Distribution of integers with prescribed arithmetic structure and applications

Kam Hung Yau

A THESIS IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF PURE MATHEMATICS
FACULTY OF SCIENCE
UNSW SYDNEY

June 2020

Thesis/Dissertation Sheet

Surname/Family Name	:	Yau
Given Name/s	:	Kam Hung
Abbreviation for degree as give in the University calendar	:	PhD
Faculty	:	Faculty of Science
School	:	School of Mathematics and Statistics
Thesis Title	:	Distribution of integers with prescribed arithmetic structure and applications

Abstract 350 words maximum: (PLEASE TYPE)

This thesis contains results about the distribution of integers with prescribed arithmetic structure and an application. These include a counting problem in Diophantine approximation, an asymptotic formula for the number of solutions to congruence's with certain arithmetic conditions, lower bounds on the number of smooth square-free integers in arithmetic progression, an estimate on the smallest square-full number in almost all residue classes modulo a prime, a relaxation of Goldbach's conjecture from the point of view of Ramaré's local model, and lastly a refinement of the classical Burgess bound.

ORIGINALITY STATEMENT

‘I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.’

Signed …….....

Date 12/06/2020…….....

INCLUSION OF PUBLICATIONS STATEMENT

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in their thesis in lieu of a Chapter if:

- The candidate contributed greater than 50% of the content in the publication and is the "primary author", ie. the candidate was responsible primarily for the planning, execution and preparation of the work for publication
- The candidate has approval to include the publication in their thesis in lieu of a Chapter from their supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis

Please indicate whether this thesis contains published material or not:

☐ This thesis contains no publications, either published or submitted for publication
(if this box is checked, you may delete all the material on page 2)

☒ Some of the work described in this thesis has been published and it has been documented in the relevant Chapters with acknowledgement
(if this box is checked, you may delete all the material on page 2)

☐ This thesis has publications (either published or submitted for publication) incorporated into it in lieu of a chapter and the details are presented below

CANDIDATE'S DECLARATION

I declare that:

- I have complied with the UNSW Thesis Examination Procedure
- where I have used a publication in lieu of a Chapter, the listed publication(s) below meet(s) the requirements to be included in the thesis.

Candidate's Name	Signature	Date (dd/mm/yy)
Kam Hung Yau		12/06/2020

COPYRIGHT STATEMENT

Signed …….....

Date: 12/06/2020…….....

AUTHENTICITY STATEMENT

‘I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis.’

Signed: …….....

Date: 12/06/2020…….....

Acknowledgements

"What do you call a unihorn with a corn for a horn?"

–Unknown

Let me have a look, there are many people I would like to express my gratitude. Firstly I thank my family for all their support and dangerously good times.

I am indebted to Prof. Steven Galbraith for starting me on this analytic journey of numbers. I am also very grateful to my sensational supervisors Prof. Igor E. Shparlinski, and Dr. Liangyi (Lee) Zhao for their constant encouragement, advice, and exceptional feedback on my research conducted during my PhD candidature. I have learnt a great deal of analytic number theory, so thank you both!

I am also thankful to Prof. John Friedlander, Dr. Bryce Kerr, Prof. Olivier Ramaré, and Prof. Ilya Shkredov for very useful discussions on some of the research contained in this thesis. In particular to Prof. Valentin Blomer for providing the idea of the argument in Appendix 4.5. Thanks must also be given to the anonymous referees for their extremely constructive comments on the submitted articles, all of which are incorporated into this thesis. I am thankful to my collaborators, it has been an absolutely pleasurable experience and I hope there is more to come.

Praise goes to Prof. Igor Klep, and Dr. Timothy Trudgian for their constant encouragement, before, during, and after my PhD studies.

I would like to acknowledge the Australian Government for the financial support provided through by the Research Training Program (RTP) Scholarship, the School of Mathematics and Statistics for a top-up scholarship and sublime working/drinking conditions, UNSW Sydney for the Postgraduate Research Student Support (PRSS) Scheme, the Australian Mathematical Society for financial support to attend the 2019 annual meeting, Prof. Igor E. Shparlinski and Dr. Liangyi (Lee) Zhao for providing me funding to attend various domestic and international conferences, the UNSW Sydney library for constructing a fresh number theory section of over fifty books solely for my research.

Thanks to the many people in the department who has made my stay in Sydney very enjoyable. In particular to Fadi Antown, Changhao Chen, Harry Crimmins, Billy Dingo, Timothy J. Evans, Bryce Kerr, Sean Lynch, Simon Macourt, Jorge Mello, Jeremy Nugent, Bob Pepper, Thomas Scheckter, and Susannah Waters.

Have a look at the thesis, I hope you find some interesting results ☺☺☺.

Sydney, June 2020
Kam Hung Yau

Abstract

This thesis contains results about the distribution of integers with prescribed arithmetic structure and an application. These include a counting problem in Diophantine approximation, an asymptotic formula for the number of solutions to congruence's with certain arithmetic conditions, lower bounds on the number of smooth square-free integers in arithmetic progression, an estimate on the smallest square-full number in almost all residue classes modulo a prime, a relaxation of Goldbach's conjecture from the point of view of Ramaré's local model, and lastly a refinement of the classical Burgess bound.

Summary of Thesis

"Isn't a three legged duck just a tripod!?"

–Topologist

In this thesis, we are concerned with the distribution of integers with prescribed arithmetic structure. We also include an application to bounds of character sums in Chapter 6.

In Chapter 1, we consider a problem in Diophantine approximation. Let $\|\cdot\|$ be the distance to the nearest integer function. For any $\varepsilon > 0$, we acquire an asymptotic formula for the number of solutions $n \leq x$ to

$$\|\alpha n + \beta\| < x^{-1/4+\varepsilon},$$

where n is $[y, z]$-smooth (numbers whose prime factors lie in the interval $[y, z] \subseteq [1, x]$) for infinitely many real numbers x. In addition, we also establish an asymptotic formula with an extra square-free condition on n. Moreover, if α is quadratic irrational then the asymptotic formulas hold for all sufficiently large x.

Our tools come from the Harman sieve [51] which we adapt suitably to sieve for $[y, z]$-smooth numbers. The arithmetic information comes from estimates for exponential sums. The results in Chapter 1 has been published in Acta Arithmetica, see [100].

In Chapter 2, we consider a variant of a conjecture (EOSC) due to Erdös, Odlyzko, and Sárközy [29], which states that for all sufficiently large q, every reduced residue class modulo q can be written as a product of two primes, each no more than q. We establish estimates for the number of ways to represent any reduced residue class as a product of a prime and an integer free of small prime factors. That is, for $(a, q) = 1$ and positive real number z, we count the number of pairs (p, u) such that

$$pu \equiv a \pmod{q},$$

where prime $p \leq x$, $u \leq y$, and the smallest prime factor of u is no less than z. The best results we obtain is conditional on the Generalised Riemann Hypothesis (GRH). Our proof technique uses the Harman sieve [51] together with the arithmetic information supplied by bounds for multiplicative character sums.

In Chapter 3, we consider yet another variant of EOSC. We obtain an asymptotic formula for the number of ways to represent every reduced residue class as a product of a

prime and square-free integer. Specifically, for $(a, q) = 1$, we count the number of pairs (p, s) such that

$$ps \equiv a \pmod{q},$$

where prime $p \leq P$, square-free $s \leq S$. The main tool is a bound of Kloostermann sum over primes provided by Fouvry & Shparlinski [33]. This work has been accepted by the New Zealand Journal of Mathematics.

In Chapter 4, we derive new lower bounds on the number of smooth square-free integers up to x in residue classes modulo a prime p, relatively large compared to x, which in some ranges of p and x improve that of Balog & Pomerance [7]. We also obtain an estimate on the smallest square-full integer in almost all residue classes modulo a prime p. This is joint work with M. Munsch & I. E. Shparlinski, and has been published in Mathematika, see [77].

In Chapter 5, we consider a relaxation of the binary Goldbach conjecture, which states that all even integer greater than two can be written as the sum of two primes. Uniformly for small q and $(a, q) = 1$, we obtain an estimate for the weighted number of ways a sufficiently large integer N can be represented as the sum of a prime congruent to a modulo q and a square-free integer. That is, we obtain an estimate for the quantity

$$\mathcal{R}_{a,q}(N) := \sum_{\substack{N=p+n \\ p \equiv a \pmod{q}}} \mu^2(n) \log p.$$

Here μ is the Möbius function. Our method is based on the notion of local model developed by Ramaré [81], and may be viewed as an abstract circle method.

In Chapter 6, we provide a refinement of the classical Burgess bound for multiplicative character sums modulo a prime number q. This continues a series of previous logarithmic improvements, which are mostly due to Iwaniec & Kowalski [59]. In particular, for any non-trivial multiplicative character χ modulo a prime q and any integer $r \geq 2$, we show that

$$\sum_{M < n \leq M+N} \chi(n) = O\left(N^{1-1/r} q^{(r+1)/4r^2} (\log q)^{1/4r}\right),$$

which sharpens previous results by a factor $(\log q)^{1/4r}$. Our improvement comes from averaging over numbers with no small prime factors rather than an interval as in previous approaches. This is joint work with B. Kerr & I. E. Shparlinski and has been published in the Michigan Journal of Mathematics, see [63]. Finally, we remark that de la Bretèche & Munsch [21], and de la Bretèche, Munsch & Tenenbaum [22] has improved our result building on this idea.

Notation

Let f and g be complex valued functions. We use the notation $f = O(g)$ and $f \ll g$ to mean there exists an absolute constant $C > 0$ such that $|f(x)| \leq C|g(x)|$ for all x. If the constant C depends on a parameter, say A, then we may write $f \ll_A g$ and $f = O_A(g)$. Specialised notation will be introduced later in the relevant chapters but first we recall the following standard notation in analytic number theory:

$\mathbb{N}$: the set of positive integers {1,2,3, ...}.

$\sum_{m \sim M}$: means $\sum_{m \in [M,2M) \cap \mathbb{N}}$.

$f = o(g)$: means $\lim_{x \to \infty} f(x)/g(x) = 0$.

$f \sim g$: means $\lim_{x \to \infty} f(x)/g(x) = 1$.

$f \asymp g$: means both $f \ll g$ and $g \ll f$.

$a \mid b$: a divides b.

$a \nmid b$: a does not divide b.

p : with or without subscript is exclusively a prime number.

$p^\alpha \parallel n$: means both $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$.

$(a_1, \ldots, a_n)$: the greatest common divisor of $a_1, \ldots, a_n$.

$[b_1, \ldots, b_n]$: the lowest common multiple of $b_1, \ldots, b_n$.

$\tau(n)$: the number of positive divisors of n.

$\sigma(n)$: the sum of all positive divisors of n.

$\varphi(n)$: the number of integers in the interval $[1, n]$ coprime to n.

μ : the Möbius function $\mu : \mathbb{N} \to \mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has a repeated prime factor,} \\ 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct prime factors.} \end{cases}$$

Λ : the von-Mangoldt function $\Lambda : \mathbb{N} \to \mathbb{N}$ defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

$\mathbf{e}_k(t)$: is $\exp(2\pi i t/k)$ for any non-zero real number k, and $\mathbf{e}(t) = \mathbf{e}_1(t)$.

Contents

CHAPTER 1

Distribution of $\alpha n + \beta$ Modulo 1 over Integers Free from Large and Small Primes

"Stop the bus, I will get off here."

–Bob

Certain arithmetic problems in number theory can be translated into problems in Diophantine approximation. For instance, the polynomial $n^2 + 1$ captures infinitely many primes is equivalent to the statement there exists infinitely many primes p such that

$$\{\sqrt{p}\} < \frac{1}{\sqrt{p}}. \tag{1.0.1}$$

Here $\{n\}$ is the fractional part of n. Indeed if $p = n^2 + 1$ then

$$\begin{aligned} \{\sqrt{p}\} &\leq \sqrt{n^2+1} - n \\ &= \frac{1}{\sqrt{n^2+1} + n} \\ &< \frac{1}{\sqrt{p}}. \end{aligned}$$

Conversely if (1.0.1) holds then

$$\begin{aligned} (\lfloor\sqrt{p}\rfloor)^2 \leq p &= (\lfloor\sqrt{p}\rfloor + \{\sqrt{p}\})^2 \\ &= (\lfloor\sqrt{p}\rfloor)^2 + \{\sqrt{p}\}(\sqrt{p} + \lfloor\sqrt{p}\rfloor) \\ &< (\lfloor\sqrt{p}\rfloor)^2 + 2, \end{aligned}$$

and therefore $p = (\lfloor\sqrt{p}\rfloor)^2 + 1$.

A classical theorem of Dirichlet [47, Theorem 185] states that if α is irrational then there exists infinitely many pairs of integers (m, n) satisfying the inequality

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}. \tag{1.0.2}$$

Such problems fall in the area of Diophantine approximation. Equivalently by defining

$$\|x\| = \min_{v \in \mathbb{Z}} |x - v|$$

to be the distance from x to the nearest integer, (1.0.2) implies

$$\|\alpha n\| < \frac{1}{n}$$

for infinitely many positive integers n. We remark that we can also write

$$\|x\| = \min\left(\{x\}, 1 - \{x\}\right).$$

A natural extension to this problem is to consider if there exist infinitely many solutions to

$$\|\alpha n + \beta\| < \frac{1}{n^{\kappa}}. \tag{1.0.3}$$

Here $\beta \in \mathbb{R}$, $\kappa > 0$, $n \in \mathcal{N} \subseteq \mathbb{N}$, where $\mathcal{N}$ is some set of arithmetic interest.

Various results have been obtained when $\mathcal{N}$ is the set of prime numbers. These include the results of Harman [48,50], Heath-Brown & Jia [56] and Jia [60], which involve sieve methods and bounds of exponential sums, while Vaughan [93] obtained his result by applying what is now known as the *Vaughan identity* [94], together with bounds for exponential sums.

We remark that Harman's sieve method first appeared when Harman [48] studied this exact problem to get the exponent $\kappa = 3/10$. For more details on the Harman sieve, see the monograph [51]. The best result to date is by Matomäki [70] with $\kappa < 1/3$ under the condition $\beta = 0$ and employs Harman's sieve method where the arithmetic information comes from bounds for averages of Kloosterman sums.

Let $k > 1$ be a fixed positive integer and $\mathcal{N}$ the set of k-th powers of primes. Baker & Harman [5] showed that we can take $\kappa < 3/20$ if $k = 2$ and $\kappa < (3 \cdot 2^{k-1})^{-1}$ if $k \geq 3$, where this time the exponent is in the prime p. In particular, when $k = 2$ this improves a result of Ghosh [41]. Later, Wong [99] provided an improvement of Baker & Harman [5] in the range $3 \leq k \leq 12$.

When $\mathcal{N}$ is the set of square-free numbers, the best result is due to Heath-Brown [53] with $\kappa < 2/3$ using essentially an elementary method. The result improves the previous work by Harman [49] and Balog & Perelli [6], who independently showed we can essentially take the exponent $\kappa < 1/2$.

In this chapter, we consider the problem of establishing an asymptotic formula for the number of $[y, z]$-smooth $n \leq x$ solutions to (1.0.3) (numbers with prime factors in the interval $[y, z] \subseteq [1, x]$) with $\kappa = 1/4 - \varepsilon$, where $\varepsilon > 0$. We also consider a hybrid problem that interpolates between square-free and $[y, z]$-smooth integers.

We note that in the special case of smooth numbers we are able to obtain a non-trivial lower bound immediately. Indeed, for any fixed $\varepsilon > 0$, consider the set

$$\left\{n = ab \leq x \ : \ x^{1/3} \leq a < 2x^{1/3}, p \mid n \Rightarrow p < x^{\varepsilon}\right\}.$$

By applying Lemma 1.2.1 and our Type II information (Lemma 1.2.4 with (1.2.3)), we can show immediately that for infinitely many x chosen correctly there are at least $x^{2/3+\varepsilon-o(1)}$ integers up to x which are x^{ε}-smooth and satisfies

$$\|\alpha n+\beta\|<x^{-1/3+\varepsilon}.$$

The statement remains valid if we additionally require n to be square-free.

1.1 Main results

For any real numbers $0<y\leq z\leq x$, we denote by

$$S(x;y,z)=\{a\in[1,x]\cap\mathbb{N}\ :\ p\mid a\Rightarrow p\in[y,z]\}$$

the set of all integers in $[1,x]$ whose prime factors lie in $[y,z]$. Moreover, we denote the cardinality of $S(x;y,z)$ by $\Psi(x;y,z)$.

For any positive integer A, we write

$$\mathcal{I}(A)=\{\alpha\in\mathbb{R}\backslash\mathbb{Q}\ :\ \alpha=[a_0;a_1,\ldots],|a_j|\leq A,j\geq 0\}.$$

We note that $\bigcup_{A\in\mathbb{N}}\mathcal{I}(A)$ contains the set of all quadratic irrationals. The following two results are published in Acta Arithmetica, see [100]. We state our first result.

Theorem 1.1.1. *There exists an increasing sequence $(x_k)_{k\in\mathbb{N}}$ of positive integers such that if $2\leq y<x_k^{1/2}$, $y<z\leq x_k$, $\varepsilon>0$ and $\delta=x_k^{-1/4+\varepsilon}$, then*

$$\sum_{\substack{n\in S(x_k;y,z)\\ \|\alpha n+\beta\|<\delta}}1=2\delta\Psi(x_k;y,z)+O\left(x_k^{3/4+\varepsilon/2+o(1)}\right). \tag{1.1.1}$$

Moreover, (1.1.1) holds for the sequence $(x_k)_{k\in\mathbb{N}}=(k)_{k\in\mathbb{N}}$ uniformly for all $\alpha\in\mathcal{I}(A)$ and any fixed positive integer A.

For any real numbers $0<y\leq z\leq x$, we denote by

$$S^*(x;y,z)=\left\{a\in[1,x]\cap\mathbb{N}\ :\ \mu^2(a)=1,p\mid a\Rightarrow p\in[y,z]\right\}$$

the set of all square-free integers in $[1,x]$ whose prime factors lie in $[y,z]$. We also denote the cardinality of $S^*(x;y,z)$ by $\Psi^*(x;y,z)$. The next theorem is essentially Theorem 1.1.1, where we also require the integers we are counting to be square-free.

Theorem 1.1.2. *There exists an increasing sequence $(x_k)_{k\in\mathbb{N}}$ of positive integers such that if $2\leq y<x_k^{1/2}$, $y<z\leq x_k$, $\varepsilon>0$ and $\delta=x_k^{-1/4+\varepsilon}$, then we have*

$$\sum_{\substack{n\in S^*(x_k;y,z)\\ \|\alpha n+\beta\|<\delta}}1=2\delta\Psi^*(x_k;y,z)+O\left(x_k^{3/4+\varepsilon/2+o(1)}\right). \tag{1.1.2}$$

Moreover, (1.1.2) *holds for the sequence* $(x_k)_{k\in\mathbb{N}} = (k)_{k\in\mathbb{N}}$ *uniformly for all* $\alpha \in \mathcal{I}(A)$ *and any fixed positive integer* A.

If we fix $0 < u_2 < u_1$ with $2 < u_1,\ u_2 < \lfloor u_1 \rfloor$ and set $y = x_k^{1/u_1}$ and $z = x_k^{1/u_2}$ then both $\Psi(x_k; y, z)$, $\Psi^*(x_k; y, z)$ in the main term of (1.1.1) and (1.1.2) respectively are bounded below by the number of integers $n = p_1 \dots p_j$ that are products of $j = \lfloor u_1 \rfloor$ distinct primes with $p_i \in [y, z]$. This gives the lower bound

$$x_k^{1-o(1)} < \Psi(x_k; y, z), \Psi^*(x_k; y, z).$$

It follows that our Theorem 1.1.1 and 1.1.2 are non-trivial in this region.

We note that by [34, Theorem 1] of Friedlander, we can obtain an asymptotic formula for $\Psi(x; y, z)$ in certain regions. We also mention that Saias [83–85] has extensively studied this quantity. In particular, our $\Psi(x_k; y, z)$ is $\theta(x_k, z, y)$ or $\Theta(x_k, z, y)$ in the notation of Friedlander [34] and Saias [83–85] respectively.

We remark that we assume $y < x_k^{1/2}$ in Theorem 1.1.1 and 1.1.2 since if $y \geq x_k^{1/2}$ and $z \geq x_k$ then both $S(x_k; y, z)$ and $S^*(x_k; y, z)$ essentially count primes in the interval $[y, x_k]$, and the result of Harman [51, Theorem 3.2] covers this case with $\delta = x_k^{-1/4+\varepsilon}$.

It is easy to see that the proof of Theorem 1.1.1 can be adjusted to prove Theorem 1.1.2, so we will only give full details for the proof of Theorem 1.1.1.

1.2 Preparations

For any $\delta > 0$, we define

$$\chi(r) = \begin{cases} 1 & \text{if } \|r\| < \delta, \\ 0 & \text{otherwise.} \end{cases}$$

We recall a Lemma from [3, Chapter 2], which provides a finite Fourier approximation to χ. This converts the problem of detecting solutions to (1.0.3) to a problem about estimates for exponential sums.

Lemma 1.2.1. *For any positive integer* L, *there exist complex sequences* $(c_\ell^-)_{|\ell|\leq L}$ *and* $(c_\ell^+)_{|\ell|\leq L}$ *such that*

$$2\delta - \frac{1}{L+1} + \sum_{0<|\ell|\leq L} c_\ell^- \, \mathbf{e}(\ell\theta) \leq \chi(\theta) \leq 2\delta + \frac{1}{L+1} + \sum_{0<|\ell|\leq L} c_\ell^+ \, \mathbf{e}(\ell\theta),$$

where

$$|c_\ell^+|, |c_\ell^-| \leq \min\left\{2\delta + \frac{1}{L+1}, \frac{3}{2\ell}\right\}.$$

For the rest of this chapter we assume the following. Let $\alpha,\ x \in \mathbb{R}$ be such that

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2},$$

where $1 \leq a \leq q \ll x^{O(1)}$ and $(a,q)=1$.

Let $(a_m)_{m\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$, $(c_\ell)_{\ell\in\mathbb{N}}$ be complex sequences satisfying

$$|a_m| \leq \tau(m), \quad |b_n| \leq \tau(n), \quad |c_\ell| \leq \min\left\{2\delta + \frac{1}{\lfloor x\rfloor + 1}, \frac{3}{2\ell}\right\},$$

whenever $m,n,\ell \in \mathbb{N}$. We will also use the classical divisor bound

$$\tau(r) \ll x^{o(1)}$$

for $r \leq x$. Lastly for $\varepsilon > 0$, we denote

$$\delta = x^{-1/4+\varepsilon}.$$

Firstly we recall a result from [59, Lemma 13.7].

Lemma 1.2.2. *We have*

$$\sum_{1\leq m\leq M} \min\left\{\frac{x}{m}, \frac{1}{\|\alpha m\|}\right\} \ll \left(M + \frac{x}{q} + q\right)\log 2qx, \tag{1.2.1}$$

and

$$\sum_{|m|\leq M} \min\left\{N, \frac{1}{\|\alpha m\|}\right\} \ll \left(M + N + \frac{MN}{q} + q\right)\log 2q. \tag{1.2.2}$$

The next two lemmas provide our Type I and II information respectively and can be obtained by following the method of [51, Section 2.3]. For completeness we shall include their proofs below.

Lemma 1.2.3. *We have*

$$\sum_{\ell\leq x}\left|c_\ell \sum_{\substack{mn\leq x\\ m\sim M}} a_m\, \mathbf{e}(\alpha\ell mn)\right| \ll \left(M + xq^{-1} + \delta q\right)x^{o(1)}.$$

Proof. Let S denote the left hand side of our claim, we get

$$\begin{aligned}
|S| &\leq x^{o(1)} \sum_{\ell\leq x}|c_\ell| \sum_{m\sim M}\left|\sum_{n\leq x/m} \mathbf{e}(\alpha\ell mn)\right| \\
&\leq x^{o(1)} \sum_{\ell\leq x}|c_\ell| \sum_{m\sim M} \min\left\{\frac{x}{m}, \frac{1}{\|\alpha\ell m\|}\right\} \\
&= x^{o(1)}(S_1 + S_2),
\end{aligned}$$

where

$$S_1 = \sum_{\ell \le \delta^{-1}} |c_\ell| \sum_{m \sim M} \min\left\{\frac{x}{m}, \frac{1}{\|\alpha \ell m\|}\right\},$$

and

$$S_2 = \sum_{\delta^{-1} < \ell \le x} |c_\ell| \sum_{m \sim M} \min\left\{\frac{x}{m}, \frac{1}{\|\alpha \ell m\|}\right\}.$$

By Lemma 1.2.2 with (1.2.1) and noting that $c_\ell \ll \delta$ for $\ell \le \delta^{-1}$, gluing the variables ℓ, m to get $w = \ell m$, we have

$$\begin{aligned} S_1 &\ll x^{o(1)}\delta \sum_{w \le 2\delta^{-1}M} \min\left\{\frac{x\delta^{-1}}{w}, \frac{1}{\|\alpha w\|}\right\} \\ &\ll x^{o(1)}\left(M + xq^{-1} + \delta q\right) \end{aligned}$$

since $q \ll x^{O(1)}$.

Next we bound S_2. By Lemma 1.2.2 with (1.2.1) and noting that $c_\ell \ll \ell^{-1}$ for $\delta^{-1} < \ell$, gluing the variables ℓ, m to get $w = \ell m$, we obtain

$$\begin{aligned} S_2 &\ll x^{o(1)} \sum_{L \le \log x} \delta^L \sum_{\ell \sim \delta^{-L}} \sum_{m \sim M} \min\left\{\frac{x}{m}, \frac{1}{\|\alpha \ell m\|}\right\} \\ &\ll x^{o(1)} \sum_{L \le \log x} \delta^L \sum_{w \le 4\delta^{-L}M} \min\left\{\frac{x\delta^{-L}}{w}, \frac{1}{\|\alpha w\|}\right\} \\ &\ll x^{o(1)}\left(M + xq^{-1} + \delta q\right). \end{aligned}$$

The result follows. □

Lemma 1.2.4. *We have*

$$\sum_{\ell \le x} \left| c_\ell \sum_{\substack{mn \le x \\ m \sim M}} a_m b_n \, \mathbf{e}(\alpha \ell m n) \right| \ll x^{1+o(1)} \left(\frac{\delta}{M} + \frac{M}{x} + \frac{1}{q} + \frac{q\delta}{x}\right)^{1/2} \tag{1.2.3}$$

for $M \ll x^{1/2}$, *and*

$$\sum_{\ell \le x} \left| c_\ell \sum_{\substack{mn \le x \\ m \sim M}} a_m b_n \, \mathbf{e}(\alpha \ell m n) \right| \ll x^{1+o(1)} \left(\frac{M\delta}{x} + \frac{1}{M} + \frac{1}{q} + \frac{q\delta}{x}\right)^{1/2} \tag{1.2.4}$$

for $x^{1/2} \ll M$.

Proof. First, suppose $M \ll x^{1/2}$ and let S denote the left hand side of the claim, we have

$$|S| \ll x^{o(1)} \sum_{\ell \leq x} |c_\ell| \sum_{m \sim M} \left| \sum_{mn \leq x} b_n \, \mathbf{e}(\alpha \ell m n) \right|.$$

Notice that

$$\sum_{a \leq \frac{x}{m}} \frac{1}{\lfloor x/M \rfloor} \sum_{z=0}^{\lfloor x/M \rfloor - 1} \mathbf{e}\left(\frac{z(a-n)}{\lfloor x/M \rfloor} \right) = \begin{cases} 1 & \text{if } n \leq \frac{x}{m}, \\ 0 & \text{otherwise,} \end{cases}$$

and the bound [59, Equation (8.6)] gives

$$\sum_{a \leq \frac{x}{m}} \mathbf{e}\left(\frac{za}{\lfloor x/M \rfloor} \right) \ll \frac{x/M}{z}$$

for $z = 0, \ldots, \lfloor x/M \rfloor - 1$. Therefore, we assert

$$\begin{aligned} S &\ll x^{o(1)} \sum_{\ell \leq x} |c_\ell| \sum_{m \sim M} \left| \sum_{n \leq \frac{x}{M}} b_n \, \mathbf{e}(\alpha \ell m n) \right| \\ &= x^{o(1)} (S_1 + S_2), \end{aligned}$$

where

$$S_1 = \sum_{\ell \leq \delta^{-1}} |c_\ell| \sum_{m \sim M} \left| \sum_{n \leq \frac{x}{M}} b_n \, \mathbf{e}(\alpha \ell m n) \right|,$$

and

$$S_2 = \sum_{\delta^{-1} < \ell \leq x} |c_\ell| \sum_{m \sim M} \left| \sum_{n \leq \frac{x}{M}} b_n \, \mathbf{e}(\alpha \ell m n) \right|.$$

We bound S_1 first. Gluing the variables ℓ, m to get $w = \ell m$, we obtain

$$S_1 \ll x^{o(1)} \delta \sum_{w \leq 2\delta^{-1} M} \left| \sum_{n \leq \frac{x}{M}} b_n \, \mathbf{e}(\alpha w n) \right|,$$

since $|c_\ell| \ll \delta$ in the range $\ell \leq \delta^{-1}$. By the Cauchy-Schwarz inequality, expanding the square and interchanging the order of summations, we have

$$\begin{aligned} S_1^2 &\ll x^{o(1)} \delta M \sum_{w \leq 2\delta^{-1} M} \left| \sum_{n \leq \frac{x}{M}} b_n \, \mathbf{e}(\alpha w n) \right|^2 \\ &= x^{o(1)} \delta M \sum_{w \leq 2\delta^{-1} M} \sum_{n_1, n_2 \leq \frac{x}{M}} b_{n_1} \overline{b_{n_2}} \, \mathbf{e}(\alpha w (n_1 - n_2)) \end{aligned}$$

$$\ll x^{o(1)}\delta M \sum_{n_1,n_2\leq \frac{x}{M}} \left| \sum_{w\leq 2\delta^{-1}M} \mathbf{e}(\alpha w(n_1-n_2)) \right|.$$

Since $n_1 - n_2$ may take a value in the interval $[-x/M, x/M]$ at most $O(x/M)$ times, we arrive at

$$\begin{aligned} S_1^2 &\ll x^{1+o(1)}\delta \sum_{|n|\leq \frac{x}{M}} \left| \sum_{w\leq 2\delta^{-1}M} \mathbf{e}(\alpha w n) \right| \\ &\ll x^{1+o(1)}\delta \sum_{|n|\leq \frac{x}{M}} \min\left\{ \delta^{-1}M, \frac{1}{\|\alpha n\|} \right\}. \end{aligned}$$

Applying Lemma 1.2.2 with (1.2.2) and taking the square-root, we bound

$$\begin{aligned} S_1 &\ll x^{1/2+o(1)}\delta^{1/2} \left(\frac{x}{M} + \frac{M}{\delta} + \frac{x}{\delta q} + q \right)^{1/2} \\ &\ll x^{1+o(1)} \left(\frac{\delta}{M} + \frac{M}{x} + \frac{1}{q} + \frac{q\delta}{x} \right)^{1/2}. \end{aligned}$$

We also get the same bound for S_2 by applying the same method and noting that $c_\ell \ll \ell^{-1}$ for $\delta^{-1} < \ell$.

Lastly, we suppose $x^{1/2} \ll M$ and proceeding like the above but instead we glue the variables ℓ and n, we assert

$$S \ll x^{1+o(1)} \left(\frac{M\delta}{x} + \frac{1}{M} + \frac{1}{q} + \frac{q\delta}{x} \right)^{1/2}.$$

The result follows. □

1.2.1 Estimates for Type I & II sums

Denote

$$\mathcal{B} = \{n \in \mathbb{N} \ : \ 2 \leq n \leq x\}$$

and

$$\mathcal{A} = \{n \in \mathcal{B} \ : \ \|\alpha n + \beta\| < \delta\}.$$

We will first state our Type I estimate.

Lemma 1.2.5 (Type I estimate)**.** *For $q = x^{2/3}$ we have*

$$\sum_{\substack{mn\in\mathcal{A}\\ m\sim M}} a_m = 2\delta \sum_{\substack{mn\in\mathcal{B}\\ m\sim M}} a_m + O\left(x^{3/4+\varepsilon/2}\right),$$

whenever $M \ll x^{3/4}$.

