+1}-p_n < \epsilon \log p_n$, *or* that there are infinitely many triples of consecutive primes p_n, p_{n+1}, p_{n+2} with $p_{n+2} - p_n < \epsilon \log p_n$. Presumably both statements are true, however one can only deduce that one of them is true, and one does not know which one, from the result in [19].

In [32], Shiu proved an old conjecture of Chowla that there are infinitely many pairs of consecutive primes p_n, p_{n+1} which are both $\equiv a \bmod q$. Indeed he was even able to extend this to k consecutive primes. This was a spectacular accomplishment. We will combine the methods of Goldston-Pintz-Yıldırım and of Shiu to establish the following hybrid of those results:

Theorem 1. *Let $q \geqslant 3$ and a be integers with $(q, a) = 1$, and fix any $\epsilon > 0$. There exist infinitely many pairs of consecutive primes p_n, p_{n+1} such that $p_n \equiv p_{n+1} \equiv a \bmod q$ and $p_{n+1} - p_n < \epsilon \log p_n$.*

We will adapt the proof of Theorem 1 to obtain a lower bound for the number of prime strings up to a given number Y:

Theorem 2. *Let q, a and ϵ be fixed as in Theorem 1. For all sufficiently large Y, the number of pairs of consecutive primes $p_n, \ldots, p_{n+1} \leqslant Y$, with $p_n \equiv p_{n+1} \equiv a \bmod q$ and $p_{n+1} - p_n < \epsilon \log p_n$, is at least $Y^{1/3(\log\log Y)^A}$, where $A = A(q)$ is a constant depending only on q.*

This is rather weak as a quantitative result, but we will see that a technical improvement in a certain part of the proof of Theorem 1 would yield something better.

The notion of the level of distribution of the primes, which we will define in Section 3.2, plays an important role in the literature on short gaps between primes. It is known, by the celebrated Bombieri-Vinogradov theorem (see Lemma 2.4.5), that the primes have level of distribution at least 1/2, and the well-known Elliott-Halberstam conjecture (see [16]) asserts that they have level of distribution 1. Goldston-Pintz-Yıldırım [17, 21] proved that if the primes have level of distribution $\theta > 1/2$, then $\liminf_{n\to\infty}(p_{n+1} - p_n) \leqslant H(\theta)$ for some constant $H(\theta)$ depending only on θ, $H(0.971) = 16$ ([21, Theorem 1]). We will prove:

Theorem 3. *Let $q \geqslant 3$ and a be integers with $(q,a)=1$, and assume the primes have level of distribution $\theta > 1/2$. Then there exist infinitely many pairs of consecutive primes p_n, p_{n+1} such that $p_n \equiv p_{n+1} \equiv a \bmod q$ and $p_{n+1} - p_n \leqslant H$, where $H := H(q,\theta)$ is a constant depending only on q and θ. Moreover, if $\theta > 20/21$, then there is a constant L such that $H(q,\theta) \ll q^L$.*

This conditional result also has a quantitative form:

Theorem 4. *Let $q \geqslant 3$ and a be integers with $(q,a)=1$, assume the primes have level of distribution $\theta > 1/2$, and let $H := H(q,\theta)$ be as in Theorem 3. Then the number of pairs of consecutive primes $p_n, p_{n+1} \leqslant Y$, with $p_n \equiv p_{n+1} \equiv a \bmod q$ and $p_{n+1} - p_n \leqslant H$, is $\gg_{q,\theta} Y/(\log Y)^{B(\theta)}$, where $B(\theta)$ is a constant depending only on θ.*

The proof of Theorem 4 concludes Part I of this thesis. In Part II we will prove two more theorems, which are largely unrelated to theorems $1-4$. There is, however, a common thread linking the two parts of this thesis. Namely, the technique used to prove Theorem 5 is based on the technique of Goldston-Pintz-Yıldırım presented in Part I. Part I is an expansion of a preprint [15] by the author, and Part II is also available as a preprint [14] by the author. Both preprints [14] and [15] have been submitted for publication.

1.2 Part II: Products of shifted primes simultaneously taking perfect power values

If we pick a large integer close to x at random, the probability that it is a perfect rth power is around $x^{1/r}/x$. We might expect the shifted primes $p+a$ to behave more or less like random integers in terms of their multiplicative properties. Thus, if we take a large squarefree integer n close to x, we might naively expect that $\sigma(n) = \prod_{p|n}(p+1) \approx n$ is an rth power with probability close to $x^{1/r}/x$. However, as we will see, the probability is much higher than this, indeed more than $x^{0.7038}/x$, for *any* given r. We will even show that the likelihood of $\phi(n)$ and $\sigma(n)$ *simultaneously* being (different) rth powers is more than $x^{0.2499}/x$. (As usual, ϕ denotes Euler's totient function and σ denotes the sum-of-divisors function.) It would seem that rth powers are 'popular' values for products of shifted primes in general.

If we only count those n with exactly r prime factors, we will show that the number of such n up to x for which $\phi(n)$ is a perfect rth power is $\gg x^{1/r}/(\log x)^{r+2}$, and likewise for $\sigma(n)$. Thus there are $\gg x^{1/2}/(\log x)^4$ integers $n \leqslant x$ for which $n = pq$, p and q distinct primes, and $(p-1)(q-1)$ is a square. This may be seen as an 'approximation' to the well-known conjecture that there are infinitely many primes p for which $p-1$ is a square. It is easily seen that there is at most one prime p for which $p+1$ is a perfect rth power $(r \geqslant 2)$, namely $3+1=2^2$, $7+1=2^3$, and so on.

Given an integer $r \geqslant 2$ and a finite, nonempty set A of nonzero integers, let

$$\mathcal{B}(x; A, r) := \Big\{ n \leqslant x : n \text{ is squarefree and } \\ \textstyle\prod_{p|n}(p+a) \text{ is an } r\text{th power for all } a \in A \Big\}.$$

Banks et. al. [4] proved, among several other results, that $|\mathcal{B}(x;\{-1\},2)|$, $|\mathcal{B}(x;\{+1\},2)| \geqslant x^{0.7039-o(1)}$, and that $|\mathcal{B}(x;\{-1,+1\},2)| \geqslant x^{1/4-o(1)}$, where $o(1)$ denotes a function tending to 0 as x tends to infinity. Theorem 5 generalizes both of these results.

Theorem 5. *Fix an integer $r \geqslant 2$, and a finite, nonempty set A of nonzero integers. As $x \to \infty$, we have*

$$|\mathcal{B}(x; A, r)| \geqslant x^{1/2|A|-o(1)}.$$

Moreover, if $|A| = 1$, then as $x \to \infty$, we have

$$|\mathcal{B}(x; A, r)| \geqslant x^{0.7039-o(1)}.$$

In the case $A = \{-1\}$ (respectively $A = \{+1\}$), $\mathcal{B}(x; A, r)$ is the set of squarefree integers n up to x for which $\phi(n)$ (respectively $\sigma(n)$) is an rth power. There is no condition on the number of prime factors of n, but Theorem 6 concerns

$$\mathcal{B}^*(x; -1, r) = \{n \leqslant x : n \text{ is squarefree, } \omega(n) = r \text{ and } \phi(n) \text{ is an } r\text{th power}\},$$
$$\mathcal{B}^*(x; +1, r) = \{n \leqslant x : n \text{ is squarefree, } \omega(n) = r \text{ and } \sigma(n) \text{ is an } r\text{th power}\},$$

where $\omega(n)$ is the number of distinct prime factors of n.

Theorem 6. *Fix an integer $r \geqslant 2$. For all sufficiently large x, we have*

$$|\mathcal{B}^*(x; -1, r)|, |\mathcal{B}^*(x; +1, r)| \gg \frac{rx^{1/r}}{(\log x)^{r+2}}.$$

The implied constant is absolute.

Part I

STRINGS OF CONGRUENT PRIMES IN SHORT INTERVALS

2. PROOF OF THEOREM 1 AND THEOREM 2

2.1 The idea of the proof

In this section, for the sake of exposition, we will proceed on the hypothesis that Siegel zeros do not exist. (In the proof of Theorem 1 we will have to deal with the possibility that Siegel zeros exist, and we do so, unconditionally, in a standard way. The complications that arise are only technical, and of little interest.) Fix coprime integers $q \geqslant 3$ and a. Let N be a real parameter tending to infinity, fix an arbitrarily small number $\epsilon > 0$, and set

$$H := \epsilon \log N, \quad Q := q \prod_{p \leqslant H/(\log H)^2} p.$$

Then the set

$$S := \{h \in (0, H] : (Q, h) = 1 \text{ and } h \equiv a \bmod q\}$$

is precisely the set of primes $p \in (H/(\log H)^2, H]$ such that $p \equiv a \bmod q$. Consider

$$\mathscr{L} := \sum_{N < n \leqslant 2N} \left(\sum_{h \in S} \vartheta(Qn + h) - \log 3QN \right) \Lambda_R(n; \mathcal{H}, k + \ell)^2,$$

where $\Lambda_R(n;\mathcal{H},k+\ell)$ is a real weight which we will define in Section 2.2 (see (2.2.7)). If $\mathscr{L}>0$, then for some $n\in(N,2N]$, the nth term of the outer sum is positive, and so the set $\{p\in(Qn,Qn+H]:p\equiv a \bmod q\}$ must contain two or more primes. Goldston, Pintz and Yıldırım [19] showed that $\mathscr{L}>0$ for all sufficiently large N, and hence there are infinitely many n for which the interval $(Qn,Qn+H]$ contains two primes. The great achievement of Goldston, Pintz and Yıldırım was to find a weight $\Lambda_R(n;\mathcal{H},k+\ell)$ that makes this argument work, and we refer to [20] for a synopsis of the evolution of ideas culminating in their groundbreaking work.

In fact, with the right parameters ($R=N^{1/4-\epsilon'}$ and a suitable $\mathcal{H}$), one can show that

$$\begin{aligned}\mathscr{L}=N\left(\frac{Q}{\phi(Q)}\right)^k\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\log N\\ \times\left\{\frac{Q}{\phi(Q)}\frac{|S|}{\log N}+\frac{2(2\ell+1)}{\ell+1}\frac{k}{k+2\ell+1}\left(\frac{1}{4}-\epsilon'\right)-(1+o(1))\right\}\end{aligned}\tag{2.1.1}$$

as $N\to\infty$. One can then apply the prime number theorem for arithmetic progressions, and Mertens' theorem, to show that

$$|S|\sim\frac{1}{\phi(q)}\frac{H}{\log H}\sim H\frac{e^\gamma}{\phi(q)}\prod_{p|Q}\left(1-\frac{1}{p}\right)=H\frac{e^\gamma}{\phi(q)}\frac{\phi(Q)}{Q}$$

as $H\to\infty$. (Here, $\gamma=0.57721\ldots$ is the Euler-Mascheroni constant.) The point here is that the first term of $\{\cdots\}$ in (2.1.1) does not vanish:

$$\frac{Q}{\phi(Q)}\frac{|S|}{\log N}\gg_q\epsilon\tag{2.1.2}$$

for all sufficiently large H, and hence N. It follows that we may choose k,ℓ and ϵ' in such a way that $\mathscr{L}\gg_{k,q}\epsilon(\log N)^{k+2\ell+1}$.

As it turns out, if we only assume that

$$\begin{aligned}
&Q \text{ is a multiple of } q,\\
&Q \text{ is composed only of primes } p \leqslant H,\\
&Q \text{ is divisible by all primes } p \leqslant \log H,\\
&Q \leqslant \exp\left(cH/(\log H)^2\right) \text{ for some constant } c > 0,
\end{aligned}$$

then the same estimate (2.1.1) still holds for $\mathscr{L}$ (with the same parameters R and $\mathcal{H}$). Now if (2.1.2) also holds, that is if

$$|S| \gg_q H\left(\frac{\phi(Q)}{Q}\right) = H\prod_{p|Q}\left(1-\frac{1}{p}\right), \tag{2.1.3}$$

as one might expect, then $\mathscr{L} > 0$. Therefore to prove there are infinitely many n for which $(Qn, Qn+H]$ contains at least two primes $\equiv a \bmod q$, we only need to show that $\mathscr{L} > 0$ for a sequence of N tending to infinity.

Relaxing the conditions on Q will allow us to incorporate the ideas of Shiu [32]. Thus, suppose $a \equiv 1 \bmod q$, and suppose for now that

$$Q := q \prod_{\substack{p\leqslant H\\ p\not\equiv 1 \bmod q}} p.$$

If there are any primes in the interval $(Qn, Qn+H]$, they must all be $\equiv 1 \bmod q$. Such a Q does not satisfy $Q \leqslant \exp(cH/(\log H)^2)$, but

$$Q := q \prod_{p\in\mathscr{P}(H)} p,$$

with

$$\mathscr{P}(H) := \{p \leqslant \log H : p \equiv 1 \bmod q\} \cup \{p \leqslant H/(\log H)^2 : p \not\equiv 1 \bmod q\},$$

does, and we might expect that, if there are any primes in $(Qn, Qn+H]$, they are more likely than not to be $\equiv 1 \bmod q$. If most of the primes in this interval are $\equiv 1 \bmod q$, then it must contain a pair of consecutive primes that are $\equiv 1 \bmod q$, by the pigeonhole principle. The goal, then, is to make these notions precise, and prove that (2.1.3) holds with this choice of Q, for a sequence of H tending to infinity.

To this end we define

$$T := \{h \in (0, H] : (Q, h) = 1 \text{ and } h \not\equiv 1 \bmod q\}.$$

Now if $h \in T$, then h must be divisible by a prime $p \not\equiv 1 \bmod q$, and since Q is divisible by all such primes $\leqslant H/(\log H)^2$, we must have $p > H/(\log H)^2$. Exploiting the fact that elements of T are divisible by large primes, we can show that

$$|T| \ll \frac{H}{\log H}. \tag{2.1.4}$$

One would expect that

$$|S \cup T| = |\{h \in (0, H] : (Q, h) = 1\}| \gg_q H \prod_{p \in \mathscr{P}(H)} \left(1 - \frac{1}{p}\right) = H\left(\frac{\phi(Q)}{Q}\right), \tag{2.1.5}$$

because we form $S \cup T$ by sieving out the interval $(0, H]$ with primes from the set $\mathscr{P}(H)$. If so, then since $|T|$ is much smaller than this by (2.1.4), the set S must be much larger than the set T. We will show that this expectation is borne out for a sequence of values H tending to infinity. Specifically, we will show that for all sufficiently large X, (2.1.3) holds from some H satisfying $\sqrt{X} \leqslant H \leqslant X$, and with more work,

$$X(\log X)^{-A} \leqslant H \leqslant X,$$

where $A = A(q)$ is a constant depending only on q. An application of Mertens' theorem for arithmetic progressions reveals that

$$H\left(\frac{\phi(Q)}{Q}\right) \gg_q \frac{H}{\log H}\left(\frac{\log H}{\log\log H}\right)^{1/\phi(q)} \gg |T|\left(\frac{\log H}{\log\log H}\right)^{1/\phi(q)},$$

in other words S contributes much more than T to $S \cup T$, and so we have

$$|S| - |T| \gg_q H\left(\frac{\phi(Q)}{Q}\right), \quad \text{that is} \quad \frac{Q}{\phi(Q)} \cdot \frac{|S|-|T|}{\log N} \gg_q \epsilon \tag{2.1.6}$$

whenever (2.1.5) holds. The case for $a \not\equiv 1 \bmod q$ is similar but slightly more involved.

Now consider

$$\mathscr{L} := \sum_{N<n\leqslant 2N}\left(\sum_{h\in S}\vartheta(Qn+h) - \sum_{h\in T}\vartheta(Qn+h) - \log 3QN\right)\Lambda_R(n;\mathcal{H},k+\ell)^2.$$

With our choice of Q, we can use (2.1.6) to show that $\mathscr{L} > 0$ for a sequence of N tending to infinity. It is not difficult to prove that if $\mathscr{L} > 0$, then for some

$n \in (N, 2N]$ we have

$$\begin{aligned}&|\{p \in (Qn, Qn + H] : p \equiv a \bmod q\}| \\ &\qquad\qquad\qquad \geqslant 2 + |\{p \in (Qn, Qn + H] : p \not\equiv a \bmod q\}|,\end{aligned}$$

From this we deduce that $(Qn, Qn + H]$ contains a pair of consecutive primes $p_m \equiv p_{m+1} \equiv a \bmod q$.

2.2 Preliminaries

In this section we will state two key technical propositions, to be proved in sections 2.4 and 2.5. The first proposition requires some preparation. We begin by quoting the Landau-Page theorem, a proof of which can be found in [10, Chapter 14]. This theorem is used to handle problems arising from possible irregularities in the distribution of primes, hence in Bombieri-Vinogradov type theorems (see lemmas 2.4.5 and 2.4.6), caused by potential Siegel zeros.

Lemma 2.2.1 (Landau-Page theorem). *There exists a constant c such that the following holds for any $Y > c$. There is at most one integer $q_0 \leqslant Y$, and at most one real primitive character $\chi_0 \bmod q_0$, such that*

$$L(1 - \delta, \chi_0, q_0) = 0 \quad \textit{for some} \quad \delta \leqslant \frac{1}{3 \log Y}.$$

If q_0 exists, then $q_0 > (\log Y)^2$. We call χ_0 an exceptional character and q_0 an exceptional modulus.

Throughout, we fix a number $\epsilon > 0$, we let H be a real parameter tending monotonically to infinity, and we set $N := \exp(H/\epsilon)$, that is $H = \epsilon \log N$. If there is an exceptional modulus

$$q_0 := q_0(H) \leqslant \exp(H/\epsilon(\log(H/\epsilon))^2) = N^{1/(\log\log N)^2},$$

let $p_0 := p_0(H)$ be its greatest prime factor; otherwise let $p_0 = 1$.

For all sufficiently large H, either

$$p_0 = 1 \text{ or } p_0 \text{ is a prime with } p_0 > \log H. \tag{2.2.1}$$

To see this, note that all real primitive characters are products of Legendre symbols with different odd primes, and possibly either the unique real character mod 4 or one of the two primitive real characters mod 8. Thus if q_0 exists it is of the form $2^\alpha p_1 \cdots p_k$, where $\alpha \leqslant 3$ and the p_i's are distinct odd primes. If this is the case and $p_0 \leqslant \log H$, then the prime number theorem implies $q_0 \ll \exp((1 + o(1)) \log H) \ll \log N$, but Lemma 2.2.1 states that $q_0 > (\log N/(\log\log N)^2)^2$.

We let $Q := Q(H)$ be a positive integer, upon which we will impose the following conditions:

$$Q \text{ is composed only of primes } p \leqslant H, \tag{2.2.2}$$

$$Q \text{ is divisible by all primes } p \leqslant \log H, \tag{2.2.3}$$

$$Q \leqslant \exp\left(cH/(\log H)^2\right) \text{ for some constant } c > 0, \tag{2.2.4}$$

$$\text{if } p_0(H) \neq 1 \text{ then } p_0(H) \text{ does not divide } Q. \tag{2.2.5}$$

We let

$$\mathcal{H} := \{Qx + h_1, \ldots, Qx + h_k\}, \quad h_1, \ldots, h_k \in [1, H] \cap \mathbb{Z}, \tag{2.2.6}$$

denote a set of distinct linear forms, and we define

$$\Lambda_R(n;\mathcal{H},j) := \frac{1}{j!}\sideset{}{'}\sum_{\substack{d \mid P(n;\mathcal{H})\\ d \leqslant R}} \mu(d)(\log R/d)^j, \tag{2.2.7}$$

where $\sum'$ denotes summation over indices coprime with Qp_0, and

$$P(n;\mathcal{H}) := (Qn+h_1)\cdots(Qn+h_k). \tag{2.2.8}$$

Finally, we let

$$\vartheta(n) := \begin{cases} \log n & \text{if } n \text{ is prime,}\\ 0 & \text{otherwise.}\end{cases}$$

Proposition 2.2.2. *Given $\epsilon > 0$ and sufficiently large H, let N and $p_0 = p_0(H)$ be as defined earlier, and let $Q = Q(H)$ be a positive integer satisfying* (2.2.2) – (2.2.5)*. Fix integers $k \geqslant 2$ and $\ell \geqslant 1$, and let*

$$\mathcal{H} = \{Qx+h_1,\ldots,Qx+h_k\}$$

be a set of distinct linear forms with

$$h_1,\ldots,h_k \in [1,H]\cap\mathbb{Z} \quad \textit{and} \quad (Q,h_1,\ldots,h_k) = 1.$$

Let $h \in [1,H]\cap\mathbb{Z}$ and suppose $(Q,h) = 1$, and let $R = N^{1/4-\epsilon'}$ for some $\epsilon' \in (0,1/4)$. As $H \to \infty$, we have

$$\frac{1}{N}\left(\frac{\phi(Q)}{Q}\right)^{k}\sum_{N<n\leqslant 2N}\Lambda_R(n;\mathcal{H},k+\ell)^2 \sim \binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}, \tag{2.2.9}$$

and

$$\frac{1}{N}\left(\frac{\phi(Q)}{Q}\right)^{k}\sum_{N<n\leqslant 2N}\vartheta(Qn+h)\Lambda_R(n;\mathcal{H},k+\ell)^2$$
$$\sim\begin{cases}\dfrac{Q}{\phi(Q)}\dbinom{2\ell}{\ell}\dfrac{(\log R)^{k+2\ell}}{(k+2\ell)!} & \text{if } Qx+h\notin\mathcal{H},\\[2ex] \dbinom{2(\ell+1)}{\ell+1}\dfrac{(\log R)^{k+2\ell+1}}{(k+2\ell+1)!} & \text{if } Qx+h\in\mathcal{H}.\end{cases} \tag{2.2.10}$$

Proposition 2.2.3. *Let $q \geqslant 3$ and a be integers with $(q,a) = 1$, and for a given H, let $p_0 = p_0(H)$ be as defined earlier. There is an infinite sequence of integers $H_1 < H_2 < \dots$ such that for any i, taking $H = H_i$, there exists a positive integer $Q = Q(H)$, divisible by q and satisfying* (2.2.2) – (2.2.5)*, such that*

$$|S| - |T| \gg_q H\left(\frac{\phi(Q)}{Q}\right),$$

where

$$\begin{aligned} S = S(H) &:= \{h\in(0,H] : (Q,h)=1 \text{ and } h\equiv a \bmod q\},\\ T = T(H) &:= \{h\in(0,H] : (Q,h)=1 \text{ and } h\not\equiv a \bmod q\}.\end{aligned} \tag{2.2.11}$$

The implied constant depends at most on q.

2.3 The proof of Theorem 1

Fix integers $q \geqslant 3$ and a with $(q,a) = 1$. Recall that $H = \epsilon \log N$, with $\epsilon > 0$ fixed, and p_0 is the greatest prime factor of the exceptional modulus $q_0 \leqslant N^{1/(\log\log N)^2}$, if it exists, otherwise $p_0 = 1$. We choose H, $Q = Q(H)$, $S = S(H)$, and $T = T(H)$ as in Proposition 2.2.3, so that Q is divisible by q and satisfies (2.2.2) – (2.2.5), and

$$\frac{Q}{\phi(Q)} \frac{|S| - |T|}{\log N} \geqslant c(q)\epsilon \tag{2.3.1}$$

for some constant $c(q) > 0$, depending on q at most.

We fix positive integers k, ℓ (to be specified later), and we let

$$\mathcal{H} = \{Qx + h_1, \ldots, Qx + h_k\}$$

be a set of distinct linear forms such that, for each i, $h_i \in [1, H] \cap a \bmod q$ and $(Q, h_i) = 1$. We let $R = N^{1/4-\epsilon'}$ with $0 < \epsilon' < 1/4$ (to be specified later), and we put

$$\begin{aligned}\mathscr{L} &:= \frac{1}{N}\left(\frac{\phi(Q)}{Q}\right)^k \\ &\times \sum_{N<n\leqslant 2N}\left(\sum_{h\in S}\vartheta(Qn+h) - \sum_{h\in T}\vartheta(Qn+h) - \log 3QN\right)\Lambda_R(n;\mathcal{H},k+\ell)^2.\end{aligned}$$

We now show that if $\mathscr{L} > 0$ for a sequence of numbers N, tending to infinity, then Theorem 1 follows.

Let

$$\begin{aligned} A_n &:= \{p \in (Qn, Qn+H] : p \equiv a \bmod q\} = \{p : p = Qn+h, h \in S\}, \\ B_n &:= \{p \in (Qn, Qn+H] : p \not\equiv a \bmod q\} = \{p : p = Qn+h, h \in T\}. \end{aligned}$$

If $\mathscr{L} > 0$, then there is some $n \in (N, 2N]$ such that

$$\begin{aligned} |A_n| \log(Qn+H) &\geqslant \sum_{h \in S} \vartheta(Qn+h) \\ &> \sum_{h \in T} \vartheta(Qn+h) + \log 3QN \\ &\geqslant |B_n| \log Qn + \log 3QN. \end{aligned}$$

Now

$$|A_n| \log\left(1 + H/Qn\right) \leqslant |A_n|\, H/Qn \leqslant H^2/QN < \log(3/2)$$

if N is sufficiently large, and so

$$\log(3/2) + (|A_n| - |B_n|) \log Qn > \log 3QN$$

and hence, as $n \leqslant 2N$, $|A_n| - |B_n| > 1$. But as these are integers,

$$|A_n| \geqslant |B_n| + 2,$$

and so, by the pigeonhole principle, A_n contains a pair of consecutive primes p_r, p_{r+1}. These primes satisfy $p_{r+1} - p_r < H < \epsilon \log QN < \epsilon \log p_r$.

Now, by our choice of $\mathcal{H}$, a straightforward application of Proposition 2.2.2

yields

$$\begin{aligned}\mathscr{L} = &\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\\ &\times\Biggl\{\frac{Q}{\phi(Q)}\sum_{\substack{h\in S\\ Qx+h\notin\mathcal{H}}} 1 + \frac{2(2\ell+1)}{\ell+1}\frac{\log R}{k+2\ell+1}\sum_{\substack{h\in S\\ Qx+h\in\mathcal{H}}} 1\\ &\qquad - \frac{Q}{\phi(Q)}\sum_{h\in T} 1 - (1+o(1))\log 3QN\Biggr\}.\end{aligned}$$

We have

$$\sum_{\substack{h\in S\\ Qx+h\in\mathcal{H}}} 1 = k, \qquad \sum_{\substack{h\in S\\ Qx+h\notin\mathcal{H}}} 1 = |S|-k,$$

$\log R = (1/4-\epsilon')\log N$, and $\log 3QN \sim \log N$ by (2.2.4), therefore

$$\begin{aligned}\mathscr{L} = &\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}(\log N)\\ &\times\left\{\frac{Q}{\phi(Q)}\frac{|S|-|T|}{\log N} + \frac{2(2\ell+1)}{\ell+1}\frac{k}{k+2\ell+1}\left(\frac{1}{4}-\epsilon'\right) - (1+o(1))\right\}.\end{aligned}$$

We have written $o(1)$ for $kQ/(\phi(Q)\log N)$, because

$$Q/\phi(Q) \ll \log\log Q \ll \log\log N.$$

By choosing $\ell = [\sqrt{k}]$ and k sufficiently large, the bracketed expression $\{\cdots\}$ above is, by (2.3.1),

$$\geqslant c(q)\epsilon + 1 - 5\epsilon' - (1+o(1)) = c(q)\epsilon - 5\epsilon' - o(1).$$

By choosing $\epsilon' = c(q)\epsilon/10$ (we may assume that ϵ is small enough so that

$\epsilon' < 1/4$), we deduce that

$$\mathscr{L} \gg_k c(q)\epsilon(\log N)^{k+2\ell+1} \tag{2.3.2}$$

holds if N is sufficiently large. By Proposition 2.2.3, we may choose H, equivalently N, from a sequence of numbers tending to infinity, and Theorem 1 follows.

2.4 Proof of Proposition 2.2.2

2.4.1 Auxiliary lemmas

In the proof of Proposition 2.2.2 we will use the following lemmas. Lemma 2.4.4 is the heart of the proof. We begin by recalling a few facts about the Riemann zeta-function $\zeta(s)$. We define

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{for} \quad \operatorname{Re} s > 1.$$

We extend this definition meromorphically to the whole complex plane by analytic continuation. It can be shown that $\zeta(s)$ is analytic except for a simple pole at $s = 1$, where the residue is 1. In fact

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(|s-1|) \quad \text{as} \quad s \to 1 \tag{2.4.1}$$

(see [34, (2.1.16)]). (Here, $\gamma = 0.57721\ldots$ is the Euler-Mascheroni constant.) The zeta-function has Euler product representation

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \text{for} \quad \operatorname{Re} s > 1. \tag{2.4.2}$$

Lemma 2.4.1. *Define contours*

$$\mathscr{C}' := \left\{1 - \tfrac{1}{6\log(|t|+3)} + it : t \in \mathbb{R}\right\}, \quad \mathscr{C} := \left\{1 - \tfrac{1}{24\log(|t|+3)} + it : t \in \mathbb{R}\right\}.$$

For s on and to the right of $\mathscr{C}'$ we have $\zeta(s) \neq 0$, and for s on and to the right of $\mathscr{C}$ we have

$$\zeta(s) - \frac{1}{s-1}, \ \frac{1}{\zeta(s)} \ll \log(|s|+3). \tag{2.4.3}$$

Proof. The explicit zero-free region for $\zeta(s)$ is due to Kadiri [29, Théorème 1.1], who in fact showed that $\zeta(s) \neq 0$ if $\operatorname{Re} s \geqslant 1 - 1/(5.69693\log(|\operatorname{Im} s|))$ and $\operatorname{Im} s \geqslant 2$. Given $A > 0$ for which $\zeta(s)$ does not vanish for

$$\operatorname{Re}(s) \geqslant 1 - A/(\log(|\operatorname{Im} s| + 3)),$$

the estimate $1/\zeta(s) \ll \log(\operatorname{Im} s + 3)$ is shown to hold for

$$\operatorname{Re}(s) \geqslant 1 - A/4(\log(|\operatorname{Im} s| + 3))$$

in [34, Section 3] (see [34, Theorem 3.11] and [34, (3.11.8)]). For any $A' > 0$, we have $\zeta(s) - 1/(s-1) \ll \log(\operatorname{Im} s + 3)$ for $\operatorname{Re}(s) \geqslant 1 - A'/(\log(|\operatorname{Im} s| + 3))$. This follows from the inequality $|\log\zeta(s)| \leqslant \log\log\operatorname{Im} s + O(1)$, which holds in the same region (see [33, II.3, Theorem 16, (57)] or [34, Setion 3]). The bounds in (2.4.3) are also explained in [21, (5.4)] and in [22, (5.2)], along with the bound $\frac{\zeta'}{\zeta}(s) + 1/s \ll \log(\operatorname{Im} s + 3)$, which holds for $\operatorname{Re}(s) \geqslant 1 - A/4(\log(|\operatorname{Im} s| + 3))$. We will not need to use any such bound for ζ'/ζ. □

In the following lemma and throughout Section 2.4, (α) denotes the vertical line in the complex plane passing through the real number α.

Lemma 2.4.2. *For any fixed real number $\alpha > 0$, we have*

$$\frac{1}{2\pi i}\int_{(\alpha)} \frac{a^s}{s^{j+1}}\,ds = \begin{cases} 0 & \text{if } 0 < a \leqslant 1, \\ \frac{1}{j!}(\log a)^j & \text{if } a \geqslant 1. \end{cases}$$

Proof. This is a variant of Perron's formula (see [30, p. 143]). □

Let us introduce some notation for the next lemma. Given a k-tuple

$$\mathcal{H} = \{Qx + h_1, \dots, Qx + h_k\}$$

of distinct linear forms, as in (2.2.6), we define

$$\Omega(d) := \Omega(d; \mathcal{H}) = \{n \bmod d : P(n; \mathcal{H}) \equiv 0 \bmod d\}$$

for positive integers d, where $P(n;\mathcal{H}) := (Qn + h_1)\cdots(Qn + h_k)$, as in (2.2.8). Given an integer $h \neq h_1, \dots, h_k$, we define

$$\mathcal{H}^+ := \mathcal{H} \cup \{Qx + h\}, \quad \Omega^+(d) := \Omega(\mathcal{H}^+; d).$$

Let H be a large real number, let $Q = Q(H)$ be a positive integer satisfying (2.2.2), (2.2.3) and (2.2.5), let $\mathcal{H} = \{Qx + h_1, \dots, Qx + h_k\}$ be a k-tuple of distinct linear forms with $h_i \in [1, H] \cap \mathbb{Z}$ for each i, and let $h \in [1, H] \cap \mathbb{Z}$ be such that $Qx + h \notin \mathcal{H}$. We are interested in

$$G(s_1, s_2; \Omega) := \prod_{p \nmid Qp_0} \left(1 - \frac{|\Omega(p)|}{p} \left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right) \\ \times \prod_{p} \left(1 - \frac{1}{p^{s_1+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_2+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_1+s_2+1}}\right)^{k} \tag{2.4.4}$$

and

$$G^{+}(s_1, s_2; \Omega^{+}) := \prod_{p \nmid Qp_0} \left(1 - \frac{|\Omega^{+}(p)| - 1}{p - 1} \left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right) \\ \times \prod_{p} \left(1 - \frac{1}{p^{s_1+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_2+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_1+s_2+1}}\right)^{k}, \tag{2.4.5}$$

where p_0 is as in (2.2.1).

The next lemma also introduces the important notion of admissibility. We say $\mathcal{H}$ is *admissible* if $|\Omega(p)| < p$ for all primes p, because in that case there could feasibly be infinitely many prime k-tuples of the form $Qn + h_1, \ldots, Qn + h_k$. For future reference we make the following observations. For any prime p not dividing Q, it is clear that

$$\Omega(p) = \{-h_1 Q^{-1}, \ldots, -h_k Q^{-1}\} \bmod p. \tag{2.4.6}$$

Hence if $p \nmid Q$, we have $1 \leqslant |\Omega(p)| \leqslant \min(k, p)$, indeed

$$1 \leqslant |\Omega(p)| \leqslant \min(k, p - 1)$$

if $\mathcal{H}$ is admissible, with $|\Omega(p)| = k$ if and only if the $-h_i Q^{-1}$ are distinct modulo

p, that is if and only if $p \nmid \Delta$, where

$$\Delta = \Delta(\mathcal{H}) := \prod_{1 \leqslant i < j \leqslant k} |h_i - h_j| \,.$$

Since $1 \leqslant |h_i - h_j| \leqslant H$ for every i, j, $p > H$ implies $p \nmid \Delta$, as well as $p \nmid Q$ by (2.2.2). Hence

$$p \nmid Q\Delta \quad \text{and} \quad |\Omega(p)| = k \quad \text{for all} \quad p > H. \tag{2.4.7}$$

We also have $\Delta \leqslant H^{\binom{k}{2}} \leqslant H^{k^2}$. For any prime p dividing $(Q, h_1 \cdots h_k)$ we have $P(n; \mathcal{H}) \equiv h_1 \cdots h_k \equiv 0 \bmod p$, hence $|\Omega(p)| = p$. This cannot happen if $\mathcal{H}$ is admissible, so if $\mathcal{H}$ is admissible, $(Q, h_1 \cdots h_k) = 1$, and for every prime p dividing Q we have $P(n; \mathcal{H}) \equiv h_1 \cdots h_k \not\equiv 0 \bmod p$, hence $|\Omega(p)| = 0$.

Lemma 2.4.3. *Let H be a real number, let $Q = Q(H)$ be a positive integer satisfying* (2.2.2), (2.2.3) *and* (2.2.5), *and let $\mathcal{H}$ be as in* (2.2.6), *with k fixed. Also let $h \in [1, H] \cap \mathbb{Z}$ be such that $Qx + h \notin \mathcal{H}$. For s_1, s_2 satisfying* $\operatorname{Re} s_1, \operatorname{Re} s_2 > -1/4$, *we have*

$$G(s_1, s_2; \Omega),\, G^{+}(s_1, s_2; \Omega^{+}) \ll \exp\left(cH^{\delta_1 + \delta_2} \log\log H\right), \tag{2.4.8}$$

where c is a constant depending only on k, and

$$\delta_i := \max\left(-\operatorname{Re} s_i, 0\right), \quad i = 1, 2.$$

Moreover, for $k \leqslant \log H$, $\mathcal{H}$ is admissible if and only if $(Q, h_1 \cdots h_k) = 1$, and *as $H \to \infty$, if $(Q, h) = (Q, h_1 \cdots h_k) = 1$, we have*

$$G(0,0;\Omega),\ G^+(0,0;\Omega^+) \sim \left(\frac{Q}{\phi(Q)}\right)^k. \tag{2.4.9}$$

Proof. Several times throughout this proof, we will tacitly use the following inequalities: the triangle inequality; $1 - |z| \leqslant |1 - z|$, that is $|1-z|^{-1} \leqslant (1-|z|)^{-1}$, for $0 < |z| < 1$; $(1-x)^{-1} \leqslant 1 + 3x$ for $0 \leqslant x \leqslant 2/3$; $\log(1+x) \leqslant x$ for $x \geqslant 0$; for all primes p,

$$0 < \frac{1}{|p^{s_i+1}|}, \frac{1}{|p^{s_1+s_2+1}|} \leqslant \frac{1}{p^{-(\delta_1+\delta_2)+1}} < 1 \quad \text{for} \quad \delta_i := \max(-\operatorname{Re} s_i, 0) < 1/4;$$

and for all primes p,

$$\frac{1}{|p^{s_i+1}|} \leqslant \frac{1}{p^{-\delta_i+1}} < \frac{1}{2^{3/4}} < 2/3 \quad \text{for} \quad \delta_i := \max(-\operatorname{Re} s_i, 0) < 1/4.$$

We will also tacitly use the standard estimate

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + c_1 + O\left(\frac{1}{\log x}\right), \quad c_1 = 0.261497\ldots$$

(see [33, I.1 Theorem 9]).

Now fix s_1 and s_2 such that $\delta_i := \max(-\operatorname{Re} s_i, 0) < 1/4$, $i = 1, 2$. We write

$$G(s_1, s_2; \Omega) = \prod_{\substack{p \nmid Qp_0 \\ p \leqslant H}} (\cdots) \prod_{p \leqslant H} (\cdots) \prod_{\substack{p \nmid Qp_0 \\ p > H}} (\cdots) \prod_{p > H} (\cdots)$$

and treat the above products separately. We have

$$\begin{aligned}
\left|\prod_{p\leqslant H}\left(1-\frac{1}{p^{s_1+s_2+1}}\right)^k\right| &\leqslant \prod_{p\leqslant H}\left(1+\frac{1}{p^{-(\delta_1+\delta_2)+1}}\right)^k \\
&= \exp\left(k\sum_{p\leqslant H}\log\left(1+\frac{1}{p^{-(\delta_1+\delta_2)+1}}\right)\right) \\
&\leqslant \exp\left(k\sum_{p\leqslant H}\frac{1}{p^{-(\delta_1+\delta_2)+1}}\right) \\
&\leqslant \exp\left(kH^{\delta_1+\delta_2}\sum_{p\leqslant H}\frac{1}{p}\right) \\
&\ll \exp\left(kH^{\delta_1+\delta_2}\log\log H\right),
\end{aligned}$$

and

$$\begin{aligned}
\left|\prod_{p\leqslant H}\left(1-\frac{1}{p^{s_i+1}}\right)^{-k}\right| &\leqslant \prod_{p\leqslant H}\left(1-\frac{1}{p^{-\delta_i+1}}\right)^{-k} \\
&\leqslant \prod_{p\leqslant H}\left(1+\frac{3}{p^{-\delta_i+1}}\right)^k \\
&= \exp\left(k\sum_{p\leqslant H}\log\left(1+\frac{3}{p^{-\delta_i+1}}\right)\right) \\
&\leqslant \exp\left(k\sum_{p\leqslant H}\frac{3}{p^{-\delta_i+1}}\right) \\
&\leqslant \exp\left(3kH^{\delta_i}\sum_{p\leqslant H}\frac{1}{p}\right) \\
&\ll \exp\left(3kH^{\delta_i}\log\log H\right),
\end{aligned}$$

$i = 1, 2$. Thus, since $\delta_1, \delta_2 \leqslant \delta_1 + \delta_2$, we have

$$\begin{aligned}\left|\prod_{p\leqslant H}\left(1-\frac{1}{p^{s_1+1}}\right)^{-k}\left(1-\frac{1}{p^{s_2+1}}\right)^{-k}\left(1-\frac{1}{p^{s_1+s_2+1}}\right)^{k}\right|& \\ \ll \exp\left(7kH^{\delta_1+\delta_2}\log\log H\right).&\end{aligned}\tag{2.4.10}$$

Also, since $|\Omega(p)| \leqslant k$ for $p \nmid Q$ (by (2.4.6)), we have

$$\begin{aligned}&\left|\prod_{\substack{p\nmid Qp_0\\ p\leqslant H}}\left(1-\frac{|\Omega(p)|}{p}\left(\frac{1}{p^{s_1}}+\frac{1}{p^{s_2}}-\frac{1}{p^{s_1+s_2}}\right)\right)\right| \\ &\qquad\leqslant \prod_{p\leqslant H}\left(1+\frac{3k}{p^{-(\delta_1+\delta_2)+1}}\right) \\ &\qquad= \exp\left(\sum_{p\leqslant H}\log\left(1+\frac{3k}{p^{-(\delta_1+\delta_2)+1}}\right)\right) \\ &\qquad\leqslant \exp\left(\sum_{p\leqslant H}\frac{3k}{p^{-(\delta_1+\delta_2)+1}}\right) \\ &\qquad\leqslant \exp\left(3kH^{\delta_1+\delta_2}\sum_{p\leqslant H}\frac{1}{p}\right) \\ &\qquad\ll \exp\left(3kH^{\delta_1+\delta_2}\log\log H\right).\end{aligned}\tag{2.4.11}$$

Now, by (2.4.7) we may write

$$\begin{aligned}&\prod_{\substack{p\nmid Qp_0\\ p>H}}(\cdots)\prod_{p>H}(\cdots) = \prod_{\substack{p>H\\ p\neq p_0}}(\cdots)(\cdots)\prod_{p>H}(\cdots) \\ &= \gamma(p_0)\prod_{p>H}\left(1-\frac{k}{p}\left(\frac{1}{p^{s_1}}+\frac{1}{p^{s_2}}-\frac{1}{p^{s_1+s_2}}\right)\right) \\ &\qquad\qquad\cdot\left(1-\frac{1}{p^{s_1+1}}\right)^{-k}\left(1-\frac{1}{p^{s_2+1}}\right)^{-k}\left(1-\frac{1}{p^{s_1+s_2+1}}\right)^{k},\end{aligned}$$

where $\gamma(p_0) = 1$ if $p_0 \leqslant H$, and

$$\gamma(p_0) = \left(1 - \frac{k}{p_0}\left(\frac{1}{p_0^{s_1}} + \frac{1}{p_0^{s_2}} - \frac{1}{p_0^{s_1+s_2}}\right)\right)^{-1}$$

otherwise. Now clearly

$$|\gamma(p_0)| \leqslant \left(1 - \frac{3k}{H^{-(\delta_1+\delta_2)+1}}\right)^{-1} = 1 + o(1).$$

We have

$$\begin{aligned}\log\left(\textstyle\prod_{p>H}(\cdots)(\cdots)\right) \leqslant \sum_{p>H}\Bigg| &\log\left(1 - \frac{k}{p^{s_1+1}} - \frac{k}{p^{s_2+1}} + \frac{k}{p^{s_1+s_2+1}}\right)\\ &- k\log\left(1 - \frac{1}{p^{s_2+1}}\right) - k\log\left(1 - \frac{1}{p^{s_1+1}}\right)\\ &+ k\log\left(1 - \frac{1}{p^{s_1+s_2+1}}\right)\Bigg|.\end{aligned}$$

In this last sum the Taylor series of the term corresponding to p is

$$\begin{aligned}&-\sum_{m\geqslant 1}\frac{1}{m}\left(\frac{k}{p^{s_1+1}} + \frac{k}{p^{s_2+1}} - \frac{k}{p^{s_1+s_2+1}}\right)^m + k\sum_{m\geqslant 1}\frac{1}{m}\left(\frac{1}{p^{s_1+1}}\right)^m\\ &\qquad + k\sum_{m\geqslant 1}\frac{1}{m}\left(\frac{1}{p^{s_2+1}}\right)^m - k\sum_{m\geqslant 1}\frac{1}{m}\left(\frac{1}{p^{s_1+s_2+1}}\right)^m\\ &\qquad = -\sum_{m\geqslant 2}\frac{k^m}{m}\left(\frac{1}{p^{s_1+1}} + \frac{1}{p^{s_2+1}} - \frac{1}{p^{s_1+s_2+1}}\right)^m + k\sum_{m\geqslant 2}\frac{1}{m}\left(\frac{1}{p^{s_1+1}}\right)^m\\ &\qquad + k\sum_{m\geqslant 2}\frac{1}{m}\left(\frac{1}{p^{s_2+1}}\right)^m - k\sum_{m\geqslant 2}\frac{1}{m}\left(\frac{1}{p^{s_1+s_2+1}}\right)^m,\end{aligned}$$

which in absolute value is at most

$$\sum_{m\geqslant 2}\frac{1}{m}\left(\frac{4k}{p^{-(\delta_1+\delta_2)+1}}\right)^m.$$

We may assume H is large enough so that $4k/H \leqslant 1/2$, and so

$$\begin{aligned}\sum_{p>H}\Big|\cdots\Big| &\leqslant \sum_{p>H}\sum_{m\geqslant 2}\frac{1}{m}\left(\frac{4k}{p^{-(\delta_1+\delta_2)+1}}\right)^m \\ &\leqslant \sum_{p>H}\left(\frac{4k}{p^{-(\delta_1+\delta_2)+1}}\right)^2\sum_{m\geqslant 2}\left(\frac{4k}{p^{-(\delta_1+\delta_2)+1}}\right)^{m-2} \\ &\ll k^2\sum_{p>H}\frac{1}{p^{-2(\delta_1+\delta_2)+2}} \\ &\ll k^2.\end{aligned} \tag{2.4.12}$$

Exponentiating yields

$$\begin{aligned}&\Bigg|\prod_{p>H}\left(1-\frac{k}{p}\left(\frac{1}{p^{s_1}}+\frac{1}{p^{s_2}}-\frac{1}{p^{s_1+s_2}}\right)\right) \\ &\qquad\cdot\left(1-\frac{1}{p^{s_1+1}}\right)^{-k}\left(1-\frac{1}{p^{s_2+1}}\right)^{-k}\left(1-\frac{1}{p^{s_1+s_2+1}}\right)^{k}\Bigg| \\ &\leqslant \exp\left(O(k^2)\right),\end{aligned}$$

and combining yields

$$\begin{aligned}&\prod_{\substack{p\nmid Qp_0\\ p>H}}\left(1-\frac{|\Omega(p)|}{p}\left(\frac{1}{p^{s_1}}+\frac{1}{p^{s_2}}-\frac{1}{p^{s_1+s_2}}\right)\right) \\ &\qquad\times\prod_{p>H}\left(1-\frac{1}{p^{s_1+1}}\right)^{-k}\left(1-\frac{1}{p^{s_2+1}}\right)^{-k}\left(1-\frac{1}{p^{s_1+s_2+1}}\right)^{k} \\ &\ll \exp\left(O(k^2)\right).\end{aligned} \tag{2.4.13}$$

Finally, combining (2.4.10), (2.4.11) and (2.4.13) yields

$$G(s_1,s_2;\Omega) \ll \exp\left(10kH^{\delta_1+\delta_2}\log\log H\right)$$

for $\delta_i := \max(-\operatorname{Re} s_i, 0) < 1/4$, $i = 1, 2$. We bound $G^+(s_1,s_2;\Omega^+)$ similarly.

Since $Qx+h \notin \mathcal{H}$, we have $|\Omega^+(p)|-1 = k < p$ for all $p > H$ as in the first case, and $0 \leqslant |\Omega^+(p)|-1 \leqslant \min(k, p-1)$ for all $p \nmid Q$. Noting that

$$\frac{\min(k,p-1)}{p-1} \leqslant \frac{k}{p(1-1/p)} \leqslant 2k$$

and carrying this through the above computations, we obtain the bound (2.4.8) for $G^+(s_1, s_2; \Omega^+)$.

Now we will prove the second statement of the lemma. As we noted prior to stating the lemma, for any prime p dividing $(Q, h_1 \cdots h_k)$ we have

$$P(n; \mathcal{H}) \equiv h_1 \cdots h_k \equiv 0 \bmod p,$$

hence $|\Omega(p)| = p$, and so $\mathcal{H}$ is not admissible if $(Q,\, h_1 \cdots h_k) \neq 1$. Now assume $(Q, h_1 \cdots h_k) = 1$ and $k \leqslant \log H$. Then for every prime p dividing Q we have $P(n; \mathcal{H}) \equiv h_1 \cdots h_k \not\equiv 0 \bmod p$, hence $|\Omega(p)| = 0$. For every other prime p we have (2.4.6), and hence $1 \leqslant |\Omega(p)| \leqslant k \leqslant \log H < p$ by (2.2.3). Hence $\mathcal{H}$ is admissible if and only if $(Q, h_1 \cdots h_k) = 1$, provided $k \leqslant \log H$.

We will now establish (2.4.9) in the case of $G(0,0;\Omega)$. We assume H is large enough so that $2k \leqslant \log H$, and that $(Q, h_1 \cdots h_k) = 1$. Thus $\mathcal{H}$ is admissible and $|\Omega(p)| = 0$ for $p \mid Q$, hence

$$\begin{aligned} G(0,0;\Omega) &= \prod_{p \nmid Qp_0} \left(1 - \frac{|\Omega(p)|}{p}\right) \prod_{p} \left(1 - \frac{1}{p}\right)^{-k} \\ &= \left(\frac{Q}{\phi(Q)}\right)^{k} \prod_{p \nmid Q} \left(1 - \frac{|\Omega(p)|}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \prod_{p \mid p_0} \left(1 - \frac{|\Omega(p)|}{p}\right)^{-1}, \end{aligned}$$

because if $p_0 \neq 1$ then $p_0 \nmid Q$; otherwise $Qp_0 = Q$ and the last product is empty. As H tends to infinity, the last product tends to 1 by (2.2.1), so it suffices to show that

$$\mathfrak{S}'(\mathcal{H}) := \prod_{p\nmid Q}\left(1-\frac{|\Omega(p)|}{p}\right)\left(1-\frac{1}{p}\right)^{-k} \sim 1. \tag{2.4.14}$$

In fact since $\mathcal{H}$ is admissible, we see that $1 \leqslant |\Omega(p)| \leqslant \min(k, p-1)$ if $p \nmid Q$, with $|\Omega(p)| = k$ if and only if $p \nmid Q\Delta$. We break $\mathfrak{S}'(\mathcal{H})$ into two products according as $p \mid \Delta$ or $p \nmid \Delta$:

$$\begin{aligned}\mathfrak{S}'(\mathcal{H}) &= \prod_{p\nmid Q}\left(1-\frac{k}{p}\right)\left(1+\frac{k-|\Omega(p)|}{p-k}\right)\left(1-\frac{1}{p}\right)^{-k}\\ &= \prod_{p\nmid Q}\left(1-\frac{k}{p}\right)\left(1-\frac{1}{p}\right)^{-k}\prod_{\substack{p\nmid Q\\ p\mid\Delta}}\left(1+\frac{k-|\Omega(p)|}{p-k}\right).\end{aligned} \tag{2.4.15}$$

In this product $p-k \neq 0$ because $p \nmid Q$ implies $p > \log H$ by (2.2.3), and we are assuming that $\log H > k$. Then $p \nmid Q$ implies $k < p/2$, and the logarithm of the first product of the last line of (2.4.15) is

$$\begin{aligned}\sum_{p\nmid Q}&\left\{\left(-\frac{k}{p}-\frac{k^2}{2p^2}-\cdots\right)-k\left(-\frac{1}{p}-\frac{1}{2p^2}-\cdots\right)\right\}\\ &= -k(k-1)\sum_{p\nmid Q}\left\{\frac{1}{p^2}\left(\frac{1}{2}+\frac{1+k}{3p}+\frac{1+k+k^2}{4p^2}+\cdots\right)\right\}\\ &\ll k^2\sum_{p>\log H}\frac{1}{p^2} \ll \frac{k^2}{\log H\log\log H}.\end{aligned}$$

For the second product, note that since

$$0 < \frac{k-|\Omega(p)|}{p-k} \leqslant \frac{k}{p-k} \leqslant \frac{2k}{p} < 1,$$

the logarithm of the second product is

$$\begin{aligned}
&\leqslant \sum_{\substack{p \mid \Delta \\ p > \log H}} \log\left(1 + \frac{k - |\Omega(p)|}{p - k}\right) \ll \sum_{\substack{p \mid \Delta \\ p > \log H}} \frac{k}{p} \\
&\ll \frac{k}{\log H} \sum_{p \mid \Delta} 1 \ll \frac{k \log \Delta}{\log H \log\log \Delta} \ll \frac{k^3}{\log\log H}
\end{aligned}$$

by the prime number theorem and since $\Delta \leqslant H^{\binom{k}{2}} \leqslant H^{k^2}$. Exponentiating and letting $H \to \infty$ yields (2.4.14), and we have shown that (2.4.9) holds for $G(0, 0; \Omega)$.

The case for $G^+(0, 0; \Omega^+)$ is similar. We have $|\mathcal{H}^+| = k + 1$ as $Qx + h \notin \mathcal{H}$, and analogously to (2.4.14) we have $\mathfrak{S}'(\mathcal{H}^+) \sim 1$ as $H \to \infty$, where

$$\begin{aligned}
\mathfrak{S}'(\mathcal{H}^+) &:= \prod_{p \nmid Q} \left(1 - \frac{|\Omega^+(p)|}{p}\right)\left(1 - \frac{1}{p}\right)^{-(k+1)} \\
&= \prod_{p \nmid Q} \left(\frac{p - |\Omega^+(p)|}{p}\right)\left(\frac{p}{p-1}\right)\left(1 - \frac{1}{p}\right)^{-k} \\
&= \prod_{p \nmid Q} \left(1 - \frac{|\Omega^+(p)| - 1}{p - 1}\right)\left(1 - \frac{1}{p}\right)^{-k}.
\end{aligned}$$

Hence

$$\begin{aligned}
G^+(0, 0; \Omega^+) &= \prod_{p \nmid Q p_0} \left(1 - \frac{|\Omega^+(p)| - 1}{p - 1}\right) \prod_{p} \left(1 - \frac{1}{p}\right)^{-k} \\
&= \left(\frac{Q}{\phi(Q)}\right)^k \mathfrak{S}'(\mathcal{H}^+) \prod_{p \mid p_0} \left(1 - \frac{|\Omega^+(p)| - 1}{p - 1}\right)^{-1} \\
&\sim \left(\frac{Q}{\phi(Q)}\right)^k
\end{aligned}$$

as $H \to \infty$, because the product over $p \mid p_0$ is ~ 1 by (2.2.1). □

In the following lemma and throughout the rest of Section 2.4, c denotes a constant depending on k and ℓ at most, which may be different at each occurrence.