Proof. By Lemma 1.2.1 with $L = \lfloor x \rfloor$, we get

$$\begin{aligned}\sum_{\substack{mn\in\mathcal{A}\\ m\sim M}} a_m &= \sum_{\substack{mn\in\mathcal{B}\\ m\sim M}} a_m\chi(\alpha mn+\beta)\\ &= 2\delta \sum_{\substack{mn\in\mathcal{B}\\ m\sim M}} a_m + O\left(E_1+E_2\right).\end{aligned}$$

Here

$$\begin{aligned}E_1 &= \frac{1}{L+1}\sum_{\substack{mn\le x\\ m\sim M}} a_m\\ &\ll x^{o(1)},\end{aligned}$$

and

$$E_2 = \sum_{0<|\ell|\le L} |c_\ell^{\pm}| \cdot \left| \sum_{\substack{mn\le x\\ m\sim m}} a_m\, \mathbf{e}(\ell(\alpha mn+\beta))\right|.$$

Clearly there exists $\xi_\ell \in \mathbb{C}$ with $|\xi_\ell| = 1$ such that

$$E_2 = \sum_{0<|\ell|\le L} \xi_\ell c_\ell^{\pm} \sum_{\substack{mn\le x\\ m\sim M}} a_m\, \mathbf{e}(\alpha\ell mn).$$

Applying Lemma 1.2.3 immediately gives the bound

$$\begin{aligned}E_2 &\ll \left(M + xq^{-1} + \delta q\right) x^{o(1)}\\ &\ll x^{3/4+\varepsilon/2},\end{aligned}$$

whenever $M \ll x^{3/4}$. □

Next, we state our Type II estimate.

Lemma 1.2.6 (Type II estimate)**.** *For $q = x^{2/3}$ we have*

$$\sum_{\substack{mn\in\mathcal{A}\\ x^\gamma\le m\le x^{\gamma+\tau}}} a_m b_n = 2\delta \sum_{\substack{mn\in\mathcal{B}\\ x^\gamma\le m\le x^{\gamma+\tau}}} a_m b_n + O\left(x^{3/4+\varepsilon/2+o(1)}\right),$$

uniformly for $1/4 \le \gamma$, $\gamma+\tau \le 3/4$.

Proof. We follow the method of Lemma 1.2.5. Partition the summation over m into dyadic intervals and apply Lemma 1.2.4. □

1.2.2 Sieve estimates

For positive real numbers u, v, w, we denote

$$P(w) = \prod_{p<w} p \qquad \text{and} \qquad P(u,v] = \prod_{u<p\leq v} p.$$

We also set

$$Y = x^{3/4+\varepsilon/2+o(1)}.$$

For any set $\mathcal{A} \subseteq [2,x]$ of integers and any positive integer s, we denote

$$\mathcal{A}_s = \{n \,:\, ns \in \mathcal{A}\}.$$

For real numbers $0 < y \leq z \leq x$, we denote

$$\mathcal{S}(\mathcal{A}; y, z) = \#\{a \in \mathcal{A} \,:\, p \mid a \Rightarrow p \in [y,z]\}$$

and in the special case $z = x$, we denote

$$\mathcal{S}(\mathcal{A}; y, z) = \mathcal{S}(\mathcal{A}; y).$$

Given a positive integer $n \geq 2$, we denote by $P^-(n)$ and $P^+(n)$ the smallest and largest prime factor of n respectively, also we set $P^-(1) = \infty$.

We state a variant of the Buchstab identity for $[y,z]$-smooth numbers which is based on taking out the largest prime factor of the integers we are counting.

Lemma 1.2.7. *For any $2 \leq y \leq z$ and any set $\mathcal{A} \subseteq [2,x]$ of integers, we have*

$$\mathcal{S}(\mathcal{A}; y, z) = \sum_{y\leq p\leq z} \mathcal{S}(\mathcal{A}_p; y, p) + \mathcal{S}(\mathcal{C}; x^{1/2}) + O\left(x^{1/2}\right)$$

where $\mathcal{C} = \{a \in \mathcal{A} \,:\, y \leq a \leq z\}$.

Proof. Take $a \in \{u \in \mathcal{A} \,:\, p \mid u \Rightarrow p \in [y,z]\}$. If a is a prime then a is contained in the set

$$\{u \in \mathcal{A} \,:\, y \leq u \leq z, u \text{ is prime}\},$$

and is of size

$$\mathcal{S}(\mathcal{C}; x^{1/2}) + O\left(x^{1/2}\right).$$

Otherwise a has at least two prime factors and we can write $a = P^+(a)n$ where $n > 1$ and the prime factors of n lie in the interval $[y, P^+(a)]$. The result follows immediately. □

Next we state three lemmas which give sieve estimates for different regions. In particular, the proofs will rely on ingredients coming from the Harman sieve [50, Lemma 2].

Our first sieve estimate is essentially based on an application of our Type II estimate (Lemma 1.2.6).

Lemma 1.2.8. *For $x^{1/4} \leq y < z \leq x^{3/4}$, we have*

$$\sum_{y\leq p\leq z} \mathcal{S}(\mathcal{A}_p; y, p) = 2\delta \sum_{y\leq p\leq z} \mathcal{S}(\mathcal{B}_p; y, p) + O(Y).$$

Proof. We have

$$\begin{aligned}\sum_{y\leq p\leq z} \mathcal{S}(\mathcal{A}_p; y, p) &= \sum_{y\leq p\leq z} \sum_{\substack{np\in\mathcal{A}\\(n,P(y)P(p,x])=1}} 1\\ &= \sum_{\substack{mn\in\mathcal{A}\\y\leq m\leq z}} a(m,n).\end{aligned}$$

Here

$$\begin{aligned}a(m,n) &= \mathbb{1}_{\mathbb{P}}(m) \sum_{(n,P(y)P(m,x])=1} 1\\ &= \mathbb{1}_{\mathbb{P}}(m) \sum_{\substack{d|n\\d|P(y)P(m,x]}} \mu(d),\end{aligned}$$

where $\mathbb{1}_{\mathbb{P}}(\cdot)$ is the characteristic function for the primes. We may assume that d is square-free, as otherwise it does not contribute to the sum $a(m,n)$.

Let us write

$$a(m,n) = \mathbb{1}_{\mathbb{P}}(m) \sum_{\substack{d_1d_2|n\\d_2|P(y)\\P^-(d_1)>m}} \mu(d_1d_2).$$

We may assume $d_1 > 1$ as the case $d_1 = 1$ follows immediately. We now get rid of the condition $P^-(d_1) > m$ by appealing to the truncated Perron formula

$$\frac{1}{\pi}\int_{-T}^{T} e^{i\gamma t}\frac{\sin\rho t}{t}\,\mathrm{d}t = \begin{cases} 1 + O\left(T^{-1}(\rho - |\gamma|)^{-1}\right) & \text{if } |\gamma| \leq \rho,\\ O\left(T^{-1}(|\gamma| - \rho)^{-1}\right) & \text{if } |\gamma| > \rho.\end{cases}$$

Applying the above formula with $\rho = \log\left(P^-(d_1) - \frac{1}{2}\right)$, $\gamma = \log m$, and $T = x^2\delta^{-1}$, we have

$$\sum_{\substack{mn\in\mathcal{A}\\y\leq m\leq z}} a(m,n) = M(\mathcal{A}) + O\left(R(\mathcal{A})\right).$$

Here the main term

$$M(\mathcal{A}) = \frac{1}{\pi}\int_{-T}^{T} \sum_{\substack{mn\in\mathcal{A}\\ y\le m\le z}} \mathbb{1}_{\mathbb{P}}(m) e^{i\gamma t} \left(\sum_{\substack{d_1d_2|n\\ d_2|P(y)}} \mu(d_1d_2)\sin(\rho t)\right) \frac{\mathrm{d}t}{t},$$

and the remainder term

$$R(\mathcal{A}) = T^{-1} \sum_{\substack{mn\in\mathcal{A}\\ y\le m\le z}} \mathbb{1}_{\mathbb{P}}(m) \sum_{\substack{d_1d_2|n\\ d_2|P(y)}} \frac{\mu(d_1d_2)}{\left|\log\left(P^-(d)-\frac{1}{2}\right)-\log m\right|}.$$

We will consider the remainder term $R(\mathcal{A})$ first. By the mean value theorem,

$$\frac{1}{\log\left(P^-(d)-\frac{1}{2}\right)-\log m} = \frac{\eta}{P^-(d)-\frac{1}{2}-m}$$

where $\eta \in [m, P^-(d)-\frac{1}{2}]$ or $[P^-(d)-\frac{1}{2}, m]$. In any case, we have $\eta \le \max\{m, n-\frac{1}{2}\}$, so we bound

$$\begin{aligned}\frac{\eta}{P^-(d)-\frac{1}{2}-m} &\ll \max\{m,n\}\\ &\le x.\end{aligned}$$

Therefore

$$\begin{aligned}R(\mathcal{A}) &\ll T^{-1}x^{2+o(1)}\\ &\ll \delta x^{o(1)}.\end{aligned}$$

It remains to estimate the main term. Note that the integral in the main term between $-1/T$ and $1/T$ can be trivially bounded by $\ll T^{-1}x^{1+o(1)} \ll \delta x^{-1}$. Applying our Type II estimate (Lemma 1.2.6) in the integral over

$$\mathfrak{R}(T) = (-T,-1/T)\cup(1/T,T),$$

we get

$$\begin{aligned}M(\mathcal{A}) = \frac{2\delta}{\pi}\int_{\mathfrak{R}(T)} \sum_{\substack{mn\in\mathcal{B}\\ y\le m\le z}} \mathbb{1}_{\mathbb{P}}(m) m^{it} \sum_{\substack{d_1d_2|n\\ d_2|P(y)}} \mu(d_1d_2)\sin\left(t\log\left(P^-(d_1)-\frac{1}{2}\right)\right)\frac{\mathrm{d}t}{t}\\ + O\left(Y\int_{\mathfrak{R}(T)}\frac{\mathrm{d}t}{t}\right) + O\left(\delta x^{-1}\right),\end{aligned}$$

and therefore

$$\begin{aligned} M(\mathcal{A}) &= \frac{2\delta}{\pi}\int_{-T}^{T}\sum_{\substack{mn\in\mathcal{B}\\ y\le m\le z}}\mathbb{1}_{\mathbb{P}}(m)m^{it}\sum_{\substack{d_1d_2\mid n\\ d_2\mid P(y)}}\mu(d_1d_2)\sin\left(t\log\left(P^-(d_1)-\frac{1}{2}\right)\right)\frac{\mathrm{d}t}{t} \\ &\quad + O(Y) \\ &= 2\delta M(\mathcal{B}) + O(Y), \end{aligned}$$

where the last line follows from the truncated Perron formula once again. The result follows immediately. □

The next sieve estimate is based on an idea which dates back to I. M. Vinogradov who applied it to estimate sum over primes. The idea is to systematically take out the largest prime factor until we get sums which we can estimate by our Type II estimate (Lemma 1.2.6).

Lemma 1.2.9. *For $2 \le y < z < x^{1/4}$, we have*

$$\sum_{y\le p\le z}\mathcal{S}(\mathcal{A}_p;y,p) = 2\delta\sum_{y\le p\le z}\mathcal{S}(\mathcal{B}_p;y,p) + O(Y).$$

Proof. By the method of Lemma 1.2.7 we have

$$\sum_{y\le p\le z}\mathcal{S}(\mathcal{A}_p;y,p) = \sum_{y\le p_1\le p\le z}\mathcal{S}(\mathcal{A}_{pp_1};y,p_1) + O\left(x^{1/2}\right).$$

We will first consider the sum on the right with $pp_1 > x^{1/4}$. Clearly we have

$$\sum_{\substack{y\le p_1\le p\le z\\ pp_1>x^{1/4}}}\mathcal{S}(\mathcal{A}_{pp_1};y,p_1) = \sum_{\substack{y\le p_1\le p\le z\\ pp_1>x^{1/4}}}\sum_{\substack{npp_1\in\mathcal{A}\\ (n,P(y)P(p_1,x])=1}}1.$$

Set $m = pp_1$ and note that $m < x^{1/2}$. It follows that

$$\sum_{\substack{y\le p_1\le p\le z\\ pp_1>x^{1/4}}}\mathcal{S}(\mathcal{A}_{pp_1};y,p_1) = \sum_{\substack{mn\in\mathcal{A}\\ x^{1/4}<m<x^{1/2}}}a_m\sum_{\substack{d_1d_2\mid n\\ d_1\mid P(y)\\ P^-(d_2)>P^-(m)}}\mu(d_1d_2),$$

where a_m is 1 if $m = pp_1$ with $p, p_1 \in [y, z]$ and 0 otherwise. Applying the method of Lemma 1.2.8, we get

$$\sum_{\substack{y\le p_1\le p\le z\\ pp_1>x^{1/4}}}\mathcal{S}(\mathcal{A}_{pp_1};y,p_1) = 2\delta\sum_{\substack{y\le p_1\le p\le z\\ pp_1>x^{1/4}}}\mathcal{S}(\mathcal{B}_{pp_1};y,p_1) + O(Y).$$

The only part left to consider is the sum

$$\sum_{\substack{y\le p_1\le p\le z\\ pp_1\le x^{1/4}}} \mathcal{S}(\mathcal{A}_{pp_1}; y, p_1).$$

If it is zero then we are done, otherwise we take out the next largest prime factor to get

$$\sum_{\substack{y\le p_1\le p\le z\\ pp_1\le x^{1/4}}} \mathcal{S}(\mathcal{A}_{pp_1}; y, p_1) = \sum_{\substack{y\le p_2\le p_1\le p\le z\\ pp_1\le x^{1/4}}} \mathcal{S}(\mathcal{A}_{pp_1p_2}; y, p_2) + O\left(x^{1/2}\right).$$

The sum on the right with $pp_1p_2 > x^{1/4}$ can be dealt with again by the method of Lemma 1.2.8. By induction this can go on for at most $O(\log x)$ steps. Since we have an asymptotic formula for every sum, the result follows swiftly. □

For our next sieve estimate, we note that our Type II estimates are not sufficient in this region. We bypass this complication by a role reversal that minimises the length of summation in exchange for sifting primes.

Lemma 1.2.10. *For $x^{3/4} \le z \le x$, we have*

$$\sum_{x^{3/4}<p\le z} \mathcal{S}(\mathcal{A}_p; y, p) = 2\delta \sum_{x^{3/4}<p\le z} \mathcal{S}(\mathcal{B}_p; y, p) + O(Y).$$

Proof. Take $x^{3/4} < p \le z$ and an element $np \in \mathcal{A}$ such that if $q \mid n$ where q is prime then $q \in [y, p]$. This gives

$$\sum_{x^{3/4}<p\le z} \mathcal{S}(\mathcal{A}_p; y, p) = \sum_{n<x^{1/4}} c_n \mathcal{S}(\mathcal{A}'_n; (x/n)^{1/2}) + O\left(x^{o(1)}\right). \tag{1.2.5}$$

Here

$$\begin{aligned}\mathcal{A}'_n &= \left\{\max\{y+\Delta(y), x^{3/4}\} < m \le z \ :\ mn \in \mathcal{A}\right\}\\ &= \left\{\max\left\{y+\Delta(y), x^{3/4}\right\} < m \le \min\{z, x/n\} \ :\ \|\alpha mn+\beta\| < \delta\right\},\end{aligned}$$

where c_n is 1 if all prime factors of n are at least y, and 0 otherwise, and $\Delta(y)$ is -1/2 if y is an integer, and 0 otherwise. We also recall the notation

$$\mathcal{S}(\mathcal{W}; k) = \#\left\{w \in \mathcal{W} \ :\ (w, P(k)) = 1\right\}.$$

We note that the sum in (1.2.5) may be empty depending on the choice of y. To show (1.2.5), take $m \in S(\mathcal{A}'_n; (x/n)^{1/2})$ and suppose that m has two prime factors say q_1, q_2 then we must have

$$m \ge q_1q_2$$

$$\geq (x/n)^{1/2}(x/n)^{1/2}$$
$$= x/n.$$

This is a contradiction unless $mn = x$ and this occurs at most $O\left(x^{o(1)}\right)$ times. Moreover, it is evident that

$$\sum_{n<x^{1/4}} c_n \mathcal{S}(\mathcal{A}'_n; (x/n)^{1/2}) = \sum_{n<x^{1/4}} c_n \left\{\mathcal{S}(\mathcal{A}'_n; x^{1/2}) + O\left(x^{1/2}\right)\right\}$$
$$= \sum_{n<x^{1/4}} c_n \mathcal{S}(\mathcal{A}'_n; x^{1/2}) + O\left(x^{3/4}\right).$$

Let $N \leq n < 2N$ where $N \ll x^{1/4}$ and M a positive real number such that

$$\max\{y + \Delta(y), x^{3/4}\}n \ll M(n) = M \ll \min\{zn, x\}$$

and consider the set

$$\mathcal{A}^{(M)} = \{M \leq m < 2M \ : \ \|\alpha m + \beta\| < \delta\}.$$

Then we have

$$\mathcal{A}_n^{(M)} = \{M/n \leq m < 2M/n \ : \ \|\alpha mn + \beta\| < \delta\},$$

and by the Harman sieve [50, Lemma 2] using the Type I and II estimate (Lemma 1.2.5 and 1.2.6), we get

$$\sum_{n\sim N} c_n \mathcal{S}(\mathcal{A}_n^{(M)}; x^{1/2}) = 2\delta \sum_{n\sim N} c_n \mathcal{S}(\mathcal{B}_n^{(M)}; x^{1/2}) + O(Y).$$

Therefore by summing over N, M we obtain

$$\sum_{n<x^{1/4}} c_n \mathcal{S}(\mathcal{A}'_n; x^{1/2}) = 2\delta \sum_{n<x^{1/4}} c_n \mathcal{S}(\mathcal{B}'_n; x^{1/2}) + O(Y),$$

which is what we needed to show. □

For a set $\mathcal{C} \subseteq [2, x]$ of integers and for integers $2 \leq y < z \leq x$, we denote

$$\mathcal{T}(\mathcal{C}; y, z) = \#\left\{c \in \mathcal{C} \ : \ \mu^2(c) = 1, p \mid c \Rightarrow p \in [y, z]\right\}.$$

The next three results are square-free analogue of Lemma 1.2.8–1.2.10.

Lemma 1.2.11. *For $x^{1/4} \leq y < z \leq x^{3/4}$, we have*

$$\sum_{y\leq p\leq z} \mathcal{T}(\mathcal{A}_p; y, p-1) = 2\delta \sum_{y<p\leq z} \mathcal{T}(\mathcal{B}_p; y, p-1) + O(Y).$$

Proof. By writing

$$\sum_{y\le p\le z}\mathcal{T}(\mathcal{A}_p;y,p-1)=\sum_{y\le p\le z}\sum_{\substack{np\in\mathcal{A}\\(n,P(y),P(p-1,x])=1}}\mu^2(np)$$
$$=\sum_{\substack{mn\in\mathcal{A}\\y\le m\le z}}\mathbb{1}_{\mathbb{P}}(m)\mu^2(n)\sum_{\substack{d_1d_2|n\\d_1|P(y)\\P^-(d_2)\ge m}}\mu(d_1d_2).$$

We see that the method of Lemma 1.2.8 gives the result. □

Lemma 1.2.12. *For $2\le y<z<x^{1/4}$, we have*

$$\sum_{y\le p\le z}\mathcal{T}(\mathcal{A}_p;y,p-1)=2\delta\sum_{y\le p\le z}\mathcal{T}(\mathcal{B}_p;y,p-1)+O(Y).$$

Proof. We follow as in Lemma 1.2.9 but we successively take out the largest distinct prime factors. □

Lemma 1.2.13. *For $x^{3/4}\le z\le x$, we have*

$$\sum_{x^{3/4}<p\le z}\mathcal{T}(\mathcal{A}_p;y,p-1)=2\delta\sum_{x^{3/4}<p\le z}\mathcal{T}(\mathcal{B}_p;y,p-1)+O(Y).$$

Proof. This follows immediately from the proof of Lemma 1.2.10 by taking c_n there to be 1 if n is square-free and all prime factors of n are at least y, and 0 otherwise. □

1.3 Proof of Theorem 1.1.1

By Dirichlet's theorem, we have

$$\left|\alpha-\frac{a}{q}\right|<\frac{1}{q^2}$$

for infinitely many q. Let $(q_k)_{k\in\mathbb{N}}$ be an increasing sequence of such denominators. Then we can choose an increasing sequence $(x_k)_{k\in\mathbb{N}}$ so that $q_k=x_k^{2/3}$. Now we take x_k to be a sufficiently large element in the sequence $(x_k)_{k\in\mathbb{N}}$.

By Lemma 1.2.7, we assert

$$\mathcal{S}(\mathcal{A};y,z)=\sum_{y\le p\le z}\mathcal{S}(\mathcal{A}_p;y,p)+\mathcal{S}(\mathcal{C};x_k^{1/2})+O\big(x_k^{1/2}\big). \tag{1.3.1}$$

By [93, Theorem 2] and partial summation, we have

$$\mathcal{S}(\mathcal{C};x_k^{1/2})=2\delta\mathcal{S}(\mathcal{D};x_k^{1/2})+O(Y), \tag{1.3.2}$$

where $\mathcal{D} = \{n \in \mathbb{N} \ : \ y \leq n \leq z\}$, and $Y = x_k^{3/4+\varepsilon/2+o(1)}$. Therefore by substituting (1.3.2) into (1.3.1), we obtain

$$\mathcal{S}(\mathcal{A}; y, z) = \sum_{y \leq p \leq z} \mathcal{S}(\mathcal{A}_p; y, p) + 2\delta \mathcal{S}(\mathcal{D}; x_k^{1/2}) + O(Y).$$

Suppose $y < x_k^{1/4}$. Then we write

$$\begin{aligned}
&\mathcal{S}(\mathcal{A}; y, z) \\
&= \left(\sum_{y \leq p \leq z < x_k^{1/4}} + \sum_{y \leq p < x_k^{1/4}} + \sum_{x_k^{1/4} \leq p \leq z \leq x_k^{3/4}} + \sum_{x_k^{1/4} \leq p \leq x_k^{3/4} \leq z} + \sum_{x_k^{3/4} < p \leq z} \right) \mathcal{S}(\mathcal{A}_p; y, p) \\
&\quad + 2\delta \mathcal{S}(\mathcal{D}; x_k^{1/2}) + O(Y).
\end{aligned}$$

We note that some of the sums above may be empty depending on the choice of z. Applying Lemma 1.2.8–1.2.10 then Lemma 1.2.7 to the above we get

$$\mathcal{S}(\mathcal{A}; y, z) = 2\delta \mathcal{S}(\mathcal{B}; y, z) + O(Y).$$

The case $x_k^{1/4} \leq y < x_k^{1/2}$ is similar to the case above and the first result follows.

Now suppose $\alpha \in \mathcal{I}(A)$ then we can assume $\alpha \in (0,1)\backslash\mathbb{Q}$. Indeed, we can write $\alpha = b + r$, where $b \in \mathbb{Z}$ and $r \in (0,1)\backslash\mathbb{Q}$, so that $\|\alpha n + \beta\| = \|rn + \beta\|$. Therefore we have the continued fraction expansion $\alpha = [0; a_1, a_2, \ldots]$ with $0 < a_i \leq A$ for some absolute constant A. The convergents p_s/q_s to α satisfy the inequality $|\alpha - p_s/q_s| < 1/q_s^2$. Clearly $(q_s)_{s \geq 1}$ is a strictly increasing sequence. Therefore, for any sufficiently large x there exist $s \in \mathbb{N}$ such that $q_{s-1} \leq x^{2/3} \leq q_s$. Since $q_s = a_s q_{s-1} + q_{s-2}$ for $s \geq 2$, we get $q_s \leq (A+1)q_{s-1} \leq 2Ax^{2/3} \ll x^{2/3}$, because A is fixed. Hence $x^{2/3} \ll q_s \ll x^{2/3}$ and the result follows by the argument above.

1.4 Proof of Theorem 1.1.2

We proceed as in the proof of Theorem 1.1.1 but instead we apply Lemma 1.2.11-1.2.13.

CHAPTER 2

On Products of Integers Free of Small Prime Factors and Primes in Arithmetic Progressions

"Perfect numbers like perfect men are very rare."

–Rene Descartes

We are interested in the following conjecture stated in a paper of Erdös, Odlyzko, and Sárközy [29].

Conjecture 2.0.1 (EOSC). *For all sufficiently large k and a with $(a,k)=1$, we have*

$$p_1p_2 \equiv a \pmod{k} \quad \textit{for some } p_1,p_2 \leq k. \tag{2.0.1}$$

Although EOSC is unreachable with current methods in view of the parity problem, we note that various relaxation towards EOSC had been made. Specifically Shparlinski [88] showed for any integers a and $m \geq 1$ with $(a,m)=1$, there exist several families of small integers $k,\ell \geq 1$ and real positive $\alpha,\beta \leq 1$, such that the products

$$p_1 \dots p_k s \equiv a \pmod{m}.$$

Here $p_1,\dots,p_k \leq m^{\alpha}$ are primes and $s \leq m^{\beta}$ is a product of at most ℓ primes. Shparlinski [87] also showed that there exists a solution to the congruence

$$pr \equiv a \pmod{m}$$

where p is prime, r is a product of at most 17 prime factors and $p,r \leq m$. The techniques in [87, 88] involve a sieve method by Greaves [45] applied with bounds of exponential sum over reciprocal of primes.

For products of large primes, Ramaré and Walker [82] showed that every reduced residue class modulo m can be represented by a product of three primes $p_1,p_2,p_3 \leq m^{16/3}$ as $m \to \infty$.

In another direction Friedlander, Kurlberg and Shparlinski [37] obtained an upper bound on the number of solutions to (2.0.1) on average over a and k. This implies we

should expect the following conjecture

$$\#\{(p_1,p_2) : p_i \leq x, p_1p_2 \equiv a \pmod{k}\} = \frac{\pi(x)^2}{\varphi(k)} + o\left(\frac{\pi(x)^2}{\varphi(k)}\right),$$

where $\pi(x)$ denote the number of primes up to x.

Finally, we remark that one can find results of Garaev [39] which improves results of [37] concerning the related congruences

$$p_1(p_2+p_3) \equiv a \pmod{m} \qquad \text{and} \qquad p_1p_2(p_3+h) \equiv a \pmod{m},$$

where $p_1, p_2, p_3 \leq x$ are primes and h is a fixed integer.

Let $\mathcal{U} \subseteq [2,x] \cap \mathbb{N}$, $\mathcal{V} \subseteq [2,y] \cap \mathbb{N}$, $k > 2$ and an integer a with $(a,k) = 1$. We use $\mathcal{N}_k(a;\mathcal{U},\mathcal{V},z)$ to denote the number of solutions to the congruence

$$uv \equiv a \pmod{k}, \quad u \in \mathcal{U}, v \in \mathcal{V}, P^-(u) \geq z.$$

Here $P^-(m)$ is the smallest prime factor of m for $m \geq 2$ and $P^-(1) = \infty$.

In the special case when $\mathcal{U} = [2,x] \cap \mathbb{N}$ and $\mathcal{V} = \{p \leq y \ : \ p \text{ prime}\}$, we set

$$\mathcal{N}_k(a;x,y,z) = \mathcal{N}_k(a;\mathcal{U},\mathcal{V},z).$$

Observe that showing

$$\mathcal{N}_k(a;k,k,k^{\frac{1}{2}}) > 0$$

for all sufficiently large k would immediately imply EOSC.

In this chapter, we establish various bounds for $\mathcal{N}_k(a;x,y,z)$. The best results are conditional on the Generalised Riemann Hypothesis (GRH). Our method is to apply the Harman sieve coupled with Type I & II estimates obtained from bounds for multiplicative character sums.

We write χ_0 to be the principal character modulo k and the set of all $\varphi(k)$ multiplicative characters modulo k is denoted by $\mathcal{X}_k$, where φ is the Euler totient function. Moreover, we denote $\mathcal{X}_k^* = \mathcal{X}_k \backslash \{\chi_0\}$. For relatively prime integers m and n, we denote by $\bar{n}_m$ the multiplicative inverse of n modulo m, the unique integer u defined by the conditions

$$un \equiv 1 \pmod{m} \qquad \text{and} \qquad 0 \leq u < m.$$

We always denote p, q and their subscripts to be prime.

2.1 Main results

For any $\beta \geq 0$, we denote

$$\Phi(x,x^\beta) = \#\left\{n \leq x \ : \ P^-(n) \geq x^\beta\right\}$$

as the number of x^β-rough numbers in the interval $[1, x]$ and

$$\mathcal{P}_k(y) = \{p \le y \ : \ (p, k) = 1\}$$

as the set of primes up to y coprime to k. In the special case that $k = 1$, we write $\mathcal{P}(y) = \mathcal{P}_1(y)$.

We state our first unconditional result for $\mathcal{N}_k(a; x, y, z)$.

Theorem 2.1.1. *Let $k, x \ll \log^B y$ for some fixed $B > 0$. Then for any $\beta \in (0, \frac{1}{2}]$ and fixed $C > 0$, we have*

$$\mathcal{N}_k(a; x, y, x^\beta) = \frac{\#\mathcal{P}_k(y)}{\varphi(k)}\Phi(x, x^\beta) + O\left(\frac{xy}{\varphi(k)\log^C y}\right).$$

Assuming the GRH, we obtain an estimate valid for a wider range of parameters.

Theorem 2.1.2. *Assume the GRH. Fix real numbers $\vartheta_1, \vartheta_2 > 0$ such that*

$$\vartheta_2 < \min\left\{\frac{1+\vartheta_1}{2}, \frac{2+3\vartheta_1}{5}\right\}.$$

Set $y = x^{\vartheta_1}$, $k \asymp x^{\vartheta_2}$ and fix $\beta \in (0, \frac{1}{2}]$ with $\beta < 1 + 2(\vartheta_1 - \vartheta_2)$. For any sufficiently small $\varepsilon > 0$, we have

$$\mathcal{N}_k(a; x, y, x^\beta) = \frac{\#\mathcal{P}_k(y)}{\varphi(k)}\Phi(x, x^\beta) + O\left(\frac{x^{1-\varepsilon+o(1)}y}{k}\right)$$

as $x \to \infty$.

We see from Theorem 2.1.2 even on the assumption of the GRH we need one of the two lengths x or y to be greater than the modulus k. In view of EOSC and focusing on the special case $\beta = 1/2$, our next result shows that we can reduce one of the lengths drastically.

Theorem 2.1.3. *Assume the GRH. For any fixed sufficiently small $\varepsilon > 0$, set $y = x^\varepsilon$ and $k \asymp x^\delta$. Then for all x sufficiently large, we have*

$$\mathcal{N}_k(a; x, y, x^{\frac{1}{2}}) = \frac{\#\mathcal{P}_k(y)}{\varphi(k)}\Phi(x, x^\beta) + O\left(\frac{x^{1-\varepsilon+o(1)}y}{k}\right)$$

if $\delta \in \left(\frac{1}{4}, \frac{1}{3}\right]$, and

$$\mathcal{N}_k(a; x, y, x^{\frac{1}{2}}) \ge \frac{3xy}{4\varphi(k)(\log x)(\log y)} \tag{2.1.1}$$

if $\delta \in \left(\frac{1}{3}, \frac{2}{5}\right)$.

By [59, Lemma 12.1], we have for any fixed $\beta < 1$, the asymptotic

$$\Phi(x, x^{\beta}) \sim \omega(\beta^{-1}) \frac{x}{\beta \log x}$$

as $x \to \infty$. Here ω is the Buchstab function defined by the delay differential equation

$$\begin{aligned} \omega(u) &= 1/u && \text{for } 1 \leq u \leq 2, \\ (u\omega(u))' &= \omega(u-1) && \text{for } u > 2. \end{aligned}$$

For $k = y^{O(1)}$, we have by the prime number theorem

$$\begin{aligned} \mathcal{P}_k(y) &= \mathcal{P}(y) - \sum_{p|k} 1 \\ &= \mathcal{P}(y) + O(\log y) \\ &\sim \frac{y}{\log y}, \end{aligned}$$

as $y \to \infty$. It follows the main term dominates the remainder term in Theorems 2.1.1, 2.1.2 and 2.1.3. We do not pursue to optimise the constant $3/4$ in (2.1.1).

Lastly, notice that Theorem 2.1.1 and 2.1.2 gives partial results towards EOSC, that is

$$\mathcal{N}_k(a; k, \exp(k^{\frac{1}{B}}), k^{\frac{1}{2}}) > 0,$$

and

$$\mathcal{N}_k(a; k, k^{1+\varepsilon}, k^{\frac{1}{2}}) > 0$$

(conditional on the GRH) respectively as $k \to \infty$.

2.2 Preparations

2.2.1 Bounds for multiplicative character sums

We recall a classical result proved independently by Pólya and Vinogradov [59, Theorem 12.5].

Lemma 2.2.1 (Pólya-Vinogradov)**.** *For any non-principal character modulo k, we have*

$$\max_{M,N} \left| \sum_{M < n \leq M+N} \chi(n) \right| \ll k^{\frac{1}{2}+o(1)}.$$

We also recall a result from [59, Corollary 5.29] which gives a bound for character sums over primes.

Lemma 2.2.2. *For $k > 2$ and fixed $A > 0$, we have*

$$\max_{\chi \in \mathcal{X}_k^*} \left| \sum_{p \leq y} \chi(p) \right| \ll k^{\frac{1}{2}} y (\log y)^{-A}.$$

We obtain a stronger bound under the GRH. This follows by taking $T = x^2$ in [27, Equation 13, page 120] and applying the GRH.

Lemma 2.2.3. *Assume the GRH then we have*

$$\max_{\chi \in \mathcal{X}_k^*} \left| \sum_{p \leq y} \chi(p) \right| \ll y^{\frac{1}{2}} \log ky.$$

We also recall the mean value estimate for character sums which follows immediately by orthogonality.

Lemma 2.2.4. *For $N \geq 1$ and any sequence of complex numbers a_n, we have*

$$\sum_{\chi \in \mathcal{X}_k} \left| \sum_{n \leq N} a_n \chi(n) \right|^2 \leq \varphi(k)(N/k + 1) \sum_{n \leq N} |a_n|^2.$$

2.2.2 Type I & II estimates

We recall that $k > 2$ an integer and we define the sequences $\mathcal{A} = (c_r)$ by

$$c_r = \sum_{\substack{p \leq y, (p,k)=1 \\ r \equiv a\bar{p}_k \pmod{k}}} 1,$$

and $\mathcal{B} = (1_r)$ the constant sequence 1, both supported on the interval $[1, x]$. We state our Type I estimate below.

Lemma 2.2.5 (Type I estimate)**.** *Suppose we have the bound*

$$\sum_{p \leq y} \chi(p) \ll \Delta(k, y)$$

for all $\chi \in \mathcal{X}_k^*$. For any complex sequence a_m such that $|a_m| \leq \tau(m)$, we have

$$\sum_{\substack{c_{mn} \in \mathcal{A} \\ m \leq M}} a_m c_{mn} = \frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn \in \mathcal{B} \\ m \leq M}} a_m + O\left(\Delta(k, y) M^{1+o(1)} k^{\frac{1}{2}+o(1)} \right). \tag{2.2.1}$$

Proof. We recall the orthogonality relation

$$\frac{1}{\varphi(k)} \sum_{\chi \in \mathcal{X}_k} \bar{\chi}(a)\chi(r) = \begin{cases} 1 & \text{if } r \equiv a \pmod{k}, \\ 0 & \text{otherwise,} \end{cases}$$

for $(a, k) = 1$. Applying the above identity, we get

$$\sum_{\substack{c_{mn} \in \mathcal{A} \\ m \leq M}} a_m c_{mn} = \sum_{\substack{mn \in \mathcal{B} \\ m \leq M}} a_m \sum_{\substack{p \leq y, (p,k)=1 \\ mn \equiv a\bar{p}_k \pmod{k}}} 1$$

$$= \frac{1}{\varphi(k)} \sum_{\substack{mn\in\mathcal{B}\\ m\le M}} a_m \sum_{\substack{p\le y\\ (p,k)=1}} \sum_{\chi\in\mathcal{X}_k} \chi(mn)\bar{\chi}(a\bar{p}_k).$$

Separating the main term corresponding to the principal character χ_0, the above is

$$\frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn\in\mathcal{B}\\ m\le M}} a_m + \frac{1}{\varphi(k)} \sum_{\chi\in\mathcal{X}_k^*} \bar{\chi}(a) \sum_{\substack{mn\le x\\ m\le M}} a_m\chi(mn) \sum_{\substack{p\le y\\ (p,k)=1}} \chi(p).$$

Denote the second sum on the right by R. By the Pólya-Vinogradov (Lemma 2.2.1) and our assumption, we obtain

$$\begin{aligned} R &\ll M^{1+o(1)} \sum_{\chi\in\mathcal{X}_k^*} \max_{M\le m<2M} \left| \sum_{n\le x/m} \chi(n) \right| \cdot \left| \sum_{p\le y} \chi(p) \right| \\ &\ll M^{1+o(1)} \varphi(k) k^{\frac{1}{2}+o(1)} \Delta(k,y). \end{aligned}$$

□

Using similar argument to Lemma 2.2.5, we obtain our Type II estimate.

Lemma 2.2.6 (Type II estimate)**.** *Suppose we have the bound*

$$\sum_{p\le y} \chi(p) \ll \Delta(k,y)$$

for all $\chi \in \mathcal{X}_k^*$. For any complex sequences a_m, b_n such that $|a_m| \le \tau(m)$, $|b_n| \le \tau(n)$, we have

$$\begin{aligned} \sum_{\substack{c_{mn}\in\mathcal{A}\\ m\sim M}} a_m b_n c_{mn} =& \frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn\in\mathcal{B}\\ m\sim M}} a_m b_n \\ &+ O\left(\Delta(k,y) \left\{ \frac{x}{k} + \frac{M^{\frac{1}{2}} x^{\frac{1}{2}}}{k^{\frac{1}{2}}} + \frac{x}{M^{\frac{1}{2}} k^{\frac{1}{2}}} + x^{\frac{1}{2}} \right\} (xM)^{o(1)} \right). \end{aligned}$$

Proof. We proceed as in the proof of Lemma 2.2.5 and it is enough to bound

$$R = \sum_{\chi\in\mathcal{X}_k^*} \sum_{\substack{mn\le x\\ m\sim M}} a_m b_n \chi(mn) \sum_{\substack{p\le y\\ (p,k)=1}} \bar{\chi}(a\bar{p}_k).$$

We apply

$$\sum_{a\le x/m} \frac{1}{\lfloor \frac{x}{M} \rfloor} \sum_{z=1}^{\lfloor \frac{x}{M} \rfloor} \mathbf{e}\left(\frac{z(a-n)}{\lfloor x/M \rfloor} \right) = \begin{cases} 1 & \text{if } n \le x/m, \\ 0 & \text{otherwise,} \end{cases}$$

to R in order to separate the dependence on m in the summation over n and assert

$$R \ll \log(x) \left| \sum_{\chi \in \mathcal{X}_k^*} \sum_{\substack{n \le x/M \\ m \sim M}} a_m b_n^* \chi(mn) \sum_{\substack{p \le y \\ (p,k)=1}} \bar{\chi}(a\bar{p}_k) \right|,$$

where $|b_n^*| = |b_n|$. By Cauchy inequality, Lemma 2.2.4 and our assumption, we bound

$$\begin{aligned} R &\ll (\log x) \max_{\chi \in \mathcal{X}_k^*} \left| \sum_{p \le y} \chi(p) \right| \cdot \sum_{\chi \in \mathcal{X}_k} \left| \sum_{m \sim M} a_m \chi(m) \right| \cdot \left| \sum_{n \le x/M} b_n^* \chi(n) \right| \\ &\ll (\log x) \Delta(k,y) \left(\sum_{\chi \in \mathcal{X}_k} \left| \sum_{m \sim M} a_m \chi(m) \right|^2 \cdot \sum_{\chi \in \mathcal{X}_k} \left| \sum_{n \le x/M} b_n^* \chi(n) \right|^2 \right)^{1/2} \\ &\ll (\log x) \Delta(k,y) \left(\varphi(k) \left(\frac{M}{k} + 1 \right) M \varphi(k) \left(\frac{x}{Mk} + 1 \right) \frac{x}{M} \right)^{1/2} (xM)^{o(1)} \\ &\ll \Delta(k,y) \varphi(k) \left(\frac{x}{k} + \frac{M^{\frac{1}{2}} x^{\frac{1}{2}}}{k^{\frac{1}{2}}} + \frac{x}{M^{\frac{1}{2}} k^{\frac{1}{2}}} + x^{\frac{1}{2}} \right) (xM)^{o(1)}, \end{aligned}$$

where we have used the bound $|a_m| \ll M^{o(1)}$ for $m \ll M$. □

2.2.3 Sieve method

In this section, we set $\mathcal{A} = (\xi_r)$ and $\mathcal{B} = (\eta_r)$ to be any general sequence of complex numbers support on $[1, x]$. For any positive integer s, we denote the sequence

$$\mathcal{A}_s = (\xi_{rs}).$$

Moreover, for any positive real numbers z, we define the weighted sifting function to be

$$\mathcal{S}(\mathcal{A}, z) = \sum_{\substack{r \le x \\ (r, P(z))=1}} \xi_r$$

where $P(w) = \prod_{p<w} p$ is the product of all primes less than w.

First, we recall a lemma which is essentially due to Buchstab [59, Eq. (13.58)], but we state it here with weighted sifting function.

Lemma 2.2.7 (Buchstab identity)**.** *For any $0 < z_2 \le z_1$, we have*

$$\mathcal{S}(\mathcal{A}, z_1) = \mathcal{S}(\mathcal{A}, z_2) - \sum_{z_2 \le p < z_1} \mathcal{S}(\mathcal{A}_p, p).$$

It is easy to see that the following variant of Harman sieve follows closely to the proof of [51, Lemma 2].

Proposition 2.2.8 (Harman sieve). *Suppose that for any $|a_m| \le \tau(m)$, $|b_n| \le \tau(n)$, we have for some $\lambda > 0$, $\alpha > 0$, $\beta \le \frac{1}{2}$, $M \ge 1$, that*

$$\sum_{\substack{\xi_{mn} \in \mathcal{A} \\ m \le M}} a_m \xi_{mn} = \lambda \sum_{\substack{\eta_{mn} \in \mathcal{B} \\ m \le M}} a_m \eta_{mn} + O(Y), \tag{2.2.2}$$

and

$$\sum_{\substack{\xi_{mn} \in \mathcal{A} \\ x^\alpha \le m \le x^{\alpha+\beta}}} a_m b_n \xi_{mn} = \lambda \sum_{\substack{\eta_{mn} \in \mathcal{B} \\ x^\alpha \le m \le x^{\alpha+\beta}}} a_m b_n \eta_{mn} + O(Y). \tag{2.2.3}$$

Then, if $|c_r| \le 1$, $x^\alpha < M$, $R < \min\{x^{1-\alpha}, M\}$ and $M \ge x^{1-\alpha}$ if $R > x^{\alpha+\beta}$, we have

$$\sum_{r \sim R} c_r \mathcal{S}(\mathcal{A}_r, x^\beta) = \lambda \sum_{r \sim R} c_r \mathcal{S}(\mathcal{B}_r, x^\beta) + O\left(Y \log^3 x\right).$$

2.3 Proof of Theorem 2.1.1

By Lemma 2.2.2 with $A = 3B + C + 3$, we have

$$\max_{\chi \in \mathcal{X}_k^*} \left| \sum_{p \le y} \chi(p) \right| \ll \frac{k^{\frac{1}{2}} y}{(\log y)^A}.$$

Set

$$\Delta(k, y) = \frac{k^{\frac{1}{2}} y}{(\log y)^A}.$$

To obtain our Type I estimate, we apply Lemma 2.2.5 to get

$$\sum_{\substack{c_{mn} \in \mathcal{A} \\ m \le M}} a_m c_{mn} = \frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn \in \mathcal{B} \\ m \le M}} a_m + O(R_1).$$

Here

$$\begin{aligned} R_1 &= \frac{M^{1+o(1)} k^{1+o(1)} y}{(\log y)^{3B+C+3}} \\ &\ll \frac{M^{1+o(1)} y}{(\log y)^{B+C+3}} \\ &\ll \frac{xy}{\varphi(k) \log^{C+3} y} \end{aligned}$$

whenever $M \ll x^{1-\varepsilon}$ for any fixed $\varepsilon > 0$ and x sufficiently large. We have used the assumption $k \ll \log^B y$.

To obtain our Type II estimate, we apply Lemma 2.2.6 at most $\log x$ times to get

$$\sum_{\substack{c_{mn}\in\mathcal{A}\\ m\leq M}} a_m b_n c_{mn} = \frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn\in\mathcal{B}\\ m\leq M}} a_m b_n + O(R_2)$$

where

$$\begin{aligned} R_2 &= \frac{y}{(\log y)^{3B+C+3}} \left(\frac{x}{k} + \frac{M^{\frac{1}{2}} x^{\frac{1}{2}}}{k^{\frac{1}{2}}} + \frac{x}{M^{\frac{1}{2}} k^{\frac{1}{2}}} + x^{\frac{1}{2}} \right) (xM)^{o(1)} \\ &\ll \frac{xy}{\varphi(k)\log^{C+3} y} \end{aligned}$$

whenever $1 \ll M \ll x$.

Set $\lambda = \#\mathcal{P}_k(y)/\varphi(k)$, $\alpha = \varepsilon > 0$, $\beta \in (0, \frac{1}{2}]$, $M = x^{1-\varepsilon}$, $Y = \frac{xy}{\varphi(k)\log^{C+3} y}$, $R = 1$, and $c_r = 1$ for $R \leq r < 2R$.

Appealing to the above estimates, we obtain our Type I & II estimate (2.2.2) and (2.2.3). Clearly $x^\alpha < M$ as ε is sufficiently small, therefore by appealing to the Harman sieve (Proposition 2.2.8) we get

$$\mathcal{S}(\mathcal{A}, x^\beta) = \lambda \mathcal{S}(\mathcal{B}, x^\beta) + O\left(Y \log^3 x\right),$$

and the result follows.

2.4 Proof of Theorem 2.1.2

By Lemma 2.2.3, we have

$$\max_{\chi\in\mathcal{X}_k^*} \left| \sum_{p\leq y} \chi(p) \right| \ll y^{\frac{1}{2}} \log ky.$$

Set

$$\Delta(k, y) = y^{\frac{1}{2}} \log ky.$$

By Lemma 2.2.5, we get our Type I estimate

$$\sum_{\substack{c_{mn}\in\mathcal{A}\\ m\leq M}} a_m c_{mn} = \frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn\in\mathcal{B}\\ m\leq M}} a_m + O(R_1),$$

where

$$\begin{aligned} R_1 &= M^{1+o(1)} k^{\frac{1}{2}+o(1)} y^{\frac{1}{2}} \log(ky) \\ &\ll x^{1-\varepsilon+o(1)} y\varphi^{-1}(k) \end{aligned}$$

whenever $M \ll x^{1+\frac{1}{2}(\vartheta_1-3\vartheta_2)-\varepsilon+o(1)}$.

By Lemma 2.2.6, we get our Type II estimate

$$\sum_{\substack{c_{mn}\in\mathcal{A}\\ m\sim M}} a_m c_{mn} = \frac{\#\mathcal{P}_k(y)}{\varphi(k)} \sum_{\substack{mn\in\mathcal{B}\\ m\sim M}} a_m + O(R_2).$$

Here

$$R_2 = y^{\frac{1}{2}}(\log ky)\left(\frac{x}{k} + \frac{M^{\frac{1}{2}}x^{\frac{1}{2}}}{k^{\frac{1}{2}}} + \frac{x}{M^{\frac{1}{2}}k^{\frac{1}{2}}} + x^{\frac{1}{2}}\right)(xM)^{o(1)}.$$

Since $2\vartheta_2 < 1 + \vartheta_1$, we get

$$R_2 \ll x^{1-\varepsilon+o(1)} y\varphi^{-1}(k)$$

whenever

$$x^{\vartheta_2-\vartheta_1+2\varepsilon+o(1)} \ll M \ll x^{1+\vartheta_1-\vartheta_2-2\varepsilon+o(1)}.$$

Set $\lambda = \#\mathcal{P}_k(y)/\varphi(k)$, $\alpha = \vartheta_2 - \vartheta_1 + 2\varepsilon + o(1)$, $\beta \in (0, \frac{1}{2}]$ with $\beta < 1 + 2(\vartheta_1 - \vartheta_2)$, $M = x^{1+\frac{1}{2}(\vartheta_1-3\vartheta_2)-\varepsilon+o(1)}$, $Y = x^{1-\varepsilon+o(1)}yk^{-1}$, $R = 1$ and $c_r = 1$ for $R \le r < 2R$.

Then considering above, we obtain our Type I & II estimate (2.2.2) and (2.2.3). Our assumption $5\vartheta_2 < 2 + 3\vartheta_1$ implies $x^\alpha < M$ for x sufficiently large. Therefore by the Harman sieve (Proposition 2.2.8) we get

$$\mathcal{S}(\mathcal{A}, x^\beta) = \lambda\mathcal{S}(\mathcal{B}, x^\beta) + O(Y)$$

where the $\log^3 x$ term is absorbed into Y.

2.5 Proof of Theorem 2.1.3

Let $\varepsilon' > 0$ with $\varepsilon = 3\varepsilon'$ so that $y = x^\varepsilon = x^{3\varepsilon'}$. By the proof of Theorem 2.1.2 (take $\varepsilon = \varepsilon'$ there), we have satisfactory Type I estimate as long as

$$M \ll x^{1-\frac{3}{2}\delta}.$$

The Type II estimate remains valid when

$$x^\delta \ll M \ll x^{1-\delta}.$$

Set $\lambda = \#\mathcal{P}_k(y)/\varphi(k)$ and $Y = x^{1-\varepsilon+o(1)}yk^{-1}$.

• Assume $\delta \in \left(\frac{1}{4}, \frac{1}{3}\right]$.

Write $X = x^{\frac{1}{2}}$, $z = x^{1-2\delta}$ then applying the Buchstab identity (Lemma 2.2.7), we assert

$$\mathcal{S}(\mathcal{A}, X) = \mathcal{S}(\mathcal{A}, z) - \sum_{z\le p<X} \mathcal{S}(\mathcal{A}_p, p)$$

$$= \Sigma_1 - \Sigma_2, \text{ say.}$$

Then by the Harman sieve, we have

$$\Sigma_1 = \lambda \mathcal{S}(\mathcal{B}, z) + O(Y).$$

We have $x^\delta \leq z < X \leq x^{1-\delta}$ since $\delta \in (\frac{1}{4}, \frac{1}{3}]$. Therefore Σ_2 is a Type II sum and we obtain

$$\Sigma_2 = \lambda \sum_{z \leq p < X} \mathcal{S}(\mathcal{B}_p, p) + O(Y).$$

Hence we get

$$\mathcal{S}(\mathcal{A}, X) = \lambda \mathcal{S}(\mathcal{B}, X) + O(Y).$$

• Assume $\delta \in \left(\frac{1}{3}, \frac{2}{5}\right)$.

Write $X = x^{\frac{1}{2}}$, $z = x^{1-2\delta}$, $T = x^\delta$. Then by the Buchstab identity

$$\begin{aligned}
\mathcal{S}(\mathcal{A}, X) &= \mathcal{S}(\mathcal{A}, z) - \sum_{z \leq p < X} \mathcal{S}(\mathcal{A}_p, p) \\
&= \mathcal{S}(\mathcal{A}, z) - \sum_{z \leq p < T} \mathcal{S}(\mathcal{A}_p, p) - \sum_{T \leq p < X} \mathcal{S}(\mathcal{A}_p, p) \\
&= \Sigma_1 - \Sigma_2 - \Sigma_3, \text{ say.}
\end{aligned}$$

The sums Σ_1 and Σ_3 can be estimated as above. For Σ_2, we apply Buchstab identity to get

$$\begin{aligned}
\Sigma_2 &= \sum_{z \leq p < T} \mathcal{S}(\mathcal{A}_p, z) - \sum_{z \leq q < p < T} \mathcal{S}(\mathcal{A}_{pq}, q) \\
&= \Sigma_4 - \Sigma_5, \text{ say.}
\end{aligned}$$

The sum Σ_4 can be estimated by the Harman sieve. We split Σ_5 and write

$$\begin{aligned}
\Sigma_5 &= \sum_{\substack{z \leq q < p < T \\ pq \leq x^{1-\delta}}} \mathcal{S}(\mathcal{A}_{pq}, q) + \sum_{\substack{z \leq q < p < T \\ pq > x^{1-\delta}}} \mathcal{S}(\mathcal{A}_{pq}, q) \\
&= \Sigma_6 + \Sigma_7, \text{ say.}
\end{aligned}$$

Since $T \leq z^2 \leq pq \leq x^{1-\delta}$, the sum Σ_6 can be estimated as a Type II sum.

For simplicity we drop Σ_7 and obtain

$$\begin{aligned}
\mathcal{S}(\mathcal{A}, X) &= \lambda(\Sigma_1^* - \Sigma_3^* - \Sigma_4^* + \Sigma_6^*) + \Sigma_7 + O(Y) \\
&\geq \lambda(\Sigma_1^* - \Sigma_3^* - \Sigma_4^* + \Sigma_6^* + \Sigma_7^* - \Sigma_7^*) + O(Y) \qquad (2.5.1) \\
&= \lambda \mathcal{S}(\mathcal{B}, X) - \lambda \Sigma_7^* + O(Y)
\end{aligned}$$

where Σ_j^* is Σ_j with $\mathcal{A}$ replaced by $\mathcal{B}$.

We note that if $pq^2 \geq x$ then Σ_7^* is zero, therefore we write

$$\Sigma_7^* = \sum_{\substack{z \leq q < p < T \\ x^{1-\delta}/q < p < x/q^2}} \mathcal{S}(\mathcal{B}_{pq}, q).$$

For the summands in Σ_7^*, we have

$$\begin{aligned}\mathcal{S}(\mathcal{B}_{pq}, q) &= (1+o(1))\frac{x}{pq\log q}\omega\left(\frac{\log(x/pq)}{\log q}\right) \\ &= (1+o(1))\frac{x}{pq\log q}\omega\left(\frac{\log x}{\log q}\left(1-\frac{\log p}{\log x}-\frac{\log q}{\log x}\right)\right)\end{aligned}$$

where ω is the Buchstab function. Therefore

$$\Sigma_7^* = (1+o(1))\sum_q\sum_p \frac{x}{pq\log q}\omega\left(\frac{\log x}{\log q}\left(1-\frac{\log p}{\log x}-\frac{\log q}{\log x}\right)\right)$$

where the summations over q, p satisfy

$$1-2\delta \leq \frac{\log q}{\log x} < \delta$$

and

$$\max\left\{\frac{\log q}{\log x}, 1-\delta-\frac{\log q}{\log x}\right\} < \frac{\log p}{\log x} < \min\left\{\delta, 1-2\frac{\log q}{\log x}\right\}.$$

By partial summation, we get

$$\Sigma_7^* = \frac{(1+o(1))x}{\log x} I$$

where

$$I = \int_{1-2\delta}^{\delta}\int_{\max\{\alpha_2, 1-\delta-\alpha_2\}}^{\min\{\delta, 1-2\alpha_2\}} \frac{1}{\alpha_2^2\alpha_1}\omega\left(\frac{1}{\alpha_2}(1-\alpha_1-\alpha_2)\right)\mathrm{d}\alpha_1\,\mathrm{d}\alpha_2.$$

Here we implicitly impose the condition

$$\min\{\delta, 1-2\alpha_2\} \geq \max\{\alpha_2, 1-\delta-\alpha_2\}$$

on I as Σ_7^* is non-negative.

We split I into two integrals

$$I = I_1 + I_2,$$

where

$$I_1 = \int_{\frac{1-\delta}{2}}^{\delta}\int_{\alpha_2}^{1-2\alpha_2} \frac{1}{\alpha_2^2\alpha_1}\omega\left(\frac{1}{\alpha_2}(1-\alpha_1-\alpha_2)\right)\mathrm{d}\alpha_1\,\mathrm{d}\alpha_2,$$

and

$$I_2 = \int_{1-2\delta}^{\frac{1-\delta}{2}} \int_{1-\delta-\alpha_2}^{\delta} \frac{1}{\alpha_2^2\alpha_1}\omega\left(\frac{1}{\alpha_2}(1-\alpha_1-\alpha_2)\right) \mathrm{d}\alpha_1\,\mathrm{d}\alpha_2.$$

Observe that the Buchstab function is bounded above by 1. When $\frac{1}{3} < \alpha_2 \leq \delta$ the integral $I_1 = 0$ therefore we bound

$$\begin{aligned} I_1 &\leq \int_{\frac{1-\delta}{2}}^{\frac{1}{3}} \int_{\alpha_2}^{1-2\alpha_2} \frac{1}{\alpha_2^2\alpha_1}\,\mathrm{d}\alpha_1\,\mathrm{d}\alpha_2 \\ &\leq \int_{\frac{3}{10}}^{\frac{1}{3}} \int_{\alpha_2}^{1-2\alpha_2} \frac{1}{\alpha_2^2\alpha_1}\,\mathrm{d}\alpha_1\,\mathrm{d}\alpha_2 \\ &= \frac{1}{3}(\log(256/81)-1) \leq 0.0503. \end{aligned}$$

Similarly we obtain

$$\begin{aligned} I_2 &\leq \int_{1-2\delta}^{\frac{1-\delta}{2}} \int_{1-\delta-\alpha_2}^{\delta} \frac{1}{\alpha_2^2\alpha_1}\,\mathrm{d}\alpha_1\,\mathrm{d}\alpha_2 \\ &\leq \int_{\frac{1}{5}}^{\frac{3}{10}} \int_{\frac{3}{5}-\alpha_2}^{\frac{2}{5}} \frac{1}{\alpha_2^2\alpha_1}\,\mathrm{d}\alpha_1\,\mathrm{d}\alpha_2 \\ &= \frac{5}{3}\log(9/8) \leq 0.1964. \end{aligned}$$

Appealing to (2.5.1), we have

$$\begin{aligned} \mathcal{S}(\mathcal{A}, X) &\geq \lambda(0.7533 + o(1))\frac{x}{\log x} + O(Y) \\ &\geq \frac{3xy}{4\varphi(k)(\log x)(\log y)} \end{aligned}$$

as $x \to \infty$.

CHAPTER 3

On Products of Primes and Square-free Integers in Arithmetic Progressions

"2 is a prime, 3 is a prime, 4 is a prime, 5 is a prime..."

–Billy

A conjecture of Erdös, Odlyzko, and Sárközy [29] asks if for every reduced residue class a modulo m can be represented as a product

$$p_1 p_2 \equiv a \pmod{m} \tag{3.0.1}$$

for two primes $p_1, p_2 \leq m$. Friedlander, Kurlberg, and Shparlinski [37] considered an average of (3.0.1) over a and m, and also various modification of (3.0.1). Garaev [39,40] improved on these modifications. Other interesting variants of (3.0.1) had also been considered by Baker [4], Ramaré & Walker [82], Shparlinski [87, 88], Walker [98].

In this paper, we want to bound the quantity

$$\#\left\{(p,s) \ : \ ps \equiv a \pmod{q}, p \leq P, s \leq S, \mu^2(s) = 1, (ps,q) = 1\right\}$$

for $(a,q) = 1$. This may also be viewed as a multiplicative analogue in the setting of finite fields of a result of Estermann [30]. Estermann [30] showed that all sufficiently large positive integer can be written as a sum of a prime and a square-free integer, see also [71,79]. Recently, Dudek [27] showed that this is true for all positive integer greater than two.

Our method uses the nice factoring property of the characteristic function for square-free integers

$$\mu^2(n) = \sum_{d^2 | n} \mu(d), \tag{3.0.2}$$

together with bounds for Kloosterman sums over primes supplied by Fourvy & Shparlinski [33], extending those previous result of Garaev [39].

3.1 Main result

We denote

$$\pi_q(P) = \#\left\{p \leq P \ : \ (p,q) = 1\right\}$$

to be the number of primes up to P coprime to q, and

$$s_q(S) = \#\left\{s \le S \ : \ \mu^2(s) = 1, (s,q) = 1\right\}$$

to be the number of square-free integers up to S coprime to q.

Finally, for $(a,q) = 1$, denote $\mathcal{N}^{\#}_{a,q}(P,S)$ by the quantity

$$\#\left\{(p,s) \ : \ ps \equiv a \pmod q, p \le P, s \le S, \mu^2(s) = 1, (ps,q) = 1\right\}.$$

Theorem 3.1.1. *For all fixed $A, \varepsilon > 0$ and $q \le P^{O(1)}$, we have*

$$\mathcal{N}^{\#}_{a,q}(P,S) = \frac{\pi_q(P)s_q(S)}{q} + O\left((PS)^{o(1)}S^{1/2}E\right),$$

uniformly for $q \ge 2$, $(a,q) = 1$, where

$$E = \begin{cases} Pq^{-1} & \text{if } q \le (\log P)^A, \\ \dfrac{P}{q^{3/4}} + \dfrac{P^{9/10}}{q^{3/8}} & \text{if } (\log P)^A < q < P^{3/4}, \\ \dfrac{P^{31/32}}{q^{(1-\varepsilon)/2}} + \dfrac{P^{5/6}}{q^{(3/4-\varepsilon)/2}} & \text{if } P^{3/4} \le q. \end{cases}$$

The main term in Theorem 3.1.1 is

$$\begin{aligned} \frac{\pi_q(P)s_q(S)}{q} &\gg \frac{1}{q}\frac{P}{\log P}\left(\frac{\varphi(q)S}{q} + O(\tau(q))\right) \\ &\gg P^{1+o(1)}Sq^{-1} \end{aligned}$$

since $q \le P^{O(1)}$. It follows that $\mathcal{N}^{\#}_{a,q}(P,S) > 0$ when $P \to \infty$ if either one of the following three conditions below holds.

(i) There exists an $\varepsilon > 0$ such that $S \gg P^{\varepsilon}$ and $q \le (\log P)^A$.

(ii) There exists an $\varepsilon > 0$ such that

$$S^2 \gg (PS)^{\varepsilon}q, \quad P^4S^{20} \gg (PS)^{\varepsilon}q^{25}, \text{ and } (\log P)^A < q < P^{3/4}.$$

(iii) There exists an $\varepsilon > 0$ such that

$$PS^{16} \gg (PS)^{\varepsilon}q^{16}, \quad P^4S^{12} \gg (PS)^{\varepsilon}q^{15}, \text{ and } P^{3/4} \le q.$$

3.2 Preparations

For $(a, q) = 1$, we denote the Kloosterman sum over primes by

$$S_q(a; x) = \sum_{\substack{p \le x \\ (p,q)=1}} \mathbf{e}_q(a\bar{p}).$$

Here $\bar{p}$ is the multiplicative inverse for p modulo q. Bounds in the case that q is prime had been obtained by Garaev [39]. Fouvry & Shparlinski [33] extended these results for composite q. We gather Theorem 3.1, 3.2, and Equation (3.13) from [33] into the following lemma.

Lemma 3.2.1. *For every fixed $A, \varepsilon > 0$, we have*

$$S_q(a; x) = O\left(B_q(x)\right),$$

uniformly for integer $q \ge 2$, $(a, q) = 1$, and $x \ge 2$. Here

$$B_q(x) = \begin{cases} x^{1+o(1)}q^{-1} & \text{if } q \le (\log x)^A, \\ \left(q^{-1/2}x + q^{1/4}x^{4/5}\right) x^{o(1)} & \text{if } (\log x)^A < q < x^{3/4}, \\ \left(x^{15/16} + q^{1/4}x^{2/3}\right) q^{\varepsilon} & \text{if } x^{3/4} \le q. \end{cases}$$

Denote

$$\mathcal{N}_{a,q}(P, S) = \#\left\{(p, s) \ : \ ps \equiv a \pmod q, p \le P, s \le S, (ps, q) = 1\right\}$$

for $(a, q) = 1$. Below, we provide an upper bounds for $\mathcal{N}_{a,q}(P, S)$.

Lemma 3.2.2. *For $q \le P^{O(1)}$, we have*

$$\mathcal{N}_{a,q}(P, S) \ll \left(\frac{PS}{q} + 1\right)(PS)^{o(1)}.$$

Proof. We count the number of solutions to $ps = a + kq$. Therefore we bound $k \ll (PS/q + 1)$. For each $a + kq$, the number of its distinct prime factors is no more than

$$\ll \log(kq) \ll \log(PS + q) \ll \log(PS) \ll (PS)^{o(1)},$$

from our upper bound on k. □

Denote

$$N_q(P, S) = \#\left\{(p, s) \ : \ p \le P, s \le S, (ps, q) = 1\right\}.$$

We relate the quantity $\mathcal{N}_{a,q}(P, S)$ with $N_q(P, S)$.

Lemma 3.2.3. *For all fixed $\varepsilon > 0$, we have*

$$\mathcal{N}_{a,q}(P,S) = \frac{N_q(P,S)}{q} + O\left(B_q(P)\right),$$

uniformly for $(a,q) = 1$, where B_q is defined as in Lemma 3.2.1.

Proof. We interpret this as a uniform distribution problem. Namely we consider

$$s \equiv a\bar{p} \pmod{q}$$

which fall in the interval $[1,S]$. The result follows from Lemma 3.2.1 applied with the Erdös-Turán inequality, see [25]. □

We provide a bound for $N_q(P,S)$.

Lemma 3.2.4. *For $q \leq P^{O(1)}$, we have*

$$N_q(P,S) = \frac{\varphi(q)\pi_q(P)S}{q} + O\left(P^{1+o(1)}\right).$$

Proof. Note the identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$\begin{aligned} N_q(P,S) &= \sum_{\substack{p \leq P \\ (p,q)=1}} 1 \sum_{\substack{s \leq S \\ (s,q)=1}} 1 \\ &= \pi_q(P) \sum_{s \leq S} \sum_{\substack{d|s \\ d|q}} \mu(d) \\ &= \pi_q(P) \left(\frac{\varphi(q)S}{q} + O(\tau(q)) \right) \\ &= \frac{\varphi(q)}{q}\pi_q(P)S + O\left(P^{1+o(1)}\right). \end{aligned}$$

□

We also provide a bound for $s_q(S)$.