Lemma 2.4.4. *Let k and ℓ be arbitrary but bounded positive integers. Suppose $G(s_1, s_2)$ is a function which is defined and regular for $\operatorname{Re} s_1, \operatorname{Re} s_2 > -1/4$, and satisfies*

$$G(s_1, s_2) \ll \exp\left(c(\log R)^{\delta_1+\delta_2} \log\log\log R\right) \tag{2.4.16}$$

in this domain, where c is a constant depending on k and ℓ at most, and

$$\delta_i := \max(-\operatorname{Re} s_i, 0), \quad i = 1, 2.$$

Then the estimate

$$\begin{aligned}\mathscr{I} &:= \frac{1}{(2\pi i)^2} \int_{(1)} \int_{(1)} G(s_1, s_2) \left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)} \right)^k \frac{R^{s_1+s_2}}{(s_1 s_2)^{k+\ell+1}} \, ds_1 ds_2 \\ &= G(0,0) \binom{2\ell}{\ell} \frac{(\log R)^{k+2\ell}}{(k+2\ell)!} + O\left((\log R)^{k+2\ell-1/2} (\log\log R)^c\right)\end{aligned} \tag{2.4.17}$$

holds for all sufficiently large R.

Proof. This proof is based on the outline in [18], with most of the details taken from the proof of Lemma 3 of [21]. To set up for the proof, we put

$$U := \exp\left(\sqrt{\log R}\right)$$

and define the following contours (see Figure 2.1):

$$
\begin{array}{ll}
L_1' := \{(50\log U)^{-1} + it : t \in \mathbb{R}\} & L_2' := \{(100\log U)^{-1} + it : t \in \mathbb{R}\} \\
L_1 := \{(50\log U)^{-1} + it : |t| \leqslant U\} & L_2 := \{(100\log U)^{-1} + it : |t| \leqslant U/2\} \\
\mathscr{L}_1 := \{-(50\log U)^{-1} + it : |t| \leqslant U\} & \mathscr{L}_2 := \{-(100\log U)^{-1} + it : |t| \leqslant U/2\} \\
B_1 := \{\sigma \pm iU : |\sigma| \leqslant (50\log U)^{-1}\} & B_1 := \{\sigma \pm iU : |\sigma| \leqslant (100\log U)^{-1}\} \\
\mathscr{C}_1 := L_1 \cup \mathscr{L}_1 \cup B_1 & \mathscr{C}_2 := L_2 \cup \mathscr{L}_2 \cup B_2.
\end{array}
$$

Throughout the proof all contours are traversed counter-clockwise. All of these contours are to the right of the contour $\mathscr{C} - 1$, where $\mathscr{C}$ is the contour given in Lemma 2.4.1. Thus we have good estimates (2.4.3) for $\zeta(s+1)$ and $1/\zeta(s+1)$ for s in this region. Also, c will denote a constant depending on k and ℓ at most, which may be different at each occurrence throughout the proof.

Before proceeding with the integration, let us establish some basic estimates, which will be used in the course of the proof. First of all, for

$$\delta_i := \max(-\operatorname{Re} s_i, 0) \leqslant \frac{1}{24\log U}, \quad i = 1, 2, \tag{2.4.18}$$

we have

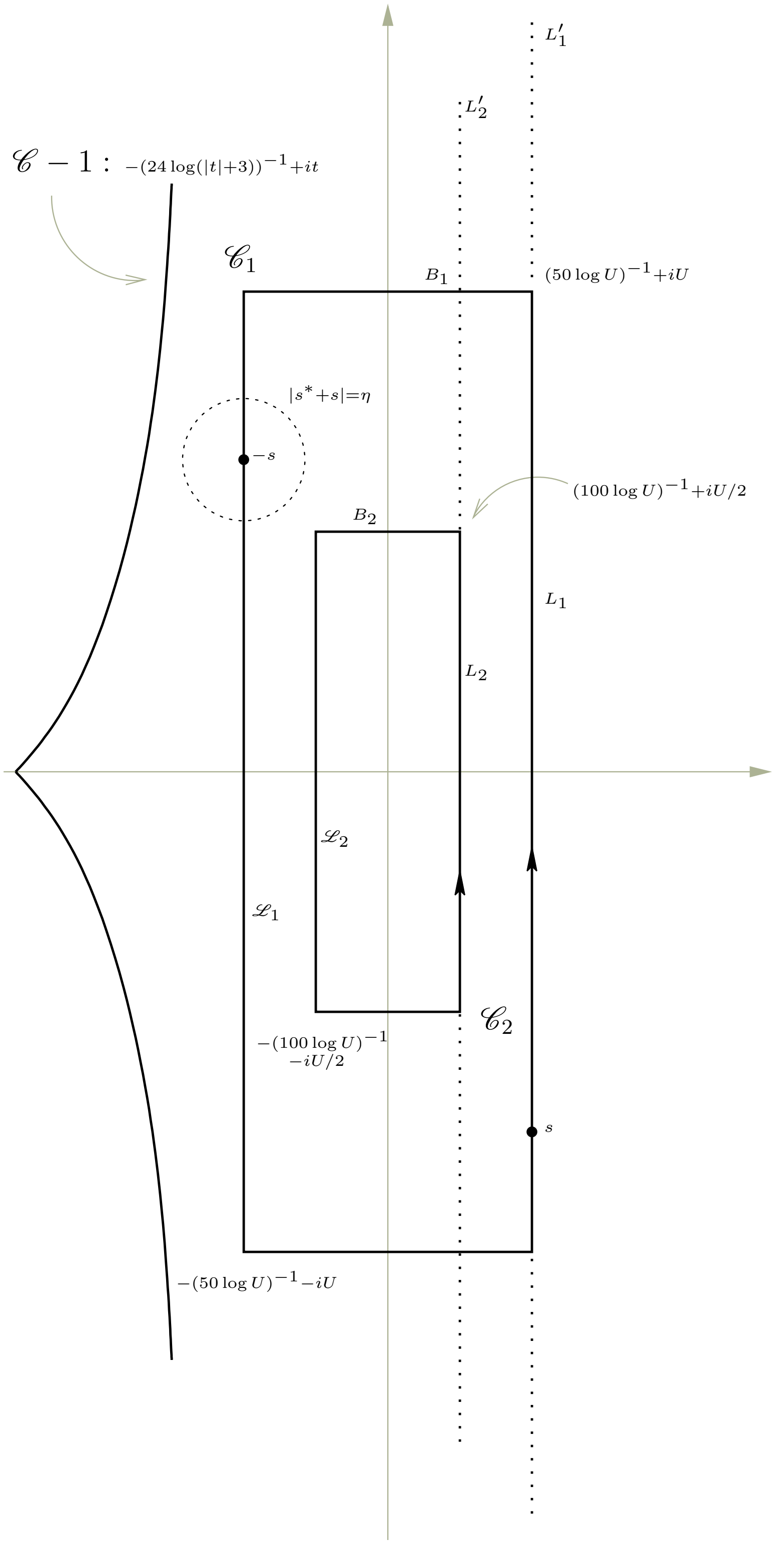
$$(\log R)^{\delta_1+\delta_2} \leqslant \exp\left(\frac{\log\log R}{12\sqrt{\log R}}\right) \ll 1.$$

Therefore, by (2.4.16), we have

$$G(s_1, s_2) \ll (\log\log R)^c \quad \text{for} \quad \operatorname{Re} s_1, \operatorname{Re} s_2 \geqslant -\frac{1}{24\log U}. \tag{2.4.19}$$

(As it turns out, we will only consider the region on or to the right of the one defined by (2.4.18), and so (2.4.19) will be applicable throughout the proof.)

Fig. 2.1:


L'_1
L'_2
$\mathscr{C}-1:\ -(24\log(|t|+3))^{-1}+it$
$\mathscr{C}_1$
B_1
$(50\log U)^{-1}+iU$
$|s^*+s|=\eta$
$-s$
$(100\log U)^{-1}+iU/2$
B_2
L_1
L_2
$\mathscr{L}_2$
$\mathscr{L}_1$
$\mathscr{C}_2$
$-(100\log U)^{-1}$
$-iU/2$
s
$-(50\log U)^{-1}-iU$

We write the integrand in (2.4.17) as

$$\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}},$$

where

$$H(s_1,s_2):=G(s_1,s_2)\left(\frac{(s_1+s_2)\zeta(s_1+s_2+1)}{s_1\zeta(s_1+1)s_2\zeta(s_2+1)}\right)^k$$

is regular in a neighborhood of $(0,0)$. We claim that if s_1, s_2 and s_1+s_2 lie on, or to the right of, $\mathscr{C}-1$, and if $\operatorname{Re} s_1, \operatorname{Re} s_2 \geqslant -(24\log U)^{-1}$, then

$$\begin{aligned} H(s_1,s_2) \ll (\log\log R)^c(\log(|s_1+s_2|+3))^k(|s_1+s_2|+1)^k \\ \times\frac{(\log(|s_1|+3))^k(\log(|s_1|+3))^k}{(|s_1|+1)^k(|s_2|+1)^k} \end{aligned} \tag{2.4.20}$$

For applying the translation $s\mapsto s+1$ to (2.4.1), we see that $(s\zeta(s+1))^{-1}\to 1$ as $s\to 0$. We fix an $\epsilon>0$ such that $(s\zeta(s+1))^{-1}\leqslant 2$ for $|s|\leqslant\epsilon$. For such s, we have $(|s|+1)^{-1}\log(|s|+3)\ll 1$, hence $(s\zeta(s+1))^{-1}\ll(|s|+1)^{-1}\log(|s|+3)$. For $|s|\geqslant\epsilon$, we have $|s|\leqslant|s|+1\leqslant|s|\,(1+1/\epsilon)\ll|s|$. If, furthermore, s lies on, or to the right of, $\mathscr{C}-1$, we have $1/\zeta(s+1)\ll\log(|s+1|+3)\ll\log(|s|+3)$ by (2.4.3) $(s\mapsto s+1)$. Thus, in any case, we have

$$(s\zeta(s+1))^{-1}\ll(|s|+1)^{-1}\log(|s|+3)$$

for s on, or to the right of, $\mathscr{C}-1$. If s_1, s_2 and s_1+s_2 are in the same range, we use this and both estimates in (2.4.3) to deduce that

$$\frac{(s_1+s_2)\zeta(s_1+s_2+1)}{s_1\zeta(s_1+1)s_2\zeta(s_2+1)} \ll (|s_1+s_2|+1)\log(|s_1+s_2|+3) \\ \times \frac{\log(|s_1|+3)\log(|s_2|+3)}{(|s_1|+1)(|s_2|+1)}.$$

To see how we used the estimate $s\zeta(s+1)-1/s \ll \log(|s|+3)$ ((2.4.3), $s\mapsto s+1$), note that this implies $s\zeta(s+1) \ll |s|\log(|s|+3)+O(1)$. When $|s|\ll 1$, $\log(|s|+3)=O(1)$, hence $s\zeta(s+1)\ll(|s|+1)\log(|s|+3)$, and clearly this also holds when $|s|\gg 1$. Now applying (2.4.19), we obtain (2.4.20) for s_1 and s_2 in the specified range.

From (2.4.20), we deduce that the following estimates hold if s_1, s_2 and s_1+s_2 lie on, or to the right of, $\mathscr{C}-1$, and if $\operatorname{Re} s_1, \operatorname{Re} s_2 \geqslant -(24\log U)^{-1}$:

$$H(s_1,s_2) \ll (\log\log R)^c(\log(|s_1|+3))^{2k}(\log(|s_1|+3))^{2k}, \tag{2.4.21}$$

and

$$H(s_1,s_2) \ll (\log\log R)^c \quad \text{if} \quad |s_1|,|s_2|\ll 1 \quad \text{or if} \quad |s_1+s_2|\ll 1. \tag{2.4.22}$$

Now we will show that

$$\int_{L_2'}\int_{L_1'\setminus L_1} \frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2 \ll \exp\left(-\tfrac{1}{2}\sqrt{\log R}\right), \tag{2.4.23}$$

and that the same bound holds if the domain of integration is replaced by $L_1'\times L_2'\setminus L_2$. For if $(s_1,s_2)\in L_1'\times L_2'$, then

$$(\log\log R)^c\frac{R^{s_1+s_2}}{(s_1+s_2)^k} \ll (\log\log R)^c(\log U)^k R^{\frac{3}{100\log U}} \ll \exp\left(\tfrac{4}{100}\sqrt{\log R}\right),$$

and so by (2.4.21),

$$\begin{aligned}\int_{L_2'}\int_{L_1'\setminus L_1} &\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &\ll \exp\left(\tfrac{1}{25}\sqrt{\log R}\right)\int_{L_2'}\int_{L_1'\setminus L_1}\frac{(\log(|s_1|+3))^{2k}}{|s_1|^{\ell+1}}\cdot\frac{(\log(|s_2|+3))^{2k}}{|s_1|^{\ell+1}}ds_1ds_2.\end{aligned} \tag{2.4.24}$$

Now, since $\ell+1\geqslant 2$,

$$\int_{L_1'\setminus L_1}\frac{(\log(|s_1|+3))^{2k}}{|s_1|^{\ell+1}}\,ds_1 \ll \int_U^\infty \frac{(\log(t+3))^{2k}}{t^{\ell+1}}\,dt \ll \frac{(\log U)^{2k}}{U^2},$$

and

$$\begin{aligned}\int_{L_2'}\frac{(\log(|s_2|+3))^{2k}}{|s_1|^{\ell+1}}\,ds_2 &\ll \left\{\int_{\frac{1}{100\log U}}^{\frac{1}{100\log U}+i}+\int_{\frac{1}{100\log U}+i}^{\frac{1}{100\log U}+i\infty}\right\}\frac{(\log(|s_2|+3))^{2k}}{|s_1|^{\ell+1}}\,ds_2\\ &\ll (\log U)^{\ell+1}+\int_1^\infty\frac{(\log(t+3))^{2k}}{t^{\ell+1}}\,dt\\ &\ll (\log U)^{\ell+1}.\end{aligned} \tag{2.4.25}$$

By (a corollary of) Fubini's theorem, we may write the double integral on the right-hand side of (2.4.24) as the product of the two integrals we have just estimated, and (2.4.23) follows. An analogous argument gives the same bound for the integral over $L_1'\times L_2'\setminus L_2$.

Next we will show that

$$\int_{\mathscr{L}_2\cup B_2}\int_{\mathscr{L}_1\cup B_1}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2 \ll \exp\left(-\tfrac{1}{200}\sqrt{\log R}\right). \tag{2.4.26}$$

For if $s_2\in\mathscr{L}_2$ then $|R^{s_2}| = R^{-(100\log U)^{-1}} = \exp\left(-\frac{1}{100}\sqrt{\log R}\right)$, and so similarly to (2.4.25) we have

$$\begin{aligned}\int_{\mathscr{L}_2} \frac{(\log(|s_2|+3))^{2k}\,|R^{s_2}|}{|s_2|^{\ell+1}}\,ds_2 &\ll \exp\left(-\tfrac{1}{100}\sqrt{\log R}\right)(\log U)^{\ell+1}\\ &\ll \exp\left(-\tfrac{1}{200}\sqrt{\log R}\right).\end{aligned}$$

If $s_2 \in B_2$ then $U \ll |s_2| \ll U$ and $|R^{s_2}| \leqslant R^{(100\log U)^{-1}} = \exp\left(\frac{1}{100}\sqrt{\log R}\right)$, thus, since $\ell + 1 \geqslant 2$, we have

$$\begin{aligned}\int_{B_2} \frac{(\log(|s_2|+3))^{2k}\,|R^{s_2}|}{|s_2|^{\ell+1}}\,ds_2 &\ll \exp\left(\tfrac{1}{100}\sqrt{\log R}\right)\frac{(\log U)^{2k-1}}{U^{\ell+1}}\\ &\ll \exp\left(-\tfrac{1}{200}\sqrt{\log R}\right),\end{aligned}$$

because B_2 is of length $\ll (\log U)^{-1}$. Hence the same bound holds for the integral over $\mathscr{L}_2 \cup B_2$ and, by the same argument, $\mathscr{L}_1 \cup B_1$. Since

$$s_1 + s_2 \gg (\log U)^{-1}$$

in this domain, we have

$$\begin{aligned}&\int_{\mathscr{L}_2\cup B_2}\int_{\mathscr{L}_1\cup B_1} \frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &\quad\ll (\log\log R)^c(\log U)^k\\ &\qquad\times\int_{\mathscr{L}_2\cup B_2}\int_{\mathscr{L}_1\cup B_1} \frac{(\log(|s_1|+3))^{2k}\,|R^{s_1}|}{|s_1|^{\ell+1}}\cdot\frac{(\log(|s_2|+3))^{2k}\,|R^{s_2}|}{|s_2|^{\ell+1}}\,ds_1ds_2\end{aligned}$$

by (2.4.21). We obtain (2.4.26) by using Fubini's theorem to write the double integral as a product of two integrals and using the above estimates.

Finally, we will use the following estimates for the partial derivatives of $H(s_1, s_2)$. Recall Cauchy's estimate for derivatives: if $f(z)$ is analytic in the domain $|z - z_0| \leqslant \eta$, and if $f(z) \leqslant M$ for $|z - z_0| = \eta$, then

$$\left|f^{(j)}(z_0)\right| \leqslant \frac{Mj!}{\eta^j}.$$

We set

$$\eta := \frac{1}{50^2 \log U}$$

so that for any s on or inside $\mathscr{C}_1$, and any s^* with $|s^* - s| \leqslant \eta$, s^*, s and $s^* + s$ are to the right of $\mathscr{C} - 1$ (see Figure 2.1). That is

$$\max(-\operatorname{Re} s, 0), \max(-\operatorname{Re} s^*, 0) \leqslant \left(\frac{1}{50} + \frac{1}{50^2}\right)\frac{1}{\log U} \leqslant \frac{1}{24 \log U},$$

and so (2.4.19) – (2.4.22) are applicable here. Thus, by (2.4.22), we have

$$\frac{\partial^m}{\partial s_2^m}\frac{\partial^j}{\partial s_1^j} H(0,0) \leqslant \frac{j!m!}{\eta^{j+m}} \sup_{|s_1|,|s_2|=\eta} |H(s_1, s_2)| \ll (\log\log R)^c (\log R)^{(j+m)/2}, \tag{2.4.27}$$

and for s_2 on or inside $\mathscr{C}_1$ we have

$$\frac{\partial^j}{\partial s_1^j} H(0, s_2) \leqslant \frac{j!}{\eta^j} \sup_{|s_1|=\eta} |H(s_1, s_2)| \ll (\log\log R)^c (\log R)^{j/2} \tag{2.4.28}$$

and

$$\frac{\partial^j}{\partial s_1^j} H(-s_2, s_2) \leqslant \frac{j!}{\eta^j} \sup_{|s_1+s_2|=\eta} |H(s_1, s_2)| \ll (\log\log R)^c (\log R)^{j/2}. \tag{2.4.29}$$

To begin to evaluate $\mathscr{I}$, we shift the s_1- and s_2-contours from (1) to the left to L_1' and L_2' respectively, then we truncate these lines to form L_1 and L_2, giving rise to our first error term. Thus

$$\begin{aligned}\mathscr{I} &= \frac{1}{(2\pi i)^2}\int_{L_2'}\int_{L_1'}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &= \frac{1}{(2\pi i)^2}\left\{\int_{L_2}\int_{L_1}+\int_{L_2'\setminus L_2}\int_{L_1}+\int_{L_2'}\int_{L_1'\setminus L_1}\right\}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &= \frac{1}{(2\pi i)^2}\int_{L_2}\int_{L_1}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2+O\left(\exp\left(-\tfrac{1}{2}\sqrt{\log R}\right)\right)\end{aligned}$$

by (2.4.23). Shifting the s_1-contour from L_1 back to $\mathscr{L}_1$, we encounter a singularity at $s_1=0$, which lies inside $\mathscr{C}_1$, and another singularity at $s_1=-s_2$, which also lies inside $\mathscr{C}_1$ since s_2 is on L_2. Thus, by the residue theorem,

$$\begin{aligned}&\int_{L_2}\int_{L_1}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &\qquad=\int_{L_2}\left\{\int_{\mathscr{C}_1}-\int_{\mathscr{L}_1\cup B_1}\right\}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &\qquad=2\pi i\int_{L_2}\left\{\operatorname*{Res}_{s_1=0}+\operatorname*{Res}_{s_1=-s_2}\right\}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2\\ &\qquad\qquad-\int_{L_2}\int_{\mathscr{L}_1\cup B_1}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2.\end{aligned}$$

Now we shift the s_2-contour from L_2 back to $\mathscr{L}_2$. We will presently see that the only singularity we encounter is at $s_2=0$, which lies inside the rectangle $\mathscr{C}_2$. Using the residue theorem to write

$$\int_{L_2}=\int_{\mathscr{C}_2}-\int_{\mathscr{L}_2\cup B_2}=2\pi i\operatorname*{Res}_{s_2=0}-\int_{\mathscr{L}_2\cup B_2}$$

and combining the last three equations, we see that

$$\begin{aligned}\mathscr{I} &= \operatorname*{Res}_{s_2=0}\operatorname*{Res}_{s_1=0}\left(\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\right)ds_1ds_2\\ &-\frac{1}{2\pi i}\int_{\mathscr{L}_2\cup B_2}\operatorname*{Res}_{s_1=0}\left(\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\right)ds_1ds_2\\ &-\frac{1}{2\pi i}\int_{\mathscr{L}_1\cup B_1}\operatorname*{Res}_{s_2=0}\left(\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\right)ds_1ds_2\\ &+\frac{1}{2\pi i}\int_{L_2}\operatorname*{Res}_{s_1=-s_2}\left(\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\right)ds_1ds_2\\ &-\frac{1}{(2\pi i)^2}\int_{\mathscr{L}_2\cup B_2}\int_{\mathscr{L}_1\cup B_1}\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k(s_1s_2)^{\ell+1}}\,ds_1ds_2+O\left(\exp\left(-\tfrac{1}{2}\sqrt{\log R}\right)\right)\\ &:=I_0-I_1-I_2+I_3+O\left(\exp\left(-\tfrac{1}{200}\sqrt{\log R}\right)\right)\end{aligned}\tag{2.4.30}$$

by (2.4.26).

Since $s\zeta(s+1)\to 1$ as $s\to 0$ by (2.4.1), the residue of the integrand at $s_1=0$ is a pole of order at most $\ell+1$. Therefore [1], by Leibniz's formula,

$$\operatorname*{Res}_{s_1=0}\frac{H(s_1,s_2)R^{s_1}}{(s_1+s_2)^k s_1^{\ell+1}}=\frac{1}{\ell!}\sum_{i=0}^{\ell}\binom{\ell}{i}(\log R)^{\ell-i}\frac{\partial^i}{\partial s_1^i}\left(\frac{H(0,s_2)}{(s_1+s_2)^k}\right)$$

and

$$\frac{\partial^i}{\partial s_1^i}\left(\frac{H(0,s_2)}{(s_1+s_2)^k}\right)=\sum_{j=0}^{i}\binom{i}{j}\frac{\partial^j}{\partial s_1^j}H(0,s_2)\frac{(-1)^{i-j}k(k+1)\cdots(k+i-j-1)}{s_2^{k+i-j}}.$$

Hence

$$\operatorname*{Res}_{s_1=0}\frac{H(s_1,s_2)R^{s_1}}{(s_1+s_2)^k s_1^{\ell+1}}=\sum_{i=0}^{\ell}\sum_{j=0}^{i}\frac{a(i,j)(\log R)^{\ell-i}}{s_2^{k+i-j}}\frac{\partial^j}{\partial s_1^j}H(0,s_2),\tag{2.4.31}$$

[1] As noted in the proof of Lemma 3 of [21], if $H(0,0)=G(0,0)=0$, the order of the pole is at most ℓ. Nevertheless, the formula we use to compute is still valid: one or more of the initial terms will be 0. However, this situation does not arise in the proof of Proposition 2.2.2, nor does it in the proof of Proposition 3.2.2 below.

where

$$a(i,j) = (-1)^{i-j}\frac{1}{\ell!}\binom{\ell}{i}\binom{i}{j}k(k+1)\cdots(k+i-j-1).$$

The (i,j)th term in (2.4.31) contributes to I_0 a pole at $s_2 = 0$ of order at most $\ell+1+k+i-j$. Applying Leibniz's formula again, we see that

$$\begin{aligned}&\operatorname*{Res}_{s_2=0}\frac{R^{s_2}}{s_2^{\ell+1+k+i-j}}\frac{\partial^j}{\partial s_1^j}H(s_1,0) = \\ &\frac{1}{(\ell+k+i-j)!}\sum_{m=0}^{\ell+k+i-j}\binom{\ell+k+i-j}{m}(\log R)^{\ell+k+i-j-m}\frac{\partial^m}{\partial s_2^m}\frac{\partial^j}{\partial s_1^j}H(0,0).\end{aligned} \tag{2.4.32}$$

Combining (2.4.31) – (2.4.32) yields

$$I_0 = \sum_{i=0}^{\ell}\sum_{j=0}^{i}\sum_{m=0}^{\ell+k+i-j} b(i,j,m)(\log R)^{\ell+k+i-j-m}\frac{\partial^m}{\partial s_2^m}\frac{\partial^j}{\partial s_1^j}H(0,0), \tag{2.4.33}$$

where

$$\begin{aligned}b(i,j,m) &= \frac{a(i,j)}{(\ell+k+i-j)!}\binom{\ell+k+i-j}{m} \\ &= (-1)^{i-j}\binom{\ell}{i}\binom{i}{j}\frac{k(k+1)\cdots(k+i-j-1)}{\ell!(\ell+k+i-j)!}\binom{\ell+k+i-j}{m}.\end{aligned}$$

By the combinatorial identity

$$\sum_{i=0}^{\ell} b(i,0,0) = \sum_{i=0}^{\ell}\binom{\ell}{i}\frac{(-1)^i k(k+1)\cdots(k+i-1)}{\ell!(\ell+k+i)!} = \binom{2\ell}{\ell}\frac{1}{(k+2\ell)!},$$

and since $H(0,0) = G(0,0)$, we see from (2.4.27) and (2.4.33) that

$$I_0 = G(0,0)\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!} + O\left((\log R)^{k+2\ell-1/2}(\log\log R)^c\right).$$

For I_1, we put (2.4.28) into (2.4.31) and estimate the resulting integral, which is similar to the one in (2.4.26). Thus

$$\begin{aligned} I_1 &\ll (\log\log R)^c(\log R)^\ell \sum_{i=0}^{\ell}\sum_{j=0}^{i}(\log R)^{-i+j/2}\int_{\mathscr{L}_2\cup B_2}\frac{ds_2}{|s_2|^{k+i-j}} \\ &\ll (\log\log R)^c(\log R)^\ell \sum_{i=0}^{\ell}\sum_{j=0}^{i}(\log R)^{-i+j/2}(\log U)^{k+i-j}. \end{aligned}$$

We estimate I_2 by an analogous argument. Hence

$$I_1, I_2 \ll (\log\log R)^c(\log R)^{\ell+k/2}.$$

Finally, for I_3 we have

$$\begin{aligned} \operatorname*{Res}_{s_1=-s_2}\left(\frac{H(s_1,s_2)R^{s_1+s_2}}{(s_1+s_2)^k s_1^{\ell+1}s_2^{\ell+1}}\right) &= \lim_{s_1\to -s_2}\frac{1}{(k-1)!}\frac{\partial^{k-1}}{\partial s_1^{k-1}}\left(\frac{H(s_1,s_2)R^{s_1+s_2}}{s_1^{\ell+1}s_2^{\ell+1}}\right) \\ &= \frac{1}{(k-1)!}\sum_{i=0}^{k-1}\mathscr{J}_i(s_2)(\log R)^{k-1-i}, \end{aligned}$$

where

$$\mathscr{J}_i(s_2) := \binom{k-1}{i}\sum_{j=0}^{i}\binom{i}{j}\frac{\partial^{i-j}}{\partial s_1^{i-j}}H(-s_2,s_2)\frac{(-1)^j(\ell+1)\cdots(\ell+j)}{(-1)^{\ell+j+1}s_2^{2(\ell+1)+j}}.$$

Now by (2.4.29), we have

$$\begin{aligned}\int_{L_2} \mathscr{J}_i(s_2)ds_2 &\ll (\log\log R)^c \sum_{j=0}^{i} (\log R)^{(i-j)/2} \int_{L_2} \frac{ds_2}{|s_2|^{2(\ell+1)+j}} \\ &\ll (\log\log R)^c \sum_{j=0}^{i} (\log R)^{(i-j)/2} (\log U)^{2(\ell+1)+j} \\ &\ll (\log\log R)^c (\log R)^{\ell+1+i/2},\end{aligned}$$

hence

$$I_3 \ll (\log\log R)^c \sum_{i=0}^{k-1} (\log R)^{k+\ell-i/2} \ll (\log\log R)^c (\log R)^{k+\ell}.$$

We obtain (2.4.17) by combining the estimates for $I_0, \ldots, I_3$ with (2.4.30).