Lemma 3.2.5. *We have*

$$s_q(S) = \frac{\varphi(q)}{q} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) S + O\left(S^{1/2} q^{o(1)}\right).$$

Proof. In a first step

$$\begin{aligned} s_q(S) &= \sum_{\substack{d\le S^{1/2}\\(d,q)=1}} \mu(d) \sum_{\substack{s\le S/d^2\\(s,q)=1}} 1 \\ &= \sum_{\substack{d\le S^{1/2}\\(d,q)=1}} \mu(d) \sum_{s\le S/d^2} \sum_{\substack{r\mid s\\ r\mid q}} \mu(r). \end{aligned}$$

Interchanging summations and completing the series, we get

$$\begin{aligned} s_q(S) &= \sum_{r\mid q} \mu(r) \sum_{\substack{d\le S^{1/2}\\(d,q)=1}} \mu(d) \left(\frac{S}{d^2 r} + O(1)\right) \\ &= \frac{\varphi(q)}{q} \left(\sum_{\substack{d=1\\(d,q)=1}}^{\infty} \frac{\mu(d)}{d^2} - \sum_{\substack{d> S^{1/2}\\(d,q)=1}} \frac{\mu(d)}{d^2} \right) S + O\left(S^{1/2}\tau(q)\right) \\ &= \frac{\varphi(q)}{q} \prod_{p\nmid q} \left(1-\frac{1}{p^2}\right) S + O\left(S^{1/2} q^{o(1)}\right), \end{aligned}$$

by noting that

$$\varphi(q) = q \prod_{p\mid q} \left(1-\frac{1}{q}\right) = q \sum_{r\mid q} \frac{\mu(r)}{r}.$$

□

3.3 Proof of Theorem 3.1.1

Appealing to (3.0.2), we obtain

$$\begin{aligned} \mathcal{N}^{\#}_{a,q}(P,S) &= \sum_{\substack{p\le P\\ ps\equiv a \,(\mathrm{mod}\ q)\\(ps,q)=1}} \sum_{s\le S} \mu^2(s) \\ &= \sum_{\substack{d\le S^{1/2}\\(d,q)=1}} \mu(d) \mathcal{N}_{ad^{-2},q}(P, S/d^2) \\ &= \Sigma_1 + \Sigma_2, \end{aligned}$$

where

$$\Sigma_1 = \sum_{\substack{d\le D\\(d,q)=1}} \mu(d) \mathcal{N}_{ad^{-2},q}(P, S/d^2),$$

and

$$\Sigma_2 = \sum_{\substack{D<d\leq S^{1/2}\\(d,q)=1}} \mu(d)\mathcal{N}_{ad^{-2},q}(P, S/d^2).$$

Here $D = D(P, S)$ is a parameter that will be chosen later.

By Lemma 3.2.2, we bound

$$\begin{aligned}\Sigma_2 &\ll \sum_{D<d\leq S^{1/2}} \left(\frac{PS}{d^2q} + 1\right)\left(\frac{PS}{d^2}\right)^{o(1)}\\ &\ll (PS)^{o(1)}\left(\frac{PS}{qD} + S^{1/2}\right).\end{aligned}$$

By Lemma 3.2.3 and 3.2.4 we get

$$\begin{aligned}\Sigma_1 &= \sum_{\substack{d\leq D\\(d,q)=1}} \mu(d)\left(\frac{N_q(P, S/d^2)}{q} + O\left(B_q(P)\right)\right)\\ &= \sum_{\substack{d\leq D\\(d,q)=1}} \mu(d)\left(\frac{\varphi(q)\pi_q(P)S}{q^2d^2} + O\left(P^{1+o(1)}q^{-1}\right)\right) + O\left(DB_q(P)\right).\end{aligned}$$

Completing the series in the summation over d, we assert

$$\begin{aligned}\Sigma_1 &= \frac{\varphi(q)\pi_q(P)S}{q^2}\left(\sum_{\substack{d=1\\(d,q)=1}}^{\infty}\frac{\mu(d)}{d^2} - \sum_{\substack{d>D\\(d,q)=1}}\frac{\mu(d)}{d^2}\right)\\ &\quad + O\left(D\left\{B_q(P) + P^{1+o(1)}q^{-1}\right\}\right)\\ &= \frac{\pi_q(P)}{q}\left(\frac{\varphi(q)S}{q}\sum_{\substack{d=1\\(d,q)=1}}^{\infty}\frac{\mu(d)}{d^2}\right) + O\left(\frac{PS}{qD} + DB_q(P)\right)\\ &= \frac{\pi_q(P)s_q(S)}{q} + O\left(\frac{S^{1/2}\pi_q(P)}{q^{1+o(1)}} + \frac{PS}{qD} + DB_q(P)\right),\end{aligned} \tag{3.3.1}$$

where the last line follows from applying Lemma 3.2.5.

Next we set

$$D = \begin{cases} S^{1/2}P^{o(1)} & \text{if } q \le (\log P)^A, \\ \left(\dfrac{PS}{Pq^{1/2} + q^{5/4}P^{4/5}}\right)^{1/2} P^{o(1)} & \text{if } (\log P)^A < q < P^{3/4}, \\ \left(\dfrac{PS}{q^{1+\varepsilon}\left(P^{15/16} + q^{1/4}P^{2/3}\right)}\right)^{1/2} & \text{if } P^{3/4} \le q. \end{cases}$$

Then the last two terms in (3.3.1) are equal and it follows

$$\mathcal{N}^{\#}_{a,q}(P,S) = \frac{\pi_q(P)s_q(S)}{q} + O\left(\left(\frac{S^{1/2}\pi_q(P)}{q^{1+o(1)}} + \frac{PS}{qD} + S^{1/2}\right)(PS)^{o(1)}\right).$$

If $q \le (\log P)^A$ then the error term above is majorised by

$$\left(\frac{PS^{1/2}}{q} + S^{1/2}\right)(PS)^{o(1)} \ll PS^{1/2}q^{-1}(PS)^{o(1)}.$$

If $(\log P)^A < q < P^{3/4}$ then the error term above is majorised by

$$\begin{aligned} &\left(\frac{P^{1/2}S^{1/2}\left(Pq^{1/2} + q^{5/4}P^{4/5}\right)^{1/2}}{q} + S^{1/2}\right)(PS)^{o(1)} \\ &\ll S^{1/2}\left(\frac{P}{q^{3/4}} + \frac{P^{9/10}}{q^{3/8}}\right)(PS)^{o(1)}. \end{aligned}$$

Lastly, if $P^{3/4} \le q$ then the error term above is majorised by

$$\begin{aligned} &\left(\frac{P^{1/2}S^{1/2}\left(q^{1+\varepsilon}\left\{P^{15/16} + q^{1/4}P^{2/3}\right\}\right)^{1/2}}{q} + S^{1/2}\right)(PS)^{o(1)} \\ &\ll S^{1/2}\left(\frac{P^{31/32}}{q^{(1-\varepsilon)/2}} + \frac{P^{5/6}}{q^{(3/4-\varepsilon)/2}}\right)(PS)^{o(1)}. \end{aligned}$$

The result follows.

CHAPTER 4

Smooth Square-free and Square-full Integers in Arithmetic Progressions

"I am thinking of a number, what is it?"

–Number theorist

We call a positive integer $n \geq 2$ to be y-smooth if all prime factors of n are no more than y. Studying the distribution of y-smooth numbers $n \leq x$ in progressions modulo an integer $q \geq 2$ has always been a very active subject of research, see [7, 24, 52, 76, 89] and references therein. For instance, as pointed out in [89], a very good level of distribution would imply the truth of Vinogradov's conjecture about the smallest quadratic non-residue.

As usual, we denote by $\psi(x, y; p, a)$ the number of positive integers $n \leq x$ which are y-smooth and satisfy $n \equiv a \pmod{p}$. Furthermore, we use $\psi^\sharp(x, y; p, a)$ for the number of those integers which are also square-free.

Due to its link with Euclidean prime generators, the positivity of $\psi^\sharp(x, y; p, a)$ in the special case of $y = p$ is of special interest, see [11]. Thus, following Booker and Pomerance [11], we use $M(p)$ to denote the least x such that $\psi^\sharp(x, p; p, a) > 0$ for every integer a. The quantity $M(p)$ has been considered in [76], where in particular the conjecture of Booker and Pomerance [11] that $M(p) = p^{O(1)}$ is established in a stronger form

$$M(p) \leq p^{3/2+o(1)},$$

for all primes p, and

$$M(p) \leq p^{4/3+o(1)},$$

for all, but a set of primes p of relative zero density.

Here we use similar ideas to obtain lower bounds on $\psi^\sharp(x, y; p, a)$ of essentially the right order of magnitude in a broader range of y. These bounds, even without taking into account the square-freeness condition, that is, using

$$\psi(x, y; p, a) \geq \psi^\sharp(x, y; p, a),$$

improve the range in which the result of Balog and Pomerance [7] applies.

Subsequently, we also address a question about square-full numbers in arithmetic progressions (that is numbers, which are divisible by squares of all their prime divisors). This question is significantly less studied, see however [18, 75, 78]. In particular, Chan [18] obtained an asymptotic formula for the number of square-full numbers in an arithmetic progression. However, due to a rather complicated structure of the main term, it is not immediately clear when the main term starts to exceed the error term. Here we consider a Linnik-type version of this question. Namely, using very different arguments compared to the case of square-free numbers (and also to [18]), we investigate the quantity

$$F(a,p) = \min\left\{n \in \mathbb{Z}/p\mathbb{Z} \ : \ n \text{ square-full}, n \equiv a \pmod p\right\}.$$

We note that the question about square-full numbers in arithmetic progressions is dual to the question on square-full, and more generally k-full numbers (that is, numbers divisible by k-th power of all their prime divisors) in short intervals, which has been considered in [64, 65]. In particular, it is shown in [65, Theorem 1] that infinitely many intervals of the form $(N^k, (N+1)^k)$ contain at least

$$M \geq \left(\left(\frac{3}{8} + o(1)\right)\frac{\log N}{\log\log N}\right)^{1/3} \tag{4.0.1}$$

k-full integers (but of course no perfect k-th powers). Here we use an opportunity to present in Appendix (section 4.5) an argument of V. Blomer which allows us to replace $1/3$ with $1/2$ in the lower bound of (4.0.1).

4.0.1 Main results for square-free numbers

All results in this chapter are joint work with M. Munsch & I. E. Shparlinski, and has been published in Mathematika, see [77].

We start with a lower bound on $\psi^\sharp(x,y;p,a)$ which holds for any prime p.

Theorem 4.0.1. *Fix $\beta \in (23/24, 1]$ and $\alpha \in (9/2 - 3\beta, 3\beta]$. For $x = p^{\alpha+o(1)}$ and $y = p^{\beta+o(1)}$ we have*

$$\psi^\sharp(x,y;p,a) \geq \frac{x^{1+o(1)}}{p}$$

as $p \to \infty$.

Taking $y = p^\beta$ with $23/24 < \beta \leq 1$ and $q = p$ in the main result of Balog & Pomerance [7] gives the existence of a p^β-smooth integer (not necessary square-free)

$$\begin{aligned} n &\leq p^{\max\{3\beta/2, 3/4+\beta\}+o(1)} \\ &= p^{3/4+\beta+o(1)}, \end{aligned}$$

since $\beta \leq 1$. We note that

$$9/2 - 3\beta < 3/4 + \beta,$$

under the condition $23/24 < \beta$. Therefore, Theorem 4.0.1 is always better than the bound given by the main result of Balog & Pomerance [7]. We remark that removing the square-free condition does not help us to improve on Theorem 4.0.1 due to the method used.

We also obtain a result for almost all primes. Firstly, let us define

$$\alpha_0(\beta) = \begin{cases} 5(2-\beta)/3 & \text{if } \beta \in (7/8, 13/14], \\ 12 - 11\beta & \text{if } \beta \in (13/14, 17/18], \\ (7-4\beta)/2 & \text{if } \beta \in (17/18, 25/26], \\ 16 - 15\beta & \text{if } \beta \in (25/26, 31/32], \\ (18-11\beta)/5 & \text{if } \beta \in (31/32, 41/42], \\ 20 - 19\beta & \text{if } \beta \in (41/42, 49/50], \\ (11-7\beta)/3 & \text{if } \beta \in (49/50, 61/62], \\ 24 - 23\beta & \text{if } \beta \in (61/62, 68/69], \\ 4/3 & \text{if } \beta \in (68/69, 1], \end{cases}$$

and the interval

$$\mathcal{I}(\beta) = (\alpha_0(\beta), \beta + 1)\,.$$

Theorem 4.0.2. *Fix $\beta \in (7/8, 1]$, $\alpha \in \mathcal{I}(\beta)$ and let $x = Q^{\alpha+o(1)}$, $y = Q^{\beta+o(1)}$. As $Q \to \infty$, we have*

$$\psi^\sharp(x, y; p, a) \geq \frac{x^{1+o(1)}}{p}$$

for all but $o(Q/\log Q)$ primes $p \in [Q, 2Q]$.

4.0.2 Main result for square-full numbers

First we observe that if a is a quadratic residue modulo p (or $a = 0$), then $a \equiv b^2 \pmod p$ for some integer $b \in [0, p-1]$ and so we have trivially $F(a, p) \leq (p-1)^2$ in this case.

To estimate $F(a, p)$ for a quadratic non-residue a we denote

$$\eta_0 = \frac{1}{4\sqrt{e}} \tag{4.0.2}$$

and recall that by the classical bound of Burgess [14] on the smallest quadratic non-residue n_p we have

$$n_p \leq p^\eta \tag{4.0.3}$$

for any $\eta > \eta_0$ and a sufficiently large p. Noticing that $a\overline{n}_p^3$ is a quadratic residue modulo p, we now obtain $F(a, p) \leq n_p^3(p-1)^2$. Hence, we have the trivial bound $F(a, p) \leq p^{2+3\eta_0+o(1)}$ for any a, which we unfortunately do not know how to improve. However, we remark that assuming the Vinogradov's conjecture that $n_p \leq p^{o(1)}$ (which is implied by the Generalised Riemann Hypothesis in the stronger form $n_p \ll \log^2 p$ proved by Ankeny

[1], see also [59, Section 5.9] for a discussion), we have the bound $F(a,p) \le p^{2+o(1)}$. Even though we cannot reach such a bound, we obtain an unconditional better bound for almost all $a \in \{0,\dots,p-1\}$.

We also note that from a result on counting square-full integers [90], for any set $\mathcal{A}$ of A distinct residues modulo p we have

$$\max_{a\in\mathcal{A}} F(a,p) \gg A^2,$$

where, as usual, we use $A \ll B$ and $B \gg A$ as an equivalent to the inequality $|A| \le cB$ with some constant $c > 0$, which occasionally, where obvious, may depend on the real parameter $\varepsilon > 0$. Our first theorem slightly refine this result.

Theorem 4.0.3. *For all but $o(p)$ quadratic non-residues $a \in [0, p-1]$, we have*

$$p^2 n_p f(p) \ll F(a,p) \le p^{2+\eta_0+o(1)}$$

for any function $f(p)$ such that $f(p) \to 0$ as $p \to \infty$ and

$$\max_{a \,(\mathrm{mod}\ p)} F(a,p) \gg p^2 n_p,$$

where n_p denotes the least quadratic non-residue modulo p.

Using the lower bound in Theorem 4.0.3, together with an unconditional result of Graham and Ringrose [43] on primes with large values of n_p and a conditional result on the Generalised Riemann Hypothesis (GRH) of Montgomery [72], we immediately derive

Corollary 4.0.4. *For infinitely many primes p we have*

$$\max_{a \,(\mathrm{mod}\ p)} F(a,p) \gg \begin{cases} p^2(\log p)(\log\log\log p) & \textit{unconditionally,} \\ p^2(\log p)(\log\log p) & \textit{under the GRH.} \end{cases}$$

In Section 4.1, we collect some results which will be used to prove the main results.

4.1 Preparations

4.1.1 Exponential sums with reciprocals of primes

For an integer k with $(k,p) = 1$ we use $\overline{k}$ to denote the multiplicative inverse of k modulo p, that is, the unique integer with

$$k\overline{k} \equiv 1 \pmod{p} \qquad \text{and} \qquad 1 \le \overline{k} < p.$$

It is convenient to introduce the quantity

$$B(p,L)=\begin{cases}L^{3/2}p^{1/8} & \text{if } L<p^{1/3},\\ L^{15/8} & \text{if } p^{1/3}\le L<p.\end{cases} \tag{4.1.1}$$

The following bound of double exponential sum over primes is a combination of [76, Lemma 3.5] for $L\le p^{1/3}$, and of [39, Lemma 2.4] for $p^{1/3}\le L<p$.

Lemma 4.1.1. *For any $L\le p$, we have*

$$\max_{(a,p)=1}\left|\sum_{\ell_1,\ell_2\in\mathcal{L}}\mathbf{e}_p\left(a\bar{\ell}_1\bar{\ell}_2\right)\right|\le B(p,L)p^{o(1)},$$

as $p\to\infty$, where $\mathcal{L}$ is the set of primes $\ell\in[L,2L]$.

4.1.2 Some congruences with products of primes

Let $N_{a,p}(L,h)$ to be the number of solutions in ℓ_1,ℓ_2, and u to the congruence

$$\ell_1\ell_2u\equiv a\pmod p,\qquad \ell_1,\ell_2\in\mathcal{L},\quad 1\le u\le h, \tag{4.1.2}$$

where h and L are two positive real numbers and $\mathcal{L}$ as in Lemma 4.1.1.

We now use Lemma 4.1.1 to derive an analogue of [76, Lemma 3.10] which also applies to $L\ge p^{1/3}$.

Lemma 4.1.2. *Let a be an integer and p prime with $(a,p)=1$. For $1\le h,L<p$, we have*

$$N_{a,p}(L,h)=\frac{K^2h}{p}+O\left(B(p,L)p^{o(1)}\right),$$

where $K=\#\mathcal{L}$ is the cardinality of $\mathcal{L}$ and $B(p,L)$ is defined by (4.1.1).

We also recall [76, Lemma 3.12].

Lemma 4.1.3. *Let a be an integer and p prime with $(a,p)=1$. For $1\le h,L<p$, we have*

$$N_{a,p}(L,h)\le\left(L^2h/p+1\right)p^{o(1)}.$$

Furthermore, let $N^\sharp_{a,p}$ count the number of solutions to the congruence (4.1.2) with square-free u. Following the proof of [76, Theorem 1.4], but using a more general bound of Lemma 4.1.2 instead of [76, Lemma 3.10] as well as Lemma 4.1.3, we derive

Lemma 4.1.4. *For any integer a and prime p with $(a,p)=1$ and reals h, D and L with*

$$1\le h,L<p\qquad\text{and}\qquad 1\le D\le h^{1/2},$$

we have

$$N^\sharp_{a,p}(L,h)=\frac{K^2h}{\zeta(2)p}+O\left(\left(\frac{L^2h}{Dp}+DB(p,L)+h^{1/2}\right)p^{o(1)}\right),$$

where $K = \#\mathcal{L}$ is the cardinality of $\mathcal{L}$ and $B(p, L)$ is defined by (4.1.1).

We also need the bound of [76, Lemma 3.14] on the number of solutions denoted by $Q_{a,p}(L, h)$ to the congruence

$$\ell_1\ell_2^2 v \equiv a \pmod p, \qquad \ell_1, \ell_2 \in \mathcal{L},\ 1 \le v \le h.$$

Lemma 4.1.5. *For any integer a and prime p with $(a, p) = 1$ and reals $1 \le L, h \le p$ with $2Lh \le p$, we have*

$$Q_{a,p}(L, h) \le (Lh/p + 1)\, Lp^{o(1)}.$$

It is shown in [76, Lemma 3.11], that for almost all primes p, the asymptotic formula of Lemma 4.1.2 can be improved as follows.

Lemma 4.1.6. *Let a be an integer with $(a, p) = 1$ and $1 \le h \le p$. Moreover, let $1 \le L \le Q$ and fix an integer $k \ge 1$. For all but $o(Q/\log Q)$ primes $p \in [Q, 2Q]$, we have*

$$N_{a,p}(L, h) = \frac{K^2 h}{p} + O\left(\left(L^{(3k-1)/2k} p^{1/2k} + L^{(4k-1)/(2k)}\right) p^{o(1)}\right)$$

as $Q \to \infty$.

Finally, we also recall [76, Lemma 3.13].

Lemma 4.1.7. *Let a be an integer, and real numbers $1 \le F, L, h \le p$ with $F, L^2 h < p$. As $Q \to \infty$, for all but $o(Q/\log Q)$ primes $p \in [Q, 2Q]$, we have*

$$R_{a,p}(F, L, h) \le \max\{F(L^2h)^{1/4}p^{-1/4}, F^{1/2}(L^2h)^{1/4}\}p^{o(1)}.$$

Here

$$R_{a,p}(F, L, h) = \sum_{F \le d \le 2F} N_{ad^{-2},p}(L, h).$$

4.1.3 Moments of character sums

Let $\mathcal{X}_p$ denote the set of all Dirichlet characters modulo p and let $\mathcal{X}_p^* = \mathcal{X}_p \setminus \{\chi_0\}$ denote the set of all non-principal Dirichlet characters modulo p.

We need the following result of Ayyad, Cochrane and Zheng [2, Theorem 2], see also [62] for a slightly sharper bound (which however does not change our final result).

Lemma 4.1.8. *For any integer $K \ge 1$, we have*

$$\sum_{\chi \in \mathcal{X}_p^*} \left| \sum_{1 \le n \le K} \chi(n) \right|^4 \le K^2 p^{1+o(1)}.$$

4.1.4 Quadratic non-residues in short intervals

Let $T_p(K)$ denote the number of quadratic non-residues modulo p in the interval $[1, K]$.

We need an extension of (6.0.4). The following bound is given in [8, Theorem 2.1].

Lemma 4.1.9. *For any real $\eta > \eta_0$, where η_0 is given by (4.0.2), there is a constant $c > 0$, such that for a sufficiently large p and $K \geq p^{\eta}$ we have*

$$T_p(K) \geq cK.$$

4.2 Proof of Theorem 4.0.1

For a sufficiently small $\varepsilon > 0$, we set

$$L = p^{(\alpha-\beta)/2-\varepsilon/2} \qquad \text{and} \qquad h = p^{\beta}.$$

Since $L \leq h \leq y$, $N^{\sharp}_{a,p}(L,h)$ counts a subset of y-smooth integers in an arithmetic progression. Noticing that $L^2 h \leq p^{\alpha-\varepsilon} = x^{1-\varepsilon+o(1)}$, we see that for a sufficiently large p we have

$$\begin{aligned} \psi^{\sharp}(x,y;p,a) &\geq N^{\sharp}_{a,p}(L,h) + O\left((h/p+1)\, Lp^{o(1)}\right) \\ &= N^{\sharp}_{a,p}(L,h) + O\left(Lp^{o(1)}\right), \end{aligned} \tag{4.2.1}$$

where we estimated the contribution coming from non-square-free products $\ell_1\ell_2 u$ (precisely products with $\ell_1 = \ell_2$ or with $\ell_1 \mid u$ or with $\ell_2 \mid u$) using Lemma 4.1.5 with h/L replacing h as in the end of the proof of [76, Theorem 1.4].

We use a crude estimate for the main term via

$$\begin{aligned} \frac{K^2 h}{p} &\sim \frac{L^2 h}{p\,(\log L)^2} \\ &= p^{\alpha-1-\varepsilon+o(1)}. \end{aligned} \tag{4.2.2}$$

Choosing

$$D = p^{\varepsilon/2}$$

and using Lemma 4.1.4, we derive

$$\begin{aligned} \psi^{\sharp}(x,y;p,a) &\gg \frac{K^2 h}{p} + O\left(\left(p^{\varepsilon/2}B(p,L) + L + h^{1/2}\right) p^{o(1)}\right) \\ &= \frac{K^2 h}{p} + O\left(\left(p^{\varepsilon/2}B(p,L) + h^{1/2}\right) p^{o(1)}\right) \end{aligned} \tag{4.2.3}$$

since $B(p,L)$ dominates L and the main term (4.2.2) dominates the first error term $L^2 h(Dp)^{-1}$ in Lemma 4.1.4.

To begin, we remark that the term $h^{1/2}$ in (4.2.3) is dominated by the main term due to the inequality $\alpha - 1 > 9/2 - 3\beta - 1 > \beta/2$ for $\beta \leq 1$. We split the discussion on the contribution of $B(p,L)$ into two cases depending on α.

Firstly, suppose that $\alpha \in (9/2-3\beta, 2/3+\beta]$. Since $\alpha \leq 2/3+\beta$, this implies $L < p^{1/3}$ and hence $B(p,L) = L^{3/2}p^{1/8}$ by (4.1.1). Therefore, recalling (4.2.3) and (4.2.2), we

obtain

$$\psi^\sharp(x,y;p,a) \gg p^{\alpha-1-\varepsilon+o(1)} + O\left(p^{3(\alpha-\beta)/4-\varepsilon/4+1/8+o(1)}\right). \tag{4.2.4}$$

For $\varepsilon > 0$ sufficiently small, we have $\alpha > 9/2 - 3\beta + 3\varepsilon$ which implies that the main term dominates trivially the remainder term in (4.2.4).

Secondly, assume that $\alpha \in (2/3+\beta, 3\beta]$. In particular, since $\beta \le 1$ we have

$$2/3 + \beta + \varepsilon \le \alpha < 3\beta < 2 + \beta + \varepsilon,$$

for $\varepsilon > 0$ chosen sufficiently small. Hence $p^{1/3} \le L < p$ and we have $B(p,L) = L^{15/8}$ by (4.1.1). Therefore, recalling (4.2.3) and (4.2.2), we obtain

$$\psi^\sharp(x,y;p,a) \ge p^{\alpha-1-\varepsilon+o(1)} + O\left(p^{15(\alpha-\beta)/16-7\varepsilon/16+o(1)}\right). \tag{4.2.5}$$

Notice that we have

$$\begin{aligned}\alpha &> 2/3 + \beta \\ &\ge 16 - 15\beta + 9\varepsilon + o(1)\end{aligned}$$

when $\beta \in (23/24, 1]$ and $\varepsilon > 0$ is sufficiently small. It follows that the main term dominates the remainder term in (4.2.5). Therefore, in all cases we conclude

$$\psi^\sharp(x,y;p,a) \ge p^{\alpha-\varepsilon-1+o(1)}.$$

Since this is valid for all sufficiently small $\varepsilon > 0$, the result follows.

4.3 Proof of Theorem 4.0.2

We follow the proof of [76, Theorem 1.6]. For $\varepsilon > 0$, we set

$$L = Q^{(\alpha-\beta)/2-\varepsilon/2}, \quad h = Q^\beta, \quad D = Q^{\varepsilon/2}, \quad E = Q^{(\alpha-1)/2}. \tag{4.3.1}$$

We note that $(\alpha-1)/2 > 0$ for $\alpha \in \mathcal{I}(\beta)$ and so $D < E$ if $\varepsilon > 0$ is sufficiently small. We also have $E < h^{1/2}$ since $\alpha < \beta + 1$.

Since $\alpha < \beta + 1 \le 3\beta$ in the range $\beta \in (7/8, 1]$, we get $L \le h$. In particular, we have as before the inequality (4.2.1).

By inclusion and exclusion, we have

$$\begin{aligned}N^\sharp_{a,p}(L,h) &= \sum_{d \le h^{1/2}} \mu(d) N_{ad^{-2},p}(L, h/d^2) \\ &= \Sigma_1 + \Sigma_2 + \Sigma_3,\end{aligned} \tag{4.3.2}$$

where

$$\Sigma_1 = \sum_{d \le D} \mu(d) N_{ad^{-2},p}(L, h/d^2),$$
$$\Sigma_2 = \sum_{D < d \le E} \mu(d) N_{ad^{-2},p}(L, h/d^2),$$
$$\Sigma_3 = \sum_{E < d \le h^{1/2}} \mu(d) N_{ad^{-2},p}(L, h/d^2).$$

To abstain from clutter, all the bounds below are valid for all but $o(Q/\log Q)$ primes $p \in [Q, 2Q]$.

Since $\alpha < \beta + 1 < 2 + \beta + \varepsilon + o(1)$ and $\beta \le 1$, we obtain respectively $L \le Q$ and $h \le p$. By Lemma 4.1.6

$$\Sigma_1 = \frac{K^2 h}{\zeta(2)p} + O\left(\frac{K^2 h}{Dp} + D\left(L^{(3k-1)/(2k)} p^{1/(2k)} + L^{(4k-1)/(2k)}\right) p^{o(1)}\right) \tag{4.3.3}$$

for any fixed positive integer k.

By Lemma 4.1.3 with h/d^2 replacing h there, we have

$$\Sigma_2 \le \left(\frac{L^2 h}{Dp} + E\right) p^{o(1)}. \tag{4.3.4}$$

We split Σ_3 into $O(\log p)$ sums with intervals of the form $[F, 2F]$ where $E \le F \le h^{1/2}$.

From the choice of E in (4.3.1) we see that

$$\begin{aligned} L^2 h/d^2 &\le L^2 h/F^2 \\ &\le L^2 h/E^2 \\ &< p, \end{aligned}$$

and hence by Lemma 4.1.7,

$$\begin{aligned} R_{a,p}(F, L, h/F^2) &\le \max\{F(L^2 h/F^2)^{1/4} p^{-1/4}, F^{1/2}(L^2 h/F^2)^{1/4}\} p^{o(1)} \\ &= (L^2 h)^{1/4} p^{o(1)}, \end{aligned}$$

since $F \le h^{1/2} \le p^{1/2}$. Therefore

$$\Sigma_3 \le (L^2 h)^{1/4} p^{o(1)}. \tag{4.3.5}$$

Substituting (4.3.3), (4.3.4), and (4.3.5) in (4.3.2), we obtain

$$N^{\sharp}_{a,p}(L, h) = \frac{K^2 h}{\zeta(2)p} + O\left(R p^{o(1)}\right),$$

where

$$R = D\left(L^{(3k-1)/(2k)}p^{1/(2k)} + L^{(4k-1)/(2k)}\right) + \frac{L^2h}{Dp} + E + (L^2h)^{1/4},$$

and the main term verifies an analogue of (4.2.2), precisely,

$$\begin{aligned}\frac{K^2h}{p} &\sim \frac{L^2h}{p\left(\log L\right)^2}\\ &= Q^{\alpha-1-\varepsilon+o(1)}.\end{aligned} \tag{4.3.6}$$

Notice that the choice of E in (4.3.1) implies that E is smaller than the main term (4.3.6). We now see from (4.3.6) that if

$$\alpha - 1 > \max\left\{\frac{3k-1}{2k}\frac{\alpha-\beta}{2} + \frac{1}{2k}, \frac{4k-1}{2k}\frac{\alpha-\beta}{2}, \frac{\alpha}{4}, \frac{\alpha-\beta}{2}\right\} \tag{4.3.7}$$

for some positive integer k, then for a sufficiently small $\varepsilon > 0$ the main term dominates the remainder term in (4.2.1) and the result follows.

Rearranging (4.3.7) gives

$$\alpha > \max\left\{\frac{(1-3k)\beta + 2 + 4k}{k+1}, (1-4k)\beta + 4k, 4/3, 2-\beta\right\}. \tag{4.3.8}$$

First, we remark that $2 - \beta \leq (1-4k)\beta + 4k$ since $\beta \leq 1$, and therefore we can discard $2-\beta$ from the maximum in (4.3.8).

Furthermore, for $k \leq 5$, we see that $4/3$ is dominated by the first term of the right hand side of (4.3.8). In this case, a quick computation shows that

$$\frac{(1-3k)\beta + 2 + 4k}{k+1} \geq (1-4k)\beta + 4k$$

if and only if $\beta \geq 1 - 1/2k^2$. Thus, in the interval $(1-1/2k^2, 1-1/2(k+1)^2]$, the maximum is given either by $\left((1-3k)\beta + 2 + 4k\right)/(k+1)$ or by $(1-4m)\beta + 4m$ with $m \geq k+1$. Since the function $f(z) = (1-4z)\beta + 4z$ is a monotonically increasing function of z, we check only the case $m = k+1$ and verify that

$$\begin{aligned}\frac{(1-3k)\beta + 2 + 4k}{k+1} &\geq f(k+1)\\ &= (1-4(k+1))\beta + 4(k+1)\end{aligned}$$

if and only if

$$\beta \geq \beta_0(k),$$

where

$$\beta_0(k) = 1 - \frac{1}{2(k^2+k+1)}.$$

Splitting the interval

$$\mathcal{I}_k = \left(1 - \frac{1}{2k^2}, 1 - \frac{1}{2(k+1)^2}\right]$$

into two intervals as follows

$$\mathcal{I}_k = \left(1 - \frac{1}{2k^2}, 1 - \frac{1}{2(k^2+k+1)}\right] \bigcup \left(1 - \frac{1}{2(k^2+k+1)}, 1 - \frac{1}{2(k+1)^2}\right]$$

and recalling that $k \leq 5$, we deduce after short computations the result for $\beta \leq \beta_0(5) = 61/62$.

For $k \geq 6$, noticing that $(1-4\beta) + 4k \geq 4/3$ in the range

$$\beta \leq 1 - \frac{1}{3(4k-1)},$$

we also deduce the case $\beta \in (61/62, 68/69]$.

For the remaining case $\beta \in (68/69, 1]$ and $k \geq 6$, we see that

$$\frac{(1-3k)\beta + 2 + 4k}{k+1} \leq 4/3.$$

Based on the above argument, we now give explicit choices of k and corresponding intervals which optimise our bound.

- If $\beta \in (7/8, 13/14]$, we take $k = 2$ and (4.3.8) simplifies to

$$\begin{aligned} \alpha &> \max\{5(2-\beta)/3, 8 - 7\beta, 4/3, 2-\beta\} \\ &= 5(2-\beta)/3. \end{aligned}$$

- If $\beta \in (13/14, 17/18]$, we take $k = 3$ and (4.3.8) simplifies to

$$\begin{aligned} \alpha &> \max\{(7-4\beta)/2, 12 - 11\beta, 4/3, 2-\beta\} \\ &= 12 - 11\beta. \end{aligned}$$

- If $\beta \in (17/18, 25/26]$, we take $k = 3$ and (4.3.8) simplifies to

$$\begin{aligned} \alpha &> \max\{(7-4\beta)/2, 12 - 11\beta, 4/3, 2-\beta\} \\ &= (7-4\beta)/2. \end{aligned}$$

- If $\beta \in (25/26, 31/32]$, we take $k = 4$ and (4.3.8) simplifies to

$$\alpha > \max\{(18-11\beta)/5, 16 - 15\beta, 4/3, 2-\beta\}$$

$$= 16 - 15\beta.$$

- If $\beta \in (31/32, 41/42]$, we take $k = 4$ and (4.3.8) simplifies to

$$\begin{aligned}\alpha &> \max\{(18 - 11\beta)/5, 16 - 15\beta, 4/3, 2 - \beta\} \\ &= (18 - 11\beta)/5.\end{aligned}$$

- If $\beta \in (41/42, 49/50]$, we take $k = 5$ and (4.3.8) simplifies to

$$\begin{aligned}\alpha &> \max\{(11 - 7\beta)/3, 20 - 19\beta, 4/3, 2 - \beta\} \\ &= 20 - 19\beta.\end{aligned}$$

- If $\beta \in (49/50, 61/62]$, we take $k = 5$ and (4.3.8) simplifies to

$$\begin{aligned}\alpha &> \max\{(11 - 7\beta)/3, 20 - 19\beta, 4/3, 2 - \beta\} \\ &= (11 - 7\beta)/3.\end{aligned}$$

- If $\beta \in (61/62, 68/69]$, we take $k = 6$ and (4.3.8) simplifies to

$$\begin{aligned}\alpha &> \max\{(26 - 17\beta)/7, 24 - 23\beta, 4/3, 2 - \beta\} \\ &= 24 - 23\beta.\end{aligned}$$

- If $\beta \in (68/69, 1]$, we take $k = 6$ and (4.3.8) simplifies to

$$\begin{aligned}\alpha &> \max\{(26 - 17\beta)/7, 24 - 23\beta, 4/3, 2 - \beta\} \\ &= 4/3.\end{aligned}$$

Therefore in all cases, where we also recall the condition $\alpha < \beta + 1$, we have

$$\psi^\sharp(x, y; p, a) \geq p^{\alpha - 1 - \varepsilon + o(1)}.$$

Since this is true for all $\varepsilon > 0$, the result follows immediately.

4.4 Proof of Theorem 4.0.3

Let M be a parameter which will be fixed later. We introduce the subset of residues modulo p

$$\mathcal{S} = \{a \ : \ a \text{ quadratic non-residue mod } p \text{ such that } F(a, p) \leq M\}.$$

Firstly, we remark that every square-full integer n can be written as $n = r^2 s$ with $s \mid r$. Furthermore, if a is a quadratic non-residue, we notice that s has to be a quadratic non-residue in this representation, in particular $s \geq n_p$.

Let us count the number of products $r^2 s \le M$ with $s \mid r$ and $s \ge n_p$, the smallest quadratic non-residue modulo p. Noticing that $r \le (M/s)^{1/2}$, we have at most $M^{1/2} s^{-3/2}$ possible values of r. Thus the number of different products $r^2 s$ is bounded by

$$\sum_{s \ge n_p} M^{1/2} s^{-3/2} \ll M^{1/2} n_p^{-1/2}.$$

This implies

$$\#\mathcal{S} \ll M^{1/2} n_p^{-1/2}.$$

Setting $M = p^2 n_p f(p)$, we get $\#\mathcal{S} = o(p)$ which concludes the proof of the lower bound. The assertion

$$\max_{a \,(\mathrm{mod}\ p)} F(a,p) \gg p^2 n_p$$

follows by the same argument by setting

$$\mathcal{S} = \{a \ : \ a \text{ quadratic non-residue modulo } p \ \}$$

and

$$M = \max_{a \in \mathcal{S}} F(a,p).$$

So we now turn our attention to the upper bound.

Clearly, if $a \equiv u^2 \,(\mathrm{mod}\ p)$, $0 \le u < p$, is quadratic residue (or $a = 0$), then $F(a,p) \le u^2 \le p^2$.

We now fix some $\varepsilon > 0$ and denote by $\mathcal{A}$ the set of quadratic non-residues modulo p for which $F(a,p) \ge p^{2+\eta_0+\varepsilon}$.

It is enough to show that the cardinality of $\mathcal{A}$ satisfies

$$\#\mathcal{A} = o(p). \tag{4.4.1}$$

Set

$$K = \left\lceil p^{\eta_0+\varepsilon/2} \right\rceil \qquad \text{and} \qquad U = \left\lceil p^{1-\eta_0} \right\rceil.$$

Let $\mathcal{N}$ be the set of quadratic non-residues modulo p in the interval $[1, K]$. In particular

$$\#\mathcal{N} = T_p(K).$$

Clearly for $a \in \mathcal{A}$ the congruence

$$a \equiv n^3 u^2 \ (\mathrm{mod}\ p), \ \ n \in \mathcal{N}, \ 1 \le u \le U, \tag{4.4.2}$$

has no solution. Thus expressing the number of solutions to (4.4.2) via characters we see that

$$\sum_{n\in\mathcal{N}}\sum_{1\le u\le U}\frac{1}{p-1}\sum_{\chi\in\mathcal{X}_p}\chi\left(\overline{a}n^3u^2\right)=0.$$

Summing over all $a\in\mathcal{A}$ and using the multiplicativity of characters, we arrive to

$$\sum_{\chi\in\mathcal{X}_p}\sum_{a\in\mathcal{A}}\overline{\chi}\left(a\right)\sum_{n\in\mathcal{N}}\chi^3\left(n\right)\sum_{u=1}^{U}\chi^2\left(u\right)=0, \tag{4.4.3}$$

where $\overline{\chi}$ denotes the complex conjugate character of χ.

The contribution to (4.4.3) from the principal character is clearly $\#\mathcal{A}T_p(K)U$.

Furthermore, since all elements of $\mathcal{A}$ are quadratic non-residues, the contribution to (4.4.3) from the quadratic character, that is, from the Legendre symbol is

$$\begin{aligned}\sum_{a\in\mathcal{A}}\left(\frac{a}{p}\right)\sum_{n\in\mathcal{N}}\left(\frac{n}{p}\right)^3\sum_{u=1}^{U}\left(\frac{u}{p}\right)^2&=\sum_{a\in\mathcal{A}}(-1)\sum_{n\in\mathcal{N}}(-1)^3\sum_{u=1}^{U}1\\&=\#\mathcal{A}T_p(K)U.\end{aligned}$$

This allows us to write (4.4.3) as

$$2\#\mathcal{A}T_p(K)U=-\sum_{\chi\in\mathcal{X}_p^\sharp}\sum_{a\in\mathcal{A}}\overline{\chi}\left(a\right)\sum_{n\in\mathcal{N}}\chi^3\left(n\right)\sum_{u=1}^{U}\chi^2\left(u\right) \tag{4.4.4}$$

with $\mathcal{X}_p^\sharp$ being the subset of $\mathcal{X}_p^*$ where we removed the quadratic character.

For $\chi\in\mathcal{X}_p^\sharp$ we have by definition $\chi^2\neq\chi_0$. Furthermore, each character from $\mathcal{X}_p^*$ occurs at most twice as χ^2 and each character from $\mathcal{X}_p$ (including also χ_0 in this case) occurs at most three times as χ^3 for $\chi\in\mathcal{X}_p^\sharp$.

Using the Hölder's inequality, we now derive from (4.4.4) that

$$2\#\mathcal{A}T_p(K)U\le\Sigma_1^{1/2}\Sigma_2^{1/4}\Sigma_3^{1/4} \tag{4.4.5}$$

where

$$\begin{aligned}\Sigma_1&=\sum_{\chi\in\mathcal{X}_p^\sharp}\left|\sum_{a\in\mathcal{A}}\overline{\chi}\left(a\right)\right|^2\le\sum_{\chi\in\mathcal{X}_p}\left|\sum_{a\in\mathcal{A}}\chi\left(a\right)\right|^2,\\\Sigma_2&=\sum_{\chi\in\mathcal{X}_p^\sharp}\left|\sum_{n\in\mathcal{N}}\chi\left(n\right)^3\right|^4\le3\sum_{\chi\in\mathcal{X}_p}\left|\sum_{n\in\mathcal{N}}\chi\left(n\right)\right|^4,\\\Sigma_3&=\sum_{\chi\in\mathcal{X}_p^\sharp}\left|\sum_{u=1}^{U}\chi\left(u\right)^2\right|^4\le2\sum_{\chi\in\mathcal{X}_p^*}\left|\sum_{u=1}^{U}\chi\left(u\right)\right|^4,\end{aligned}$$

and the upper bounds come from the discussion above. We now see by the orthogonality of characters that we have

$$\Sigma_1 \leq (p-1)\#\mathcal{A}. \tag{4.4.6}$$

For Σ_2, using again the orthogonality of characters, we write

$$\begin{aligned}\Sigma_2 &= 3(p-1)\#\left\{(n_1,n_2,n_3,n_4)\in\mathcal{N}\ :\ n_1n_2\equiv n_3n_4 \pmod p\right\}\\ &\leq 3(p-1)\#\left\{(n_1,n_2,n_3,n_4)\in[1,K]\ :\ n_1n_2\equiv n_3n_4 \pmod p\right\}\\ &= 3\sum_{\chi\in\mathcal{X}_p}\left|\sum_{n=1}^{K}\chi(n)\right|^4\\ &= 3K^4+\sum_{\chi\in\mathcal{X}_p^*}\left|\sum_{n=1}^{K}\chi(n)\right|^4.\end{aligned}$$

Applying Lemma 4.1.8 and using that $K^2\leq p$ provided that ε is small enough, we derive

$$\Sigma_2 \leq K^2p^{1+o(1)}. \tag{4.4.7}$$

Finally, we also estimate Σ_3, directly by Lemma 4.1.8 getting

$$\Sigma_3 \leq U^2p^{1+o(1)}. \tag{4.4.8}$$

Substituting (4.4.6), (4.4.7), and (4.4.8) in (4.4.5), we now derive

$$\#\mathcal{A}T_p(K)U \leq (\#\mathcal{A})^{1/2}K^{1/2}U^{1/2}p^{1+o(1)}$$

which together with Lemma 4.1.9 yields

$$\begin{aligned}\#\mathcal{A} &\leq K^{-1}U^{-1}p^{2+o(1)}\\ &= p^{1-\varepsilon/2+o(1)}.\end{aligned}$$

We now see that (4.4.1) holds which concludes the proof.

4.5 Appendix: Short intervals with many k-full numbers

Theorem 4.5.1. *For any fixed integer $k\geq 2$, there are infinitely many N, such that the open interval $\left(N^k,(N+1)^k\right)$ contains at least*

$$M \geq \sqrt{\left(\frac{k}{2(k+1)}+o(1)\right)\frac{\log N}{\log\log N}}$$

k-full integers.

Proof. Let $1 < d_1 < \ldots < d_{2\ell}$ be the first 2ℓ square-free integers greater than 1, so we have $d_j = \pi^2 j/6 + o(j)$ and $d_j \le 4\ell$, provided that ℓ is large enough.

Let $\alpha_j = d_j^{-(k+1)/k}$ for $j = 1, \ldots, 2\ell$. We define

$$R = \left(k2^{k-1}(4\ell)^{(k+1)/k}\right)^{2\ell}$$

and let q be the smallest integer

$$q \ge R$$

for which, for some integers r_j,

$$\left|\alpha_j - \frac{r_j}{q}\right| \le \frac{1}{q^{1+1/2\ell}} \tag{4.5.1}$$

for $j = 1, \ldots, 2\ell$. We see that $q \le Q$, where $Q = C(\alpha_1, \delta)^{-2\ell} R^{2\ell(1+\delta)}$ for some constant $C(\alpha_1, \delta) > 0$ depending only on α_1 and δ. Indeed, otherwise applying the Dirichlet Approximation Theorem, see [86, Corollary 1B, p. 27], we conclude that

$$\left|\alpha_j - \frac{r_j}{s}\right| \le \frac{1}{sQ^{1/2\ell}}$$

for $j = 1, \ldots, 2\ell$ and some positive integer $s \le Q$. Due to the minimality condition on q, we have $s \le R$. On the other hand, by the Roth Theorem, see [86, Theorem 2A, p. 116], we have

$$\frac{C(\alpha_1, \delta)}{s^{2+\delta}} < \left|\alpha_1 - \frac{r_1}{s}\right| \le \frac{1}{sQ^{1/2\ell}}.$$

Therefore

$$\begin{aligned} s &> \left(C(\alpha_1, \delta)Q^{1/2\ell}\right)^{1/(1+\delta)} \\ &= R, \end{aligned}$$

which is impossible.

We see from (4.5.1) that, for $j = 1, \ldots, 2\ell$,

$$\begin{aligned} \left|q - d_j^{(k+1)/k} r_j\right| &\le \frac{(4\ell)^{(k+1)/k}}{q^{1/2\ell}} \\ &\le 1, \end{aligned} \tag{4.5.2}$$

provided that ℓ is large enough. Therefore,

$$\begin{aligned} d_j^{(k+1)/k} r_j &= \alpha_j^{-1} r_j \\ &\le q + 1, \end{aligned}$$

for $j = 1, \dots, 2\ell$. We now derive using (4.5.2),

$$\begin{aligned}
\left|q^k - d_j^{k+1} r_j^k\right| &= \left|q - d_j^{(k+1)/k} r_j\right| \cdot \sum_{\nu=0}^{k-1} q^{k-1-\nu} \left(d_j^{(k+1)/k} r_j\right)^\nu \\
&\le k(q+1)^{k-1} \left|q - d_j^{(k+1)/k} r_j\right| \\
&\le \frac{k(4\ell)^{(k+1)/k}(q+1)^{k-1}}{q^{1/2\ell}} \\
&< \frac{k2^{k-1}(4\ell)^{(k+1)/k}}{q^{1/2\ell}} q^{k-1} \\
&\le \frac{k2^{k-1}(4\ell)^{(k+1)/k}}{R^{1/2\ell}} q^{k-1}.
\end{aligned}$$

Recalling the choice of R we now see that

$$\left|q^k - d_j^{k+1} r_j^k\right| < q^{k-1}.$$

Therefore one of the intervals $((q-1)^k, q^k)$ or $(q^k, (q+1)^k)$ contains at least $M \ge \ell$ of the integers $d_j^{k+1} r_j^k$, for $j = 1, \dots, 2\ell$, which are obviously pairwise distinct (because d_j is square-free for all $j = 1, \dots, 2\ell$) and k-full. We now have

$$\begin{aligned}
q &\le Q \\
&= C(\alpha_1, \delta)^{-2\ell} R^{2\ell(1+\delta)} \\
&\le C(\alpha_1, \delta)^{-2\ell} \left(k2^{k-1}(4\ell)^{(k+1)/k}\right)^{4\ell^2(1+\delta)} \\
&= \exp\left(\left(4(k+1)k^{-1}(1+\delta) + o(1)\right) \ell^2 \log \ell\right).
\end{aligned}$$

Hence, since k is fixed,

$$\ell^2 \log \ell \ge \left(\frac{k}{4(k+1)(1+\delta)} + o(1)\right) \log q.$$

In particular, considering two cases

$$\log \ell \ge \frac{1}{2} \log \log q \qquad \text{and} \qquad \log \ell < \frac{1}{2} \log \log q,$$

this implies that

$$M \ge \ell \ge \left(\left(\frac{k}{2(k+1)(1+\delta)}\right)^{1/2} + o(1)\right) \left(\frac{\log q}{\log \log q}\right)^{1/2}.$$

Recalling that δ is arbitrary, the proof is complete. □

CHAPTER 5

A Relaxation of Goldbach's Conjecture

"Meow"

–Dog

The Goldbach conjecture states that every even integer greater than two can be expressed as the sum of two primes. Although this remains an open problem due to the parity phenomenon, there are various progress and relaxations which contributes toward this direction.

Table 5.1 lists all even integers (but two) up to 102, and to each even integer n, the entires of the associated prime tuple (p, q) can be summed to give n.

n	(p, q)	n	(p, q)	n	(p, q)	n	(p, q)	n	(p, q)
4	$(2, 2)$	6	(3,3)	8	(5,3)	10	(7,3)	12	(7,5)
14	$(11, 3)$	16	(13,3)	18	(13,5)	20	(17,3)	22	(19,3)
24	$(19, 5)$	26	(23,3)	28	(23,5)	30	(23,7)	32	(29,3)
34	$(31, 3)$	36	(31,5)	38	(31,7)	40	(37,3)	42	(37,5)
44	$(41, 3)$	46	(43,3)	48	(43,5)	50	(47,3)	52	(47,5)
54	$(47, 7)$	56	(53,3)	58	(53,5)	60	(53,7)	62	(59,3)
64	(61,3)	66	(61,5)	68	(61,7)	70	(67,3)	72	(67,5)
74	(71,3)	76	(73,3)	78	(73,5)	80	(73,7)	82	(79,3)
84	(79, 5)	86	(83,3)	88	(83,5)	90	(83,7)	92	(89,3)
94	(89,5)	96	(89,7)	98	(79,19)	100	(97,3)	102	(97,5)

Table 5.1: The Goldbach conjecture manually checked up to 102.

Mordern sieve method can be traced back to the earlier works of Brun. In 1920, Brun [13] showed that every sufficiently large even integer can be written as the sum of two numbers which have together at most nine prime divisors. Later, the celebrated result of Chen [19] established that every sufficiently large even integer can be written as the sum of a prime and a number with at most two prime factors.

Initiated by Linnik [67] in 1953, he showed that every sufficiently large even integer can be written as a sum of two primes and at most K powers of two, where K is an absolute constant although non-explicit. Many authors had made K explicit where the best known result $K = 12$ is due to Liu & Lü [69], improving the remarkable result $K = 13$ by Heath-Brown & Puchta [55].

Another relaxation is the ternary Goldbach conjecture which states that all odd integer greater than five is the sum of three primes. Vinogradov [97] developed a way to estimate

sums over primes which combined with the circle method showed the ternary Goldbach conjecture is true for all large odd integer greater than $C > 0$. Recently, Helfgott [57] completed the proof of ternary Goldbach conjecture by sufficiently reducing the size C and verified that no counterexample exists below C.

We also have results when we replace one of the primes in the Goldbach conjecture by a square-free integer. Estermann [30] obtained an asymptotic formula for the number of representation of a sufficently large integer as the sum of a prime and a square-free number. Later, Page [79] improved on the error term of Estermann [30] and Mirsky [71] improved and extended these results to count the number of represention of an integer as the sum of a prime and a k-free number. Recently, Dudek [27], by tools of explicit number theory, demonstrated that every integer greater than two can be the sum of a prime and a square-free integer.

In this paper we are motivated by a question posed in the PhD thesis of Dudek [26, Chapter 6, Problem 8]. Specifically Dudek asked for $(a, q) = 1$, can all sufficiently large integer without local obstruction be a sum of a prime p such that $p \equiv a \pmod q$ and a square-free integer.

There are mainly three advanced techniques for attacking certain binary additive problems: the circle method [95], sieve methods [36] and the dispersion method of Linnik [68]. Our method applied here is due to Ramaré [81] on his notion of local model and can be viewed as an abstract circle method. We remarked that Heath-Brown [54] had already notice this connection for his alternate prove of Vinogradov's three prime theorem [97].

Lastly the techniques used here may be adapted for various other binary additive problems. In particular, the author expects that it should be possible to prove an asymptotic bound for the number of representation of an integer as the sum of a square-free integer and a prime p such that $p + 1$ is square-free.

Before we dive into the main result, we will use the following notation in this chapter:

i) $\sum_{a=1}^{n}{}^{*}$ is a summation over the integers in $[1, n]$ coprime to n,

ii) $c_r(k)$ is the Ramanujan sum $\sum_{a=1}^{r}{}^{*} \mathbf{e}_r(ka)$,

iii) $\mathbb{1}_S$ is 1 if S is true and 0 otherwise,

iv) $a \equiv b[k]$ means $a \equiv b \pmod k$,

v) $\mathcal{L}$ is $\log N$.

5.1 Main result

We denote

$$\mathcal{R}_{a,q}(N) = \sum_{\substack{N=p+n \\ p\equiv a[q]}} \mu^2(n) \log p$$

to be the weighted number of representations for N as the sum of a prime congruent to a modulo q and a square-free integer.

We now state a bound for $\mathcal{R}_{a,q}(N)$ which is uniform for small q.

Theorem 5.1.1. *Let $C_1, C_2 > 0$ then we have*

$$\mathcal{R}_{a,q}(N) = \mathfrak{S}_{a,q}(N)N\left\{1 + O_{C_1,C_2}\left(\mathcal{L}^{-C_2}\right)\right\}$$

uniformly for $(a,q) = 1$ and $q \leq \mathcal{L}^{C_1}$ where $\mathcal{L} = \log N$. The singular series is given by

$$\mathfrak{S}_{a,q}(N) = \frac{6}{\varphi(q)\pi^2} \prod_{\substack{p=2\\(p,q)=1}}^{\infty} \left(1 + \frac{c_p(N)}{(p^2-1)(p-1)}\right) \prod_{p\parallel q} \left(1 - \frac{c_p(N-a)}{p^2-1}\right)$$
$$\times \prod_{p^2|q} \left(1 - \frac{c_p(N-a) + c_{p^2}(N-a)}{p^2-1}\right).$$

The implied constant in the reminder term is ineffective because the Siegel-Walfisz Theorem (Lemma 5.3.5) is used. In view of Lemma 5.3.3, we can rewrite the *singular series* $\mathfrak{S}_{a,q}(N)$ in a more rudimentary form

$$\frac{\mu^2\left((q,N-a)\right)6}{\varphi(q)\pi^2} \prod_{\substack{p|N\\p\nmid q}} \left(1 + \frac{1}{p^2-1}\right) \prod_{\substack{p=2\\p\nmid Nq}}^{\infty} \left(1 - \frac{1}{(p^2-1)(p-1)}\right) \prod_{\substack{p\parallel q\\p|(N-a)}} \left(1 - \frac{1}{p+1}\right)$$
$$\times \prod_{\substack{p\parallel q\\p\nmid(N-a)}} \left(1 + \frac{1}{p^2-1}\right) \prod_{\substack{p^2|q\\p\nmid(N-a)}} \left(1 + \frac{1}{p^2-1}\right) \prod_{\substack{p^2|q\\p\parallel(N-a)}} \left(1 + \frac{1}{p^2-1}\right).$$

Observe that when we take $q = 1$ in Theorem 5.1.1, we obtain a special case of Mirsky [71] (after weighing but with a weaker error term). Indeed our *singular series* simplifies to

$$\mathfrak{S}_{0,1}(N) = \prod_{p=2}^{\infty} \left(\frac{p^2-1}{p^2}\right) \prod_{\substack{p=2\\p|N}}^{\infty} \left(1 + \frac{1}{p^2-1}\right) \prod_{\substack{p=2\\p\nmid N}}^{\infty} \left(1 - \frac{1}{(p^2-1)(p-1)}\right)$$
$$= \prod_{\substack{p=2\\p\nmid N}}^{\infty} \left(\frac{p^2-1}{p^2} - \frac{1}{p^2(p-1)}\right)$$
$$= \prod_{\substack{p=2\\p\nmid N}}^{\infty} \left(1 - \frac{1}{p(p-1)}\right).$$

Lastly if $p_1^2 \mid q$ and $p_1^2 \mid (N-a)$ then it follows for all primes $p \equiv a[q]$ that $N-p$ is never square-free and hence $\mathcal{R}_{a,q}(N) = 0$. This coincide exactly to the case when $\mathfrak{S}_{a,q}(N)$ vanishes.

A neat corollary of Theorem 5.1.1 is the following.

Corollary 5.1.2. *Fix $k \in \mathbb{N}$, let $q = 10^k$, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ and write the base 10 decimal representation of a as $a_1 \dots a_\ell$. If N is sufficiently large and $(q, N-a)$ is square-free then N can be written as $N = s + p$ where s is square-free and p is a prime such that the last ℓ digits of p is $a_1 \dots a_\ell$.*

5.2 Outline of Method

For a more thorough exposition, see [81, Chapters 1,4 &17].

Our method will model that of [81, Chapter 19] where in there Ramaré proved an asymptotic bound for the number of representations of a sufficiently large integer to be the sum of two square-free integers. We note that results of that kind had already been obtained by Evelyn & Linfoot [32] and later simplified by Estermann [31]. The best result is achieved by Brüdern & Perelli [12].

We press forward and recall the definition of *local* and *global* product, see (5.3.5) and (5.3.8) respectively.

Let $\mathcal{H}$ be an inner product space over $\mathbb{C}$. Define $\mathcal{H}$ as an *almost orthogonal system* by the following collection of information:

(i) let I be a finite indexing set,
(ii) a finite family $(\phi_i^*)_{i\in I}$ of elements of $\mathcal{H}$,
(iii) a finite family $(M_i)_{i\in I}$ of positive real numbers,
(iv) a finite family $(\omega_{i,j})_{i,j\in I}$ of complex numbers with $\omega_{j,i} = \overline{\omega_{i,j}}$

and

$$\left\| \sum_{i\in I} \xi_i \phi_i^* \right\|^2 \leq \sum_{i\in I} M_i |\xi_i|^2 + \sum_{i,j\in I} \xi_i \overline{\xi_j} \omega_{i,j}$$

for all $(\xi_i)_{i\in I} \in \mathbb{C}^I$.

The special case of choosing an orthogonal basis is enlightening. If $(\phi_i^*)_{i\in I}$ are orthogonal then we may take $M_i = \|\phi_i^*\|^2$ and $\omega_{i,j} = [\phi_i^*|\phi_j^*]$ for $i, j \in I$.

We recall the von-Mangoldt function Λ defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Let $(a, q) = 1$ and set

$$f(n) = \Lambda(n)\mathbb{1}_{n\equiv a[q]} \qquad \text{and} \qquad g(n) = \mu^2(N-n)$$

for $n \leq N$. Observe that the product gives

$$[f|g] = \sum_{n\leq N} \Lambda(n)\mathbb{1}_{n\equiv a[q]} \cdot \mu^2(N-n)$$

$$= \sum_{\substack{N=n_1+n_2 \\ n_1 \equiv a[q]}} \Lambda(n_1)\mu^2(n_2)$$

is the weighted number of representations for N to be a sum of a prime power congruent to a modulo q and a square-free integer. Our ultimate goal is to compute $[f|g]$ and we shall use the notion of local model.

Indeed let $\mathcal{Q} \subseteq \mathbb{N}$ be a carefully chosen set of moduli. We construct two local models $(\rho_q^*)_{q\in\mathcal{Q}}$ and $(\gamma_q^*)_{q\in\mathcal{Q}}$ to approximate f and g respectively, and in some sense they are made to copy the distribution of f and g in arithmetic progression respectively.

Next we take $(\frac{1}{2}\Delta_q^*)_{q\in\mathcal{Q}}$ to be essentially the union of some linear combination of $(\rho_q^*)_{q\in\mathcal{Q}}$ and $(\gamma_q^*)_{q\in\mathcal{Q}}$. This will be the local model accountable for both f and g. Furthermore for all $q_1, q_2 \in \mathcal{Q}$, we set $M_{q_1} = \sum_{t\in\mathcal{Q}} |[\Delta_t^*|\Delta_{q_1}^*]|$ and $\omega_{q_1,q_2} = 0$, see [81, Lemma 1.1]. This gives rise to an *almost orthogonal system* and in particular will imply

$$\left[f - \frac{1}{2}\sum_{q\in\mathcal{Q}} \xi_q(f)\Delta_q^* \middle| g - \frac{1}{2}\sum_{q\in\mathcal{Q}} \xi_q(g)\Delta_q^*\right]$$

is small in a suitable sense. The construction will also secure $[\Delta_{q_1}^*|\Delta_{q_2}^*]$ to be small when $q_1 \neq q_2$. Expanding the inner product, we have

$$\begin{aligned}\left[f - \frac{1}{2}\sum_{q\in\mathcal{Q}} \xi_q(f)\Delta_q^* \middle| g - \frac{1}{2}\sum_{q\in\mathcal{Q}} \xi_q(g)\Delta_q^*\right] &= [f|g] - \frac{1}{2}\sum_{q\in\mathcal{Q}} \xi_q(f)[\Delta_q^*|g] - \frac{1}{2}\sum_{q\in\mathcal{Q}} \xi_q(g)[f|\Delta_q^*] \\ &\quad + \frac{1}{4}\sum_{q_1,q_2\in\mathcal{Q}} \xi_{q_1}(f)\xi_{q_2}(g)[\Delta_{q_1}^*|\Delta_{q_2}^*].\end{aligned}$$

Here we take $\xi_q(f) = [f|\Delta_q^*]/M_q$ and $\xi_q(g) = [g|\Delta_q^*]/M_q$ as motivated by the orthogonal case. Simplifying gives

$$[f|g] = \sum_{q\in\mathcal{Q}} \frac{[f|\Delta_q^*][\Delta_q^*|g]}{M_q} + O(R).$$

The error term can be shown to be sufficiently small by appealing to the local model. The summands above can then be replaced by a tractable expression for which we can compute explicitly and the result soon follows.

5.3 Preparations

5.3.1 Number theoretical considerations

We record here various number theoretical lemmas needed in the subsequent sections. For completeness, we will also include several straightforward lemmas that may be applied freely without reference.

First we recall the well-known orthogonality of exponential sums [74, Equation 4.1].

Lemma 5.3.1. *For any positive integer k, we have*

$$\sum_{a=1}^{k} \mathbf{e}_k(ar) = \begin{cases} k & \text{if } r \equiv 0[k], \\ 0 & \text{otherwise.} \end{cases}$$

Next we recall the Chinese remainder theorem for not necessarily coprime moduli [61, Theorem 3.12].

Lemma 5.3.2 (Chinese remainder theorem)**.** *Let $a_i, m_i \in \mathbb{N}$ for $i = 1, \dots, n$ and $L = [m_1, \dots, m_n]$. The following system of congruences $x \equiv a_i[m_i]$ for $i = 1, \dots, n$ is solvable if and only if $a_i \equiv a_j[(m_i, m_j)]$ for any $1 \leq i, j \leq n$. If the system is solvable then $x \equiv \sigma[L]$ for some $1 \leq \sigma \leq L$ and any two such x are congruent modulo L. Moreover, $(a_i, m_i) = 1$ for $1 \leq i \leq n$ if and only if $(\sigma, L) = 1$.*

We recall from [74, Theorem 4.1] some fundamental properties of Ramanujan sums.

Lemma 5.3.3. *For any positive integers n and r, the Ramanujan sum defined by*

$$c_r(n) = \sum_{\substack{a=1 \\ (a,n)=1}}^{r} \mathbf{e}_r(ka)$$

is a multiplicative function of r. Moreover we have

$$c_r(n) = \sum_{d|(r,n)} d\mu\left(\frac{r}{d}\right) = \frac{\mu(r/(r,n))}{\varphi(r/(r,n))}\varphi(r),$$

and hence $|c_r(n)| = \varphi((r,n))$. In particular

$$c_p(n) = \begin{cases} -1 & \text{if } p \nmid n, \\ \varphi(p) & \text{if } p \mid n, \end{cases} \quad \text{and} \quad c_{p^2}(n) = \begin{cases} 0 & \text{if } p \nmid n, \\ -p & \text{if } p \parallel n, \\ \varphi(p^2) & \text{if } p^2 \mid n. \end{cases}$$

The next result provides an explicit expression for detecting equality for divisors [81, Corollary 3.1].

Lemma 5.3.4. *For integer $a \geq 1$ and any divisor d of a, we have*

$$\sum_{\substack{k|a \\ d|k}} \mu(k/d) = \mathbb{1}_{d=a}.$$

We record below a well-known result which gives an estimate for the number of primes in an arithmetic progression for small moduli [59, Corollary 5.29].

Lemma 5.3.5 (Siegel-Walfisz)**.** *For any $A, B > 0$, we have*

$$\sum_{\substack{n \leq N \\ n \equiv a[q]}} \Lambda(n) = \frac{N}{\varphi(q)} + O_{A,B}(N\mathcal{L}^{-B})$$

uniformly for $(a, q) = 1$ and $q \leq \mathcal{L}^A$.

Finally, we state an auxiliary lemma that will be needed later.