□

We will need to estimate an error term involving

$$E^*(N,q) := \max_{x \leqslant N} \max_{(a,q)=1} \left| \sum_{\substack{p \leqslant x \\ p \equiv a \bmod q}} \log p - \frac{x}{\phi(q)} \right|.$$

Lemma 2.4.5 (Bombieri-Vinogradov theorem). *For any fixed positive number A there exists a positive number $B = B(A)$, depending only on A, such that*

$$\sum_{q \leqslant N^{1/2}(\log N)^{-B}} E^*(N,q) \ll_A N(\log N)^{-A}.$$

Proof. See [6, Théorème 17]. □

This, the usual Bombieri-Vinogradov theorem, will not suffice here, but the next lemma, which is Lemma 2 of [19], will.

Lemma 2.4.6. *Let Q be an integer, and let Y and M be numbers, such that*

$$Q^2 \leqslant Y \leqslant M, \quad \exp\left(2\sqrt{\log M}\right) \leqslant Y. \tag{2.4.34}$$

If there is an exceptional modulus $q_0 \leqslant Y$, suppose $p_0 \nmid Q$ for some $p_0 \mid q_0$; otherwise, let $p_0 = 1$. If

$$R^* = M^{1/2} Q^{-3} \exp\left(-\sqrt{\log M}\right),$$

then we have, with explicitly calculable positive constants c_1 and c_2,

$$\sum_{\substack{D \leqslant R^* \\ (D, Qp_0)=1}} E^*(M, QD) \leqslant c_1 \frac{M}{Q} \exp\left(-\frac{c_2 \log M}{\log Y}\right). \tag{2.4.35}$$

Proof. See [22, Theorem 6]. □

2.4.2 The proof of Proposition 2.2.2

We now assume all but one of the hypotheses of Proposition 2.2.2. The hypothesis we do not assume is that $k \geqslant 2$: until stated otherwise at the very end of the proof, we assume only that $k \geqslant 1$. Thus H, N and R are real parameters such that $H = \epsilon \log N$, $\epsilon > 0$ arbitrarily small but fixed, and $R = N^{1/4-\epsilon'}$. We assume H, N and R are sufficiently large, where the meaning of 'sufficiently large' will be made clear in the context of the proof. Integers $k, \ell \geqslant 1$ are fixed, $Q = Q(H)$ is a number satisfying (2.2.2) – (2.2.5), and $\mathcal{H} = \{Qx + h_1, \ldots, Qx + h_k\}$ as in (2.2.6).

Recall that

$$\Omega(d) = \Omega(d; \mathcal{H}) := \{n \bmod d : P(n; \mathcal{H}) \equiv 0 \bmod d\},$$

where $P(n;\mathcal{H}) = (Qn+h_1)\cdots(Qn+h_k)$, as in (2.2.8). A Chinese remainder theorem argument shows that $n \bmod d \in \Omega(d)$ if and only if $p^r \mid\mid P(n;\mathcal{H})$ for every $p^r \mid\mid d$, and so $|\Omega(d)|$ defines a multiplicative function of d. Thus, if we define

$$\lambda_R(d;j) := \begin{cases} \frac{1}{j!}\mu(d)(\log R/d)^j & \text{if } d \leqslant R, \\ 0 & \text{if } d > R, \end{cases} \tag{2.4.36}$$

we see from (2.2.7) that

$$\Lambda_R(n;\mathcal{H},j) := \frac{1}{j!}\sideset{}{'}\sum_{\substack{d \mid P(n;\mathcal{H}) \\ d \leqslant R}} \mu(d)(\log R/d)^j = \sideset{}{'}\sum_{\substack{n \bmod d \\ \in \Omega(d)}} \lambda_R(d;j). \tag{2.4.37}$$

With this we are ready to begin the evaluation of the left-hand side of (2.2.9).

Let us abbreviate $\lambda_R(d;k+\ell)$ to λ_d. Expanding the square and noting that the condition

$$d_1 \mid P(n;\mathcal{H}),\ d_2 \mid P(n;\mathcal{H})$$

is equivalent to $[d_1,d_2] \mid P(n;\mathcal{H})$, which is equivalent to $n \bmod [d_1,d_2] \in \Omega([d_1,d_2])$, we obtain

$$\begin{aligned} \sum_{N<n\leqslant 2N} \Lambda_R(n;\mathcal{H},k+\ell)^2 &= \sum_{N<n\leqslant 2N}\left(\sideset{}{'}\sum_{[d_1,d_2] \mid P(n;\mathcal{H})} \lambda_{d_1}\lambda_{d_2}\right) \\ &= \sideset{}{'}\sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{m \bmod [d_1,d_2] \\ \in\Omega([d_1,d_2])}} \sum_{\substack{N<n\leqslant 2N \\ n\equiv m \bmod [d_1,d_2]}} 1 \\ &= \sideset{}{'}\sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2}\, |\Omega([d_1,d_2])| \left(\frac{N}{[d_1,d_2]} + O(1)\right) \\ &= N\mathcal{T} + O(\mathcal{E}), \end{aligned} \tag{2.4.38}$$

where

$$\mathcal{T} := {\sum_{d_1,d_2}}' \lambda_{d_1}\lambda_{d_2}\frac{|\Omega([d_1,d_2])|}{[d_1,d_2]}, \quad \mathcal{E} := {\sum_{d_1,d_2}}' |\lambda_{d_1}\lambda_{d_2}| \cdot |\Omega([d_1,d_2])| \,.$$

We consider the error term $\mathcal{E}$ first. From the definition (2.4.36) it is clear that $|\lambda_d| \leqslant (\log R)^{k+\ell}$. Also, since $(Q, h_1\cdots h_k) = 1$ we have $|\Omega(p)| \leqslant k$ for all p by (2.4.6) and since $|\Omega(p)| = 0$ if $p \nmid Q$. As we noted earlier, $|\Omega(d)|$ is multiplicative in d, so for squarefree d we have $|\Omega(d)| \leqslant k^{\omega(d)}$, where $\omega(d)$ denotes the number of distinct prime factors of d. Therefore

$$\begin{aligned}\mathcal{E} &\leqslant (\log R)^{2(k+\ell)} \sum_{d_1,d_2\leqslant R} \mu^2(d_1)\mu^2(d_2)k^{\omega([d_1,d_2])} \\ &= (\log R)^{2(k+\ell)} \sum_{D\leqslant R^2} \mu^2(D)k^{\omega(D)} \sum_{[d_1,d_2]=D} 1 \\ &= (\log R)^{2(k+\ell)} \sum_{D\leqslant R^2} \mu^2(D)(3k)^{\omega(D)}.\end{aligned} \tag{2.4.39}$$

Here we have used the elementary fact that if D is squarefree and $D = [d_1, d_2]$, then $D = ge_1e_2$, where $(d_1, d_2) = g$, $d_1 = ge_1$, $d_2 = ge_2$, and $(g, e_1) = (g, e_2) = (e_1, e_2) = 1$. Thus $\sum_{[d_1,d_2]=D} 1$ is precisely the number of ways of writing D as a product of three pairwise coprime positive integers, namely $3^{\omega(D)}$.

For positive integers κ, we have

$$\sum_{D\leqslant R^2} \frac{\mu^2(D)\kappa^{\omega(D)}}{D} = \sum_{d_1\cdots d_\kappa\leqslant R^2} \frac{\mu^2(d_1)\cdots\mu^2(d_\kappa)}{d_1\cdots d_\kappa} \ll (\log R^2)^\kappa \ll (\log N)^\kappa, \tag{2.4.40}$$

and hence

$$\sum_{D\leqslant R^2} \mu^2(D)\kappa^{\omega(D)} \leqslant R^2 \sum_{D\leqslant R^2} \frac{\mu^2(D)\kappa^{\omega(D)}}{D} \ll R^2(\log N)^{\kappa}.$$

Putting this last inequality, with $\kappa = 3k$, into (2.4.39) we obtain

$$\mathcal{E} \ll R^2(\log N)^{5k+2\ell} \ll N^{1/2}, \tag{2.4.41}$$

because $R = N^{1/4-\epsilon'}$.

Now we consider $\mathcal{T}$. First of all, by (2.4.36) and Lemma 2.4.2, we have

$$\lambda_R(d;j) = \frac{\mu(d)}{2\pi i}\int_{(1)} \left(\frac{R}{s}\right)^s \frac{ds}{s^{j+1}},$$

hence

$$\lambda_{d_1}\lambda_{d_2} = \frac{\mu(d_1)\mu(d_2)}{(2\pi i)^2}\int_{(1)}\int_{(1)} \frac{R^{s_1+s_2}\, ds_1 ds_2}{d_1^{s_1}d_2^{s_2}(s_1s_2)^{k+\ell+1}}. \tag{2.4.42}$$

Putting this into our expression for $\mathcal{T}$, we find that

$$\mathcal{T} = \frac{1}{(2\pi i)^2}\int_{(1)}\int_{(1)} F(s_1,s_2;\Omega)\frac{R^{s_1+s_2}}{(s_1s_2)^{k+\ell+1}}\, ds_1 ds_2, \tag{2.4.43}$$

where

$$\begin{aligned} F(s_1,s_2;\Omega) &:= \sum_{d_1,d_2}{}' \frac{\mu(d_1)\mu(d_2)\,|\Omega([d_1,d_2])|}{[d_1,d_2]d_1^{s_1}d_2^{s_2}} \\ &= \prod_{p\nmid Qp_0}\left(1 - \frac{|\Omega(p)|}{p}\left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right) \qquad (2.4.44) \\ &= G(s_1,s_2;\Omega)\left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)}\right)^k \end{aligned}$$

when $\operatorname{Re} s_1, \operatorname{Re} s_2 > 0$, by (2.4.2) and (2.4.4). (Recall that $\sum'$ means that the sum is taken over indices coprime with Qp_0.) Putting (2.4.44) into (2.4.43), we see that $\mathcal{T}$ is the same as $\mathscr{I}$ of Lemma 2.4.4, with $G(s_1, s_2; \Omega)$ in the role of $G(s_1, s_2)$.

Since $H \ll \log R$, we have

$$G(s_1, s_2; \Omega) \ll \exp\big(c(\log R)^{\delta_1+\delta_2} \log\log\log R\big)$$

when $\delta_i := \max(-\operatorname{Re} s_i, 0) < 1/4$, $i = 1, 2$, by (2.4.8). (Recall that c denotes a constant depending at most on k and ℓ, which may be different at each occurrence.) Also, $G(0, 0; \Omega) \sim (Q/\phi(Q))^k$ as $H \to \infty$ by (2.4.9). In particular we may assume H is large enough so that $G(0, 0; \Omega) \gg 1$. Thus the hypotheses of Lemma 2.4.4 are satisfied with $G(s_1, s_2) = G(s_1, s_2; \Omega)$, therefore by (2.4.17) and since $G(0, 0; \Omega) \gg 1$, we have

$$\mathcal{T} = G(0, 0; \Omega)\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\left(1 + O\left((\log R)^{-1/2}(\log\log R)^c\right)\right) \qquad (2.4.45)$$

for all sufficiently large R. Since $\log R \ll \log N$, putting (2.4.41) and (2.4.45) into (2.4.38), then using (2.4.9), we obtain

$$\begin{aligned}\frac{1}{N}\sum_{N<n\leqslant 2N} \Lambda_R(n; \mathcal{H}, k+\ell)^2 &= (1+o(1))G(0, 0; \Omega)\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\\ &= (1+o(1))\left(\frac{Q}{\phi(Q)}\right)^k\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\end{aligned}$$

as $H, N, R \to \infty$. We have established (2.2.9) of Proposition 2.2.2.

We now turn to (2.2.10). Similarly to (2.4.38), we have

$$\begin{aligned}\sum_{N<n\leqslant 2N} \vartheta(Qn+h)\Lambda_R(n;\mathcal{H},k+\ell)^2 \\ &= \sum_{d_1,d_2}{}' \lambda_{d_1}\lambda_{d_2} \sum_{\substack{N<n\leqslant 2N \\ [d_1,d_2]|P(n;\mathcal{H})}} \vartheta(Qn+h) \\ &= \sum_{d_1,d_2}{}' \lambda_{d_1}\lambda_{d_2} \sum_{\substack{m \bmod [d_1,d_2] \\ \in\Omega([d_1,d_2])}} \sum_{\substack{QN+h<p\leqslant 2QN+h \\ p\equiv h \bmod Q \\ p\equiv Qm+h \bmod [d_1,d_2]}} \log p.\end{aligned} \tag{2.4.46}$$

We may assume $(Qm+h,[d_1,d_2]) = (Q,[d_1,d_2]) = 1$ in the last sum, so we define

$$\Omega^*(d) = \Omega(d) \setminus \{m \bmod d : (Qm+h,d) \neq 1\}.$$

For d_1, d_2 with $(Q,[d_1,d_2]) = 1$ and $m \bmod [d_1,d_2] \in \Omega^*([d_1,d_2])$, we let

$$h_m \bmod Q[d_1,d_2]$$

be the unique congruence class mod $Q[d_1,d_2]$ satisfying $h_m \equiv h \bmod Q$ and $h_m \equiv Qm+h \bmod [d_1,d_2]$. Thus, the last sum in (2.4.46) is equal to

$$\sum_{\substack{QN+h<p\leqslant 2QN+h \\ p\equiv h_m \bmod Q[d_1,d_2]}} \log p = \frac{2QN+h}{\phi(Q[d_1,d_2])} - \frac{QN+h}{\phi(Q[d_1,d_2])} + O\left(E^*(3QN,Q[d_1,d_2])\right),$$

where we recall that

$$E^*(3QN,Q[d_1,d_2]) := \max_{x\leqslant 3QN} \max_{(a,Q[d_1,d_2])=1} \left| \sum_{\substack{p\leqslant x \\ p\equiv a \bmod Q[d_1,d_2]}} \log p - \frac{x}{\phi(Q[d_1,d_2])} \right|.$$

We now have

$$\sum_{N<n\leqslant 2N} \vartheta(Qn+h)\Lambda_R(n;\mathcal{H},k+\ell)^2 = \frac{QN}{\phi(Q)}\mathcal{T}^* + O(\mathcal{E}^*), \tag{2.4.47}$$

where

$$\begin{aligned}\mathcal{T}^* &:= \sum_{d_1,d_2}{}' \frac{\lambda_{d_1}\lambda_{d_2}\,|\Omega^*([d_1,d_2])|}{\phi([d_1,d_2])},\\ \mathcal{E}^* &:= \sum_{d_1,d_2}{}' |\lambda_{d_1}\lambda_{d_2}|\cdot|\Omega^*([d_1,d_2])|\,E^*(3QN,Q[d_1,d_2]).\end{aligned}$$

We consider the error term $\mathcal{E}^*$ first. Similarly to (2.4.39) we have

$$\begin{aligned}\mathcal{E}^* &\leqslant (\log R)^{2(k+\ell)} \sum_{D\leqslant R^2}{}' \mu^2(D)k^{\omega(D)}E^*(3QN,QD)\sum_{[d,e]=D} 1\\ &= (\log R)^{2(k+\ell)} \sum_{D\leqslant R^2}{}' \mu^2(D)(3k)^{\omega(D)}E^*(3QN,QD),\end{aligned}$$

for clearly $|\Omega^*(d)|\leqslant|\Omega(d)|$, and $|\Omega(d)|\leqslant k^{\omega(d)}$ for squarefree d as noted prior to (2.4.39). By the trivial inequality

$$E^*(3QN,QD) \ll \frac{QN\log QN}{QD} \ll \frac{N\log N}{D},$$

and the Cauchy-Schwarz inequality, we have

$$\begin{aligned}&\sum_{D\leqslant R^2}{}' \mu^2(D)(3k)^{\omega(D)}E^*(3QN,QD)\\ &\quad\ll \left(N\log N\sum_{D\leqslant R^2}\frac{\mu^2(D)(3k)^{2\omega(D)}}{D}\right)^{1/2}\left(\sum_{D\leqslant R^2}{}' E^*(3QN,QD)\right)^{1/2}.\end{aligned} \tag{2.4.48}$$

Now we apply Lemma 2.4.6. By (2.2.2) – (2.2.5), we see that (2.4.34) is satisfied with

$$Y = \exp\left(2cH/(\log H)^2\right) = N^{2c\epsilon(1+o(1))/(\log\log N)^2}$$

and $M = 3QN$, where in this instance c is the constant in (2.2.4). We also have

$$R^2 = N^{1/2-2\epsilon'} \leqslant R^* = (3QN)^{1/2}Q^{-3}\exp\left(-\sqrt{\log 3QN}\right)$$

for all sufficiently large N, and

$$c_2 \log M/\log Y = c_2(1+o(1))\log N/\log Y = c_2(1+o(1))(\log\log N)^2/2c\epsilon.$$

Letting $c_3 = c_2/12c\epsilon$ and putting this into (2.4.35), we deduce from Lemma 2.4.6 that

$$\sum_{D\leqslant R^2}{}' E^*(3QN, QD) \ll N(\log N)^{-5c_3\log\log N}$$

for all sufficiently large N. Putting this, as well as (2.4.40) with $\kappa = (3k)^2$, into (2.4.48) yields

$$\mathcal{E} \ll N\frac{(\log N)^{2(k+\ell)+(3k)^2/2+1/2}}{(\log N)^{2c_3\log\log N}} \ll N(\log N)^{-c_3\log\log N}. \qquad (2.4.49)$$

We will now evaluate $\mathcal{T}^*$, assuming first that $Qx+h \notin \mathcal{H}$. Thus

$$|\mathcal{H}^+| := |\mathcal{H}\cup\{Qx+h\}| = k+1,$$

and for $p \nmid Q$ we have

$$\begin{aligned}|\Omega^*(p)| &:= |\Omega(p) \setminus \{m \bmod p : (Qm+h,p) \neq 1\}| \\ &= \left|\{-Q^{-1}h_1, \dots, -Q^{-1}h_k\} \bmod p \setminus \{-Q^{-1}h \bmod p\}\right| \\ &= \left|\{-Q^{-1}h_1, \dots, -Q^{-1}h_k, -Q^{-1}h\} \bmod p \setminus \{-Q^{-1}h \bmod p\}\right| \\ &= |\Omega^+(p)| - 1.\end{aligned}$$

(Recall that $\Omega^+(p) = \Omega(p; \mathcal{H}^+)$.) As with $|\Omega(d)|$, a Chinese remainder theorem argument shows that $|\Omega^*(d)|$ defines a multiplicative function of d. Thus

$$|\Omega^*([d_1,d_2])| = \prod_{p|[d_1,d_2]} \big(|\Omega^+(p)| - 1\big),$$

provided $[d_1,d_2]$ is squarefree and $(Q,[d_1,d_2]) = 1$, as is the case for d_1, d_2 appearing in the sum defining $\mathcal{T}^*$.

Therefore, putting (2.4.42) into our expression for $\mathcal{T}^*$, we find that

$$\mathcal{T}^* = \frac{1}{(2\pi i)^2} \int_{(1)} \int_{(1)} F^+(s_1,s_2;\Omega^+) \frac{R^{s_1+s_2}}{(s_1s_2)^{k+\ell+1}}\, ds_1 ds_2, \tag{2.4.50}$$

where

$$\begin{aligned}F^+(s_1,s_2;\Omega^+) &:= {\sum_{d_1,d_2}}' \frac{\mu(d_1)\mu(d_2)\,|\Omega^*([d_1,d_2])|}{\phi([d_1,d_2]) d_1^{s_1} d_2^{s_2}} \\ &= \prod_{p \nmid Qp_0} \left(1 - \frac{|\Omega^+(p)|-1}{p-1}\left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right) \qquad (2.4.51) \\ &= G^+(s_1,s_2;\Omega^+)\left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)}\right)^k\end{aligned}$$

when $\operatorname{Re} s_1, \operatorname{Re} s_2 > 0$, by (2.4.2) and (2.4.5). Putting (2.4.51) into (2.4.50), we see that $\mathcal{T}^*$ is the same as $\mathscr{I}$ of Lemma 2.4.4, with $G^+(s_1,s_2;\Omega^+)$ in the role of $G(s_1, s_2)$.

Since $H \ll \log R$, we have

$$G^+(s_1, s_2; \Omega^+) \ll \exp\left(c(\log R)^{\delta_1+\delta_2} \log\log\log R\right)$$

when $\delta_i = \max(-\operatorname{Re} s_i, 0) < 1/4$, $i = 1, 2$, by (2.4.8). Also,

$$G^+(0, 0; \Omega^+) \sim (Q/\phi(Q))^k$$

as $H \to \infty$ by (2.4.9). In particular we may assume H is large enough so that $G^+(0, 0; \Omega^+) \gg 1$. Thus the hypotheses of Lemma 2.4.4 are satisfied with $G(s_1, s_2) = G^+(s_1, s_2; \Omega^+)$, therefore by (2.4.17) and since $G^+(0, 0; \Omega^+) \gg 1$, we have

$$\mathcal{T}^* = G^+(0, 0; \Omega^+)\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\left(1 + O\left((\log R)^{-1/2}(\log\log R)^c\right)\right) \quad (2.4.52)$$

for all sufficiently large R. Since $\log R \ll \log N$, putting (2.4.49) and (2.4.52) into (2.4.47), then using (2.4.9), we obtain

$$\begin{aligned}\frac{1}{N}\sum_{N<n\leqslant 2N} &\vartheta(Qn+h)\Lambda_R(n; \mathcal{H}, k+\ell)^2 \\ &= (1+o(1))\,(Q/\phi(Q))\,G^+(0, 0; \Omega^+)\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!} \qquad (2.4.53) \\ &= (1+o(1))\left(\frac{Q}{\phi(Q)}\right)^{k+1}\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\end{aligned}$$

as $H, R, N \to \infty$, provided $Qx + h \notin \mathcal{H}$. We have established the first case of (2.2.10).

We can reduce the case $Qx + h \in \mathcal{H}$ to the first case as follows. Here we assume $|\mathcal{H}| = k \geqslant 2$. Observe that if $n \in (N, 2N]$ and $Qn + h = p$, a prime, then $Qn+h \equiv 0 \bmod [d_1, d_2]$ only if $[d_1, d_2] = 1$ or p. If $d_i = 1$ then $\lambda_{d_1}\lambda_{d_2} = 0$, and if $d_i = p$ then $d_i \geqslant QN + 1 > R$. That is, $P(n; \mathcal{H}) \equiv 0 \bmod [d_1, d_2]$ is equivalent to $P(n; \mathcal{H} \setminus \{Qx+h\}) \equiv 0 \bmod [d_1, d_2]$ when $\lambda_{d_1}\lambda_{d_2}, \vartheta(Qn+h) \neq 0$ and $d_1, d_2 \leqslant R$. Therefore

$$\begin{aligned}
&\sum_{N<n\leqslant 2N} \vartheta(Qn+h)\Lambda_R(n; \mathcal{H}, k+\ell)^2 \\
&\qquad = \sum_{N<n\leqslant 2N} \vartheta(Qn+h) \left(\sideset{}{'}\sum_{[d_1,d_2]|P(n;\mathcal{H})} \lambda_{d_1}\lambda_{d_2} \right) \\
&\qquad = \sum_{N<n\leqslant 2N} \vartheta(Qn+h) \left(\sideset{}{'}\sum_{[d_1,d_2]|P(n;\mathcal{H}\setminus\{Qx+h\})} \lambda_{d_1}\lambda_{d_2} \right) \\
&\qquad = \sum_{N<n\leqslant 2N} \vartheta(Qn+h)\Lambda_R(n; \mathcal{H} \setminus \{Qx+h\}, k-1+\ell+1)^2.
\end{aligned}$$

Applying the above evaluation with the translation

$$\mathcal{H} \mapsto \mathcal{H} \setminus \{Qx+h\}, \quad k \mapsto k-1, \quad \ell \mapsto \ell+1,$$

(2.4.53) becomes

$$\begin{aligned}
&\frac{1}{N} \sum_{N<n\leqslant 2N} \vartheta(Qn+h)\Lambda_R(n; \mathcal{H} \setminus \{Qx+h\}, k-1+\ell+1)^2 \\
&\qquad = (1+o(1)) \left(\frac{Q}{\phi(Q)} \right)^{k-1+1} \binom{2(\ell+1)}{\ell+1} \frac{(\log R)^{k-1+2(\ell+1)}}{(k-1+2(\ell+1))!}
\end{aligned} \tag{2.4.54}$$

as $H, R, N \to \infty$. The second case of (2.2.10) being established, the proof of Proposition (2.2.2) is complete.

2.5 Proof of Proposition 2.2.3

2.5.1 Auxiliary lemmas

To prove Proposition 2.2.3, we will use the following lemmas.

Lemma 2.5.1. *Fix integers q and a with $(q, a) = 1$. There is a constant $c(q, a) > 0$, depending only on q and a, such that*

$$\prod_{\substack{p \leqslant x \\ p \equiv a \bmod q}} \left(1 - \frac{1}{p}\right) \sim \frac{c(q, a)}{(\log x)^{1/\phi(q)}}$$

as $x \to \infty$.

Proof. This follows from the prime number theorem for arithmetic progressions. For a more precise estimate, with the constant $c(q, a)$ given explicitly, see [35, Theorem 1]. □

Lemma 2.5.2. *Let $\mathscr{S}(x)$ denote the set of positive integers which are $\leqslant x$ and composed only of primes $p \equiv 1 \bmod q$. There is a constant $c(q) > 0$, depending only on q, such that*

$$|\mathscr{S}(x)| = \left(c(q) + O\left(\frac{1}{\log x}\right)\right) \frac{x}{\log x} (\log x)^{1/\phi(q)}.$$

Proof. See [32, Lemma 3], in which the constant $c(q)$ is given explicitly. □

The next lemma concerns $\Psi(x, y)$, the number of positive integers which are $\leqslant x$ and free of prime factors $> y$ (y-smooth numbers). The ratio $\Psi(x, y)/x$ depends essentially on $u = \log x / \log y$, and for u in a certain range is approximated by $\rho(u)$, where $\rho(u)$ is the Dickman-de Bruijn ρ-function, defined as the continuous solution to

$$\rho(u) = \begin{cases} 1 & 0 \leqslant u \leqslant 1, \\ \frac{1}{u}\int_{u-1}^{u} \rho(t)\,dt & u > 1. \end{cases} \tag{2.5.1}$$

Lemma 2.5.3. *The estimate*

$$\frac{\Psi(y^u, y)}{y^u} = \rho(u)\left(1 + O\left(\frac{\log(u+2)}{\log y}\right)\right) \tag{2.5.2}$$

holds uniformly in the range

$$y \geqslant 3, \quad 1 \leqslant u \leqslant \exp\left((\log y)^{3/5-\delta}\right), \tag{2.5.3}$$

where δ is any fixed positive number. The estimate

$$\rho(u) = \exp\left(-u\log u - u\log\log u + O(u)\right) \tag{2.5.4}$$

holds for $u > 3$, and

$$\frac{\Psi(y^u, y)}{y^u} = \exp\left(-u\log u - u\log\log u + O(u)\right) \tag{2.5.5}$$

holds uniformly in the range

$$3 < u \leqslant y^{1-\delta}. \tag{2.5.6}$$

Finally, as $y \to \infty$,

$$\frac{\Psi(y, (\log y)^A)}{y} = \frac{1}{y^{1/A+o(1)}} \tag{2.5.7}$$

holds for any fixed number $A > 1$.

Proof. We refer to the survey article of Granville [23]. The asymptotic (2.5.2) was shown to hold for the range (2.5.3) by Hildebrand [27]: see [23, (1.8), (1.10)]. Hildebrand [27] also established that the less precise estimate

$$\frac{\Psi(y^u, y)}{y^u} = \rho(u) \exp\left(O_\delta\left(u \exp\left(-(\log u)^{3/5-\delta}\right)\right)\right)$$

holds, for any fixed number $\delta > 0$, in the wider range (2.5.6) (see [23, (1.11), (1.13)]). That (2.5.5) holds in the same range can be deduced from (2.5.4). (The estimate (2.5.5) is less precise, but sufficient for our purposes.) For the estimate (2.5.7), see [23, (1.14)].

The value of the Dickman-de Bruijn ρ-function is discussed in [23, 3.7 – 3.9], and (2.5.4) was proved by de Bruijn in [8]. □

Lemma 2.5.4. *Let* $\mathscr{P}$ *be a subset of the primes. As* $y \to \infty$*, the estimate*

$$\prod_{\substack{p \leqslant y \\ p \in \mathscr{P}}} \left(1 - \frac{1}{p}\right) \sum_{\substack{n > y^u \\ p \mid n \Rightarrow p \leqslant y \\ p \in \mathscr{P}}} \frac{1}{n} \leqslant (1 + o(1)) e^{-\gamma} \int_u^\infty \rho(v)\, dv. \tag{2.5.8}$$

holds uniformly for u *satisfying*

$$u \geqslant 1, \quad u = \exp\left((\log y)^{3/5-\delta}\right), \tag{2.5.9}$$

where δ *is any fixed positive number.*

Proof. Define

$$\varrho(x, y; \mathscr{P}) = \prod_{\substack{p \leqslant y \\ p \in \mathscr{P}}} \left(1 - \frac{1}{p}\right) \sum_{\substack{n \leqslant x \\ p \mid n \Rightarrow p \leqslant y \\ p \in \mathscr{P}}} \frac{1}{n}.$$

If $\ell \leqslant y$ is prime, then

$$\varrho(x,y;\mathscr{P}) = \prod_{\substack{p\leqslant y\\ p\in\mathscr{P}\cup\{\ell\}}} \left(1-\frac{1}{p}\right)\cdot\left(1-\frac{1}{\ell}\right)^{-1} \sum_{\substack{n\leqslant x\\ p\mid n\Rightarrow p\leqslant y\\ p\in\mathscr{P}}} \frac{1}{n}.$$

Now

$$\left(1-\frac{1}{\ell}\right)^{-1} \sum_{\substack{n\leqslant x\\ p\mid n\Rightarrow p\leqslant y\\ p\in\mathscr{P}}} \frac{1}{n} = \left(1+\frac{1}{\ell}+\frac{1}{\ell^2}+\cdots\right) \sum_{\substack{n\leqslant x\\ p\mid n\Rightarrow p\leqslant y\\ p\in\mathscr{P}}} \frac{1}{n} \geqslant \sum_{\substack{m\leqslant x\\ p\mid m\Rightarrow p\leqslant y\\ p\in\mathscr{P}\cup\{\ell\}}} \frac{1}{m},$$

because every m appearing in the last sum may be written as $n\ell^\alpha$ for some $\alpha \geqslant 0$ and some n appearing in the second last sum. Hence,

$$\varrho(x,y;\mathscr{P}) \geqslant \varrho(x,y;\mathscr{P}\cup\{\ell\}),$$

and applying this inequality repeatedly, we obtain

$$\varrho(x,y;\mathscr{P}) \geqslant \prod_{p\leqslant y}\left(1-\frac{1}{p}\right) \sum_{\substack{n\leqslant x\\ p\mid n\Rightarrow p\leqslant y}} \frac{1}{n}.$$

Subtracting both sides from $\varrho(\infty,y;\mathscr{P}) = 1 = \varrho(\infty,y;\{p\leqslant y\})$, we deduce that

$$\prod_{\substack{p\leqslant y\\ p\in\mathscr{P}}}\left(1-\frac{1}{p}\right) \sum_{\substack{n>x\\ p\mid n\Rightarrow p\leqslant y\\ p\in\mathscr{P}}} \frac{1}{n} \leqslant \prod_{p\leqslant y}\left(1-\frac{1}{p}\right) \sum_{\substack{n>x\\ p\mid n\Rightarrow p\leqslant y}} \frac{1}{n}. \qquad (2.5.10)$$

By partial summation,

$$\begin{aligned}\sum_{\substack{n>x\\ p\mid n\Rightarrow p\leqslant y}}\frac{1}{n}&=\int_x^\infty\frac{d\Psi(t,y)}{t}=-\frac{\Psi(x,y)}{x}+\int_x^\infty\frac{\Psi(t,y)}{t^2}\,dt\\ &\leqslant\int_x^\infty\frac{\Psi(t,y)}{t^2}\,dt.\end{aligned}\tag{2.5.11}$$

Now we assume $x=y^u$, with u satisfying (2.5.9) and y tending to infinity. We will divide the range of the last integral in (2.5.11) into three parts. First of all, fix any $\epsilon\in(0,1)$ and suppose $t\geqslant\exp(y^\epsilon)$, that is $y\leqslant(\log t)^{1/\epsilon}$. By (2.5.7) we have

$$\frac{\Psi(t,y)}{t^2}\leqslant\frac{\Psi(t,(\log t)^{1/\epsilon})}{t^2}=\frac{1}{t^{1+\epsilon+o(1)}}$$

as t, and hence as y, tends to infinity. Thus, we may suppose y is large enough so that $\Psi(t,y)/t^2\leqslant 1/t^{1+\epsilon/2}$, say, and

$$\int_{\exp(y^\epsilon)}^\infty\frac{\Psi(t,y)}{t^2}\,dt\leqslant\int_{\exp(y^\epsilon)}^\infty\frac{dt}{t^{1+\epsilon/2}}=\frac{2}{\epsilon\exp\left(\epsilon y^\epsilon/2\right)}.\tag{2.5.12}$$

For the range $x\leqslant t\leqslant\exp(y^\epsilon)$, the substitution $t=y^v$ yields

$$\int_x^{\exp(y^\epsilon)}\frac{\Psi(t,y)}{t^2}\,dt=\log y\int_u^{y^\epsilon/\log y}\frac{\Psi(y^v,y)}{y^v}\,dv.\tag{2.5.13}$$

Next, we let $u_1=2\exp\left((\log y)^{3/5-\delta}\right)$, and for $u_1\leqslant v\leqslant y^\epsilon$, we use the estimate (2.5.5):

$$\frac{\Psi(y^v,y)}{y^v}=\exp\left(-v\log v-v\log\log v+O(v)\right)\leqslant\frac{1}{v^v},$$

where the last inequality holds for all sufficiently large v, hence for all sufficiently large y. Thus

$$\int_{u_1}^{y^{\epsilon}/\log y} \frac{\Psi(y^v, y)}{y^v}\, dv \leqslant \int_{u_1}^{\infty} \frac{dv}{v^v} \ll \frac{1}{u_1^{u_1}} \tag{2.5.14}$$

for all sufficiently large y.

For $u \leqslant v \leqslant u_1$, we use the estimate (2.5.2):

$$\begin{aligned} \int_{u}^{u_1} \frac{\Psi(y^v, y)}{y^v}\, dv &= \int_{u}^{u_1} \rho(v) \left(1 + O\left(\frac{\log(v+2)}{\log y}\right)\right) dv \\ &= (1+o(1)) \int_{u}^{\infty} \rho(v)\, dv - (1+o(1)) \int_{u_1}^{\infty} \rho(v)\, dv. \end{aligned} \tag{2.5.15}$$

By (2.5.4) we have, similarly to (2.5.12), the estimate

$$\int_{u_1}^{\infty} \rho(v)\, dv \leqslant \int_{u_1}^{\infty} \frac{dv}{v^v} \ll \frac{1}{u_1^{u_1}} \tag{2.5.16}$$

for all sufficiently large y.

Combining (2.5.11) – (2.5.16), we see that

$$\int_{x}^{\infty} \frac{\Psi(t, y)}{t^2}\, dt = (1+o(1)) \log y \int_{u}^{\infty} \rho(v)\, dv + O\left(u_1^{-u_1} \log y\right) \tag{2.5.17}$$

for all sufficiently large y. Now by definition (2.5.1),

$$\int_{u}^{\infty} \rho(v)\, dv \geqslant \int_{u}^{u+1} \rho(v)\, dv = (u+1)\rho(u+1),$$

and by (2.5.4), $u_1^{-u_1} = o((u+1)\rho(u+1))$ as $u_1 \geqslant 2u$, and u_1 tends to infinity with y. Therefore, combining (2.5.17) with (2.5.11) in fact gives

$$\sum_{\substack{n > y^u \\ p \mid n \Rightarrow p \leqslant y}} \frac{1}{n} \leqslant (1+o(1)) \log y \int_{u}^{\infty} \rho(v)\, dv \tag{2.5.18}$$

as $y \to \infty$, for u in the range (2.5.9). Finally, combining (2.5.18) with (2.5.10) and applying Mertens' theorem, we obtain (2.5.8). □

2.5.2 The proof of Proposition 2.2.3

We are now ready to define Q explicitly. The construction is modelled on that of Shiu's [32]. For the rest of this section we let $q \geqslant 3$ and a be integers with $(q,a) = 1$. If $a \equiv 1 \bmod q$, let

$$\mathscr{P}(H) := \{p \leqslant \log H : p \equiv 1 \bmod q\} \cup \{p \leqslant H/(\log H)^2 : p \not\equiv 1 \bmod q\},$$

otherwise let

$$\begin{aligned}\mathscr{P}(H) := &\{p \leqslant \log H : p \equiv 1 \bmod q\} \\ &\cup \{p \leqslant H/(\log H)^2 : p \not\equiv 1, a \bmod q\} \\ &\cup \{t(H) \leqslant p \leqslant H/(\log H)^2 : p \equiv 1 \bmod q\} \\ &\cup \{p \leqslant H/t(H) : p \equiv a \bmod q\},\end{aligned}$$

with

$$t(H) := \exp\left(\frac{\log H \log\log\log H}{2\log\log H}\right),$$

and put

$$\tilde{Q}(H) := q \prod_{p \in \mathscr{P}(H)} p, \quad Q = Q(H) := q \prod_{\substack{p \in \mathscr{P}(H) \\ p \neq p_0}} p. \tag{2.5.19}$$

We check that (2.2.2) – (2.2.5) are indeed satisfied by Q: only (2.2.4) is not immediate, but it follows from the prime number theorem.

Analogously to (2.2.11), we define

$$\tilde{S}(H) := \{h \in (0, H] : (\tilde{Q}(H), h) = 1 \text{ and } h \equiv a \bmod q\},$$
$$\tilde{T}(H) := \{h \in (0, H] : (\tilde{Q}(H), h) = 1 \text{ and } h \not\equiv a \bmod q\}.$$

Proposition 2.2.3 will follow from the next lemma.

Lemma 2.5.5. *Let H be a real parameter tending to infinity, and let $\tilde{Q}(H)$ be as in* (2.5.19). *We have*

$$|\tilde{T}(H)| \ll \frac{H}{\log H}. \tag{2.5.20}$$

Moreover, there is a constant $A = A(q)$, depending on q at most, such that for all sufficiently large X, there is some H satisfying

$$\frac{X}{(\log X)^A} \leqslant H \leqslant X, \tag{2.5.21}$$

such that

$$|\tilde{S}(H)| \gg_q H \frac{\phi(\tilde{Q}(H))}{\tilde{Q}(H)}. \tag{2.5.22}$$

The implied constant in (2.5.20) *is absolute, and that in* (2.5.22) *depends on q at most.*

Proof of Proposition 2.2.3. Let $S(H)$ and $T(H)$ be as in (2.2.11). If $p_0 \neq 1$ then by (2.2.1) there are at most $H/p_0 < H/\log H$ multiples of p_0 in $T(H)$, so

$$|T(H)| \ll \frac{H}{\log H}$$

by (2.5.20). We also have $|S(H)| \geqslant |\tilde{S}(H)|$. An application of Lemma 2.5.1 reveals that, as $H \to \infty$,

$$\frac{\phi(\tilde{Q}(H))}{\tilde{Q}(H)} = \prod_{p \in \mathscr{P}(H)} \left(1 - \frac{1}{p}\right) \sim \begin{cases} \frac{e^{-\gamma}}{\log H} \left(\frac{\log H}{\log\log H}\right)^{1/\phi(q)} & \text{if } a \equiv 1 \bmod q, \\ \frac{e^{-\gamma}}{\log H} \left(\frac{\log t(H)}{\log\log H}\right)^{1/\phi(q)} & \text{if } a \not\equiv 1 \bmod q. \end{cases}$$

Therefore, in either case, combining (2.5.20) and (2.5.22) gives

$$|S(H)| - |T(H)| \gg |\tilde{S}(H)| - |\tilde{T}(H)| \gg_q H \frac{\phi(\tilde{Q}(H))}{\tilde{Q}(H)} \gg H \frac{\phi(Q(H))}{Q(H)}.$$

Proposition 2.2.3 now follows from Lemma 2.5.5. □

Proof of Lemma 2.5.5. There are $\ll H/\log H$ primes in $\tilde{T}(H)$, so let us count the composites $h \in \tilde{T}(H)$. If $h = pm$ for some prime $p > H/(\log H)^2$, with $m > 1$, then $m < (\log H)^2$ is composed only of primes $> \log H$ and $\equiv 1 \bmod q$, by the construction of $\mathscr{P}(H)$. Thus, m must be prime itself, and $p \leqslant H/\log H$. We partition $(H/(\log H)^2, H/\log H]$ into sub-intervals $I_l = (e^{l-1}H/(\log H)^2, e^l H/(\log H)^2]$, and $(\log H,\ (\log H)^2]$ into sub-intervals $J_l = (\log H, (\log H)^2/e^l]$, $1 \leqslant l \leqslant \log\log H$, and using the prime number theorem, we deduce that the contribution from elements with a prime factor $> H/(\log H)^2$ is at most

$$\sum_{1 \leqslant l \leqslant \log\log H} \sum_{\substack{p \in I_l \\ p \not\equiv 1 \bmod q}} \sum_{\substack{p' \in J_l \\ p' \equiv 1 \bmod q}} 1 \ll \sum_{1 \leqslant l \leqslant \log\log H} \frac{e^l H}{(\log H)^3} \frac{(\log H)^2}{e^l \log\log H} \ll \frac{H}{\log H}.$$

In the case $a \equiv 1 \bmod q$, then any h in $\tilde{T}(H)$ must be divisible by a prime $p \not\equiv 1 \bmod q$, and such a prime p must satisfy $p > H/(\log H)^2$ by construction of $\mathscr{P}(H)$. Therefore we have counted all of the elements of $\tilde{T}(H)$, and we have

(2.5.20).

There are other elements to count in the case $a \not\equiv 1 \bmod q$. If $h \in \tilde{T}(H)$ and $h = pm$ with $p \equiv a \bmod q$, then $p > H/t(H)$, and $m < t(H)$ must be composed only of primes $\equiv 1 \bmod q$, a contradiction as $h \not\equiv a \bmod q$. The only elements we have not counted must therefore be composed only of primes $p \equiv 1 \bmod q$ with $\log H < p < t(H)$. By (2.5.5), the number of such elements is at most

$$\Psi(H, t(H)) = H \exp\left(-u \log u - u \log\log u + O(u)\right),$$

where

$$u = \frac{\log H}{\log t(H)} = \frac{2 \log\log H}{\log\log\log H}.$$

Thus

$$u \log u + u \log\log u + O(u) \sim u \log u \sim 2 \log\log H,$$

and so

$$\Psi(H, t(H)) \ll \frac{H}{\log H}.$$

Combining these estimates, we see that (2.5.20) also holds in the case $a \not\equiv 1 \bmod q$.

Now suppose H is in the range (2.5.21). To bound the size of $\tilde{S}(H)$ from below we will first do the same for

$$S'(X) = \{h \in (0, X] : (Q'(X), h) = 1 \text{ and } h \equiv a \bmod q\},$$

where

$$Q'(X) = q \prod_{p \in \mathscr{P}'(X)} p, \quad \mathscr{P}'(X) = \mathscr{P}(X) \setminus \{p \leqslant \log X : p \equiv 1 \bmod q\}.$$

In the case $a \equiv 1 \bmod q$, $S'(X)$ contains any positive integer $m \leqslant X$ which is composed only of primes $\equiv 1 \bmod q$, that is $S'(X) \supseteq \mathscr{S}(X)$. Therefore by Lemma 2.5.2,

$$|S'(X)| \geqslant |\mathscr{S}(X)| \gg_q \frac{X}{\log X}(\log X)^{1/\phi(q)}. \tag{2.5.23}$$

In the case $a \not\equiv 1 \bmod q$, $pm \in S'(X)$ if $X/t(X) < p \equiv a \bmod q$ and $m \in \mathscr{S}(X/p)$. We partition $(X/t(X), X]$ into sub-intervals

$$I_l = (e^{l-1}X/t(X), e^l X/t(X)], \quad 1 \leqslant l \leqslant \log t(X),$$

and deduce, using the prime number theorem for arithmetic progressions and Lemma 2.5.2, that

$$\begin{aligned} |S'(X)| &\geqslant \sum_{1 \leqslant l \leqslant \log t(X)} \sum_{\substack{p \in I_l \\ p \equiv a \bmod q}} \sum_{m \in \mathscr{S}(t(X)/e^l)} 1 \\ &\gg_q \sum_{1 \leqslant l \leqslant \frac{1}{2}\log t(X)} \frac{e^l X}{t(X)\log X} \cdot \frac{t(X)}{e^l \log t(X)} (\log t(X))^{1/\phi(q)} \qquad (2.5.24) \\ &\gg \frac{X}{\log X}(\log t(X))^{1/\phi(q)}. \end{aligned}$$

In either case, we may write any $h \in S'(X)$ uniquely as $h = dm$, where d is composed only of primes $p \leqslant \log X$ with $p \equiv 1 \bmod q$, and $m \in \tilde{S}(X)$. Thus, in the case $a \equiv 1 \bmod q$, by (2.5.23) there is a constant $c_1(q) > 0$, depending on q at most, such that for all sufficiently large X,

$$\begin{aligned} c_1(q)\frac{X}{\log X}(\log X)^{1/\phi(q)} \leqslant |S'(X)| &= \sum_{\substack{d\leqslant X\\ p\mid d \Rightarrow p\leqslant \log X\\ p\equiv 1 \bmod q}} \sum_{\substack{m\leqslant X/d\\ m\in\tilde{S}(X)}} 1 \\ &\leqslant \sum_{\substack{d\leqslant X\\ p\mid d \Rightarrow p\leqslant \log X\\ p\equiv 1 \bmod q}} |\tilde{S}(X/d)|. \end{aligned} \tag{2.5.25}$$

The inequality on the right is not immediate: in fact if $Z \leqslant X$, then $\tilde{S}(X) \cap (0, Z] \subseteq \tilde{S}(Z)$. To see this, first note that as all of the functions used to define $\mathscr{P}(X)$ are monotonically increasing with X,

$$\mathscr{P}(Z) \subseteq \mathscr{P}(X) \cup \{t(Z) \leqslant p \leqslant t(X) : p \equiv 1 \bmod q\}.$$

Suppose $m \in \tilde{S}(X) \cap (0, Z]$, but $m \notin \tilde{S}(Z)$. Then $p \in \mathscr{P}(Z)$ for some $p \mid m$, but $p \notin \mathscr{P}(X)$, so $t(Z) \leqslant p \leqslant t(X)$ and $p \equiv 1 \bmod q$. Since $m \equiv a \not\equiv 1 \bmod q$, there must be some $p' \mid m$ with $p' \not\equiv 1 \bmod q$ and

$$p' \leqslant m/p \leqslant Z/t(Z) \leqslant X/t(X).$$

Then $p' \in \mathscr{P}(X)$, a contradiction.

Similarly, in the case $a \not\equiv 1 \bmod q$, by (2.5.24) there is a constant $c_1(q) > 0$, depending on q at most, such that for all sufficiently large X, we have

$$c_1(q)\frac{X}{\log X}(\log t(X))^{1/\phi(q)} \leqslant |S'(X)| \leqslant \sum_{\substack{d\leqslant X\\ p\mid d \Rightarrow p\leqslant \log X\\ p\equiv 1 \bmod q}} |\tilde{S}(X/d)|. \tag{2.5.26}$$

Suppose for a contradiction that for some constant $c_2(q) > 0$, depending on

q at most, we have the following for all H in the range (2.5.21):

$$|\tilde{S}(H)| \leqslant \frac{c_1(q)}{3c_2(q)} \frac{H}{\log X} \left(\frac{\log X}{\log\log X} \right)^{1/\phi(q)}$$

in the case $a \equiv 1 \bmod q$, and

$$|\tilde{S}(H)| \leqslant \frac{c_1(q)}{3c_2(q)} \frac{H}{\log X} \left(\frac{\log t(X)}{\log\log X} \right)^{1/\phi(q)}$$

in the case $a \not\equiv 1 \bmod q$. Then in the case $a \equiv 1 \bmod q$,

$$\begin{aligned} \sum_{\substack{d \leqslant (\log X)^A \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| &\leqslant \frac{c_1(q)}{3c_2(q)} \frac{X}{\log X} \left(\frac{\log X}{\log\log X} \right)^{1/\phi(q)} \sum_{\substack{d \leqslant (\log X)^A \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} \frac{1}{d} \\ &\leqslant \frac{c_1(q)}{3c_2(q)} \frac{X}{\log X} \left(\frac{\log X}{\log\log X} \right)^{1/\phi(q)} \prod_{\substack{p \leqslant \log X \\ p \equiv 1 \bmod q}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\leqslant \frac{c_1(q)}{3} \frac{X}{\log X} \left(\log X\right)^{1/\phi(q)}, \end{aligned} \tag{2.5.27}$$

provided X is sufficiently large, and for a suitable choice of $c_2(q)$ (given by Lemma 2.5.1). Similarly, in the case $a \not\equiv 1 \bmod q$,

$$\sum_{\substack{d \leqslant (\log X)^A \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| \leqslant \frac{c_1(q)}{3} \frac{X}{\log X} \left(\log t(X)\right)^{1/\phi(q)}. \tag{2.5.28}$$

Now, by the fundamental lemma of Brun's sieve [24, Chapter 2, Section 8], we have

$$|\tilde{S}(X/d)| \ll \frac{X}{d} \prod_{p \in \mathscr{P}(X/d)} \left(1 - \frac{1}{p}\right) \tag{2.5.29}$$

for any d. If $(\log X)^A < d \leqslant \sqrt{X}$, then $\log(X/d) \asymp \log X$, and applying Lemma 2.5.1 to the sieve upper bound (2.5.29), we see that for some constant $c_3(q) > 0$,

$$\sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| \leqslant c_3(q) \frac{X}{\log X} \left(\frac{\log X}{\log\log X} \right)^{1/\phi(q)} \sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} \frac{1}{d} \tag{2.5.30}$$

in the case $a \equiv 1 \bmod q$, and

$$\sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| \leqslant c_3(q) \frac{X}{\log X} \left(\frac{\log t(X)}{\log\log X} \right)^{1/\phi(q)} \sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} \frac{1}{d} \tag{2.5.31}$$

in the case $a \not\equiv 1 \bmod q$.

By lemmas 2.5.4 and 2.5.1 respectively, we have

$$\begin{aligned} \sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p|d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} \frac{1}{d} &\leqslant \prod_{\substack{p \leqslant \log X \\ p \equiv 1 \bmod q}} \left(1 - \frac{1}{p}\right)^{-1} (1 + o(1)) e^{-\gamma} \int_A^\infty \rho(v)\, dv \\ &\leqslant c_4(q) (\log\log X)^{1/\phi(q)} \int_A^\infty \rho(v)\, dv \end{aligned} \tag{2.5.32}$$

for some constant $c_4(q) > 0$. Now by (2.5.4),

$$\int_A^\infty \rho(v)\, dv \to 0 \quad \text{as} \quad A \to \infty,$$

so we may choose $A = A(c_1(q), c_3(q), c_4(q)) = A(q)$ so that

$$\int_A^\infty \rho(v)\,dv \leqslant \frac{c_1(q)}{4c_3(q)c_4(q)}.$$

For any such A, combining (2.5.30) (respectively (2.5.31)) with (2.5.32) yields

$$\sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p \mid d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| \leqslant \frac{c_1(q)}{4} \frac{X}{\log X} (\log X)^{1/\phi(q)} \tag{2.5.33}$$

in the case $a \equiv 1 \bmod q$, and

$$\sum_{\substack{(\log X)^A < d \leqslant \sqrt{X} \\ p \mid d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| \leqslant \frac{c_1(q)}{4} \frac{X}{\log X} (\log t(X))^{1/\phi(q)} \tag{2.5.34}$$

in the case $a \not\equiv 1 \bmod q$.

Finally, using Rankin's trick, we see that

$$\begin{aligned}
\sum_{\substack{\sqrt{X} < d \leqslant X \\ p \mid d \Rightarrow p \leqslant \log X \\ p \equiv 1 \bmod q}} |\tilde{S}(X/d)| &\leqslant \sum_{\substack{\sqrt{X} < d \leqslant X \\ p \mid d \Rightarrow p \leqslant \log X}} \frac{X}{d} \left(\frac{d}{\sqrt{X}} \right)^{1/3} \leqslant X^{5/6} \prod_{p \leqslant \log X} \left(1 - \frac{1}{p^{2/3}} \right)^{-1} \\
&\leqslant X^{5/6} \exp\left(\sum_{p \leqslant \log X} \frac{3}{p^{2/3}} \right) \leqslant X^{5/6} \exp\left(9 (\log X)^{1/3} \right) \\
&= X^{5/6 + o(1)}
\end{aligned} \tag{2.5.35}$$

by the prime number theorem.