Lemma 5.3.6. *For all positive cubefree integers m and n, we have*

$$\sum_{d_1|m} \sum_{d_2|n} \mu(m/d_1)\mu(n/d_2)(d_1, d_2) = \varphi(m) \cdot \mathbb{1}_{m=n}.$$

Proof. Write $n = n_1 n_2^2$ and $m = m_1 m_2^2$ where $\mu^2(n_1 n_2) = \mu^2(m_1 m_2) = 1$. We factor our sum

$$\begin{aligned}
&\mu^2(n_1)\mu^2(n_2) \sum_{d_1|m} \mu\left(\frac{m}{d_1}\right) \sum_{d_2|n_1} \mu\left(\frac{n_1}{d_2}\right)(d_1, d_2) \sum_{d_2'|n_2^2} \mu\left(\frac{n_2^2}{d_2'}\right)(d_1, d_2') \\
&= \sum_{d_1|m} \mu\left(\frac{m}{d_1}\right) \prod_{p|n_1}((d_1, p) - 1) \prod_{p|n_2}((d_1, p^2) - (d_1, p)).
\end{aligned}$$

The sum vanishes if $n \nmid m$ and by symmetry it also vanishes when $m \nmid n$. Hence the remaining case to consider is when $m = n$, and the sum simplifies to

$$\begin{aligned}
&\prod_{p|m_1}((m, p) - 1) \prod_{p|m_2}((m, p^2) - (m, p)) \\
&= \prod_{p|m_1}(p - 1) \prod_{p|m_2} p(p - 1) = \varphi(m_1)\varphi(m_2^2) = \varphi(m).
\end{aligned}$$

□

5.3.2 Arithmetic functions in arithmetic progressions

We canonically extend the characteristics function of the square-free integers to negative integers by $\mu^2(-n) = \mu^2(|n|)$. The following result provides an asymptotic formula for the number of square-free integers in an arithmetic progression [81, Lemma 19.1].

Lemma 5.3.7. *For any $\varepsilon > 0$, we have*

$$\sum_{\substack{n \le N \\ n \equiv a[q]}} \mu^2(N-n) = (N/q)\gamma_q(N-a) + O_\varepsilon\left(q^\varepsilon \sqrt{N/q}\right)$$

uniformly for all integers a. Here

$$\gamma_q(a) = \begin{cases} 0 & \text{if there exists a prime } p \text{ such that } p^2 \mid (a,q), \\ \dfrac{6}{\pi^2} \displaystyle\prod_{p \mid q} \frac{p^2}{p^2-1} \prod_{\substack{p \| q \\ a \equiv 0[p]}} \left(1 - \frac{1}{p}\right) & \text{otherwise.} \end{cases}$$

As in the notation of [81, Chapter 19], we define

$$\gamma_q^*(a) = \sum_{d \mid q} \mu\left(\frac{q}{d}\right) \gamma_d(a)$$

and

$$t(q) = \prod_{p \mid q} \frac{-1}{p^2-1} \tag{5.3.1}$$

for all positive integer q and integer a. Note that in some sense $\gamma_q^*(N-n)$ is defined to imitate $\mu^2(N-n)$ in arithmetic progression.

We recall the following result from [81, Lemma 19.2] which provides an explicit expression for γ_q^*.

Lemma 5.3.8. *We have $\gamma_q^*(a) = 6t(q)c_q(a)/\pi^2$ if q is a positive cubefree integer, while if q has a cubic factor greater than 1 then $\gamma_q^*(a) = 0$.*

Let $(a', q') = 1$ and q be a positive cubefree integer, denote

$$\rho_q(a) = \begin{cases} 0 & \text{if } (a,q) > 1 \text{ or } (q,q') \nmid (a-a'), \\ \dfrac{q}{\varphi([q,q'])} & \text{if } (q,q') \mid (a-a') \text{ and } (a,q) = 1. \end{cases} \tag{5.3.2}$$

To motivate the definition of ρ_q, consider the sum

$$S = \sum_{\substack{n \le N \\ n \equiv a'[q'] \\ n \equiv a[q]}} \Lambda(n).$$

By the Chinese remainder theorem, the simultaneous congruence equations is solvable if and only if $(a,q) = 1$ and $(q,q') \mid (a-a')$. If this is the case then for some

$0 \leq \sigma < [q, q']$ we should expect

$$\begin{aligned} S &= \sum_{\substack{n \leq N \\ n \equiv \sigma [[q,q']]}} \Lambda(n) \\ &= \rho_q(a)\frac{N}{q} + o\left(\frac{N}{\varphi([q,q'])}\right). \end{aligned}$$

We remark that if $a_1 \equiv a_2[q]$ then $\rho_q(a_1) = \rho_q(a_2)$. The next result states a property of ρ_q.

Lemma 5.3.9. *For q_1, q_2 positive cubefree integers with $(q_1, q_2) = 1$, we have*

$$\rho_{q_1 q_2}(a) = \varphi(q')\rho_{q_1}(a)\rho_{q_2}(a).$$

In particular for any positive integer a, $\varphi(q')\rho_q(a)$ is a multiplicative function of q.

Proof. If $(a, q_1q_2) > 1$ then either $(a, q_1) > 1$ or $(a, q_2) > 1$. If $(q_1q_2, q') \nmid (a - a')$ then we have $(q_1, q') \nmid (a - a')$ or $(q_2, q') \nmid (a - a')$. Consequently for both cases we obtain

$$\begin{aligned} \rho_{q_1q_2}(a) &= \rho_{q_1}(a)\rho_{q_2}(a) \\ &= 0. \end{aligned}$$

Clearly $(q_1q_2, q') \mid (a - a')$ and $(a, q_1q_2) = 1$ if and only if we satisfy both the conditions

$$\begin{cases} (q_1, q') \mid (a - a') \text{ and } (a, q_1) = 1, \\ (q_2, q') \mid (a - a') \text{ and } (a, q_2) = 1. \end{cases}$$

Hence it is enough to show

$$\varphi(q')\varphi([q_1q_2, q']) = \varphi([q_1, q'])\varphi([q_2, q']).$$

Let us recall the identity $ab = [a, b] \cdot (a, b)$ for all positive integers a, b. Consequently

$$\begin{aligned} \varphi(q')\varphi([q_1q_2, q']) &= \varphi(q')\varphi\left(\frac{q_1q_2q'}{(q_1, q')(q_2, q')}\right) \\ &= \varphi(q')\varphi\left(\frac{[q_1, q'] \cdot [q_2, q']}{q'}\right) \\ &= \varphi(q')\varphi([q_1, q'])\varphi\left(\frac{[q_2, q']}{q'}\right) \\ &= \varphi([q_1, q'])\varphi([q_2, q']), \end{aligned}$$

since

$$\left([q_1, q'], \frac{[q_2, q']}{q'}\right) = \left(q', \frac{[q_2, q']}{q'}\right) = 1.$$

The result follows immediately. □

We are now ready to define our local approximation for f. Set

$$\rho_q^*(c) = \sum_{d|q} \mu\left(\frac{q}{d}\right) \rho_d(c)$$

for any positive cubefree integer q.

The next result provides an explicit expression for ρ_q^*.

Lemma 5.3.10. *Let $q = q_1 q_2^2$ with $\mu^2(q_1 q_2) = 1$. If $a_1 \equiv a_2[q]$ then $\rho_q^*(a_1) = \rho_q^*(a_2)$. For any positive integer a, $\varphi(q')\rho_q^*(a)$ is a multiplicative function of q. Furthermore*

$$\rho_q^*(a) = \mathbb{1}_{q_2^2|q'} \cdot \frac{\mu(q_1/(q_1,q'))c_{q_1/(q_1,q')}(a)c_{(q_1,q')q_2^2}(a-a')}{\varphi(q')\varphi(q_1/(q_1,q'))}.$$

Here $c_r(a)$ is the Ramanujan sum.

Proof. We note that if $a_1 \equiv a_2[q]$ then $a_1 \equiv a_2[d]$ for all divisors d of q. Hence

$$\begin{aligned}\rho_q^*(a_1) &= \sum_{d|q} \mu(q/d)\rho_d(a_1) \\ &= \sum_{d|q} \mu(q/d)\rho_d(a_2) \\ &= \rho_q^*(a_2).\end{aligned}$$

By appealing to Lemma 5.3.9, $\varphi(q')\rho_q^*$ is a Dirichlet convolution of two multiplicative functions, hence $\varphi(q')\rho_q^*$ is multiplicative in q. Therefore we factor

$$\varphi(q')\rho_q^* = \varphi(q')\rho_{q_1}^* \cdot \varphi(q')\rho_{q_2^2}^*.$$

We first consider $\varphi(q')\rho_{q_1}^*$. Recall that $\rho_1(a) = 1/\varphi(q')$ and so

$$\varphi(q')\rho_p^*(a) = \varphi(q')\rho_p(a) - 1.$$

From (5.3.2), we check

$$\varphi(q')\rho_p^*(a) = \begin{cases} -1 & \text{if } p \nmid q', p \mid a, \\ 1/(p-1) & \text{if } p \nmid q', p \nmid a, \\ -1 & \text{if } p \mid q', p \nmid (a-a'), \\ p-1 & \text{if } p \mid q', p \mid (a-a'). \end{cases} \tag{5.3.3}$$

In the last line, we note that the condition implies that $(a,p)=1$ since $(a',q')=1$. Next, we rewrite (5.3.3) in a more condense expression

$$\begin{aligned}\varphi(q')\rho^*_{q_1}(a) &= \prod_{\substack{p\mid q_1\\ p\nmid q'\\ p\mid a}}(-1)\prod_{\substack{p\mid q_1\\ p\nmid q'\\ p\nmid a}}\frac{1}{p-1}\prod_{\substack{p\mid (q_1,q')\\ p\nmid (a-a')}}(-1)\prod_{\substack{p\mid (q_1,q')\\ p\mid (a-a')}}(p-1)\\ &= \frac{\mu(q_1/(q_1,q'))c_{q_1/(q_1,q')}(a)c_{(q_1,q')}(a-a')}{\varphi(q_1/(q_1,q'))}.\end{aligned}$$

Lastly, we turn to $\varphi(q')\rho^*_{q_2^2}$ and we see that for any $p^2\mid q_2^2$, we get

$$\begin{aligned}\varphi(q')\rho^*_{p^2}(a) &= \sum_{d\mid p^2}\mu(p^2/d)\varphi(q')\rho_d(a)\\ &= \varphi(q')\rho_{p^2}(a)-\varphi(q')\rho_p(a).\end{aligned}$$

In view of (5.3.2), we readily check that

$$\varphi(q')\rho^*_{p^2}(a)=\begin{cases}0 & \text{if } (p^2,q')=1,\ p\nmid a,\\ 0 & \text{if } (p^2,q')=p,\ p\nmid a,\ p\mid (a-a'),\\ 0 & \text{if } (p^2,q')=p,\ p\nmid a,\ p\nmid (a-a'),\\ 0 & \text{if } (p^2,q')=p^2,\ p\nmid a,\ p\nmid (a-a'),\\ -p & \text{if } (p^2,q')=p^2,\ p\nmid a,\ p\parallel (a-a'),\\ p(p-1) & \text{if } (p^2,q')=p^2,\ p\nmid a,\ p^2\mid (a-a'),\\ 0 & \text{if } p\mid a.\end{cases}$$

We condense the expression to the following simpler form

$$\varphi(q')\rho^*_{p^2}(a)=\begin{cases}0 & \text{if } (p^2,q')\le p,\\ 0 & \text{if } p^2\mid q',\ p\nmid (a-a'),\\ -p & \text{if } p^2\mid q',\ p\parallel (a-a'),\\ p(p-1) & \text{if } p^2\mid q',\ p^2\mid (a-a'),\end{cases}$$

since $(a',q')=1$. It follows that

$$\varphi(q')\rho^*_{q_2^2}(a)=\mathbb{1}_{q_2^2\mid q'}\cdot c_{q_2^2}(a-a'),$$

and the result follows immediately. □

5.3.3 Local Hermitian products

In this section we compute various *local* Hermitian products explicitly.

We denote

$$\vartheta_q^*(a) = \gamma_q^*(N-a) \tag{5.3.4}$$

for all positive cubefree integer q.

For fixed q, we denote $\mathscr{F}(\mathbb{Z}/q\mathbb{Z})$ to be the vector space of complex valued functions over $\mathbb{Z}/q\mathbb{Z}$. We endow this vector space with the *local* Hermitian product by setting

$$[f|g]_q = \frac{1}{q}\sum_{n \,(\mathrm{mod}\ q)} f(n)\overline{g(n)} \tag{5.3.5}$$

for all $f, g \in \mathscr{F}(\mathbb{Z}/q\mathbb{Z})$.

We now state an explicit expression for the norms of ϑ_q^* and ρ_q^*.

Lemma 5.3.11. *For all $q = q_1q_2^2$ with $\mu^2(q_1q_2) = 1$, we have*

$$\|\vartheta_q^*\|_q^2 = \left(\frac{6t(q)}{\pi^2}\right)^2 \varphi(q)$$

and

$$\|\rho_q^*\|_q^2 = \mathbb{1}_{q_2^2|q'} \cdot \frac{\varphi(q_2^2)\varphi((q_1,q'))^2}{\varphi(q')^2\varphi(q_1)}.$$

Proof. The expression for $\|\vartheta_q^*\|_q^2$ can be derived as in [81, Equation (19.10)].

Write

$$\begin{aligned}\|\rho_q^*\|_q^2 &= \frac{1}{q\varphi(q')^2}\sum_{a \,(\mathrm{mod}\ q)} \left|\varphi(q')\rho_q^*(a)\right|^2 \\ &= \frac{1}{q\varphi(q')^2} S(q), \text{ say.}\end{aligned}$$

If $q_2^2 \nmid q'$ then we are done since $\rho_q^* = 0$ by Lemma 5.3.10. Otherwise, by the Chinese remainder theorem we factor

$$\begin{aligned}S(q) &= S(q_1)S(q_2^2) \\ &= \prod_{p|q_1} S(p) \prod_{p^2|q_2^2} S(p^2).\end{aligned}$$

Appealing to (5.3.3), we readily check

$$S(p) = \begin{cases} 1 + 1/(p-1) = p/(p-1) & \text{if } p \nmid q', \\ (p-1)^2 + (p-1) = p(p-1) & \text{if } p \mid q'. \end{cases}$$

By Lemma 5.3.10, expanding the Ramanujan sum and interchanging summations, we obtain

$$\begin{aligned} S(p^2) &= \sum_{a \,(\mathrm{mod}\ p^2)} \left|c_{p^2}(a-a')\right|^2 \\ &= \sum_{r_1=1}^{p^2}{}^{*} \sum_{r_2=1}^{p^2}{}^{*} \mathbf{e}_{p^2}\left(a'(r_2-r_1)\right) \sum_{a \,(\mathrm{mod}\ p^2)} \mathbf{e}_{p^2}\left(a(r_1-r_2)\right). \end{aligned}$$

By orthogonality, we get

$$S(p^2) = p^2\varphi(p^2).$$

It follows

$$\begin{aligned} \|\rho_q^*\|_q^2 &= \frac{1}{q\varphi(q')^2} \prod_{p\mid q_1} S(p) \prod_{p\mid q_2} S(p^2) \\ &= \frac{1}{q\varphi(q')^2} \prod_{\substack{p\mid q_1 \\ p\nmid q'}} \frac{p}{p-1} \prod_{\substack{p\mid q_1 \\ p\mid q'}} p(p-1) \prod_{p\mid q_2} (p^2\varphi(p^2)) \\ &= \frac{1}{\varphi(q')^2} \prod_{\substack{p\mid q_1 \\ p\nmid q'}} \frac{1}{p-1} \prod_{\substack{p\mid q_1 \\ p\mid q'}} (p-1) \prod_{p\mid q_2} \varphi(p^2) \\ &= \frac{\varphi(q_2^2)\varphi((q_1,q'))^2}{\varphi(q')^2\varphi(q_1)}, \end{aligned}$$

since

$$\left((q_1,q'), \frac{q_1}{(q_1,q')}\right) = 1.$$

□

For all positive cubefree integer q, we denote

$$b(q) = \sum_{r=1}^{q}{}^{*} \mathbf{e}_q\left(rN\right) h_q(r),$$

where

$$h_q(r) = \sum_{a \,(\mathrm{mod}\ q)} \varphi(q')\rho_q^*(a)\mathbf{e}_q\left(-ra\right).$$

We now state a result which provides an explicit expression for $b(p)$ and $b(p^2)$.

Lemma 5.3.12. *The function $b(q)$ is a multiplicative function of q. Moreover we have*

$$b(p) = \begin{cases} \dfrac{-pc_p(N)}{\varphi(p)} & \text{if } p \nmid q', \\ pc_p(N-a') & \text{if } p \mid q', \end{cases}$$

and

$$b(p^2) = \mathbb{1}_{p^2|q'} \cdot p^2 c_{p^2}(N-a').$$

Proof. For positive cubefree integers q_1, q_2 with $(q_1, q_2) = 1$, we have by the Chinese remainder theorem

$$\begin{aligned} h_{q_1q_2}(r) &= \sum_{\substack{a_1 \pmod{q_1} \\ a_2 \pmod{q_2}}} \varphi(q')\rho^*_{q_1q_2}(a_1q_2 + a_2q_1)\mathbf{e}_{q_1}(-ra_1)\,\mathbf{e}_{q_2}(-ra_2) \\ &= \sum_{\substack{a_1 \pmod{q_1} \\ a_2 \pmod{q_2}}} \varphi(q')\rho^*_{q_1}(a_1)\varphi(q')\rho^*_{q_2}(a_2)\mathbf{e}_{q_1}(-ra_1)\,\mathbf{e}_{q_2}(-ra_2) \\ &= h_{q_1}(r)h_{q_2}(r) \end{aligned}$$

where in the second line we used Lemma 5.3.10. Similarly, we show that $b(q)$ is a multiplicative function in q.

First we assume that $(p, q') = 1$, appealing to (5.3.3) we get

$$b(p) = \sum_{r=1}^{p-1} \mathbf{e}_p(rN) \left\{ \frac{-1}{p-1} - 1 + \frac{1}{p-1} \sum_{a \pmod{p}} \mathbf{e}_p(-ra) \right\}.$$

Since $(r, p) = 1$ and hence by orthogonality we have

$$\begin{aligned} b(p) &= \frac{-p}{\varphi(p)} \sum_{r=1}^{p-1} \mathbf{e}_p(rN) \\ &= \frac{-pc_p(N)}{\varphi(p)}. \end{aligned}$$

Now assume $p \mid q'$ and appealing to (5.3.3) we obtain

$$b(p) = \sum_{r=1}^{p-1} \mathbf{e}_p(rN) \left\{ (p-1)\mathbf{e}_p(-ra') + \mathbf{e}_p(-ra') - \sum_{a \pmod{p}} \mathbf{e}_p(-ra) \right\}.$$

Since $(r,p)=1$, orthogonality gives

$$\begin{aligned} b(p) &= p\sum_{r=1}^{p-1}\mathbf{e}_p\left(r(N-a')\right) \\ &= pc_p(N-a'). \end{aligned}$$

Next we consider $b(p^2)$. If $p^2 \nmid q'$ then we are done, otherwise expanding the Ramanujan sum and interchanging summations, we obtain

$$\begin{aligned} b(p^2) &= \sideset{}{^*}\sum_{r=1}^{p^2}\mathbf{e}_{p^2}\left(rN\right)\sum_{a\,(\mathrm{mod}\ p^2)}c_{p^2}(a-a')\mathbf{e}_{p^2}\left(-ra\right) \\ &= \sideset{}{^*}\sum_{r=1}^{p^2}\sideset{}{^*}\sum_{r_1=1}^{p^2}\mathbf{e}_{p^2}\left(rN\right)\mathbf{e}_{p^2}\left(-ra'\right)\sum_{a\,(\mathrm{mod}\ p^2)}\mathbf{e}_{p^2}\left(a(r_1-r)\right). \end{aligned}$$

Appealing to orthogonality then gives

$$\begin{aligned} b(p^2) &= p^2\sideset{}{^*}\sum_{r=1}^{p^2}\mathbf{e}_{p^2}\left(r(N-a')\right) \\ &= p^2c_{p^2}(N-a'). \end{aligned}$$

□

Next, we derive an explicit expression for the inner product $[\vartheta_q^*|\rho_q^*]_q$.

Lemma 5.3.13. *For all $q=q_1q_2^2$ with $\mu^2(q_1q_2)=1$, we have*

$$[\vartheta_q^*|\rho_q^*]_q = \mathbb{1}_{q_2^2|q'}\cdot\frac{6t(q)c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')}{\pi^2\varphi(q')\mu(q_1/(q_1,q'))\varphi(q_1/(q_1,q'))}.$$

Proof. If $q_2^2\nmid q'$ then we are done, otherwise

$$\begin{aligned} [\vartheta_q^*|\rho_q^*]_q &= \frac{1}{q}\sum_{a\,(\mathrm{mod}\ q)}\gamma_q^*(N-a)\rho_q^*(a) \\ &= \frac{6t(q)}{\pi^2q\varphi(q')}\sum_{a\,(\mathrm{mod}\ q)}c_q(N-a)\varphi(q')\rho_q^*(a) \\ &= \frac{6t(q)}{\pi^2q\varphi(q')}\sideset{}{^*}\sum_{r=1}^{q}\mathbf{e}_q\left(rN\right)\sum_{a\,(\mathrm{mod}\ q)}\varphi(q')\rho_q^*(a)\mathbf{e}_q\left(-ra\right). \end{aligned}$$

Therefore by the previous lemma, we arrive at

$$[\vartheta_q^*|\rho_q^*]_q = \frac{6t(q)}{\pi^2q\varphi(q')}b(q)$$

$$= \frac{6t(q)}{\pi^2 q\varphi(q')} \prod_{p|q_1} b(p) \prod_{p|q_2} b(p^2)$$
$$= \mathbb{1}_{q_2^2|q'} \cdot \frac{6t(q)}{\pi^2 q\varphi(q')} \prod_{\substack{p|q_1\\ p\nmid q'}} \frac{-pc_p(N)}{\varphi(p)} \prod_{\substack{p|q_1\\ p|q'}} pc_p(N-a') \prod_{p|q_2} p^2 c_{p^2}(N-a')$$
$$= \mathbb{1}_{q_2^2|q'} \cdot \frac{6t(q)\mu(q_1/(q_1,q'))}{\pi^2\varphi(q')} \frac{c_{q_1/(q_1,q')}(N)}{\varphi(q_1/(q_1,q'))} c_{(q_1,q')q_2^2}(N-a'),$$

and the result follows. □

5.3.4 *Local models and their products*

For a positive cubefree integer $q = q_1q_2^2$ with $\mu^2(q_1q_2) = 1$, we denote

$$\eta_q^* = \frac{1}{2}\left(\frac{\pi^2}{6t(q)}\vartheta_q^* + \frac{\varphi(q')\varphi(q_1/(q_1,q'))}{\mu(q_1/(q_1,q'))}\widetilde{\rho}_q^*\right), \tag{5.3.6}$$

$$\kappa_q^* = \frac{1}{2}\left(\frac{\pi^2}{6t(q)}\vartheta_q^* - \frac{\varphi(q')\varphi(q_1/(q_1,q'))}{\mu(q_1/(q_1,q'))}\widetilde{\rho}_q^*\right), \tag{5.3.7}$$

where

$$\widetilde{\rho}_q^*(a) = \frac{\mu(q_1/(q_1,q'))c_{q_1/(q_1,q')}(a)c_{(q_1,q')q_2^2}(a-a')}{\varphi(q')\varphi(q_1/(q_1,q'))}$$

is just ρ_q^* but without the divisibility condition on q', see Lemma 5.3.10. In particular, we can write

$$\rho_q^* = \mathbb{1}_{q_2^2|q'} \cdot \widetilde{\rho}_q^*.$$

Below, we compute the norms of η_q^* and κ_q^*.

Lemma 5.3.14. *We have*

$$\|\eta_q^*\|_q^2 = \frac{1}{2}\left(\varphi(q) + c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')\right),$$

$$\|\kappa_q^*\|_q^2 = \frac{1}{2}\left(\varphi(q) - c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')\right),$$

and

$$[\eta_q^*|\kappa_q^*]_q = [\kappa_q^*|\eta_q^*]_q = 0.$$

Proof. The norms for η_q^* and κ_q^* follows immediately from Lemma 5.3.11, 5.3.13, and that both ϑ_q^* and ρ_q^* are real valued.

Showing

$$[\eta_q^*|\kappa_q^*]_q = [\kappa_q^*|\eta_q^*]_q = 0$$

also follows from Lemmas 5.3.11 and 5.3.13. □

Note that $\|\eta_q^*\|_q^2 \neq 0$ and $\|\kappa_q^*\|_q^2 = 0$ when

$$\frac{q_1}{(q_1, q')} \mid N \qquad \text{and} \qquad (q_1, q')q_2^2 \mid (N - a').$$

We denote $\mathscr{F}([1, N])$ to be the vector space of all complex valued functions on the positive integers in $[1, N]$. We endow the *global* hermitian product

$$[f|g] = \sum_{n \leq N} f(n)\overline{g(n)} \tag{5.3.8}$$

for all $f, g \in \mathscr{F}([1, N])$. Next, we will show there is a Hermitian relationship between the *global* and *local* products.

Given a function $h \in \mathscr{F}(\mathbb{Z}/q\mathbb{Z})$, we denote $\nabla_q(h)$ to be a function on $[1, N]$ defined by

$$\nabla_q(h)(x) = h(x \pmod q).$$

This peculiarity is particularly important for the *global* Hermitian product.

For a function $j \in \mathscr{F}([1, N])$, we denote $\Delta_q(j)$ to be a function on the positive integers such that

$$\Delta_q(j)(x) = q \sum_{\substack{n \leq N \\ n \equiv x[q]}} j(n).$$

For $h_1 \in \mathscr{F}([1, N])$ and $h_2 \in \mathscr{F}(\mathbb{Z}/q\mathbb{Z})$, we readily check that

$$[\Delta_q(h_1)|h_2]_q = [h_1|\nabla_q(h_2)]. \tag{5.3.9}$$

Indeed

$$\begin{aligned}
[\Delta_q(h_1)|h_2]_q &= \sum_{a \pmod q} \sum_{\substack{n \leq N \\ n \equiv a[q]}} h_1(n)\overline{h_2(a)} \\
&= \sum_{n \leq N} h_1(n)\overline{h_2(n \pmod q)} \\
&= [h_1|\nabla_q(h_2)].
\end{aligned}$$

Let us set

$$\phi_q^* = \nabla_q \eta_q^* \qquad \text{and} \qquad \psi_q^* = \nabla_q \kappa_q^*.$$

Now we are ready to define a local model which encompass both f and g, these will be the union of (ϕ_q^*) and (ψ_q^*), but we exclude those ϕ_q^* and ψ_q^* which are zero.

Next, we compute the cross products of these local models.

Lemma 5.3.15. *For all positive cubefree integers m and n, we have*

$$[\phi_m^*|\phi_n^*] = N\|\eta_m^*\|_m^2 \cdot \mathbb{1}_{m=n} + O(\sigma(m)\sigma(n)),$$

$$[\psi_m^*|\psi_n^*] = N\|\kappa_m^*\|_m^2 \cdot \mathbb{1}_{m=n} + O(\sigma(m)\sigma(n)),$$

and

$$[\psi_m^*|\phi_n^*] = [\phi_m^*|\psi_n^*] = O(\sigma(m)\sigma(n)).$$

Proof. Write $m = m_1 m_2^2$ and $n = n_1 n_2^2$ with $\mu^2(m_1 m_2) = \mu^2(n_1 n_2) = 1$. By appealing to (5.3.4), (5.3.6), Lemma 5.3.8 and 5.3.10, we expand

$$[\phi_m^*|\phi_n^*] = \frac{1}{4}\left(S_1 + S_2 + S_3 + S_4\right),$$

where

$$\begin{aligned}
S_1 &= \sum_{n \le N} c_m(N-n)c_n(N-n),\\
S_2 &= \sum_{n \le N} c_m(N-n)c_{n_1/(n_1,q')}(n)c_{(n_1,q')n_2^2}(n-a'),\\
S_3 &= \sum_{n \le N} c_n(N-n)c_{m_1/(m_1,q')}(n)c_{(m_1,q')m_2^2}(n-a'),\\
S_4 &= \sum_{n \le N} c_{m_1/(m_1,q')}(n)c_{(m_1,q')m_2^2}(n-a')c_{n_1/(n_1,q')}(n)c_{(n_1,q')n_2^2}(n-a').
\end{aligned}$$

Using the explicit form of ϑ_q^* and applying Lemma 5.3.3, we have

$$\begin{aligned}
S_1 &= \sum_{n \le N} \sum_{\substack{d_1|m\\ d_1|(N-n)}} \sum_{\substack{d_2|n\\ d_2|(N-n)}} d_1\mu(m/d_1)d_2\mu(n/d_2)\\
&= \sum_{d_1|m}\sum_{d_2|n} d_1\mu(m/d_1)d_2\mu(n/d_2) \sum_{\substack{n \le N\\ n \equiv N [[d_1,d_2]]}} 1\\
&= N\sum_{d_1|m}\sum_{d_2|n} \frac{d_1\mu(m/d_1)d_2\mu(n/d_2)}{[d_1,d_2]} + O(\sigma(m)\sigma(n))\\
&= N\sum_{d_1|m}\sum_{d_2|n} \mu(m/d_1)\mu(n/d_2)(d_1,d_2) + O(\sigma(m)\sigma(n)).
\end{aligned}$$

By Lemma 5.3.6, we get

$$S_1 = N\phi(m) \cdot \mathbb{1}_{m=n} + O(\sigma(m)\sigma(n)).$$

Next we deal with S_4. Expanding each of the four Ramanujan sums and taking the summation over n inside, we obtain

$$S_4 = \sum_{\substack{d_1|m_1/(m_1,q') \\ d_2|n_1/(n_1,q')}} d_1\mu\left(\frac{m_1}{d_1(m_1,q')}\right) d_2\mu\left(\frac{n_1}{d_2(n_1,q')}\right) \times \sum_{\substack{d_3|(m_1,q')m_2^2 \\ d_4|(n_1,q')n_2^2}} d_3\mu\left(\frac{(m_1,q')m_2^2}{d_3}\right) d_4\mu\left(\frac{(n_1,q')n_2^2}{d_4}\right) \sum_{\substack{n\le N \\ n\equiv 0[d_i],i=1,2 \\ n\equiv a'[d_j],j=3,4}} 1.$$

Observe that $(d_1,d_3)=(d_1,d_4)=(d_2,d_3)=(d_2,d_4)=1$, since $m_2^2 \mid q'$ and $n_2^2 \mid q'$. By the Chinese reminder theorem, the system of congruences in the summation over n can be reduced to one congruence, namely

$$n \equiv \sigma[[d_1,d_2,d_3,d_4]]$$

for some $1 \le \sigma \le [d_1,d_2,d_3,d_4]$. Since $(d_1,d_3)=(d_2,d_4)=1$, we verify that

$$[d_1,d_2,d_3,d_4] = [d_1d_3, d_2d_4].$$

Next, we glue the variables d_1, d_3 and d_2, d_4 together to get

$$S_4 = N\sum_{\substack{d_1|m \\ d_2|n}} \frac{d_1\mu(m/d_1)d_2\mu(n/d_2)}{[d_1,d_2]} + O\left(\sigma(m)\sigma(n)\right).$$

By Lemma 5.3.6, we obtain

$$S_4 = N\varphi(m)\cdot \mathbb{1}_{m=n} + O(\sigma(m)\sigma(n)).$$

Now we consider S_2. Again, expanding the Ramanujan sums and interchanging summations, we assert

$$S_2 = \sum_{d_1|m} d_1\mu\left(\frac{m}{d_1}\right) \sum_{d_2|n_1/(n_1,q')} d_2\mu\left(\frac{n_1}{d_2(n_1,q')}\right) \sum_{d_3|(n_1,q')n_2^2} d_3\mu\left(\frac{(n_1,q')n_2^2}{d_3}\right) \sum_{\substack{n\le N \\ n\equiv N[d_1] \\ n\equiv 0[d_2] \\ n\equiv a'[d_3]}} 1.$$

Since $(d_2,d_3)=1$, the system of congruences in the inner sum is solvable if and only if $(d_1,d_3) \mid (N-a')$ and $(d_1,d_2) \mid N$. It follows by the Chinese remainder theorem that

$$S_2 = M + O(\sigma(m)\sigma(n)),$$

where

$$M = N \sum_{d_1 \mid m} d_1 \mu\left(\frac{m}{d_1}\right) \sum_{\substack{d_2 \mid n_1/(n_1,q') \\ (d_1,d_2)\mid N}} d_2 \mu\left(\frac{n_1}{d_2(n_1,q')}\right) \sum_{\substack{d_3 \mid (n_1,q')n_2^2 \\ (d_1,d_3)\mid (N-a')}} \frac{d_3 \mu((n_1,q')n_2^2/d_3)}{[d_1,d_2d_3]}.$$