Combining (2.5.25), (2.5.27) and (2.5.33) (respectively (2.5.26), (2.5.28) and (2.5.34)) with (2.5.35), we obtain $c_1(q) \leqslant 2c_1(q)/3$, which is absurd. We conclude that for all sufficiently large X, there is some H in the range (2.5.21) for which

$$|\tilde{S}(H)| \gg_q \frac{H}{\log X}\left(\frac{\log X}{\log\log X}\right)^{1/\phi(q)} \gg \frac{H}{\log H}\left(\frac{\log X}{\log\log H}\right)^{1/\phi(q)}.$$

in the case $a \equiv 1 \bmod q$, and

$$|\tilde{S}(H)| \gg_q \frac{H}{\log X}\left(\frac{\log t(X)}{\log\log X}\right)^{1/\phi(q)} \gg \frac{H}{\log H}\left(\frac{\log t(H)}{\log\log H}\right)^{1/\phi(q)}$$

in the case $a \not\equiv 1 \bmod q$. In either case, a final application of Lemma 2.5.1 shows that this is $\gg H\phi(\tilde{Q}(H))/\tilde{Q}(H)$. □

We remark that replacing $(\log X)^A$ by $\sqrt{X}$ in the above proof establishes the same result for some $H \in [\sqrt{X}, X]$ and all sufficiently large X, without appealing to Lemma 2.5.4. However, a sharper range for H is important when it comes to obtaining a quantitative result, as we will see in Section 2.7.

2.6 Longer strings of congruent primes

In this section we will show that for any given integers $q \geqslant 3$ and a with $(q, a) = 1$, and $\nu \geqslant 1$, there exist infinitely many strings of $\nu + 1$ consecutive primes $p_n \equiv \cdots \equiv p_\nu \equiv a \bmod q$. However, we only show that these strings satisfy $p_{n+\nu} - p_n < c(q)(\nu - 1 + \epsilon)\log p_n$, for some constant $c(q) > 0$, depending only on q.

We fix integers $\nu \geqslant 1$, $q \geqslant 3$ and a with $(q, a) = 1$, and we let H be a real parameter tending monotonically to infinity. We let $\mathscr{P}(H)$, $\tilde{Q}(H)$, $\tilde{S}(H)$ and $\tilde{T}(H)$ be as defined in Section 2.5. By Lemma 2.5.5, we have

$$|\tilde{T}(H)| \ll \frac{H}{\log H} \tag{2.6.1}$$

for all sufficiently large H. We let $c'(q)$ be the constant implied by $\gg_q$ in (2.5.22). Thus, for all sufficiently large X, there exist a constant $A = A(q)$ such that

$$|\tilde{S}(H)| \geqslant c'(q)H \prod_{p\in\mathscr{P}(H)} \left(1 - \frac{1}{p}\right) \tag{2.6.2}$$

for some H satisfying $X(\log X)^{-A} \leqslant H \leqslant X$. As noted in Section 2.5, Lemma 2.5.1 implies that

$$\prod_{p\in\mathscr{P}(H)} \left(1 - \frac{1}{p}\right) \sim \begin{cases} \frac{e^{-\gamma}}{\log H} \left(\frac{\log H}{\log\log H}\right)^{1/\phi(q)} & \text{if } a \equiv 1 \bmod q, \\ \frac{e^{-\gamma}}{\log H} \left(\frac{\log t(H)}{\log\log H}\right)^{1/\phi(q)} & \text{if } a \not\equiv 1 \bmod q, \end{cases} \tag{2.6.3}$$

as $H \to \infty$. We conclude from (2.6.1) – (2.6.3) that for all sufficiently large X, we have

$$|\tilde{S}(H)| - \nu|\tilde{T}(H)| \geqslant (1 - o(1))c'(q)H \prod_{p\in\mathscr{P}(H)} \left(1 - \frac{1}{p}\right) \tag{2.6.4}$$

for some $H \in [X(\log X)^{-A}, X]$.

We fix an $\epsilon > 0$ and define

$$N := \exp\left(\tfrac{c'(q)H}{(\nu-1+\epsilon)}\right),$$

so that

$$c'(q)H = (\nu - 1 + \epsilon)\log N. \tag{2.6.5}$$

If there is an exceptional modulus

$$q_0 := q_0(H) \leqslant \exp\left(\tfrac{c'(q)H}{(\nu-1+\epsilon)}\left(\log\left(\tfrac{c'(q)H}{(\nu-1+\epsilon)}\right)\right)^{-2}\right) = N^{1/(\log\log N)^2},$$

let $p_0 := p_0(H)$ be its greatest prime factor; otherwise let $p_0 = 1$. Just as in Section 2.2, one can show that $p_0 > \log H$ if $p_0 \neq 1$. Thus, letting $S = S(H)$ and $T = T(H)$ be as in Section 2.5, we have $|T(H)| \ll H/\log H$ and $|S(H)| \geqslant |\tilde{S}(H)|$. Therefore, by (2.6.4), for all sufficiently large X there is some $H \in [X(\log X)^{-A}, X]$ such that

$$\begin{aligned} |S(H)| - \nu|T(H)| &\geqslant |\tilde{S}(H)| - \nu|T(H)| \\ &\geqslant (1-o(1))c'(q)H \prod_{p\in\mathscr{P}(H)}\left(1-\frac{1}{p}\right) \\ &= (1-o(1))c'(q)H \prod_{p|p_0}\left(1-\frac{1}{p_0}\right) \prod_{\substack{p\in\mathscr{P}(H)\\ p\neq p_0}}\left(1-\frac{1}{p}\right) \\ &= (1-o(1))c'(q)H \prod_{\substack{p\in\mathscr{P}(H)\\ p\neq p_0}}\left(1-\frac{1}{p}\right). \end{aligned}$$

In particular, letting

$$Q = Q(H) = q \prod_{\substack{p\in\mathscr{P}(H)\\ p\neq p_0}} p$$

as in Section 2.5, so that

$$\frac{\phi(Q)}{Q} = \prod_{\substack{p\in\mathscr{P}(H)\\ p\neq p_0}}\left(1-\frac{1}{p}\right),$$

we have

$$\frac{Q}{\phi(Q)}\frac{|S|-\nu\,|T|}{\log N} \geqslant (1-o(1))(\nu-1+\epsilon) \tag{2.6.6}$$

for some $H \in [X(\log X)^{-A}, X]$ and all sufficiently large X, by (2.6.5).

Next, we fix an $\epsilon' \in (0,1/4)$ such that $\epsilon' \leqslant \epsilon/10$, and we choose integers $k \geqslant 2$ and $\ell = [\sqrt{k}]$ large enough so that

$$\frac{k}{k+2\ell+1}\frac{2(2\ell+1)}{\ell+1}\left(\frac{1}{4}-\epsilon'\right) \geqslant 1-5\epsilon' \geqslant 1-\epsilon/2. \tag{2.6.7}$$

Let $\mathcal{H} := \{Qx+h_1,\ldots,Qx+h_k\}$ be a k-tuple of distinct linear forms with $h_i \in [1,H]\cap a \bmod q$ for each i, let $R := N^{1/4-\epsilon'}$, and consider

$$\mathscr{L}_\nu :=$$
$$\frac{1}{N}\sum_{N<n\leqslant 2N}\left(\sum_{h\in S}\vartheta(Qn+h)-\nu\sum_{h\in T}\vartheta(Qn+h)-\nu\log 3QN\right)\Lambda_R(n;\mathcal{H},k+\ell)^2,$$

where $\Lambda_R(n;\mathcal{H},j)$ is as defined in (2.2.7).

We are in precisely the same situation as Proposition 2.2.2, except we have changed the definition of N in an inessential way. In fact, to prove Proposition 2.2.2 for our new N, we only have to replace each occurrence of ϵ by $(\nu-1+\epsilon)/c'(q)$ in (2.4.48) – (2.4.49). Therefore we may apply the estimates (2.2.9) and (2.2.10) to $\mathscr{L}_\nu$: we find that

$$\begin{aligned}\mathscr{L}_\nu = &\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}(\log N)\\ &\times\left\{\frac{Q}{\phi(Q)}\frac{|S|-\nu\,|T|}{\log N}+\frac{2(2\ell+1)}{\ell+1}\frac{k}{k+2\ell+1}\left(\frac{1}{4}-\epsilon'\right)-(\nu+o(1))\right\}.\end{aligned}$$

By (2.6.6) and (2.6.7), the expression $\{\cdots\}$ is $\geqslant \epsilon/2 - o(1)$, and hence

$$\mathscr{L}_\nu \gg_k \epsilon(\log N)^{k+2\ell+1}, \tag{2.6.8}$$

for some $H \in [X(\log X)^{-A}, X]$ and all sufficiently large X.

Thus $\mathscr{L}_\nu > 0$ for a sequence of values H, equivalently N, tending to infinity. Choose such an N, and for $n \in (N, 2N]$, consider

$$\begin{aligned} A_n &:= \{p \in (Qn, Qn+H] : p \equiv a \bmod q\} = \{p : p = Qn + h, h \in S\}, \\ B_n &:= \{p \in (Qn, Qn+H] : p \not\equiv a \bmod q\} = \{p : p = Qn + h, h \in T\}. \end{aligned}$$

Since $\mathscr{L}_\nu > 0$, there must be some $n \in (N, 2N]$ such that

$$\begin{aligned} |A_n| \log(Qn+H) &\geqslant \sum_{h \in S} \vartheta(Qn+h) \\ &> \nu \sum_{h \in T} \vartheta(Qn+h) + \nu \log 3QN \\ &\geqslant \nu\, |B_n| \log Qn + \nu \log 3QN. \end{aligned}$$

Now

$$|A_n| \log\left(1 + H/Qn\right) \leqslant |A_n|\, H/Qn \leqslant H^2/QN < \log(3/2)$$

if N is sufficiently large, and so

$$\log(3/2) + (|A_n| - \nu\, |B_n|) \log Qn > \nu \log 3QN$$

and hence, as $n \leqslant 2N$, $|A_n| - \nu\, |B_n| > \nu$. But as these are integers,

$$|A_n| \geqslant \nu\, |B_n| + \nu + 1,$$

and so, by the pigeonhole principle, A_n contains a string of $\nu + 1$ consecutive primes $p_r, \ldots, p_{r+\nu}$. These primes satisfy

$$p_{r+\nu} - p_r < H < \tfrac{1}{c'(q)}(\nu - 1 + \epsilon)\log QN < c(q)(\nu - 1 + \epsilon)\log p_r,$$

where $c(q) = 1/c'(q)$.

As we have not made the constant $c(q)$ explicit, we do not know whether these prime strings are contained in short intervals, that is whether

$$p_{r+\nu} - p_r < \phi(q)(\nu - 1 + \epsilon)\log p_r.$$

However, Proposition 2.2.2 is similar to a special case of Propositions 1 and 2 of [19], which are used to prove that for a given $\nu \geqslant 1$,

$$\liminf_{r\to\infty} \frac{p'_{r+\nu} - p'_r}{\phi(q)\log p'_r} \leqslant e^{-\gamma}(\sqrt{\nu} - 1)^2,$$

where $p'_1 < p'_2 < \cdots$ is sequence of all primes in the arithmetic progression $a \bmod q$, $(q, a) = 1$. It may be feasible to prove a similar result for prime strings, that is to replace $c(q)(\nu-1+\epsilon)$, above, by something like $\phi(q)(e^{-\gamma}(\sqrt{\nu}-1)^2+\epsilon)$.

2.7 The proof of Theorem 2

Let us continue with the notation and hypotheses of Section 2.5. We will first show that the estimate

$$\sum_{N<n\leqslant 2N} \Lambda(n; \mathcal{H}, k + \ell)^4 \ll N(\log N)^{19k+4\ell} \tag{2.7.1}$$

holds, with an absolute implied constant. For by (2.4.36) and (2.4.37),

$$\begin{aligned}
&\sum_{N<n\leqslant 2N} \Lambda(n;\mathcal{H},k+\ell)^4 \\
&\quad = \sum_{d_1,d_2,d_3,d_4}{}' \lambda_{d_1}\lambda_{d_2}\lambda_{d_3}\lambda_{d_4} \sum_{\substack{N<n\leqslant 2N \\ [d_1,d_2,d_3,d_4]\mid P(n;\mathcal{H})}} 1 \\
&\quad = \sum_{d_1,d_2,d_3,d_4}{}' \lambda_{d_1}\lambda_{d_2}\lambda_{d_3}\lambda_{d_4} \sum_{\substack{m \bmod [d_1,d_2,d_3,d_4] \\ \in\Omega([d_1,d_2,d_3,d_4])}} \sum_{\substack{N<n\leqslant 2N \\ n\equiv m \bmod [d_1,d_2,d_3,d_4]}} 1 \qquad (2.7.2) \\
&\quad \leqslant \sum_{\substack{d_1,d_2,d_3,d_4 \\ \text{squarefree}}} |\lambda_{d_1}\lambda_{d_2}\lambda_{d_3}\lambda_{d_4}| \sum_{\substack{m \bmod [d_1,d_2,d_3,d_4] \\ \in\Omega([d_1,d_2,d_3,d_4])}} \left(\frac{N}{[d_1,d_2,d_3,d_4]} + O(1)\right) \\
&\quad \ll N(\log R)^{4(k+\ell)} \sum_{\substack{d_1,d_2,d_3,d_4\leqslant R \\ \text{squarefree}}} \frac{|\Omega([d_1,d_2,d_3,d_4])|}{[d_1,d_2,d_3,d_4]}.
\end{aligned}$$

To see the last inequality, note that $[d_1,d_2,d_3,d_4] \leqslant R^4 = N^{1-4\epsilon'} = o(N)$, and so $N/[d_1,d_2,d_3,d_4] + O(1) \ll N/[d_1,d_2,d_3,d_4]$, and also that $\lambda_d \ll (\log R)^{k+\ell}$ by (2.4.36).

As observed in Section 2.4, $|\Omega(d)| \leqslant k^{\omega(d)}$ for squarefree d, and if D is squarefree then $\sum_{[d_1,d_2,d_3,d_4]=D} 1 = 15^{\omega(D)}$, so

$$\begin{aligned}
\sum_{\substack{d_1,d_2,d_3,d_4\leqslant R \\ \text{squarefree}}} \frac{|\Omega([d_1,d_2,d_3,d_4])|}{[d_1,d_2,d_3,d_4]} &\leqslant \sum_{D\leqslant R^4} \frac{\mu^2(D)k^{\omega(D)}}{D} \sum_{\substack{d_1,d_2,d_3,d_4 \\ [d_1,d_2,d_3,d_4]=D}} 1 \\
&= \sum_{D\leqslant R^4} \frac{\mu^2(D)(15k)^{\omega(D)}}{D} \leqslant \prod_{p\leqslant R^4}\left(1+\frac{15k}{p}\right) \\
&\ll_k (\log R^4)^{15k}.
\end{aligned} \qquad (2.7.3)$$

Since $R^4 < N$, combining (2.7.2) and (2.7.3) yields (2.7.1).

Now we choose H and $N := \exp\left(\frac{H}{\epsilon}\right)$ so that (2.3.2) holds. If we restrict the outer sum in the definition of $\mathscr{L}$ to those n for which $(Qn, Qn+H]$ contains a pair of consecutive primes $p_r \equiv p_{r+1} \equiv a \bmod q$, we remove no positive terms. Thus, if $\sum^*$ denotes this restricted sum, then

$$\begin{aligned}\mathscr{L} &\leqslant \frac{1}{N}\left(\frac{\phi(Q)}{Q}\right)^k \\ &\times \sideset{}{^*}\sum_{N<n\leqslant 2N}\left(\sum_{h\in S}\vartheta(Qn+h) - \sum_{h\in T}\vartheta(Qn+h) - \log 3QN\right)\Lambda_R(n;\mathcal{H},k+\ell)^2.\end{aligned} \tag{2.7.4}$$

For each $n \in (N, 2N]$,

$$\sum_{h\in S}\vartheta(Qn+h) - \sum_{h\in T}\vartheta(Qn+h) - \log 3QN \leqslant H\log 3QN, \tag{2.7.5}$$

and by the Cauchy-Schwartz inequality,

$$\left(\sideset{}{^*}\sum_{N<n\leqslant 2N}\Lambda_R(n;\mathcal{H},k+\ell)^2\right)^2 \leqslant \left(\sideset{}{^*}\sum_{N<n\leqslant 2N} 1\right)\left(\sum_{N<n\leqslant 2N}\Lambda_R(n;\mathcal{H},k+\ell)^4\right). \tag{2.7.6}$$

Combining (2.7.4) – (2.7.6) yields

$$\sideset{}{^*}\sum_{N<n\leqslant 2N} 1 \geqslant N^2(Q/\phi(Q))^{2k}\mathscr{L}^2(H\log 3QN)^{-2}\left(\sum_{N<n\leqslant 2N}\Lambda_R(n;\mathcal{H},k+\ell)^4\right)^{-1}.$$

Using $H = \epsilon\log N$, $\log 3QN = (1+o(1))\log N$, and $Q/\phi(Q) \geqslant 1$, then applying (2.3.2) and (2.7.1), we see that

$$\sideset{}{^*}\sum_{N<n\leqslant 2N} 1 \gg_{k,q} \frac{N}{(\log N)^{17k+2}}. \tag{2.7.7}$$

Now fix a sufficiently large number Y, and let

$$X = \epsilon \left(1 + \frac{2c\epsilon}{(\log\log Y)^2}\right)^{-1} \log Y$$

with $c > 0$ fixed. We choose some H in the range

$$X/(\log X)^A \leqslant H \leqslant X$$

so that (2.3.2), and hence (2.7.7), holds with $N = \exp(H/\epsilon)$. By (2.2.4),

$$3QN \leqslant \exp\left(\frac{H}{\epsilon} + \frac{cH}{(\log H)^2}\right) \leqslant Y,$$

because

$$\frac{H}{\epsilon} + \frac{cH}{(\log H)^2} = \frac{H}{\epsilon}\left(1 + \frac{c\epsilon}{(\log H)^2}\right) \leqslant \frac{X}{\epsilon}\left(1 + \frac{2c\epsilon}{(\log\log Y)^2}\right) = \log Y.$$

Here we have used $\log H = (1 + o(1))\log X = (1 + o(1))\log\log Y$. Also,

$$\log N = H/\epsilon \geqslant X/\epsilon(\log X)^A \geqslant \log Y/2(\log\log Y)^A.$$

Therefore, using (2.7.7) as a lower bound for the number of pairs of consecutive primes up to Y, we deduce that

$$\sum_{\substack{p_{r+1} \leqslant Y \\ p_r \equiv p_{r+1} \equiv a \bmod q \\ p_{r+1} - p_r < \epsilon \log p_r}} 1 \geqslant \sum_{\substack{p_{r+1} \leqslant 3QN \\ p_r \equiv p_{r+1} \equiv a \bmod q \\ p_{r+1} - p_r < \epsilon \log p_r}} 1 \geqslant \sideset{}{^*}\sum_{N < n \leqslant 2N} 1 \geqslant N^{1-o(1)}$$

$$\geqslant Y^{1/3(\log\log Y)^A}.$$

What we are counting here is the number of n such that $Qn + h \leqslant 3QN \leqslant Y$

and the interval $(Qn, Qn+H]$ contains a pair of consecutive primes. Since $Qn+H < Q(n+1)$, these intervals are disjoint and we do not count any prime pair twice. This completes the proof of Theorem 2.

At best, we may have $H = X$, in which case

$$\begin{aligned}\log N = \frac{H}{\epsilon} = \frac{X}{\epsilon} &= \left(1 + \frac{2c\epsilon}{(\log\log Y)^2}\right)^{-1} \log Y \\ &\geqslant \left(1 - \frac{2c\epsilon}{(\log\log Y)^2}\right) \log Y.\end{aligned}$$

Then

$$\sum_{\substack{p_{r+1} \leqslant Y \\ p_r \equiv p_{r+1} \equiv a \bmod q \\ p_{r+1} - p_r < \epsilon \log p_r}} 1 \geqslant \sum_{N<n\leqslant 2N}^{*} 1 \geqslant N^{1-o(1)} \geqslant Y^{1-c'/(\log\log Y)^2},$$

for some constant $c' > 0$.

2.8 Some remarks on the proof of Theorem 1

The so-called *singular series* for a k-tuple $\mathcal{H}$ is defined as

$$\mathfrak{S}(\mathcal{H}) := \prod_p \left(1 - \frac{|\Omega(p)|}{p}\right)\left(1 - \frac{1}{p}\right)^{-k}. \tag{2.8.1}$$

If $\mathcal{H} = \{Qx+h_1, \dots, Qx+h_k\}$ is admissible, we have $\mathfrak{S}(\mathcal{H}) = (Q/\phi(Q))^k \mathfrak{S}'(\mathcal{H})$, where $\mathfrak{S}'(\mathcal{H})$ was defined in (2.4.14). In the proof of Lemma 2.4.3, we showed that $\mathfrak{S}'(\mathcal{H}) \sim 1$, hence

$$\mathfrak{S}(\mathcal{H}) \sim \left(\frac{Q}{\phi(Q)}\right)^k$$

as $H \to \infty$, provided Q satisfies (2.2.2) and (2.2.3). We then had

$$\begin{aligned} G(0,0;\Omega) &= \mathfrak{S}(\mathcal{H}) \prod_{p \mid p_0} \left(1 - \frac{|\Omega(p)|}{p}\right)^{-1} \\ &\sim \mathfrak{S}(\mathcal{H}) \end{aligned}$$

and

$$\begin{aligned} G^+(0,0;\Omega^+) &= \left(\frac{\phi(Q)}{Q}\right) \mathfrak{S}(\mathcal{H}^+) \prod_{p \mid p_0} \left(1 - \frac{|\Omega^+(p)| - 1}{p-1}\right)^{-1} \\ &\sim \left(\frac{\phi(Q)}{Q}\right) \mathfrak{S}(\mathcal{H}^+). \end{aligned}$$

If we drop the assumption that Q satisfies (2.2.3), Proposition 2.2.2 still holds if we replace $(Q/\phi(Q))^k$ by $\mathfrak{S}(\mathcal{H})$, $(Q/\phi(Q))^{k+1}$ by $\mathfrak{S}(\mathcal{H}^+)$, and assume $\mathcal{H}$ and $\mathcal{H}^+$ are admissible. (See Proposition 3.2.2 for instance.)

Let us suppose that Q satisfies (2.2.2), (2.2.4) and (2.2.5), but not necessarily (2.2.3). As we saw in the proof of Lemma 2.5.5, the fact that Q was divisible by *all* small primes $p \leqslant \log H$ prevented us from proving that $|S| - |T| \gg_q H(\phi(Q)/Q)$ for all sufficiently large H, rather than just for some $H \in [X/(\log X)^A, X]$ and all sufficiently large X. With a view towards improving the lower bound in Theorem 2, we might consider

$$\mathscr{L} := \frac{1}{N} \sum_{N < n \leqslant 2N} \left(\sum_{h \in S} \vartheta(Qn+h) - \sum_{h \in T} \vartheta(Qn+h) - \log 3QN \right) \Lambda_R(n;\mathcal{H},k+\ell)^2.$$

We could show that if $\mathcal{H} = \{Qx+h_1, \ldots, Qx+h_k\}$ is admissible and such that

$h_i \in [1, H] \cap a \bmod q$ for each i, then

$$\begin{aligned}\mathscr{L} = \binom{2\ell}{\ell} &\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}(\log N)\\ &\times \Bigg\{ \frac{1}{\log N} \sum_{\substack{h \in S \\ Qx+h \notin \mathcal{H}}} \mathfrak{S}(\mathcal{H}^+) - \frac{1}{\log N} \sum_{h \in T} \mathfrak{S}(\mathcal{H}^+)\\ &\qquad - \frac{k}{k+2\ell+1} \frac{2(2\ell+1)}{\ell+1} \left(\frac{1}{4} - \epsilon'\right) \mathfrak{S}(\mathcal{H}) - (1+o(1)\mathfrak{S}(\mathcal{H}) \Bigg\},\end{aligned}$$

where $\mathcal{H}^+$ is short for $\mathcal{H} \cup \{Qx + h\}$ in the first two sums. This is precisely what we had in Section 2.3, except there we had $\mathfrak{S}(\mathcal{H}) \sim (Q/\phi(Q))^k$ and $\mathfrak{S}(\mathcal{H}^+) \sim (Q/\phi(Q))^{k+1}$. (Here we also have to consider h for which $\mathcal{H}^+$ is not admissible, but such h only give rise to error terms, corresponding to $G(0,0) = G^+(0,0;\Omega^+) = 0$ in Lemma 2.4.4.)

Now let $\mathscr{A}_k$ denote the set of all k-tuples of the form $\{Qx+h_1, \dots, Qx+h_k\}$, with $h_i \in [1, H] \cap a \bmod q$ for each i. We might consider

$$\begin{aligned}\sum_{\mathcal{H} \in \mathscr{A}_k} \mathscr{L} = \binom{2\ell}{\ell} &\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\\ &\times \Bigg\{ \frac{1}{\log N} \sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{\substack{h \in S \\ Qx+h \notin \mathcal{H}}} \mathfrak{S}(\mathcal{H}^+) - \frac{1}{\log N} \sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{h \in T} \mathfrak{S}(\mathcal{H}^+)\\ &\qquad - \left(\frac{k}{k+2\ell+1} \frac{2(2\ell+1)}{\ell+1} \left(\frac{1}{4} - \epsilon'\right) - (1+o(1)) \right) \sum_{\mathcal{H} \in \mathscr{A}_k} \mathfrak{S}(\mathcal{H}) \Bigg\}.\end{aligned}$$

If the expression $\{\cdots\}$ were positive for all sufficiently large H, we could deduce that for all sufficiently large N there is some $\mathcal{H}$ such that $\mathscr{L}$ is positive. However we will sketch a proof that $\{\cdots\}$ is negative for all sufficiently large H, that is $\sum_{\mathcal{H} \in \mathscr{A}_k} \mathscr{L}$ is negative for all sufficiently large N.

Now since $\mathfrak{S}(\mathcal{H}^+) = \mathfrak{S}(\mathcal{H} \cup \{Qx + h\}) = 0$ if $(Q, h) \neq 1$, we have

$$\begin{aligned}\sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{\substack{h \in S \\ Qx+h \notin \mathcal{H}}} \mathfrak{S}(\mathcal{H}^+) &= \sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{\substack{1 \leqslant h \leqslant H \\ h \equiv a \bmod q \\ Qx+h \notin \mathcal{H}}} \mathfrak{S}(\mathcal{H}^+) \\ &= \left(\frac{Q}{\phi(Q)} \right)^{k+1} \sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{\substack{1 \leqslant h \leqslant H \\ h \equiv a \bmod q \\ Qx+h \notin \mathcal{H}}} \mathfrak{S}'(\mathcal{H}^+) \\ &= \left(\frac{Q}{\phi(Q)} \right)^{k+1} (k+1) \sum_{\mathcal{H} \in \mathscr{A}_{k+1}} \mathfrak{S}'(\mathcal{H}).\end{aligned}$$

Similarly, letting $\mathscr{A}_k^{(b)}$ denote the set of all k-tuples of the form

$$\{Qx + h_1, \ldots, Qx + h_k\},$$

with $h_j \in [1, H] \cap b \bmod q$ for precisely one j, and $h_i \in [1, H] \cap a \bmod q$ for every other i, we have

$$\begin{aligned}\sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{h \in T} \mathfrak{S}(\mathcal{H}^+) &= \sum_{\mathcal{H} \in \mathscr{A}_k} \sum_{\substack{b \not\equiv a \bmod q \\ (q,b)=1}} \sum_{\substack{1 \leqslant h \leqslant H \\ h \equiv b \bmod q \\ Qx+h \notin \mathcal{H}}} \mathfrak{S}(\mathcal{H}^+) \\ &= \left(\frac{Q}{\phi(Q)} \right)^{k+1} \sum_{\substack{b \not\equiv a \bmod q \\ (q,b)=1}} \sum_{\mathcal{H} \in \mathscr{A}_{k+1}^{(b)}} \mathfrak{S}'(\mathcal{H}).\end{aligned}$$

We have now lost all information about S and T. It is possible to show that

$$\sum_{\mathcal{H} \in \mathscr{A}_{k+1}} \mathfrak{S}'(\mathcal{H}) \sim \frac{1}{(k+1)!} \left(\frac{H}{\phi(q)} \right)^{k+1},$$

and that for $(q,b)=1$, $b\not\equiv a \bmod q$,

$$\sum_{\mathcal{H}\in\mathscr{A}_{k+1}^{(b)}} \mathfrak{S}'(\mathcal{H}) \sim \frac{1}{k!}\left(\frac{H}{\phi(q)}\right)^{k+1}.$$

Combining all of this yields

$$\begin{aligned} &k!\left(\frac{\phi(q)\phi(Q)}{HQ}\right)^{k}\sum_{\mathcal{H}\in\mathscr{A}_k}\mathscr{L} \\ &= \binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}(\log N)\left\{\frac{QH}{\phi(q)\phi(Q)\log N}(1-(\phi(q)-1))\right. \\ &\quad \left. -\frac{k}{k+2\ell+1}\frac{2(2\ell+1)}{\ell+1}\left(\frac{1}{4}-\epsilon'\right)-(1+o(1)\right\}. \end{aligned}$$

This goes to show how atypical our choices for Q and $\mathcal{H}$ were in the proof of Theorem 1 (and Theorem 2).

3. PROOF OF THEOREM 3 AND THEOREM 4

3.1 The idea of the proof

The proof of Theorem 3 is much simpler than that of Theorem 1. The estimates involved are much the same; the key difference is that on the conditional hypothesis of the theorem, we are able to prove the following. There is an integer $k = k(\theta)$ such that if $\mathcal{H} = \{Qx + h_1, \ldots, Qx + h_k\}$ is admissible, and if Q satisfies certain conditions, then there are two or more primes among $Qn + h_1, \ldots, Qn + h_k$, for infinitely many n. We then choose $\mathcal{H}$ in such a way that $Qn + h_i \equiv a \bmod q$ for each i, $h_1 < \cdots < h_k$, and every integer in the interval $[Qn + h_1, Qn + h_k]$ is composite, except perhaps for the integers $Qn + h_1, \ldots, Qn + h_k$.

3.2 Preliminaries

Recall that

$$E^*(N, q) := \max_{x \leqslant N} \max_{(a,q)=1} \left| \sum_{\substack{p \leqslant x \\ p \equiv a \bmod q}} \log p - \frac{x}{\phi(q)} \right|.$$

We say that the primes have level of distribution θ if

$$\sum_{q \leqslant N^{\theta - \epsilon}} E^*(N, q) \ll_A N (\log N)^{-A} \tag{3.2.1}$$

holds for any $A > 0$ and any $\epsilon > 0$. The primes have level of distribution at least $1/2$ by the Bombieri-Vinogradov theorem (Lemma 2.4.5), and the Elliott-Halberstam conjecture (see [16]) asserts that the primes have level of distribution 1.

In the present discussion, we let N be a real parameter tending monotonically to infinity, and we set $R = N^{\theta/2-\epsilon'}$ with some $\epsilon' \in (0, \theta/2)$, where θ is the level of distribution of the primes. We let H be a real parameter satisfying $H \ll \log N$, though we do not necessarily assume H is tending to infinity: thus H may be bounded.

We let Q be a positive integer such that

$$Q \text{ is composed only of primes } p \ll \log N, \tag{3.2.2}$$

$$Q \ll (\log N)^B \text{ for some constant } B \geqslant 0. \tag{3.2.3}$$

As before, we let

$$\mathcal{H} = \{Qx + h_1, \ldots, Qx + h_k\}, \quad h_1, \ldots, h_k \in [1, H] \cap \mathbb{Z}, \tag{3.2.4}$$

denote a set of distinct linear forms, $P(n; \mathcal{H}) := (Qn + h_1) \cdots (Qn + h_k)$, and we redefine

$$\Lambda_R(n; \mathcal{H}, j) := \frac{1}{j!} \sideset{}{'}\sum_{\substack{d \mid P(n;\mathcal{H}) \\ d \leqslant R}} \mu(d)(\log R/d)^j,$$

where $\sum'$ denotes summation over indices coprime with Q. Accordingly we redefine

$$G(s_1, s_2; \Omega) := \prod_{p \nmid Q} \left(1 - \frac{|\Omega(p)|}{p} \left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right)$$
$$\times \prod_{p} \left(1 - \frac{1}{p^{s_1+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_2+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_1+s_2+1}}\right)^{k}$$

and

$$G^+(s_1, s_2; \Omega^+) := \prod_{p \nmid Q} \left(1 - \frac{|\Omega^+(p)| - 1}{p-1} \left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right)$$
$$\times \prod_{p} \left(1 - \frac{1}{p^{s_1+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_2+1}}\right)^{-k} \left(1 - \frac{1}{p^{s_1+s_2+1}}\right)^{k}.$$

(Formally, these definitions are the same as (2.2.7), (2.4.4) and (2.4.5) in the case $p_0 = 1$.)

Lemma 3.2.1. *Let C be a positive constant. Let H and R be a real parameters with R tending to infinity and $H \leqslant C \log R$, let Q be a positive integer composed only of primes $p \leqslant C \log R$, and let $\mathcal{H}$ be as in* (3.2.4)*, with k fixed. Also let $h \in [1, H] \cap \mathbb{Z}$ be such that $Qx+h \notin \mathcal{H}$. For s_1, s_2 satisfying $\operatorname{Re} s_1, \operatorname{Re} s_2 > -1/4$, we have*

$$G(s_1, s_2; \Omega),\ G^+(s_1, s_2; \Omega^+) \ll \exp\left(c(\log R)^{\delta_1+\delta_2} \log\log\log R\right), \qquad (3.2.5)$$

where c is a constant depending only on k, and

$$\delta := \max(-\operatorname{Re} s_i, 0), \quad i = 1, 2.$$

Moreover, we have

$$G(0,0;\Omega) = \mathfrak{S}(\mathcal{H}), \quad G^{+}(0,0;\Omega^{+}) = \left(\frac{\phi(Q)}{Q}\right)\mathfrak{S}(\mathcal{H}^{+}). \tag{3.2.6}$$

and for admissible $\mathcal{H}$ and $\mathcal{H}^{+}$, we have

$$\mathfrak{S}(\mathcal{H}),\, \mathfrak{S}(\mathcal{H}^{+}) \gg_{k} 1. \tag{3.2.7}$$

Proof. Recall the discussion leading up to (2.4.7), in which we showed that $|\Omega(p)| = k$ if $p \nmid Q\Delta$. The prime factors of Δ do not exceed $H \leqslant C \log R$, and the prime factors of Q do not exceed $C \log R$. Thus, analogously to (2.4.7), we have

$$p \nmid Q\Delta \quad \text{and} \quad |\Omega(p)| = k \quad \text{for all} \quad p > C \log R.$$

The proof of (3.2.5) is now identical to the proof of (2.4.8), except here we have $C \log R$ in place of H, and we do not have to deal with p_0.

Now suppose $\mathcal{H}$ is admissible. Then $|\Omega(p)| = 0$ if $p \mid Q$, as we saw in the proof of Lemma 2.4.3, hence

$$\begin{aligned} G(0,0;\Omega) &= \prod_{p \nmid Q}\left(1 - \frac{|\Omega(p)|}{p}\right)\prod_{p}\left(1 - \frac{1}{p}\right)^{-k} \\ &= \prod_{p}\left(1 - \frac{|\Omega(p)|}{p}\right)\left(1 - \frac{1}{p}\right)^{-k} \\ &= \mathfrak{S}(\mathcal{H}). \end{aligned}$$

Similarly, supposing $\mathcal{H}^+$ is admissible, we have $|\Omega^+(p)| = 0$ when $p \mid Q$, hence

$$\begin{aligned} G^+(0,0;\Omega^+) &= \prod_{p \nmid Q} \left(1 - \frac{|\Omega^+(p)| - 1}{p-1}\right) \prod_{p} \left(1 - \frac{1}{p}\right)^{-k} \\ &= \prod_{p \mid Q} \left(\frac{p-1}{p}\right) \left(1 - \frac{1}{p}\right)^{-(k+1)} \\ &\quad \times \prod_{p \nmid Q} \left(\frac{p - |\Omega^+(p)|}{p-1}\right) \left(\frac{p-1}{p}\right) \left(1 - \frac{1}{p}\right)^{-(k+1)} \\ &= \left(\frac{\phi(Q)}{Q}\right) \prod_{p \mid Q} \left(1 - \frac{1}{p}\right)^{-(k+1)} \prod_{p \nmid Q} \left(1 - \frac{|\Omega^+(p)|}{p}\right) \left(1 - \frac{1}{p}\right)^{-(k+1)} \\ &= \left(\frac{\phi(Q)}{Q}\right) \mathfrak{S}(\mathcal{H}^+). \end{aligned}$$

Next, we have

$$\begin{aligned} \mathfrak{S}(\mathcal{H}) = \prod_{p \leqslant k} &\left(1 - \frac{|\Omega(p)|}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \\ &\times \prod_{p > k} \left(1 - \frac{k}{p}\right) \left(1 + \frac{k - |\Omega(p)|}{p-k}\right) \left(1 - \frac{1}{p}\right)^{-k}. \end{aligned}$$

Now

$$\prod_{p \leqslant k} \left(1 - \frac{|\Omega(p)|}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \geqslant \prod_{p \leqslant k} \left(1 - \frac{p-1}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \gg_k 1,$$

and since $p \nmid Q\Delta$ implies $|\Omega(p)| = k$,

$$\begin{aligned} &\prod_{p > k} \left(1 - \frac{k}{p}\right) \left(1 - \frac{k - |\Omega(p)|}{p-k}\right) \left(1 - \frac{1}{p}\right)^{-k} \\ &\qquad = \prod_{p > k} \left(1 - \frac{k}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \prod_{\substack{p > k \\ p \mid Q\Delta}} \left(1 + \frac{k - |\Omega(p)|}{p-k}\right). \end{aligned}$$

The last product is $\geqslant 1$ because $|\Omega(p)| \leqslant k$ for all p as $\mathcal{H}$ is admissible. Now

$$\begin{aligned}\sum_{p>k} &\left\{\log\left(1-\frac{k}{p}\right) - k\log\left(1-\frac{1}{p}\right)\right\} \\ &= \sum_{p>k}\left\{\left(-\frac{k}{p}-\frac{k^2}{2p^2}-\cdots\right) - k\left(-\frac{1}{p}-\frac{1}{2p^2}-\cdots\right)\right\} \\ &= -k(k-1)\sum_{p>k}\left\{\frac{1}{p^2}\left(\frac{1}{2}+\frac{1+k}{3p}+\frac{1+k+k^2}{4p^2}+\cdots\right)\right\} \\ &\ll k^3\sum_{p>k}\frac{1}{p^2} \ll \frac{k^2}{\log k},\end{aligned}$$

and exponentiating this we obtain

$$\prod_{p>k}\left(1-\frac{k}{p}\right)\left(1+\frac{1}{p}\right)^{-k} \gg_k 1.$$

Combining yields (3.2.7) for $\mathfrak{S}(\mathcal{H})$ and the case for $\mathfrak{S}(\mathcal{H}^+)$ is the same. □

Proposition 3.2.2. *Suppose the primes have level of distribution θ. Let H, N and R be real parameters with $H \ll \log N$ and $R = N^{\theta/2-\epsilon'}$ for some $\epsilon' \in (0, \theta/2)$. Fix integers $k \geqslant 2$ and $\ell \geqslant 1$, let Q be a positive integer satisfying (3.2.2) and (3.2.3), and let $\mathcal{H} = \{Qx+h_1, \dots, Qx+h_k\}$ be an admissible set of distinct linear forms with $h_1, \dots, h_k \in [1, H] \cap \mathbb{Z}$. Also let $h \in [1, H] \cap \mathbb{Z}$ and suppose $\mathcal{H}^+ := \mathcal{H} \cup \{Qx+h\}$ is admissible. Then as $N \to \infty$, we have*

$$\frac{1}{N}\sum_{N<n\leqslant 2N}\Lambda_R(n;\mathcal{H},k+\ell)^2\sim\mathfrak{S}(\mathcal{H})\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!},\tag{3.2.8}$$

and

$$\begin{aligned}\frac{1}{N}&\sum_{N<n\leqslant 2N}\vartheta(Qn+h)\Lambda_R(n;\mathcal{H},k+\ell)^2\\&\sim\begin{cases}\mathfrak{S}(\mathcal{H}^+)\dbinom{2\ell}{\ell}\dfrac{(\log R)^{k+2\ell}}{(k+2\ell)!} & \textit{if } Qx+h\notin\mathcal{H},\\[2em]\mathfrak{S}(\mathcal{H})\dbinom{2(\ell+1)}{\ell+1}\dfrac{(\log R)^{k+2\ell+1}}{(k+2\ell+1)!} & \textit{if } Qx+h\in\mathcal{H}.\end{cases}\end{aligned}\tag{3.2.9}$$

Proof. The proof is *mutatis mutandis* the same as the proof of Proposition 2.2.2: we have done little more than modify our assumptions on Q, and the effect is as described in Section 2.8. We let $H, N, R, Q, \mathcal{H}$ and $\mathcal{H}^+$ be as in the statement of the proposition, with R and N sufficiently large, except we only assume $k\geqslant 1$ for now. Since $H\ll\log N\ll\log R$ and Q is composed only of primes $\ll\log N$, there is a constant C such that $H\leqslant C\log R$ and the prime factors of Q do not exceed $C\log R$. Therefore (3.2.5) and (3.2.7) hold.

We note that by (3.2.6) and (3.2.7),

$$G(0,0;\Omega)=\mathfrak{S}(\mathcal{H})\gg_k 1,\tag{3.2.10}$$

and

$$G^+(0,0;\Omega^+) = \left(\frac{\phi(Q)}{Q}\right)\mathfrak{S}(\mathcal{H}^+) \gg_k (\log\log Q)^{-1} \gg (\log\log\log R)^{-1} \tag{3.2.11}$$

by (3.2.3) and since $\log R \gg \log N$. As in the proof of Proposition 2.2.2, we have

$$\frac{1}{N}\sum_{N<n\leqslant 2N} \Lambda_R(n;\mathcal{H},k+\ell)^2 = N\mathcal{T} + O(\mathcal{E}),$$

where

$$\mathcal{E} := \sideset{}{'}\sum_{d_1,d_2} |\lambda_{d_1}\lambda_{d_2}|\cdot|\Omega([d_1,d_2])| \ll R^2(\log N)^{5k+2\ell} \ll N^{\theta-\epsilon'},$$

because $R = N^{\theta/2-\epsilon'}$, and

$$\begin{aligned}\mathcal{T} &:= \sideset{}{'}\sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2}\frac{|\Omega([d_1,d_2])|}{[d_1,d_2]} \\ &= \frac{1}{(2\pi i)^2}\int_{(1)}\int_{(1)} G(s_1,s_2;\Omega)\left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)}\right)^k \frac{R^{s_1+s_2}}{(s_1s_2)^{k+\ell+1}}\,ds_1ds_2 \\ &= \mathfrak{S}(\mathcal{H})\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\left(1+O\left((\log R)^{-1/2}(\log\log R)^c\right)\right)\end{aligned}$$

for all sufficiently large R, by Lemma 2.4.4 and (3.2.10). Hence (3.2.8).

Also as in the proof of Proposition 2.2.2, assuming $Qx+h \notin \mathcal{H}$ we have

$$\frac{1}{N}\sum_{N<n\leqslant 2N} \vartheta(Qn+h)\Lambda_R(n;\mathcal{H},k+\ell)^2 = \frac{Q\mathcal{T}^*}{\phi(Q)} + O(\mathcal{E}^*),$$

where

$$\begin{aligned}\mathcal{T}^* &:= \sum_{d_1,d_2}{}' \lambda_{d_1}\lambda_{d_2}\frac{|\Omega^*([d_1,d_2])|}{\phi([d_1,d_2])}\\ &= \frac{1}{(2\pi i)^2}\int_{(1)}\int_{(1)} G^+(s_1,s_2;\Omega^+)\left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)}\right)^k \frac{R^{s_1+s_2}}{(s_1s_2)^{k+\ell+1}}\,ds_1ds_2\\ &= \left(\frac{\phi(Q)}{Q}\right)\mathfrak{S}(\mathcal{H}^+)\binom{2\ell}{\ell}\frac{(\log R)^{k+2\ell}}{(k+2\ell)!}\left(1+O\left((\log R)^{-1/2}(\log\log R)^c\right)\right)\end{aligned}$$

for all sufficiently large R, by Lemma 2.4.4 and (3.2.11), and

$$\begin{aligned}\mathcal{E}^* &:= \sum_{d_1,d_2}{}' |\lambda_{d_1}\lambda_{d_2}|\cdot|\Omega^*([d_1,d_2])|\,E^*(3QN,Q[d_1,d_2])\\ &\ll \left(N\log N\sum_{D\leqslant R^2}\frac{\mu^2(D)(3k)^{2\omega(D)}}{D}\right)^{1/2}\left(\sum_{D\leqslant R^2}{}' E^*(3QN,QD)\right)^{1/2}\\ &\ll N^{1/2}(\log N)^{2(k+\ell)+(3k)^2/2+1/2}\left(\sum_{D\leqslant R^2}{}' E^*(3QN,QD)\right)^{1/2}.\end{aligned}$$

Now $Q\leqslant(\log N)^B$ by (3.2.3), so we may assume N is large enough so that

$$QR^2 = QN^{\theta-2\epsilon'}\leqslant(3QN)^{\theta-\epsilon'}.$$

Therefore by (3.2.1),

$$\begin{aligned}\sum_{D\leqslant R^2}{}' E^*(3QN,QD) &= \sum_{QD\leqslant QR^2}{}' E^*(3QN,QD)\\ &\leqslant \sum_{D\leqslant(3QN)^{\theta-\epsilon'}} E^*(3QN,D)\\ &\ll_{B,k,\ell} QN(\log N)^{-\left(B+4(k+\ell)+(3k)^2+4\right)}\\ &\ll N(\log N)^{-\left(4(k+\ell)+(3k)^2+4\right)}\end{aligned}$$

for all sufficiently large N. Thus we may suppose N is large enough so that $\mathcal{E}^* \ll N(\log N)^{-1}$. Combining yields (3.2.9) in the case $Qx + h \notin \mathcal{H}$, assuming $\mathcal{H}^+$ is admissible. For the case $Qx + h \notin \mathcal{H}$, we assume $k \geqslant 2$ and apply the above evaluation with the translation $\mathcal{H} \mapsto \mathcal{H} \setminus \{Qx + h\}$, $k \mapsto k - 1$, $\ell \mapsto \ell + 1$. □

To prove the last statement in Theorem 3, we will make use of the following quantitative formulation of Linnik's theorem, which gives an upper bound for the least prime in an arithmetic progression.

Lemma 3.2.3. *There is an absolute constant L such that for all sufficiently large integers q, the estimate*

$$\sum_{\substack{p \leqslant x \\ p \equiv a \bmod q}} 1 \gg \frac{x}{\phi(q) q^{1/2} \log x}$$

holds for all $x \geqslant q^L$, where a is an integer such that $(q, a) = 1$.

Proof. Let q be a sufficiently large integer and let a be an integer with $(q, a) = 1$. That there exists a constant L such that for all $x \geqslant q^L$,

$$\sum_{\substack{p \leqslant x \\ p \equiv a \bmod q}} \log p \gg \frac{x}{\phi(q)\sqrt{q}},$$

can be read directly out of [28, Corollary 18.8]. Hence

$$\sum_{\substack{p \leqslant x \\ p \equiv a \bmod q}} 1 \geqslant \sum_{\substack{p \leqslant x \\ p \equiv a \bmod q}} \frac{\log p}{\log x} \gg \frac{x}{\phi(q) q^{1/2} \log x}.$$

□

3.3 The proof of Theorem 3 and Theorem 4

Fix integers $q \geqslant 3$ and a such that $(q,a)=1$. Suppose the primes have level of distribution $\theta = 1/2+\delta$, $\delta > 0$. Fix an $\epsilon' \in (0, \delta/4)$ so that $\theta/2 - \epsilon' \geqslant (1+\delta)/4$, then fix integers $k = k(\theta)$ and $\ell = [\sqrt{k}]$ such that

$$\frac{2(2\ell+1)}{\ell+1}\frac{k}{k+2\ell+1}\left(\frac{\theta}{2}-\epsilon'\right) = 1+\epsilon, \quad \epsilon > 0. \tag{3.3.1}$$

Now let

$$\mathcal{H}' := \{x+h_{t+1}, \dots, x+h_{t+k}\},$$

where $h_1 < h_2 < \cdots$ is the sequence of all primes $\equiv a \bmod q$, $h_{t+1} > k$. Then $\mathcal{H}'$ is admissible, for clearly $|\Omega(\mathcal{H}';p)| \leqslant k \leqslant p-1$ for primes $p > k$, and for primes $p \leqslant k$ we have $0 \bmod p \notin \Omega(\mathcal{H}';p)$, hence $|\Omega(\mathcal{H}';p)| \leqslant p-1$. We assume t is large enough so that $h_{t+k} < h_{t+1}^2$, which is possible by the prime number theorem for arithmetic progressions.

Put

$$Q := q \prod_{\substack{p \leqslant h_{t+k} \\ p \neq h_{t+1},\dots,h_{t+k}}} p$$

and let

$$\mathcal{H} := \{Qx+h_{t+1}, \dots, Qx+h_{t+k}\}.$$

Let h be a integer with $h_{t+1} \leqslant h \leqslant h_{t+k}$ and suppose $Qn+h$ is prime for some positive integer n. Then $(Q,h)=1$ and so h is composed only of the primes $h_{t+1}, \dots, h_{t+k}$. But then $h = h_{t+i}$ for some $i = 1, \dots, k$, for otherwise $h \geqslant h_{t+1}^2 > h_{t+k}$. Therefore if, for some integer n, there are any primes among $Qn + h_{t+1}, \dots, Qn + h_{t+k}$, they must be the only primes in the interval $[Qn + h_{t+1}, Qn + h_{t+k}]$. If there are at least two primes among them, there is a pair of consecutive primes $p_{n+1} \equiv p_n \equiv a \bmod q$ among them, and

$$p_{n+1} - p_n \leqslant h_{t+k} - h_{t+1} := H(q, \theta) = H.$$

Now if $p \nmid Q$ then

$$\begin{aligned} |\Omega(p)| &= \left|\{-h_{t+1}Q^{-1}, \dots, -h_{t+k}Q^{-1}\} \bmod p\right| \\ &= |\{-h_{t+1}, \dots, -h_{t+k}\} \bmod p| \\ &< p \end{aligned}$$

because $\mathcal{H}'$ is admissible. If $p \mid Q$ then $p \nmid h_{t+1} \cdots h_{t+k}$, and so

$$P(n; \mathcal{H}) \equiv h_{t+1} \cdots h_{t+k} \not\equiv 0 \bmod p$$

for all $n \bmod p$, hence $|\Omega(p)| = 0$. We have just shown that $\mathcal{H}$ is admissible.

Letting $R = N^{\theta/2-\epsilon'}$ and applying Proposition 3.2.2 and (3.3.1), we obtain

$$\begin{aligned}
\mathscr{L} &:= \frac{1}{N} \sum_{N<n\leqslant 2N} \left(\sum_{i=1}^{k} \vartheta(Qn+h_i) - \log 3QN \right) \Lambda_R(n;\mathcal{H},k+\ell)^2 \\
&= \sum_{i=1}^{k} \frac{1}{N} \sum_{N<n\leqslant 2N} \vartheta(Qn+h_i)\Lambda_R(n;\mathcal{H},k+\ell)^2 \\
&\qquad\qquad - \frac{\log 3QN}{N} \sum_{N<n\leqslant 2N} \Lambda_R(n;\mathcal{H},k+\ell)^2 \\
&= k(1+o(1))\mathfrak{S}(\mathcal{H}) \binom{2(\ell+1)}{\ell+1} \frac{(\log R)^{k+2\ell+1}}{(k+2\ell+1)!} \\
&\qquad\qquad - (1+o(1))(\log N)\mathfrak{S}(\mathcal{H}) \binom{2\ell}{\ell} \frac{(\log R)^{k+2\ell}}{(k+2\ell)!} \\
&= \mathfrak{S}(\mathcal{H}) \binom{2\ell}{\ell} \frac{(\log R)^{k+2\ell}}{(k+2\ell)!} (\log N) \\
&\qquad\qquad \times \left\{ \frac{2(2\ell+1)}{\ell+1} \frac{k}{k+2\ell+1} \left(\frac{\theta}{2} - \epsilon' \right) - (1+o(1)) \right\} \\
&\gg_k \epsilon (\log N)^{k+2\ell+1}.
\end{aligned}$$

We deduce that there are at least two primes among $Qn+h_{t+1},\ldots,Qn+h_{t+k}$ for infinitely many integers n, and the first part of Theorem 3 follows.

If $\theta = \delta + 20/21$ for some $\delta > 0$, then choosing $k = 7, \ell = 1$ and $\epsilon' = \delta/4$ yields

$$\frac{2(2\ell+1)}{\ell+1} \frac{k}{k+2\ell+1} \left(\frac{\theta}{2} - \epsilon' \right) = \frac{42}{20} \left(\frac{20}{42} + \frac{\delta}{4} \right) = 1 + \epsilon, \quad \epsilon = 21\delta/40.$$

Now by Lemma 3.2.3 we may suppose that q is large enough so that the following holds for some number L. Letting $h_1 < h_2 < \cdots$ be the sequence of all primes $\equiv a \bmod q$, and M be the integer satisfying $L \leqslant M < L+1$, we have $h_{6M+2} \ll q^L$. We claim that there exist 7 primes $h_{t+1},\ldots,h_{t+7}$, $1 \leqslant t \leqslant 6M-5$, such that $h_{t+7} < h_{t+1}^2$. For otherwise

$$h_{6M+2} \geqslant h_{6(M-1)+2}^2 \geqslant h_{6(M-2)+2}^4 \geqslant \cdots \geqslant h_2^{2M},$$

and so $h_2 \leqslant h_{6M+2}^{1/2L} \ll q^{1/2}$, which, for all sufficiently large q, is absurd. It follows that $H(q,\theta) \leqslant h_{6M+2} \ll q^L$, provided that q is sufficiently large and $\theta > 20/21$. This concludes the proof of Theorem 3.