The divisibility conditions over the summations of d_2 and d_3 are troublesome. We deal with this by Lemma 5.3.4 and observe that

$$\begin{aligned}\mathbb{1}_{(d_1,d_3)\mid(N-a')} &= \sum_{\substack{t\mid(N-a') \\ t\mid(d_1,d_3)}} \mathbb{1}_{t=(d_1,d_3)} \\ &= \sum_{\substack{t\mid(N-a') \\ t\mid(d_1,d_3)}} \sum_{\substack{k\mid(d_1,d_3) \\ t\mid k}} \mu(k/t),\end{aligned}$$

and

$$\begin{aligned}\mathbb{1}_{(d_1,d_2)\mid N} &= \sum_{\substack{t'\mid N \\ t'\mid(d_1,d_2)}} \mathbb{1}_{t'=(d_1,d_2)} \\ &= \sum_{\substack{t'\mid N \\ t'\mid(d_1,d_2)}} \sum_{\substack{k'\mid(d_1,d_2) \\ t'\mid k'}} \mu(k'/t').\end{aligned}$$

Substituting this into M and gluing the variables d_2, d_3 and noticing that $(k,k') = 1$ since $(d_2,d_3) = 1$, $k' \mid d_2$ and $k \mid d_3$, we assert

$$\begin{aligned}M = N &\sum_{\substack{t'\mid N \\ t'\mid k'\mid(\frac{n_1}{(n_1,q')},m)}} \sum_{\substack{t\mid(N-a') \\ t\mid k\mid((n_1,q')n_2^2,m)}} \mu\left(\frac{k}{t}\right)\mu\left(\frac{k'}{t'}\right)kk' \\ &\times \sum_{d_1\mid\frac{m}{kk'}} \mu\left(\frac{m}{d_1kk'}\right) \sum_{d_2\mid\frac{n}{kk'}} \mu\left(\frac{n}{d_2kk'}\right)(d_1,d_2).\end{aligned}$$

If $m \neq n$ then $M = 0$ by Lemma 5.3.6. If $m = n$ then again by Lemma 5.3.6, we get

$$M = N \sum_{\substack{t'\mid N \\ t'\mid k'\mid\frac{n_1}{(n_1,q')}}} \sum_{\substack{t\mid(N-a') \\ t\mid k\mid(n_1,q')n_2^2}} \mu\left(\frac{k}{t}\right)\mu\left(\frac{k'}{t'}\right)kk'\varphi\left(\frac{n}{kk'}\right).$$

For $k' \mid \frac{n_1}{(n_1,q')}$ and $k \mid (n_1,q')n_2^2$, we rewrite the Euler totient function as a Dirichlet convolution

$$\varphi\left(\frac{n}{kk'}\right) = \sum_{s\mid\frac{n}{kk'}} s\mu\left(\frac{n}{skk'}\right)$$

$$= \sum_{d_1 | \frac{n_1}{(n_1,q')k'}} d_1 \mu\left(\frac{n_1}{k' d_1 (n_1,q')}\right) \sum_{d_2 | \frac{(n_1,q')n_2^2}{k}} d_2 \mu\left(\frac{(n_1,q')n_2^2}{k d_2}\right).$$

Substituting this into M and interchanging summations, we have

$$\begin{aligned} M =& N \sum_{\substack{t' | N \\ t' | k' | \frac{n_1}{(n_1,q')}}} \sum_{t | (N-a') \atop t | k | (n_1,q')n_2^2} \mu\left(\frac{k}{t}\right) \mu\left(\frac{k'}{t'}\right) \\ & \times \sum_{d_1 | \frac{n_1}{(n_1,q')k'}} k' d_1 \mu\left(\frac{n_1}{k' d_1 (n_1,q')}\right) \sum_{d_2 | \frac{(n_1,q')n_2^2}{k}} k d_2 \mu\left(\frac{(n_1,q')n_2^2}{k d_2}\right) \\ =& N \sum_{d_1 | \frac{n_1}{(n_1,q')}} d_1 \mu\left(\frac{n_1}{d_1 (n_1,q')}\right) \sum_{d_2 | (n_1,q')n_2^2} d_2 \mu\left(\frac{(n_1,q')n_2^2}{d_2}\right) \\ & \times \sum_{\substack{t' | N \\ t' | d_1}} \sum_{\substack{k' | d_1 \\ t' | k'}} \mu\left(\frac{k'}{t'}\right) \sum_{t | (N-a') \atop t | d_2} \sum_{k | d_2 \atop t | k} \mu\left(\frac{k}{t}\right). \end{aligned}$$

In view of Lemma 5.3.3, we get

$$\begin{aligned} \mathbb{1}_{d_1 | N} &= \sum_{\substack{t' | N \\ t' | d_1}} \mathbb{1}_{t' = d_1} \\ &= \sum_{\substack{t' | N \\ t' | d_1}} \sum_{\substack{k' | d_1 \\ t' | k'}} \mu(k'/t'), \end{aligned}$$

and

$$\begin{aligned} \mathbb{1}_{d_2 | (N-a')} &= \sum_{t | (N-a') \atop t | d_2} \mathbb{1}_{t = d_2} \\ &= \sum_{t | (N-a') \atop t | d_2} \sum_{k | d_2 \atop t | k} \mu(k/t). \end{aligned}$$

Therefore the sum M in question collapses into

$$\begin{aligned} M &= \sum_{\substack{d_1 | \frac{n_1}{(n_1,q')} \\ d_1 | N}} d_1 \mu\left(\frac{n_1}{d_1 (n_1,q')}\right) \sum_{\substack{d_2 | (n_1,q')n_2^2 \\ d_2 | (N-a')}} d_2 \mu\left(\frac{(n_1,q')n_2^2}{d_2}\right) \\ &= c_{n_1/(n_1,q')}(N) c_{(n_1,q')n_2^2}(N-a'). \end{aligned}$$

Hence we have

$$S_2 = Nc_{n_1/(n_1,q')}(N)c_{(n_1,q')n_2^2}(N-a')\cdot \mathbb{1}_{m=n} + O(\sigma(m)\sigma(n)).$$

Similarly we also claim

$$S_3 = Nc_{m_1/(m_1,q')}(N)c_{(m_1,q')m_2^2}(N-a')\cdot \mathbb{1}_{m=n} + O(\sigma(m)\sigma(n)).$$

Gathering all the estimates above, we finally arrive at

$$\begin{aligned}[\phi_m^*|\phi_n^*] =& \frac{\mathbb{1}_{m=n}\cdot N}{2}\left(\varphi(m) + c_{m_1/(m_1,q')}(N)c_{(m_1,q')m_2^2}(N-a')\right)\\ &+ O(\sigma(m)\sigma(n)),\end{aligned}$$

and the result follows from Lemma 5.3.14.

The remaining bounds for $[\psi_m^*|\psi_n^*]$, $[\psi_m^*|\phi_n^*]$ and $[\phi_m^*|\psi_n^*]$ follows immediately from our computation of S_1, S_2, S_3, S_4. □

5.3.5 Approximating f and g

In this section we impose implicitly the condition

$$q' \leq \mathcal{L}^{C_1}.$$

Take our set of moduli to be

$$\mathcal{Q} = \left\{q_1q_2^2 \ :\ q_1 \leq Q_1, q_2 \leq Q_2, \mu^2(q_1q_2) = 1\right\}. \tag{5.3.10}$$

Here

$$Q_1 = \mathcal{L}^{D_1} \qquad \text{and} \qquad Q_2 = \mathcal{L}^{D_2},$$

where $D_1, D_2 \geq C_1$ will be chosen later. We also set

$$Q = \max\left\{Q_1, Q_2\right\},$$

and in particular this implies $q' \leq Q \ll_\varepsilon N^\varepsilon$.

Finally, we recall $(a', q') = 1$ and let

$$f(n) = \Lambda(n)\cdot \mathbb{1}_{n\equiv a'[q']} \tag{5.3.11}$$

and

$$g(n) = \mu^2(N-n) \tag{5.3.12}$$

for all $n \leq N$.

Lemma 5.3.16. *For any $A > 0$ and $q \in \mathcal{Q}$, we have*

$$\begin{aligned}[\phi_q^*|f] &= N[\eta_q^*|\rho_q^*]_q + O\left(q^2 N\mathcal{L}^{-A}\right),\\ [\phi_q^*|g] &= N[\eta_q^*|\vartheta_q^*]_q + O\left(q^{3/2+\varepsilon}N^{1/2}\right),\end{aligned}$$

and

$$\begin{aligned}[\psi_q^*|f] &= -N[\kappa_q^*|\rho_q^*]_q + O\left(q^2 N\mathcal{L}^{-A}\right),\\ [\psi_q^*|g] &= N[\kappa_q^*|\vartheta_q^*]_q + O\left(q^{3/2+\varepsilon}N^{1/2}\right).\end{aligned}$$

In particular, we have

$$|[\phi_q^*|f]| + |[\psi_q^*|f]| \ll \mathbb{1}_{q_2^2|q'} \cdot N\varphi((q_1,q')q_2^2)\varphi(q')^{-1} + q^2 N\mathcal{L}^{-A}$$

and

$$|[\phi_q^*|g]| + |[\psi_q^*|g]| \ll N|t(q)|\varphi(q) + q^{3/2+\varepsilon}N^{1/2}.$$

All implied constant above may depend on $A, C_1, D_1, D_2, \varepsilon$.

Proof. By (5.3.9), we get

$$\begin{aligned}[\nabla_q \eta_q^*|f] &= [\eta_q^*|\Delta_q f]_q\\ &= [\eta_q^*|N\rho_q]_q + [\eta_q^*|\Delta_q f - N\rho_q]_q.\end{aligned}$$

Note that by (5.3.6) and (5.3.7), we have

$$\rho_q^* = \frac{\mathbb{1}_{q_2^2|q'} \cdot \mu(q_1/(q_1,q'))}{\varphi(q')\varphi(q_1/(q_1,q'))}\left(\eta_q^* - \kappa_q^*\right). \tag{5.3.13}$$

By the Möbius inversion formula

$$\rho_q = \sum_{d|q} \rho_d^*,$$

and it follows

$$\begin{aligned}[\eta_q^*|\rho_q]_q &= \sum_{d|q}[\eta_q^*|\rho_d^*]_q\\ &= \frac{\mathbb{1}_{q_2^2|q'} \cdot \mu(q_1/(q_1,q'))}{\varphi(q')\varphi(q_1/(q_1,q'))}\sum_{d|q}\left([\eta_q^*|\eta_d^*]_q - [\eta_q^*|\kappa_d^*]_q\right).\end{aligned}$$

Following the proof of Lemma 5.3.15, the summand is zero unless $d = q$, and hence $[\eta_q^*|\rho_q]_q = [\eta_q^*|\rho_d^*]_q$. It follows

$$[\eta_q^*|\rho_q]_q = \frac{\mathbb{1}_{q_2^2|q'} \cdot \mu(q_1/(q_1,q'))}{2\phi(q')\varphi(q_1/(q_1,q'))}\left(\varphi(q) + c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')\right)$$

$$\ll \mathbb{1}_{q_2^2|q'} \cdot \varphi((q_1, q')q_2^2)\varphi(q')^{-1}.$$

Write

$$[\eta_q^*|\Delta_q f - N\rho_q]_q = \frac{1}{2}(S_1 + S_2),$$

where

$$S_1 = \sum_{a \,(\mathrm{mod}\ q)} c_q(N-a) \left(\sum_{\substack{n \le N \\ n \equiv a[q]}} f(n) - \frac{N}{q}\rho_q(a) \right),$$

$$S_2 = \sum_{a \,(\mathrm{mod}\ q)} c_{q_1/(q_1,q')}(a) c_{(q_1,q')q_2^2}(a-a') \left(\sum_{\substack{n \le N \\ n \equiv a[q]}} f(n) - \frac{N}{q}\rho_q(a) \right).$$

We crudely bound using the Siegel-Walfisz Theorem (Lemma 5.3.5) to get

$$\begin{aligned} S_1, S_2 &\le q^2 \max_{a \,(\mathrm{mod}\ q)} \left| \sum_{\substack{n \le N \\ n \equiv a[q]}} f(n) - \frac{N}{q}\rho_q(a) \right| \\ &\ll_{A,C_1,D_1,D_2} q^2 N \mathcal{L}^{-A}. \end{aligned}$$

Next we turn to $[\phi_q^*|g]$. Similarly we get

$$\begin{aligned} [\nabla_q \eta_q^*|g] &= [\eta_q^*|\Delta_q g]_q \\ &= [\eta_q^*|N\vartheta_q]_q + [\eta_q^*|\Delta_q g - N\vartheta_q]_q. \end{aligned}$$

Note that by (5.3.6) and (5.3.7), we have

$$\vartheta_q^* = \frac{6t(q)}{\pi^2} \left(\eta_q^* + \kappa_q^* \right). \tag{5.3.14}$$

By the Möbius inversion formula, we have

$$\vartheta_q = \sum_{d|q} \vartheta_q^*,$$

and it follows

$$\begin{aligned} [\eta_q^*|\vartheta_q]_q &= \sum_{d|q} [\eta_q^*|\vartheta_d^*]_q \\ &= \frac{6t(q)}{\pi^2} \sum_{d|q} \left([\eta_q^*|\eta_d^*]_q + [\eta_q^*|\kappa_d^*]_q \right). \end{aligned}$$

Again following the proof of Lemma 5.3.15, the summand vanishes unless $d = q$, and hence $[\eta_q^*|\vartheta_q]_q = [\eta_q^*|\vartheta_d^*]_q$. Therefore

$$\begin{aligned}[\eta_q^*|\vartheta_q]_q &= \frac{3t(q)}{\pi^2}\left(\varphi(q) + c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')\right)\\ &\ll |t(q)|\varphi(q).\end{aligned}$$

We can deal with $[\eta_q^*|\Delta_q g - N\vartheta_q]_q$ just like above but we apply Lemma 5.3.7 instead of Lemma 5.3.5 to get

$$[\eta_q^*|\Delta_q g - N\vartheta_q]_q \ll_\varepsilon q^{3/2+\varepsilon}N^{1/2}.$$

The bounds for $[\psi_q^*|f]$ and $[\psi_q^*|g]$ follow similarly. □

Denote

$$\mathcal{E} = \left\{q_1q_2^2 \in \mathcal{Q} \ : \ \frac{q_1}{(q_1,q')} \mid N, (q_1,q')q_2^2 \mid (N-a')\right\}.$$

Note that $\|\kappa_q^*\|_q = 0$ if and only if $q \in \mathcal{E}$.

Now we give upper and lower bounds for these norms.

Lemma 5.3.17. *For all $q = q_1q_2^2 \in \mathcal{Q}$, we have*

$$\varphi(q)/4 \le \|\eta_q^*\|_q^2 \le \varphi(q).$$

The same holds when we replace $\left(\eta_q^*, \mathcal{Q}\right)$ with $\left(\kappa_q^*, \mathcal{Q}\backslash\mathcal{E}\right)$.

Proof. From Lemma 5.3.14, we get

$$\|\eta_q^*\|_q^2 = \frac{1}{2}\left(\varphi(q) + c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')\right).$$

Clearly

$$\left|c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')\right| \le \varphi(q),$$

and so the upper bound follows.

For the lower bound, note that

$$c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')$$

strictly divides $\varphi(q)$, and hence

$$\varphi(q) + c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a') \ge \varphi(q) - \frac{1}{2}\varphi(q).$$

The bounds for $\|\kappa_q^*\|_q^2$ is similar. □

Next we need to estimate the sums

$$\sum_{t\in\mathcal{Q}} |[\phi_q^*|\phi_t^*]| + \sum_{t\in\mathcal{Q}} |[\phi_q^*|\psi_t^*]| \tag{5.3.15}$$

for all $q \in \mathcal{Q}$, and

$$\sum_{t\in\mathcal{Q}} |[\psi_q^*|\phi_t^*]| + \sum_{t\in\mathcal{Q}} |[\psi_q^*|\psi_t^*]| \tag{5.3.16}$$

for all $q \in \mathcal{Q}$. But first, we need an a priori bound.

Lemma 5.3.18. *We have*

$$\sum_{q\in\mathcal{Q}} \sigma(q) \ll_\varepsilon N^\varepsilon.$$

Proof. The sum is majorized by

$$\begin{aligned}\sum_{q_1\le Q_1} \sigma(q_1) \sum_{q_2\le Q_2} \sigma(q_2^2) &\ll_\varepsilon Q^\varepsilon \sum_{q_1\le Q_1} q_1 \sum_{q_2\le Q_2} q_2^2 \\ &\ll_\varepsilon Q^{5+\varepsilon} \\ &\ll_\varepsilon N^\varepsilon.\end{aligned}$$

□

We only show the following for (5.3.15) as (5.3.16) is similar. By Lemma 5.3.15 and 5.3.18, we get that (5.3.15) is

$$\begin{aligned}&N\|\eta_q^*\|_q^2 + O\left(\sigma(q)^2 + \sum_{\substack{t\in\mathcal{Q}\\ t\neq q}} |[\phi_q^*|\phi_t^*]| + \sum_{t\in\mathcal{Q}} |[\phi_q^*|\psi_t^*]|\right) \\ &= N\|\eta_q^*\|_q^2 + O_\varepsilon\left(N^\varepsilon\right).\end{aligned}$$

This motivates the following definition. Let $\varepsilon > 0$ and $C = C(\varepsilon) > 0$ be sufficiently large, and set

$$M(\phi_q^*) = N\|\eta_q^*\|_q^2 + CN^\varepsilon$$

for all $q \in \mathcal{Q}$, and

$$M(\psi_q^*) = N\|\kappa_q^*\|_q^2 + CN^\varepsilon$$

for all $q \in \mathcal{Q}\backslash\mathcal{E}$.

The following result shows that we can replace $M(\phi_q^*)$ and $M(\psi_q^*)$ by $N\|\eta_q^*\|_q^2$ and $N\|\kappa_q^*\|_q^2$ respectively in the summands at the cost of an acceptable error term.

Lemma 5.3.19. *If*

$$\gamma_q \ll (N|t(q)|\varphi(q))^2 \tag{5.3.17}$$

for all $q \in \mathcal{Q}$, or if

$$\gamma_q \ll \frac{N^2|t(q)|\varphi(q)\varphi((q_1,q')q_2^2)}{\varphi(q')} \tag{5.3.18}$$

for all $q \in \mathcal{Q}$, then

$$\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}\gamma_q = \sum_{q\in\mathcal{Q}} \frac{\gamma_q}{N\|\eta_q^*\|_q^2} + O_\varepsilon\left(N^\varepsilon\right). \tag{5.3.19}$$

The same holds if we replace $\left(\phi_q^*, \eta_q^*, \mathcal{Q}\right)$ by $\left(\psi_q^*, \kappa_q^*, \mathcal{Q}\backslash\mathcal{E}\right)$.

Proof. Taking the difference and by Lemma 5.3.17, it is enough to bound

$$N^\varepsilon \sum_{q\in\mathcal{Q}} \frac{\gamma_q}{N\varphi(q)\left(N\varphi(q)+CN^\varepsilon\right)}. \tag{5.3.20}$$

First we suppose (5.3.17) holds and by recalling (5.3.1), we majorize the sum above by

$$\begin{aligned}\sum_{q\in\mathcal{Q}}|t(q)|^2 &\ll \sum_{q_1\le Q_1}|t(q_1)|^2 \sum_{\substack{q_2\le Q_2\\ q_2^2|q'}}|t(q_2^2)|^2\\ &\ll_\varepsilon Q^\varepsilon \sum_{q_1\le Q_1}\frac{1}{q_1^4}\sum_{\substack{q_2\le Q_2\\ q_2^2|q'}}\frac{1}{q_2^4}\\ &\ll_\varepsilon N^\varepsilon.\end{aligned}$$

Therefore (5.3.19) holds. The argument also holds if we replace $\left(\phi_q^*, \eta_q^*, \mathcal{Q}\right)$ by $\left(\psi_q^*, \kappa_q^*, \mathcal{Q}\backslash\mathcal{E}\right)$.

Next we assume (5.3.18). Using (5.3.20) and Lemma 5.3.17, we are lead to bound

$$N^\varepsilon \sum_{q\in\mathcal{Q}} \frac{|t(q)|\varphi((q_1,q')q_2^2)}{\varphi(q')\varphi(q)}.$$

Recalling (5.3.1), the sum above is majorized by

$$\begin{aligned}\frac{1}{\varphi(q')}\sum_{q_1\le Q_1}\frac{|t(q_1)|\varphi((q_1,q'))}{\varphi(q_1)}\sum_{\substack{q_2\le Q_2\\ q_2^2|q'}}|t(q_2^2)| &\ll_\varepsilon Q^\varepsilon \sum_{q_1\le Q_1}\frac{1}{q_1^2}\sum_{q_2\le Q_2}\frac{1}{q_2^2}\\ &\ll_\varepsilon N^\varepsilon.\end{aligned}$$

The same holds when we replace $\left(\phi_q^*, \eta_q^*, \mathcal{Q}\right)$ by $\left(\psi_q^*, \kappa_q^*, \mathcal{Q}\backslash\mathcal{E}\right)$. □

Lemma 5.3.20. *For all $A, \varepsilon > 0$, we have*

$$[g|g] - \sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[g|\phi_q^*]|^2 - \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}|[g|\psi_q^*]|^2$$

is

$$O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon} + NQ_1^{-2} + NQ_2^{-1}\right).$$

Proof. Write

$$\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[g|\phi_q^*]|^2 = \sum_{q\in\mathcal{Q}} \beta_q[\phi_q^*|g],$$

where $\beta_q = M(\phi_q^*)^{-1}[g|\phi_q^*]$. By Lemma 5.3.16, we replace $[\phi_q^*|g]$ by $N[\eta_q^*|\vartheta_q^*]$ up to an error term. Indeed

$$\begin{aligned}\sum_{q\in\mathcal{Q}} \beta_q[\phi_q^*|g] &= N\sum_{q\in\mathcal{Q}} \beta_q[\eta_q^*|\vartheta_q^*]_q + O_\varepsilon\left(N^{1/2}\sum_{q\in\mathcal{Q}} \beta_q q^{3/2+\varepsilon}\right)\\ &= N\sum_{q\in\mathcal{Q}} \beta_q[\eta_q^*|\vartheta_q^*]_q + O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon}\right)\end{aligned}$$

after recalling (5.3.1) and by using the bound

$$\begin{aligned}\beta_q &\ll (N|t(q)|\varphi(q) + q^{3/2+\varepsilon}N^{1/2})/(N\phi(q))\\ &\ll 1\end{aligned}$$

collected from Lemma 5.3.16 and 5.3.17. Reiterating again we have

$$\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[g|\phi_q^*]|^2 = N^2\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[\eta_q^*|\vartheta_q^*]_q|^2 + O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon}\right).$$

We repeat this for the other sum and in total we get

$$\begin{aligned}&\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[g|\phi_q^*]|^2 + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}|[g|\psi_q^*]|^2\\ &= N^2\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[\eta_q^*|\vartheta_q^*]_q|^2 + N^2\sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}|[\vartheta_q^*|\kappa_q^*]_q|^2\\ &\quad + O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon}\right).\end{aligned}$$

By Lemma 5.3.19, we replace $M(\phi_q^*)$ by $N\|\eta_q^*\|_q^2$ up to an error term to get

$$N^2\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[\eta_q^*|\vartheta_q^*]_q|^2 = N\sum_{q\in\mathcal{Q}} \frac{|[\eta_q^*|\vartheta_q^*]_q|^2}{\|\eta_q^*\|_q^2} + O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon}\right).$$

We recall from (5.3.14) that

$$\vartheta_q^* = \frac{6t(q)}{\pi^2}\left(\eta_q^* + \kappa_q^*\right),$$

it follows

$$\begin{aligned}\frac{|[\vartheta_q^*|\eta_q^*]_q|^2}{\|\eta_q^*\|_q^2} + \frac{|[\vartheta_q^*|\kappa_q^*]_q|^2}{\|\kappa_q^*\|_q^2} &= \left(\frac{6t(q)}{\pi^2}\right)^2 \|\eta_q^*\|_q^2 + \left(\frac{6t(q)}{\pi^2}\right)^2 \|\kappa_q^*\|_q^2 \\ &= \|\vartheta_q^*\|_q^2\end{aligned}$$

by (5.3.13), (5.3.14) and Lemma 5.3.11, 5.3.14.

Next, we reiterate the process and replace $M(\psi_q^*)$ by $N\|\kappa_q^*\|_q^2$ up to an error term. In total we get

$$\begin{aligned}&\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[g|\phi_q^*]|^2 + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}|[g|\psi_q^*]|^2 \\ &= N\sum_{q\in\mathcal{Q}} \frac{|[\vartheta_q^*|\eta_q^*]_q|^2}{\|\eta_q^*\|_q^2} + N\sum_{q\in\mathcal{Q}\setminus\mathcal{E}} \frac{|[\vartheta_q^*|\kappa_q^*]_q|^2}{\|\kappa_q^*\|_q^2} + O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon}\right) \\ &= N\sum_{q\in\mathcal{Q}} \|\vartheta_q^*\|_q^2 + O_\varepsilon\left(N^{1/2}Q^{7+\varepsilon}\right).\end{aligned}$$

By Lemma 5.3.11 we have

$$\|\vartheta_q^*\|_q^2 = \left(\frac{6t(q)}{\pi^2}\right)^2 \varphi(q),$$

and thus completing the series we obtain

$$\begin{aligned}\sum_{q\in\mathcal{Q}} \|\vartheta_q^*\|_q^2 &= \left(\frac{6}{\pi^2}\right)^2 \sum_{q\in\mathcal{Q}} t(q)^2\varphi(q) \\ &= \left(\frac{6}{\pi^2}\right)^2 \sum_{q_1\le Q_1, q_2\le Q_2} \mu^2(q_1q_2)t(q_1)^2t(q_2)^2\varphi(q_1)\varphi(q_2^2) \\ &= \left(\frac{6}{\pi^2}\right)^2 \prod_{p=2}^{\infty}\left(1 + \frac{p-1}{(p^2-1)^2} + \frac{p(p-1)}{(p^2-1)^2}\right) + O\left(Q_1^{-2} + Q_2^{-1}\right) \\ &= \frac{6}{\pi^2} + O\left(Q_1^{-2} + Q_2^{-1}\right).\end{aligned}$$

Here the product over primes reduces to $\zeta(2) = \pi^2/6$, where ζ is the Riemann zeta function. Observe that by Lemma 5.3.7

$$[g|g] = \sum_{n\le N} \mu^2(N-n)$$

$$= \frac{6}{\pi^2} N + O\left(N^{1/2}\right)$$

and the result follows. □

Lemma 5.3.21. *The sum*

$$[f|f] - \sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[f|\phi_q^*]|^2 - \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}|[f|\psi_q^*]|^2 \ll N\mathcal{L}.$$

Proof. By [81, Lemma 1.1 and 1.2], we see that

$$0 \le \sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}|[f|\phi_q^*]|^2 + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}|[f|\psi_q^*]|^2 \le [f|f].$$

Therefore it is enough to bound $[f|f]$ and indeed the trivial bound suffices

$$[f|f] = \sum_{\substack{n\le N\\ n\equiv a'[q']}} \Lambda(n)^2 \le \mathcal{L}\sum_{n\le N}\Lambda(n) \ll N\mathcal{L}.$$

□

Lemma 5.3.22. *For all $A, \varepsilon > 0$, we have*

$$\sum_{q\in\mathcal{Q}} M(\varphi_q^*)^{-1}[f|\phi_q^*][\phi_q^*|g] + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}[f|\psi_q^*][\psi_q^*|g]$$

is

$$\mathfrak{S}_{a',q'}(N)N + O_{A,C_1,D_1,D_2,\varepsilon}\left(NQ^8\mathcal{L}^{-A} + NQ^{\varepsilon}Q_1^{-1}\right),$$

where $\mathfrak{S}_{a',q'}(N)$ is the singular series defined in Theorem 5.1.1.

Proof. For simplicity all implied constant in the $O(\cdot)$ term may depend on A, C_1, D_1, D_2, and ε.

Set $\alpha_q = M(\phi_q^*)^{-1}[f|\phi_q^*]$. By Lemma 5.3.16, we obtain

$$\begin{aligned}\sum_{q\in\mathcal{Q}} \alpha_q[\phi_q^*|g] &= N\sum_{q\in\mathcal{Q}} \alpha_q[\eta_q^*|\vartheta_q^*]_q + O\left(N^{1/2}\sum_{q\in\mathcal{Q}}\alpha_q q^{3/2+\varepsilon}\right)\\ &= N\sum_{q\in\mathcal{Q}} \alpha_q[\eta_q^*|\vartheta_q^*]_q + O\left(N^{1/2}Q^{10+\varepsilon}\right),\end{aligned}$$

by using the bound

$$\begin{aligned}\alpha_q &\ll \frac{N\varphi((q_1,q')q_2^2)\varphi(q')^{-1} + q^2N\mathcal{L}^{-A}}{N\varphi(q)}\\ &\ll_{\varepsilon} q^{1+\varepsilon},\end{aligned}$$

provided by Lemma 5.3.16 and 5.3.17.

Next, we set $\beta_q = M(\phi_q^*)^{-1}N[\eta_q^*|\vartheta_q^*]_q$. Then again by Lemma 5.3.16, we have

$$\sum_{q\in\mathcal{Q}}\beta_q[f|\phi_q^*] = N\sum_{q\in\mathcal{Q}}\beta_q[\rho_q^*|\eta_q^*]_q + O\left(N^{1/2}Q^{10+\varepsilon} + N\mathcal{L}^{-A}\sum_{q\in\mathcal{Q}}\beta_q q^2\right).$$

By Lemma 5.3.16 and 5.3.17, we assert

$$\begin{aligned}\beta_q &\ll \frac{N|t(q)|\varphi(q)}{N\varphi(q)}\\ &\ll 1,\end{aligned}$$

and by recalling (5.3.1) we get that the error term above is $O\left(NQ^8\mathcal{L}^{-A}\right)$.

We do the same for the other sum and we ultimately obtain

$$\begin{aligned}&\sum_{q\in\mathcal{Q}}M(\phi_q^*)^{-1}[f|\phi_q^*][\phi_q^*|g] + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}}M(\psi_q^*)^{-1}[f|\psi_q^*][\psi_q^*|g]\\ &= N^2\sum_{q\in\mathcal{Q}}M(\phi_q^*)^{-1}[\rho_q^*|\eta_q^*][\eta_q^*|\vartheta_q^*] + N^2\sum_{q\in\mathcal{Q}\setminus\mathcal{E}}M(\psi_q^*)^{-1}[\rho_q^*|\kappa_q^*][\kappa_q^*|\vartheta_q^*] + O\left(NQ^8\mathcal{L}^{-A}\right).\end{aligned}$$

Next by applying Lemma 5.3.19 we replace $M(\phi_q^*)$ with $N\|\eta_q^*\|_q^2$ up to an error term to obtain

$$N^2\sum_{q\in\mathcal{Q}}M(\phi_q^*)^{-1}[\rho_q^*|\eta_q^*][\eta_q^*|\vartheta_q^*] = N\sum_{q\in\mathcal{Q}}\frac{[\rho_q^*|\eta_q^*][\eta_q^*|\vartheta_q^*]}{\|\eta_q^*\|_q^2} + O\left(NQ^8\mathcal{L}^{-A}\right).$$

We recall from (5.3.14) and (5.3.13) that

$$\vartheta_q^* = \frac{6t(q)}{\pi^2}\left(\eta_q^* + \kappa_q^*\right)$$

and

$$\rho_q^* = \frac{\mathbb{1}_{q_2^2|q'}\cdot\mu(q_1/(q_1,q'))}{\varphi(q')\varphi(q_1/(q_1,q'))}\left(\eta_q^* - \kappa_q^*\right).$$

It follows

$$\begin{aligned}\frac{[\rho_q^*|\eta_q^*]_q\cdot[\eta_q^*|\vartheta_q^*]_q}{\|\eta_q^*\|_q^2} + \frac{[\rho_q^*|\kappa_q^*]_q\cdot[\kappa_q^*|\vartheta_q^*]_q}{\|\kappa_q^*\|_q^2} &= \mathbb{1}_{q_2^2|q'}\cdot\frac{6t(q)\mu(q_1/(q_1,q'))}{\pi^2\varphi(q')\varphi(q_1/(q_1,q'))}\left(\|\eta_q^*\|_q^2 - \|\kappa_q^*\|_q^2\right)\\ &= [\rho_q^*|\vartheta_q^*]_q\end{aligned}$$

by (5.3.13), (5.3.14) and Lemma 5.3.13, 5.3.14.