We now turn to Theorem 4. If $\sum^*$ denotes summation over n for which

$$\sum_{i=1}^{k} \vartheta(Qn + h_i) - \log 3QN$$

is positive, and hence $\{Qn + h_1, \ldots, Qn + h_k\}$ contains at least two primes, then

$$\begin{aligned} N\mathscr{L} &\leqslant \sideset{}{^*}\sum_{N<n\leqslant 2N} \left(\sum_{i=1}^{k} \vartheta(Qn + h_i) - \log 3QN \right) \Lambda_R(n; \mathcal{H}, k+\ell)^2 \\ &\leqslant k \log 3QN \sideset{}{^*}\sum_{N<n\leqslant 2N} \Lambda_R(n; \mathcal{H}, k+\ell)^2 \\ &\leqslant k \log 3QN \left(\sideset{}{^*}\sum_{N<n\leqslant 2N} 1 \right)^{1/2} \left(\sum_{N<n\leqslant 2N} \Lambda_R(n; \mathcal{H}, k+\ell)^4 \right)^{1/2} \end{aligned}$$

by the Cauchy-Schwartz inequality. Now just as in Section 2.7, we have

$$\sum_{N<n\leqslant 2N} \Lambda_R(n; \mathcal{H}, k+\ell)^4 \ll N(\log N)^{19k+4\ell}$$

(see (2.7.1)). Therefore, using this and $\mathscr{L} \gg_k (\log N)^{k+2\ell+1}$, we see that

$$\sideset{}{^*}\sum_{N<n\leqslant 2N} 1 \geqslant \frac{(N\mathscr{L})^2}{(k \log 3QN)^2} \left(\sum_{N<n\leqslant 2N} \Lambda_R(n; \mathcal{H}, k+\ell)^4 \right)^{-1} \gg_k \frac{N}{(\log N)^{17k}}.$$

The intervals $(Qn, Qn+H]$, $n \in (N, 2N]$, are disjoint, because $Q > H$. Therefore, letting $Y := 3QN > 2QN + H$, we have

$$\sum_{\substack{p_{r+1} \leqslant Y \\ p_r \equiv p_{r+1} \equiv 1 \bmod q \\ p_{r+1} - p_r \leqslant H}} 1 \geqslant \sideset{}{^*}\sum_{N < n \leqslant 2N} 1 \gg_k \frac{N}{(\log N)^{17k}} \gg \frac{Y}{Q(\log Y)^{17k}} \gg_{k,q} \frac{Y}{(\log Y)^{17k}}$$

for all sufficiently large N, and hence Y, because $Q \ll_{q,k} 1$. Since k depends on θ, Theorem 4 follows by putting $B(\theta) := 17k$.

Part II

PRODUCTS OF SHIFTED PRIMES SIMULTANEOUSLY TAKING PERFECT POWER VALUES

4. PROOF OF THEOREM 5 AND THEOREM 6

4.1 Restatement

Let us restate the theorems here. Given an integer $r \geqslant 2$ and a finite, nonempty set A of nonzero integers, recall that

$$\begin{aligned}\mathcal{B}(x; A, r) := \Big\{ & n \leqslant x : n \text{ is squarefree and} \\ & \textstyle\prod_{p \mid n}(p + a) \text{ is an } r\text{th power for all } a \in A\Big\},\end{aligned}$$

and that

$$\mathcal{B}^*(x; -1, r) = \{n \leqslant x : n \text{ is squarefree, } \omega(n) = r \text{ and } \phi(n) \text{ is an } r\text{th power}\},$$

$$\mathcal{B}^*(x; +1, r) = \{n \leqslant x : n \text{ is squarefree, } \omega(n) = r \text{ and } \sigma(n) \text{ is an } r\text{th power}\}.$$

We will prove:

Theorem 5. *Fix an integer $r \geqslant 2$, and a finite, nonempty set A of nonzero integers. As $x \to \infty$, we have*

$$|\mathcal{B}(x; A, r)| \geqslant x^{1/2|A|-o(1)}.$$

Moreover, if $|A| = 1$, then as $x \to \infty$, we have

$$|\mathcal{B}(x; A, r)| \geqslant x^{0.7039-o(1)}.$$

Here and throughout, $o(1)$ denotes a function tending to 0 as x tends to infinity. We will then prove:

Theorem 6. *Fix an integer $r \geqslant 2$. For all sufficiently large x, we have*

$$|\mathcal{B}^*(x; -1, r)|, |\mathcal{B}^*(x; +1, r)| \gg \frac{rx^{1/r}}{(\log x)^{r+2}}. \tag{4.1.1}$$

The implied constant is absolute.

The proof of Theorem 5 (Section 4.3) is an extension of the proof by Banks et. al. [4], who considered $\mathcal{B}(x; \{-1\}, 2)$, $\mathcal{B}(x; \{+1\}, 2)$, and $\mathcal{B}(x; \{-1, +1\}, 2)$. It employs some of the ideas of Erdős [12, 13] upon which Alford, Granville and Pomerance [1] based their proof that there are infinitely many Carmichael numbers. The proof of Theorem 6 (Section 4.4) introduces a new method, which, as we will explain, is an application of the ideas of Goldston, Pintz and Yıldırım [21].

4.2 Preliminaries

Theorem 5 is a consequence of the first four results of this section, and we use the fifth in the proof of Theorem 6.

An integer n is called y-smooth if $p \leqslant y$ for every prime p dividing n. Given a polynomial $F(X) \in \mathbb{Z}[X]$ and numbers $x \geqslant y \geqslant 2$, let

$$\pi_F(x, y) = \left|\{p \leqslant x : F(p) \text{ is } y\text{-smooth}\}\right| .$$

In the case $F = X - 1$, Erdős [12] proved that there exists a number $\epsilon \in (0, 1)$ such that $\pi_F(x, x^\epsilon) \gg_\epsilon \pi(x)$ (where $\pi(x)$ is the number of primes up to x), for all large x depending on the choice of ϵ. Several authors have improved upon this, the next two results being the best so far obtained.

Theorem 4.2.1. *Fix a nonzero integer a and let $F(X) = X + a$. For some absolute constant c, we have*

$$\pi_F(x, y) > \frac{x}{(\log x)^c}$$

for all sufficiently large x, provided $y \geqslant x^{0.2961}$.

Proof. See [2, Theorem 1]. □

Theorem 4.2.2. *Let F be a polynomial with integer coefficients. Let g be the largest of the degrees of F and let k be the number of distinct irreducible factors of F of degree g. Suppose that $F(0) \neq 0$ if $g = k = 1$, and let ϵ be any positive real number. Then the estimate*

$$\pi_F(x, y) \asymp \frac{x}{\log x}$$

holds for all sufficiently large x, provided $y \geqslant x^{g+\epsilon-1/2k}$.

Proof. See [9, Theorem 1.2]. □

For a finite additive abelian group G, denote by $n(G)$ the length of the longest sequence of (not necessarily distinct) elements of G, no nonempty subsequence of which sums to 0, the additive identity of G. For instance, if $G = (\mathbb{Z}/2\mathbb{Z})^m$, then $n(G) \leqslant m$, for any sequence of $m + 1$ elements of G contains a nonempty subsequence whose elements sum to $(0, \ldots, 0)$ mod 2, as can be seen by considering that such a sequence contains $2^{m+1} - 1 > 2^m = |G|$ nonempty subsequences. For any group G of order m, then any sequence of m elements contains a nonempty subsequence whose sum is 0, hence $n(G) \leqslant m-1$. The next theorem, due to van Emde Boas and Kruyswijk [11], gives a nontrivial upper bound for $n(G)$.

Theorem 4.2.3. *If G is a finite abelian group and m is the maximal order of an element in G, then $n(G) < m(1 + \log(|G| /m))$.*

Proof. See [11]. A proof is also given in [1, Theorem 1.1]. □

The following proposition shows that there may be many sequences in G whose elements sum to 0.

Proposition 4.2.4. *Let G be a finite abelian group and let $r > k > n = n(G)$ be integers. Then any subsequence of r elements of G contains at least $\binom{r}{k}/\binom{r}{n}$ distinct subsequences of length at most k and at least $k - n$, whose sum is the identity.*

Proof. See [1, Proposition 1.2]. □

We will use the well-known Siegel-Walfisz theorem in the proof of Theorem 6.

Theorem 4.2.5 (Siegel-Walfisz)**.** *For any positive number B, there is a constant C_B depending only on B, such that*

$$\sum_{\substack{p \leqslant N \\ p \equiv a \bmod q}} \log p = \frac{N}{\phi(q)} + O\left(N \exp\left(-C_B (\log N)^{1/2}\right)\right)$$

whenever $(a, q) = 1$ and $q \leqslant (\log N)^B$.

Proof. See [10, Chapter 22]. □

4.3 The proof of Theorem 5

The following proof hinges on Theorem 4.2.3 and Proposition 4.2.4, which are key ingredients in the celebrated proof of Alford, Granville and Pomerance [1] that there are infinitely many Carmichael numbers. (A Carmichael number is a composite number n for which $a^n \equiv a \bmod n$ for all integers a.) In fact it is shown in [1, Theorem 1] that the number of Carmichael numbers $C(x)$ up to x satisfies $C(x) \geqslant x^{\beta - \epsilon}$ for any $\epsilon > 0$ and all large x depending on the choice of ϵ, where

$$\beta = \frac{5}{12}\left(1 - \frac{1}{2\sqrt{e}}\right) = 0.29036\ldots.$$

Using a variant of the construction in [1], Harman [25] proved that $\beta = 0.3322408$ is admissible, and combining the ideas of [1, 4, 25], Banks [3] established the following result.

Theorem 4.3.1 ([3, Theorem 1]). *For every fixed $C < 1$, there is a number $x_0(C)$ such that for all $x \geqslant x_0(C)$ the inequality*

$$|\{n \leqslant x : n \textit{ is Carmichael and } \phi(n) \textit{ is an } r\textit{th power}\}| \geqslant x^{\beta-\epsilon}$$

holds, with $\beta = 0.3322408$ and any positive ϵ, for all positive integers $r \leqslant \exp\big((\log\log x)^C\big)$.

(Harman [26] has subsequently proved that $\beta = 0.7039 \times 0.4736 > 1/3$ is admissible here.) The method of the proof may yield further interesting results.

Theorems 4.2.1 and 4.2.2 are also crucial, and it will be manifest that extending the admissible range for y in those theorems will lead to better estimates for $|\mathcal{B}(x; A, r)|$. Explicitly, if $F(X) = \prod_{a\in A}(X + a)$ and

$$\pi_F(x, x^\epsilon) \asymp_{F,\epsilon} \frac{x}{\log x}$$

holds, then the following proof yields $|\mathcal{B}(x; A, r)| \geqslant x^{1-\epsilon-o(1)}$. It is suspected that any positive ϵ is admissible, in which case we would have

$$|\mathcal{B}(x; A, r)| = x^{1-o(1)}.$$

Proof of Theorem 5. Fix an integer $r \geqslant 2$ and a set $A = \{a_1, \ldots, a_s\}$ of nonzero integers. Let x be a large number, and let

$$y = \frac{\log x}{\log \log x}. \tag{4.3.1}$$

Let $t = \pi(y)$, and let $G = (\mathbb{Z}/r\mathbb{Z})^{st}$, so that by Theorem 4.2.5,

$$n(G) < r(1 + \log |G| / r) = r(1 + (st - 1)\log r). \tag{4.3.2}$$

Fix any number $\epsilon \in (0, 1/3s)$, and let

$$u = \begin{cases} (0.2961)^{-1} & \text{if } s = 1, \\ \left(1 + \epsilon - \frac{1}{2s}\right)^{-1} & \text{if } s \geqslant 2. \end{cases}$$

Let

$$F(X) := (X + a_1)(X + a_2) \cdots (X + a_s),$$

and let

$$\begin{aligned} S_F(y^u, y) &:= \{p \leqslant y^u : F(p) \text{ is } y\text{-smooth}\} \\ &= \{p \leqslant y^u : p + a_1, \ldots, p + a_s \text{ are } y\text{-smooth}\}. \end{aligned}$$

We may suppose x, and hence y, is large enough so that, by Theorem 4.2.1 and Theorem 4.2.2,

$$|S_F(y^u, y)| = \pi_F(y^u, y) \gg \frac{y^u}{(\log y^u)^c} \tag{4.3.3}$$

for some constant c. (We may suppose $c = 1$ in the case $s \geqslant 2$.) Finally, let

$$k = \left[\frac{\log x}{\log y^u} \right], \tag{4.3.4}$$

where $[\alpha]$ denotes the integer part of a real number α.

By (4.3.1), (4.3.3) and (4.3.4),

$$\frac{\pi_F(y^u, y)}{k} \gg \frac{(\log x)^{u-1}}{(\log\log x)^{u-1+c}},$$

and by (4.3.1), (4.3.2) and (4.3.4),

$$\frac{k}{n(G)} \gg_{r,s} \frac{\log x / \log y^u}{t} \gg \log\log x, \tag{4.3.5}$$

because $t = \pi(y) \sim y/\log y$ as $y \to \infty$, by the prime number theorem. Therefore, since $u > 1$, we may assume x is large enough so that

$$n(G) < k < \pi_F(y^u, y). \tag{4.3.6}$$

For primes $p \in S_F(y^u, y)$ and integers $a \in A$, we may write

$$p + a = 2^{\beta_1^{(a)}} 3^{\beta_2^{(a)}} \cdots p_t^{\beta_t^{(a)}},$$

where $\beta_i^{(a)}$, $1 \leqslant i \leqslant t$, are nonnegative integers. We define

$$\mathbf{v}_p = (\beta_1^{(a_1)}, \ldots, \beta_t^{(a_1)}, \beta_1^{(a_2)}, \ldots, \beta_t^{(a_2)}, \ldots, \beta_1^{(a_s)}, \ldots, \beta_t^{(a_s)})$$

as the ‘exponent vector’ for p. For a subset R of $S_F(y^u, y)$, $\prod_{p \in R}(p + a)$ is an rth power for every $a \in A$ if and only if

$$\sum_{p \in R} \mathbf{v}_p \equiv \mathbf{0} \bmod r,$$

where $\mathbf{0} \bmod r$ is the zero element of G. If, moreover, R is of size at most k, then by (4.3.4),

$$\prod_{p \in R} p \leqslant y^{uk} \leqslant x.$$

Thus

$$|\mathcal{B}(x; A, r)| \geqslant \left| \left\{ R \subseteq S_F(y^u, y) : |R| \leqslant k \text{ and } \textstyle\sum_{p \in R} \mathbf{v}_p \equiv \mathbf{0} \bmod r \right\} \right|, \quad (4.3.7)$$

as distinct subsets $R \subseteq S_F(y^u, y)$ give rise to distinct integers n, by uniqueness of factorization.

Because of (4.3.6), we may deduce from Proposition 4.2.4 that the right-hand side of (4.3.7) is at least

$$\binom{\pi_F(y^u, y)}{k} \Big/ \binom{\pi_F(y^u, y)}{n(G)} \geqslant \left(\frac{\pi_F(y^u, y)}{k} \right)^k \pi_F(y^u, y)^{-n(G)} := x^{f(x)},$$

where

$$f(x) = (k - n(G)) \frac{\log \pi_F(y^u, y)}{\log x} - \frac{k \log k}{\log x}.$$

Letting x tend to infinity and using (4.3.1), (4.3.3), (4.3.4), and (4.3.5), we see that $f(x) = 1 - 1/u - o(1)$. Therefore, as $x \to \infty$, we have

$$|\mathcal{B}(x; A, r)| \geqslant x^{1 - 1/u - o(1)},$$

and Theorem 5 follows by our choice for u, and letting ϵ tend to 0 in the case $s \geqslant 2$. □

4.4 The proof of Theorem 6

We use a different approach to prove Theorem 6. The proof is ‘inspired’ by the breakthrough results of Goldston, Pintz and Yıldırım [21] on short intervals containing primes. Basically, as we saw in Part I, their proof begins with the observation that if $W(n)$ is a nonnegative weight and

$$\sum_{N<n\leqslant 2N}\left(\sum_{h\leqslant H}\vartheta(n+h)-\log(2N+H)\right)W(n) \tag{4.4.1}$$

is positive, then for some $n\in(N,2N]$, the interval $(n,n+H]$ contains at least 2 primes. Here and in the sequel,

$$\vartheta(n):=\begin{cases}\log n & \text{if } n \text{ is prime,}\\ 0 & \text{otherwise,}\end{cases}$$

as in Part I. Goldston, Pintz and Yıldırım were able to obtain a nonnegative weight $W(n)$ (see Part I, (2.2.7)) for which (4.4.1), with $H=\epsilon\log N$, is positive for all sufficiently large N. In our problem, we will be led to consider

$$\sum_{n\leqslant N}\left(\sum_{a\leqslant H}\vartheta(a^r n+1)-(r-1)\log(H^r N+1)\right)$$

(see (4.4.3)). A lower bound for this expression corresponds to a lower bound for the number of $n\leqslant N$ for which $\{a^r n+1 : a\leqslant H\}$ contains at least r primes. As we do not require H to be ‘short’ compared to N, we may take $H=r\log N$: then the weight $W(n)=1$ works, and the problem is much easier.

Proof of Theorem 6. Throughout the proof, $r \geqslant 2$ is a fixed integer, and $n, a, a_1, a_2, \ldots$ are positive integers. Observe that if, for some n,

$$\ell_i = a_i^r n + 1, \quad i = 1, \ldots, r$$

are distinct primes, then

$$\phi(\ell_1 \cdots \ell_r) = (a_1 \cdots a_r n)^r.$$

If the primes ℓ_i are of the form $a_i^r n - 1$ then $\sigma(\ell_1 \cdots \ell_r) = (a_1 \cdots a_r n)^r$. We will prove that (4.1.1) holds for $|\mathcal{B}(x; -1, r)|$, provided x is sufficiently large, and the same proof applies to $|\mathcal{B}(x; +1, r)|$ if we consider primes of the form $a_i^r n - 1$ rather than $a_i^r n + 1$.

Let N be a parameter tending monotonically to infinity and set $H = r \log N$. Let $\mathcal{A}(N)$ be the set of $n \leqslant N$ for which

$$\mathcal{C}_n = \{a^r n + 1 : a \leqslant H\} \cap \mathcal{P}$$

(where $\mathcal{P}$ is the set of all primes) contains at least r primes. We will show that

$$|\mathcal{A}(N)| \gg \frac{N}{\log N}, \tag{4.4.2}$$

but first we will describe how this implies a lower bound for $|\mathcal{B}(x; -1, r)|$.

Every $n \in \mathcal{A}(N)$ gives rise, via $\mathcal{C}_n$, to some $\ell_1 \cdots \ell_r \in \mathcal{B}((H^r N + 1)^r; -1, r)$, though different n may give rise to the same r-tuple of primes. On the other hand, given $n \in \mathcal{A}(N)$ and a prime $p = a^r n + 1 \in \mathcal{C}_n$, each $m \in \mathcal{A}(N)$ for which $\mathcal{C}_m = \mathcal{C}_n$ corresponds to a solution to $a^r n = b^r m$, $b \leqslant H$. Therefore there can be at most H different $n \in \mathcal{A}(N)$ giving rise to the same element of $\mathcal{B}((H^r N+1)^r; -1, r)$. Consequently,

$$|\mathcal{B}((H^r N+1)^r; -1, r)| \geqslant \frac{|\mathcal{A}(N)|}{H} \gg \frac{N}{r(\log N)^2}$$

by (4.4.2), and (4.1.1) follows.

We will now establish (4.4.2). We will show that for all large N,

$$S(N) = \sum_{n \leqslant N} \left(\sum_{a \leqslant H} \vartheta(a^r n + 1) - (r-1)\log(H^r N + 1) \right) \gg rN \log N. \quad (4.4.3)$$

Consequently $\mathcal{A}(N)$ is nonempty for large N. Indeed, if (4.4.3) holds then

$$\begin{aligned} rN\log N \ll S(N) &\leqslant \sum_{n \in \mathcal{A}(N)} \left(\sum_{a \leqslant H} \vartheta(a^r n + 1) - (r-1)\log(H^r N + 1) \right) \\ &\leqslant |\mathcal{A}(N)|\, H \log(H^r N + 1), \end{aligned}$$

and (4.4.2) follows because $\log(H^r N + 1) \sim \log N$.

For the evaluation of $S(N)$, first note that

$$\sum_{n \leqslant N} \sum_{a \leqslant H} \vartheta(a^r n + 1) = \sum_{a \leqslant H} \sum_{\substack{p \leqslant a^r N + 1 \\ p \equiv 1 \bmod a^r}} \log p.$$

Since $a^r \ll_r (\log N)^r$ for $a \leqslant H$, we may apply Theorem 4.2.5 to the last sum. We have

$$\sum_{\substack{p \leqslant a^r N + 1 \\ p \equiv 1 \bmod a^r}} \log p = \frac{a^r N}{\phi(a^r)} + O\left(\frac{a^r N}{\phi(a^r)(\log N)^2} \right) \sim \frac{a}{\phi(a)} N.$$

Therefore, by the well-known estimate

$$\sum_{a\leqslant H}\frac{a}{\phi(a)}\sim cH,\quad c=\prod_p\left(1+\frac{1}{p(p-1)}\right)=1.943596\ldots,$$

we have

$$\sum_{n\leqslant N}\sum_{a\leqslant H}\vartheta(a^rn+1)\sim N\sum_{a\leqslant H}\frac{a}{\phi(a)}\sim cNH.$$

Also,

$$\sum_{n\leqslant N}(r-1)\log(H^rN+1)\sim N(r-1)\log N,$$

so combining all of this yields

$$S(N)\sim N(cH-(r-1)\log N)\gg rN\log N,$$

hence (4.4.3). □

BIBLIOGRAPHY

[1] W. R. Alford, A. Granville, and C. Pomerance, 'There are infinitely many Carmichael numbers', *Ann. of Math. (2)* **139** (1994), 703–722. MR1283874 (95k:11114)

[2] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.* **83** (1998), 331–361. MR1610553 (99b:11104)

[3] W. D. Banks, 'Carmichael numbers with a square totient', *Canad. Math. Bull.* **52** (2009), 3–8. MR2494305 (2010d:11107)

[4] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, 'Multiplicative structure of values of the Euler function', *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams* (eds A. van der Poorten and A. Stein), Fields Institute Communications **41** (American Mathematical Society, Providence, RI, 2004) 29–47. MR2075645 (2005f:11217)

[5] E. Bombieri, 'On the large sieve', *Mathematika* **12** (1965), 201–225. MR0197425 (33:5590)

[6] E. Bombieri, 'Le grand crible dans la théorie analytique des nombres', *Astérisque* **18** (1974/1987). MR891718 (88g:11064)

[7] E. Bombieri and H. Davenport, 'Small differences between prime numbers', *Proc. Roy. Soc. Ser. A* **293** (1966), 1–18. MR0199165 (33:7314)

[8] N. G. de Bruijn, 'The asymptotic behaviour of a function occurring in

the theory of primes', *J. Indian Math. Soc. (N.S.)* **15** (1951), 25–32. MR0043838 (13:326f)

[9] C. Dartyge, G. Martin, and G. Tenenbaum, 'Polynomial values free of large prime factors', *Period. Math. Hungar.* **43** (2001), 111–119. MR1830570 (2002c:11117)

[10] H. Davenport, *Multiplicative number theory*, 3rd edn (Revised and with a preface by H. L. Montgomery; Springer-Verlag, New York, 2000). MR1790423 (2001f:11001)

[11] P. van Emde Boas and D. Kruyswijk, 'A combinatorial problem on finite abelian groups III', *Afd. zuivere Wisk.* **1969-008** (Math. Centrum, Amsterdam, 1969).

[12] P. Erdős, 'On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's ϕ-function', *Quart. J. Math. (Oxford Ser.)* **6** (1935), 205–213.

[13] P. Erdős, 'On pseudoprimes and Carmichael numbers', *Publ. Math. Debrecen* **4** (1956), 201–206. MR0079031 (18:18e)

[14] T. Freiberg, 'Products of shifted primes simultaneously taking perfect power values', Preprint, 2010, `http://arxiv.org/abs/1008.1978`.

[15] T. Freiberg, 'Strings of congruent primes in short intervals', Preprint, 2010, `http://arxiv.org/abs/1005.4703`.

[16] J. Friedlander and A. Granville, 'Limitations to the equi-distribution of primes I', *Ann. of Math. (2)* **129** (1989), 363–382. MR986796 (90e:11125)

[17] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, 'Primes in tuples I', Preprint, 2005, `http://arxiv.org/abs/math/0508185v1`.

[18] D. A. Goldston, Y. Motohashi, J. Pintz, and C. Y. Yıldırım, 'Small gaps between primes exist', *Proc. Japan Acad. Ser. A Math. Sci.* **82** (2006), 61–65. MR2222213 (2007a:11135)

[19] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, 'Primes in tuples III. On the difference $p_{n+\nu} - p_n$', *Funct. Approx. Comment. Math.* **35** (2006), 79–89. MR2271608 (2008f:11102)

[20] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, 'The path to recent progress on small gaps between primes', *Clay Math. Proc.* **7** (2007), 129–139. MR2362197 (2008j:11122)

[21] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, 'Primes in tuples I', *Ann. of Math. (2)* **170** (2009), 819–862. MR2552109

[22] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, 'Primes in tuples II', *Acta Math.* **204** (2010), 1–47. MR2600432

[23] A. Granville, 'Smooth numbers: computational number theory and beyond', *Algorithmic number theory: lattices, number fields, curves and cryptography* (eds J. P. Buhler and P. Stevenhagen), Mathematical Sciences Research Institute Publications **44** (Cambridge University Press, Cambridge, 2008) 267–323. MR2467549

[24] H. Halberstam and H. E. Richert, *Sieve methods*, London Mathematical Society Monographs **4** (Academic Press, London-New York, 1974). MR0424730 (54:12689)

[25] G. Harman, 'On the number of Carmichael numbers up to x', *Bull. London Math. Soc.* **37** (2005), 641–650. MR2164825 (2006d:11106)

[26] G. Harman, 'Watt's mean value theorem and Carmichael numbers', *Int. J. Number Theory* **4** (2008), 241–248. MR2404800 (2009f:11118)

[27] A. Hildebrand, 'On the number of positive integers $\leqslant x$ and free of prime factors $> y$', *J. Number Theory* **22** (1986), 289–307. MR831874 (87d:11066)

[28] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53** (American Mathematical Society, Providence, RI, 2004). MR2061214 (2005h:11005)

[29] H. Kadiri, 'Une région explicite sans zéros pour la fonction ζ de Riemann', *Acta Arith.* **117** (2005), 303–339. MR2140161 (2005m:11159)

[30] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory: I. Classical theory* (Cambridge University Press, Cambridge, 2007). MR2378655 (2009b:11001)

[31] J. Pintz, 'Landau's problems on primes', *J. Théor. Nombres Bordeaux* **21** (2009), 357–404. MR2541431 (2010i:11156)

[32] D. K. L. Shiu, 'Strings of congruent primes', *J. London Math. Soc. (2)* **61** (2000), 359–373. MR1760689 (2001f:11155)

[33] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46** (Cambridge University Press, Cambridge, 1995). MR1342300 (97e:11005b)

[34] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, 2nd edn (With a preface by D. R. Heath-Brown; The Clarendon Press Oxford University Press, New York, 1986). MR882550 (88c:11049)

[35] K. S. Williams, 'Mertens' theorem for arithmetic progressions', *J. Number Theory* **6** (1974), 353–359. MR0364137 (51:392)