We reiterate the same procedure and replace $M(\psi_q^*)$ with $N\|\kappa_q^*\|_q^2$ up to an error term. In total we have

$$\begin{aligned}
&\sum_{q\in\mathcal{Q}} M(\phi_q^*)^{-1}[f|\varphi_q^*][\varphi_q^*|g] + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M(\psi_q^*)^{-1}[f|\psi_q^*][\psi_q^*|g] \\
&= N\sum_{q\in\mathcal{Q}} \frac{[\rho_q^*|\eta_q^*][\eta_q^*|\vartheta_q^*]}{\|\eta_q^*\|_q^2} + N\sum_{q\in\mathcal{Q}\setminus\mathcal{E}} \frac{[\rho_q^*|\kappa_q^*][\kappa_q^*|\vartheta_q^*]}{\|\kappa_q^*\|_q^2} \\
&\quad + O\left(NQ^8\mathcal{L}^{-A}\right) \\
&= N\sum_{q\in\mathcal{Q}} [\rho_q^*|\vartheta_q^*]_q + O\left(NQ^8\mathcal{L}^{-A}\right).
\end{aligned}$$

Next we compute the sum

$$\sum_{q\in\mathcal{Q}} [\rho_q^*|\vartheta_q^*]_q = \frac{6}{\varphi(q')\pi^2}\sum_{q\in\mathcal{Q}} \mathbb{1}_{q_2^2|q'}\cdot \frac{t(q)c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')}{\mu(q_1/(q_1,q'))\varphi(q_1/(q_1,q'))}.$$

We complete the series and so the right hand side becomes

$$\frac{6}{\varphi(q')\pi^2}\sum_{\substack{q_1,q_2=1\\ \mu^2(q_1q_2)=1}}^{\infty} \mathbb{1}_{q_2^2|q'}\cdot \frac{t(q_1q_2^2)c_{q_1/(q_1,q')}(N)c_{(q_1,q')q_2^2}(N-a')}{\mu(q_1/(q_1,q'))\varphi(q_1/(q_1,q'))},$$

at the cost of an error term of

$$\begin{aligned}
&\ll \frac{1}{\varphi(q')}\sum_{q_1>Q_1} t(q_1)\varphi((q_1,q'))\sum_{\substack{q_2>Q_2\\ \mu^2(q_1q_2)=1}} \mathbb{1}_{q_2^2|q'}\cdot t(q_2^2)\varphi(q_2^2) \\
&\ll_\varepsilon Q^\varepsilon Q_1^{-1},
\end{aligned}$$

since the number of divisors of q' is at most $O_\varepsilon(Q^\varepsilon)$ and by recalling (5.3.1). The singular series can be represented as an infinite product

$$\prod_{p=2}^{\infty}\left(1+\frac{t(p)c_{p/(p,q')}(N)c_{(p,q')}(N-a')}{\mu(p/(p,q'))\varphi(p/(p,q'))}+\mathbb{1}_{p^2|q'}\cdot t(p^2)c_{p^2}(N-a')\right).$$

If $p\nmid q'$, $p\parallel q'$, or $p^2\mid q'$ then the term in the product simplifies to

$$1+\frac{c_p(N)}{(p^2-1)(p-1)},\quad 1-\frac{c_p(N-a')}{p^2-1},\quad 1-\frac{c_p(N-a)+c_{p^2}(N-a)}{p^2-1}$$

respectively. The result follows. □

5.4 Proof of Theorem 5.1.1

For any $h_1, h_2 \in \mathscr{F}([1,N])$, let us denote

$$\langle h_1|h_2\rangle = \sum_{q\in\mathcal{Q}} M^{-1}(\phi_q^*)[h_1|\phi_q^*][\phi_q^*|h_2] + \sum_{q\in\mathcal{Q}\setminus\mathcal{E}} M^{-1}(\psi_q^*)[h_1|\psi_q^*][\psi_q^*|h_2].$$

We recall f, g from (5.3.11), (5.3.12) respectively and consequently the product

$$[f|g] = \sum_{\substack{N=n_1+n_2\\ n_1\equiv a'[q']}} \Lambda(n_1)\mu^2(n_2).$$

By Cauchy's inequality, we assert

$$|[f|g] - \langle f|g\rangle| \leq \sqrt{([f|f] - \langle f|f\rangle)\cdot([g|g] - \langle g|g\rangle)}.$$

By Lemma 5.3.20 and 5.3.21, the right hand side is majorised by

$$\begin{aligned}
&\ll_{A,C_1,D_1,D_2,\varepsilon} \sqrt{N\mathcal{L}\left(N^{1/2}Q^{7+\varepsilon} + NQ_1^{-2} + NQ_2^{-1}\right)}\\
&\ll_{A,C_1,D_1,D_2,\varepsilon} N\mathcal{L}^{1/2}\left(Q_1^{-1} + Q_2^{-1/2}\right).
\end{aligned}$$

Hence we can approximate $[f|g]$ by $\langle f|g\rangle$, and by Lemma 5.3.22 we obtain

$$\begin{aligned}
[f|g] &= \mathfrak{S}_{a',q'}(N)N\\
&\quad + O_{A,C_1,D_1,D_2,\varepsilon}\left(NQ^8\mathcal{L}^{-A} + NQ^{\varepsilon}Q_1^{-1} + N\mathcal{L}^{1/2}\left(Q_1^{-1} + Q_2^{-1/2}\right)\right).
\end{aligned}$$

Recall from (5.3.10) that $Q_1 = \mathcal{L}^{D_1}, Q_2 = \mathcal{L}^{D_2}$, and $Q = \max\{Q_1, Q_2\}$. Taking

$$\begin{aligned}
D_1 &= C_1 + C_2 + 2,\\
D_2 &= 2D_1,\\
A &= 8D_2 + C_1 + C_2 + 1,
\end{aligned}$$

our product simplifies to

$$[f|g] = \mathfrak{S}_{a',q'}(N)N + O_{C_1,C_2}\left(N\mathcal{L}^{-C_1-C_2-1}\right).$$

Now notice that

$$\mathcal{R}_{a',q'}(N) = [f|g] + \sum_{k\geq 2}\sum_{\substack{p^k\leq N\\ p^k\equiv a'[q']}} \mu^2(N-p)\log(p).$$

The double sum can be estimated crudely by

$$\sum_{k\geq 2}\sum_{p^k\leq N}\log(p) \leq \sum_{2\leq k\leq \log N} N^{1/k} \ll_\varepsilon N^{1/2+\varepsilon},$$

and consequently

$$\mathcal{R}_{a',q'}(N) = \mathfrak{S}_{a',q'}(N)N + O_{C_1,C_2}\left(N\mathcal{L}^{-C_1-C_2-1}\right).$$

If $\mathfrak{S}_{a',q'}(N) = 0$ then there exists $p^2 \mid q'$ such that $p^2 \mid (N-a)$ by our remark after Theorem 5.1.1. Hence $\mathcal{R}_{a',q'}(N) = 0$ and the result follows. Otherwise if $\mathfrak{S}_{a',q'}(N) \neq 0$ then we bound from below

$$\begin{aligned}\mathfrak{S}_{a',q'}(N) &\gg \frac{1}{\varphi(q')}\prod_{p\| q'}\left(1-\frac{1}{p+1}\right)\\ &\geq \frac{1}{\varphi(q')}\exp\left\{\sum_{p\leq q'}\log\left(1-\frac{1}{p+1}\right)\right\}.\end{aligned}$$

Applying a Taylor series expansion for the logarithm

$$\log(1-x) = -\sum_{n=1}^{\infty}\frac{x^n}{n},$$

valid for $|x|<1$, we obtain

$$\begin{aligned}\mathfrak{S}_{a',q'}(N) &\geq \frac{1}{\varphi(q')}\exp\left(-\sum_{p\leq q'}\frac{1}{p} - \sum_{p\leq q'}\sum_{n=2}^{\infty}\frac{1}{n(p+1)^n}\right)\\ &= \frac{1}{\varphi(q')}\exp\{-\log\log q' + O(1)\}\\ &\gg_{C_1} \mathcal{L}^{-C_1-1}.\end{aligned}$$

Therefore

$$N\mathcal{L}^{-C_1-C_2-1} \ll_{C_1,C_2} \mathfrak{S}_{a',q'}(N)N\mathcal{L}^{-C_2},$$

and so

$$\mathcal{R}_{a',q'}(N) = \mathfrak{S}_{a',q'}(N)N\left\{1+O_{C_1,C_2}\left(\mathcal{L}^{-C_2}\right)\right\}.$$

CHAPTER 6

A Refinement of the Burgess Bound for Character Sums

"Number theory would be much easier if we had 33 fingers on each hand"

–A number theorist

A multiplicative character modulo a positive integer k is a completely multiplicative function $\chi : \mathbb{N} \to \mathbb{C}$ such that

(i) $\chi(n) = 0$ if $(n, k) > 1$,

(ii) $\chi(n + k) = \chi(n)$ for all $n \in \mathbb{N}$.

We call $\chi = \chi_0$ a principal or trivial character if $\chi(n) = 1$ whenever $(n, k) = 1$. If χ is a character modulo k and also a character modulo k' such that $k' \mid k$ then the smallest such $k' \geq 2$ is called the conductor of χ. When $k' = k$ then we call χ a primitive character.

Given a prime number q and a multiplicative character χ modulo q, we consider bounding the sums

$$\sum_{M<n\leq M+N} \chi(n). \tag{6.0.1}$$

The first nontrivial result in this direction, which is about a century old, is due to Pólya [80] and Vinogradov [96] and takes the form

$$\sum_{M<n\leq M+N} \chi(n) = O\left(q^{1/2} \log q\right) \tag{6.0.2}$$

where the implied constant is absolute. Clearly the bound (6.0.2) is non-trivial provided $N \geq q^{1/2}(\log q)^{1+\varepsilon}$ for any fixed $\varepsilon > 0$.

Several logarithmic improvements of (6.0.2) have recently been obtained for special characters. See [38, 42, 66] and references therein.

For large values of N, the Polya-Vinogradov bound (6.0.2) is still the sharpest result known today although Montgomery and Vaughan [73] have shown that assuming the truth of the Generalized Riemann Hypothesis we have

$$\sum_{M<n\leq M+N} \chi(n) = O\left(q^{1/2} \log\log q\right).$$

The Pólya–Vinogradov bound (6.0.2) can be thought of as roughly saying that for large N, the sequence $\{\chi(n)\}_{n=M+1}^{M+N}$ behaves like a typical random sequence chosen uniformly

from the image $\chi(\{1,\dots,q-1\})$. We expect this to be true for smaller values of N although this problem is much less understood. In the special case $M = 0$, the Generalized Riemann Hypothesis (GRH) implies that

$$\left|\sum_{0<n\le N}\chi(n)\right| \le N^{1/2}q^{o(1)}, \tag{6.0.3}$$

which is non-trivial provided $N \ge q^{\varepsilon}$ and is essentially optimal. Although the conditional bound (6.0.3) on the GRH is well-known, see for example [73, Section 1], it may not be easy to find a direct reference, however it can be easily derived from [44, Theorem 2].

We also note Tao [91] has shown that the generalized Elliott-Halberstam conjecture allows one to bound short character sums in the case $M = 0$.

For values of N below the Pólya–Vinogradov range, the sharpest unconditional bound for the sums (6.0.1) is due to Burgess [15,16] and may be stated as follows. For any prime number q, nontrivial multiplicative character χ modulo q and integer $r \ge 1$ we have

$$\sum_{M<n\le M+N}\chi(n) = O\left(N^{1-1/r}q^{(r+1)/4r^2}\log q\right), \tag{6.0.4}$$

where the implied constant may depend on r, and is nontrivial provided $N \ge q^{1/4+\varepsilon}$ for any fixed $\varepsilon > 0$. This bound has remained the sharpest for short sums over the past fifty years although slight refinements have been made by improving the factor $\log q$. For example, by [59, Equation (12.58)] we have

$$\sum_{M<n\le M+N}\chi(n) = O\left(N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/r}\right), \tag{6.0.5}$$

where the implied constant is absolute. It is also announced in [59, Chapter 12, Remark, p. 329], that one can actually obtain

$$\sum_{M<n\le M+N}\chi(n) = O\left(N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/2r}\right), \tag{6.0.6}$$

provided $r \ge 2$, see also [73, Theorem 9.27].

We also remark that in the initial range, that is, for $M = 0$, slight improvements of the bounds (6.0.5), (6.0.6) and also of Theorem 6.1.1 below are given in [28, 44, 46, 58]. However these improvements do not imply any improvement of the above bound of Burgess [14] on the smallest quadratic nonresidue. We also refer to [9] for a discussion. Finally, we recall that the best known bounds on the smallest quadratic nonresidue is $O\left(q^{1/4\sqrt{e}+o(1)}\right)$, and on the gaps between quadratic nonresidues is $O\left(q^{1/4}\log q\right)$, are both due to Burgess [14, 17].

We recall that both (6.0.5) and (6.0.6) are based on a bound of Friedlander and Iwaniec [35, Section 4] on the number of solutions to the congruence (6.2.9) however

with variables u_1, u_2 from the whole interval, without any arithmetic constraints. Imposing such constraints is a new idea which underlines our approach. Using this idea, we give a further refinement of the Burgess bound (6.0.4) and thus contribute to the series of logarithmic improvements (6.0.5) and (6.0.6). More specifically, we improve (6.0.6) by replacing the factor $(\log q)^{1/2r}$ by $(\log q)^{1/4r}$. We remark that Booker [10] has previously used shifts by products u_1u_2 where one of the variables is prime in the Friedlander-Iwaniec approach [35] in order to obtain a numerically explicit Burgess bound. The benefit of prime shifts being simpler computations with estimating greatest common divisors. Our argument can be considered as an elaboration of this idea and our improvement comes from averaging over numbers with no small prime factors rather than over an entire interval which we give in Section 6.2.2. Lastly, we remark that de la Bretèche & Munsch [21], and de la Bretèche, Munsch & Tenenbaum [22] has improved our result building on this idea.

6.1 Main result

The following result is joint work with B. Kerr & I. E. Shparlinski, and has been published in the Michigan Journal of Mathematics [63].

Theorem 6.1.1. *Let q be prime, $r \geq 2$, M and N integers with*

$$N \leq q^{1/2+1/4r}.$$

For any non-trivial multiplicative character χ modulo q, we have

$$\sum_{M<n\leq M+N} \chi(n) = O\left(N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r}\right).$$

Moreover the implied constant is absolute.

6.2 Preparations

6.2.1 Preliminary transformations

First we recall the following well-known bound which is contained in [92, Theorem 1.2] (with slightly weaker constants).

Lemma 6.2.1. *Let q be prime and χ a non-trivial multiplicative character modulo q. Then we have*

$$\sum_{\lambda=1}^{q}\left|\sum_{1\leq v\leq V}\chi(\lambda+v)\right|^{2r} \leq (2r)^r V^r q + 2rV^{2r}q^{1/2}.$$

For any positive real numbers w and z we denote

$$V(w) = \prod_{p<w}\left(1-\frac{1}{p}\right),$$

and

$$P(z) = \prod_{p<z} p. \tag{6.2.1}$$

It follows from Mertens formula, see [59, Equation (2.16)], that

$$\frac{1}{\log w} \ll V(w) \ll \frac{1}{\log w}. \tag{6.2.2}$$

For positive reals U and z, we define the set $\mathcal{U}_z(U)$ by

$$\mathcal{U}_z(U) = \{1 \leq u \leq U \ : \ (u, P(z)) = 1\}. \tag{6.2.3}$$

The following result follows from combining [23, Theorem 4.1] with arguments from the proof of [23, Lemma 4.3]. We also refer the reader to [36, Equation (6.104)].

Lemma 6.2.2. *Let $C > 0$ be sufficiently large and suppose that*

$$z^C \leq U. \tag{6.2.4}$$

Then for the cardinality of $\mathcal{U}_z(U)$, we have

$$\frac{U}{\log z} \ll \#\mathcal{U}_z(U) \ll \frac{U}{\log z}.$$

Proof. Let

$$\mathcal{A} = \{1, \dots, U\},$$

so that with notation as in [23, Theorem 4.1] we have

$$\#\mathcal{U}_z(U) = S(\mathcal{A}, \mathcal{P}, z),$$

and hence by [23, Theorem 4.1], for any $v \geq 1$ we have

$$\#\mathcal{U}_z(U) = UV(z)\left(1 + O\left(\exp(-v\log v - 3v/2)\right) + O\left(\sum_{\substack{n<z^{2v}\\ n|P(z)}} 3^{\nu(n)}|r_{\mathcal{A}}(n)|\right)\right.$$

Here

$$r_{\mathcal{A}}(n) = \#\{a \in \mathcal{A} \ : \ n \mid a\} - U/n \ll O(1).$$

Considering the last term on the right

$$\sum_{\substack{n<z^{2v}\\ n|P(z)}} 3^{\nu(n)}|r_{\mathcal{A}}(n)| \ll \sum_{\substack{n<z^{2v}\\ n|P(z)}} 3^{\nu(n)}$$

$$\leq z^{2v} \sum_{n|P(z)} \frac{3^{\nu(n)}}{n}$$
$$\leq z^{2v} \prod_{p<z} \left(1+\frac{3}{p}\right),$$

and since

$$\prod_{p<z} \left(1+\frac{3}{p}\right) \leq \prod_{p<z} \left(1-\frac{1}{p}\right)^{-3}$$
$$= V(z)^{-3},$$

we obtain

$$\sum_{\substack{n<z^{2v} \\ n|P(z)}} 3^{\nu(n)} |r_{\mathcal{A}}(n)| \ll z^{2v} V(z)^{-3},$$

which implies that

$$\#\mathcal{U}_z(U) = UV(z)\,(1+\mathcal{E}_1) + \mathcal{E}_2. \tag{6.2.5}$$

with the error terms

$$\mathcal{E}_1 \ll \exp(-v \log v - 3v/2)$$

and

$$\mathcal{E}_2 \ll \frac{z^{2v}}{V(z)^3}.$$

Let $\varepsilon > 0$ be sufficiently small and take

$$v = \frac{(1-\varepsilon)}{2} \frac{\log U}{\log z}.$$

Then we have

$$\mathcal{E}_2 \ll U^{1-\varepsilon} (\log z)^3, \tag{6.2.6}$$

and by (6.2.4) we may choose C such that

$$\mathcal{E}_1 \leq \frac{1}{2}. \tag{6.2.7}$$

Combining (6.2.5) with (6.2.6) and (6.2.7), we derive

$$UV(z) \ll \#\mathcal{U}_z(U) \ll UV(z),$$

and the result follows from the Mertens estimate (6.2.2). □

We recall a simplified form of [23, Lemma 4.4].

Lemma 6.2.3. *For any integers t, z, any real $U \geq 1$ and any positive constant $0 < A < 1/2$, we have*

$$\sum_{\substack{u \in \mathcal{U}_z(U) \\ t|u}} 1 \ll_A \frac{U}{t} V(z),$$

if $z < (Ut^{-1})^A$ and

$$\sum_{\substack{u \in \mathcal{U}_z(U) \\ t|u}} 1 \ll_A \frac{U}{t} V\left(\frac{U}{t}\right),$$

if $(Ut^{-1})^A \leq z$.

Note that Lemma 6.2.3 is non-trivial only if $(t, P(z)) = 1$.

6.2.2 *Congruences with numbers free of small prime factors*

The new ingredient underlying our argument is the following:

Lemma 6.2.4. *Let q be prime and z, M, N and U integers with*

$$U \leq N, \quad UN \leq q.$$

Fix a sufficiently small positive real number $0 < A < 1/2$ and suppose z satisfies

$$1 < z \leq U^A. \tag{6.2.8}$$

Let $P(z)$ and $\mathcal{U}_z(U)$ be given by (6.2.1) and (6.2.3), respectively, and let $I(z, M, N, U)$ count the number of solutions to the congruence

$$n_1 u_1 \equiv n_2 u_2 \pmod{q}, \tag{6.2.9}$$

with integral variables satisfying $M < n_1, n_2 \leq M + N$ and $u_1, u_2 \in \mathcal{U}_z(U)$. Then we have

$$I(z, M, N, U) \ll_A \#\mathcal{U}_z(U) N \left(1 + \frac{\log U}{(\log z)^2}\right).$$

Proof. For each pair of integers u_1 and u_2, we let $J(u_1, u_2)$ count the number of solutions to the congruence (6.2.9) in variables n_1, n_2 satisfying

$$M < n_1, n_2 \leq M + N,$$

so that

$$\begin{aligned} I(z,M,N,U) &= \sum_{u_1,u_2 \in \mathcal{U}_z(U)} J(u_1,u_2) \\ &= \sum_{u_1 \in \mathcal{U}_z(U)} J(u_1,u_1) + 2 \sum_{\substack{u_1,u_2 \in \mathcal{U}_z(U) \\ u_1<u_2}} J(u_1,u_2). \end{aligned}$$

Since

$$J(u_1,u_1) = N,$$

we have

$$I(z,M,N,U) = N \sum_{u_1 \in \mathcal{U}_z(U)} 1 + 2 \sum_{\substack{u_1,u_2 \in \mathcal{U}_z(U) \\ u_1<u_2}} J(u_1,u_2).$$

Using Lemma 6.2.3 (with $t = 1$), the bound (6.2.2) and recalling (6.2.8) we see that

$$\sum_{u_1 \in \mathcal{U}_z(U)} 1 \ll \frac{U}{\log z},$$

and hence

$$I(z,M,N,U) \ll \frac{NU}{\log z} + \sum_{\substack{u_1,u_2 \in \mathcal{U}_z(U) \\ u_1<u_2}} J(u_1,u_2). \tag{6.2.10}$$

Fix some pair u_1, u_2 with $u_1 < u_2$ and consider $J(u_1,u_2)$. We first note that $J(u_1,u_2)$ is bounded by the number of solutions to the equation

$$u_1(M+n_1) - u_2(M+n_2) = kq, \tag{6.2.11}$$

with integer variables n_1, n_2, k satisfying

$$1 \le n_1, n_2 \le N.$$

Since

$$\begin{aligned} |kq - (u_1-u_2)M| &\le UN \\ &< q, \end{aligned}$$

there exists at most one value k satisfying (6.2.11) and hence $J(u_1,u_2)$ is bounded by the number of solutions to the equation (6.2.11) with variables satisfying

$$1 \le n_1, n_2 \le N.$$

We may suppose $J(u_1,u_2)\geq 1$. Fixing one solution n_1^*, n_2^* to (6.2.11), we see that for any other solution n_1, n_2 we have

$$u_1(n_1-n_1^*)=u_2(n_2-n_2^*).$$

The above equation determines the residue of n_1 modulo $u_2/(u_1,u_2)$ and for each value of n_1 there exists at most one solution n_2. Since $U\leq N$ this implies that

$$J(u_1,u_2)\ll N\frac{(u_1,u_2)}{u_2},$$

and hence by (6.2.10), we derive

$$I(z,M,N,U)\ll \frac{NU}{\log z}+N\sum_{u_1,u_2\in\mathcal{U}_z(U)}\frac{(u_1,u_2)}{u_2}. \tag{6.2.12}$$

Considering the last sum on the right hand side and collecting together u_1 and u_2 with the same value $(u_1,u_2)=d$, we have

$$\begin{aligned}\sum_{u_1,u_2\in\mathcal{U}_z(U)}\frac{(u_1,u_2)}{u_2}&\leq \sum_{d\in\mathcal{U}_z(U)}d\sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2}}\frac{1}{u_2}\sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}}1\\ &=\Sigma_1+\Sigma_2,\end{aligned} \tag{6.2.13}$$

where

$$\Sigma_1=\sum_{d\in\mathcal{U}_z(U)}d\sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2\\ z\leq(u_2/d)^A}}\frac{1}{u_2}\sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}}1,$$

and

$$\Sigma_2=\sum_{d\in\mathcal{U}_z(U)}d\sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2\\ z>(u_2/d)^A}}\frac{1}{u_2}\sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}}1.$$

Considering Σ_1, by Lemma 6.2.3 and the condition $z\leq(u_2/d)^A$ we bound

$$\begin{aligned}\Sigma_1&\ll_A \sum_{d\in\mathcal{U}_z(U)}\sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2\\ z\leq(u_2/d)^A}}V(z)\\ &\ll_A V(z)\sum_{d\in\mathcal{U}_z(U)}\sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2\\ z\leq(u_2/d)^A}}1.\end{aligned}$$

The condition $z \le (u_2/d)^A$ in the innermost summation implies that the outer summation over d is non empty only if $z \le (U/d)^A$ and hence by Lemma 6.2.3 we have

$$\begin{aligned}\Sigma_1 &\ll_A V(z) \sum_{\substack{d\in\mathcal{U}_z(U)\\ z\le(U/d)^A}} \sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d\mid u_2}} 1\\ &\ll_A UV(z)^2 \sum_{d\in\mathcal{U}_z(U)} \frac{1}{d}.\end{aligned} \tag{6.2.14}$$

Set

$$S(t) = \sum_{d\in\mathcal{U}_z(t)} 1.$$

Hence applying partial summation and Lemma 6.2.3, we obtain

$$\begin{aligned}\sum_{d\in\mathcal{U}_z(U)} d^{-1} &= \frac{S(U)}{U} + \int_1^U \frac{S(t)}{t^2}\,\mathrm{d}t\\ &\ll V(z) + \int_1^{z^{1/A}} \frac{S(t)}{t^2}\,\mathrm{d}t + \int_{z^{1/A}}^U \frac{S(t)}{t^2}\,\mathrm{d}t.\end{aligned} \tag{6.2.15}$$

For the first integral, bounding trivially $S(t) \le t$, we derive

$$\begin{aligned}\int_1^{z^{1/A}} \frac{S(t)}{t^2}\,\mathrm{d}t &\ll \int_1^{z^{1/A}} \frac{1}{t}\,\mathrm{d}t\\ &\ll \log z.\end{aligned} \tag{6.2.16}$$

For the second integral, after applying Lemma 6.2.3, we have

$$\begin{aligned}\int_{z^{1/A}}^U \frac{S(t)}{t^2}\,\mathrm{d}t &\ll V(z)\int_1^U \frac{1}{x}\,\mathrm{d}x\\ &\ll V(z)\log U.\end{aligned} \tag{6.2.17}$$

Substituting (6.2.16) and (6.2.17) in (6.2.15) we obtain

$$\sum_{d\in\mathcal{U}_z(U)} \frac{1}{d} \ll V(z) + \log z + V(z)\log U.$$

In turn, substituting this inequality in (6.2.14) and recalling the Mertens estimate (6.2.2) on $V(z)$, we derive

$$\begin{aligned}\Sigma_1 &\ll_A UV(z)^2\left(V(z) + \log z + \frac{\log U}{\log z}\right)\\ &\ll_A \frac{U}{\log z}\left(1 + \frac{\log U}{(\log z)^2}\right).\end{aligned} \tag{6.2.18}$$

It remains to bound Σ_2. Note that

$$\begin{aligned}\Sigma_2 &= \sum_{d\in\mathcal{U}_z(U)} d \sum_{\substack{u_2\in\mathcal{U}_z(\min\{U,z^{1/A}d\})\\ d|u_2}} \frac{1}{u_2} \sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}} 1\\ &= \Sigma_{21}+\Sigma_{22},\end{aligned}$$

where

$$\Sigma_{21} = \sum_{d\in\mathcal{U}_z(Uz^{-1/A})} d \sum_{\substack{u_2\in\mathcal{U}_z(z^{1/A}d)\\ d|u_2}} \frac{1}{u_2} \sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}} 1,$$

and

$$\Sigma_{22} = \sum_{\substack{d\in\mathcal{U}_z(U)\\ d>Uz^{-1/A}}} d \sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2}} \frac{1}{u_2} \sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}} 1.$$

Bounding the innermost sum of Σ_{21} trivially, we have

$$\Sigma_{21} \ll \sum_{d\in\mathcal{U}_z(Uz^{-1/A})} \sum_{\substack{u_2\in\mathcal{U}_z(z^{1/A}d)\\ d|u_2}} 1.$$

Noting that $z \le (z^{1/A})^A$, an application of Lemma 6.2.3 gives

$$\begin{aligned}\Sigma_{21} &\ll_A z^{1/A}V(z) \sum_{d\in\mathcal{U}_z(Uz^{-1/A})} 1\\ &\ll_A V(z)U\\ &\ll_A \frac{U}{\log z}.\end{aligned} \tag{6.2.19}$$

It remains to bound Σ_{22}. Recalling that

$$\Sigma_{22} = \sum_{\substack{d\in\mathcal{U}_z(U)\\ d>Uz^{-1/A}}} d \sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2}} \frac{1}{u_2} \sum_{\substack{u_1\in\mathcal{U}_z(u_2)\\ d|u_1}} 1,$$

by Lemma 6.2.3 and noting that $z > (u_2/d)^A$ since $d > Uz^{-1/A}$, we obtain

$$\Sigma_{22} \ll_A \sum_{\substack{d\in\mathcal{U}_z(U)\\ d>Uz^{-1/A}}} \sum_{\substack{u_2\in\mathcal{U}_z(U)\\ d|u_2}} V\left(\frac{u_2}{d}\right).$$

Set

$$R_d = \frac{\log(U/d)}{\log z}. \tag{6.2.20}$$

Then $R_d \geq 1$ if and only if $d \leq Uz^{-1}$ and hence

$$\Sigma_{22} \ll_A \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} \sum_{1 \leq r \leq R_d} \sum_{\substack{u_2 \in \mathcal{U}_z(dz^r) \\ d \mid u_2 \\ u_2 \geq dz^{r-1}}} V\left(\frac{u_2}{d}\right).$$

Fixing a value of r and considering the innermost summation over u_2, since $z^{r-1} \leq u_2/d$ we have $V(u_2/d) \leq V(z^{r-1})$ and therefore we assert

$$\Sigma_{22} \ll_A \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} \sum_{1 \leq r \leq R_d} V(z^{r-1}) \sum_{\substack{u_2 \in \mathcal{U}_z(dz^r) \\ d \mid u_2}} 1.$$

Appealing to Lemma 6.2.3 and separating the term $r = 1$, we have

$$\begin{aligned}\Sigma_{22} &\ll_A \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} \sum_{1 \leq r \leq R_d} V(z^{r-1}) z^r \max\{V(z), V(z^r)\} \\ &\ll_A V(z) \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} z + V(z)^2 \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} \sum_{2 \leq r \leq R_d} z^r,\end{aligned}$$

so that bounding the first sum trivially gives

$$\Sigma_{22} \ll_A UV(z) + V(z)^2 \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} \sum_{2 \leq r \leq R_d} z^r.$$

We see from (6.2.20) that $z^{R_d} = Ud^{-1}$ and hence

$$\begin{aligned}\sum_{2 \leq r \leq R_d} z^r &\ll z^{R_d} \\ &= \frac{U}{d},\end{aligned}$$

which implies that

$$\Sigma_{22} \ll_A UV(z) + UV(z)^2 \sum_{\substack{d \in \mathcal{U}_z(U/z) \\ d > Uz^{-1/A}}} \frac{1}{d},$$

and hence

$$\begin{aligned}\Sigma_{22} &\ll_A UV(z)^2 + UV(z)^2 \sum_{Uz^{-1/A} < d \leq U} \frac{1}{d} \\ &\ll_A UV(z)^2 \log z \\ &\ll_A \frac{U}{\log z}.\end{aligned} \tag{6.2.21}$$

Combining (6.2.13), (6.2.18), (6.2.19) and (6.2.21) we get

$$\sum_{u_1,u_2\in\mathcal{U}_z(U)} \frac{(u_1,u_2)}{u_2} \ll_A \frac{U\log U}{(\log z)^3} + \frac{U}{\log z},$$

and hence by (6.2.12)

$$I(z,M,N,U) \ll_A \frac{NU}{\log z}\left(1+\frac{\log U}{(\log z)^2}\right),$$

which together with Lemma 6.2.2 completes the proof since A is assumed sufficiently small. □

6.3 Proof of Theorem 6.1.1

We fix an integer $r \geq 2$ and proceed by induction on N. We formulate our induction hypothesis as follows. There exists some constant c_1, to be determined later, such that for any integer M and any integer $K < N$ we have

$$\left|\sum_{M<n\leq M+K}\chi(n)\right| \leq c_1 K^{1-1/r} q^{(r+1)/4r^2}(\log q)^{1/4r},$$

and we aim to show that

$$\left|\sum_{M<n\leq M+N}\chi(n)\right| \leq c_1 N^{1-1/r} q^{(r+1)/4r^2}(\log q)^{1/4r} \tag{6.3.1}$$

with an absolute constant c_1. Since the result is trivial for $N < q^{1/4}$ this forms the basis of our induction. We define the integers U and V by

$$U = \left\lfloor \frac{N}{16rq^{1/2r}} \right\rfloor \qquad \text{and} \qquad V = \left\lfloor rq^{1/2r} \right\rfloor, \tag{6.3.2}$$

and note that

$$UV \leq \frac{N}{16}. \tag{6.3.3}$$

We also note that with this choice of V the bound of Lemma 6.2.1 becomes

$$\begin{aligned}\sum_{\lambda=1}^{q}\left|\sum_{1\leq v\leq V}\chi(\lambda+v)\right|^{2r} &\leq (2r)^r V^r q + 2rV^{2r}q^{1/2} \\ &\leq (2r)^{2r} q^{3/2}. \end{aligned} \tag{6.3.4}$$

For any integers $1 \le u \le U$ and $1 \le v \le V$ we have

$$\begin{aligned}\sum_{M<n\le M+N}\chi(n) &= \sum_{M-uv<n\le M+N-uv}\chi(n+uv)\\ &= \sum_{M<n\le M+N}\chi(n+uv)+\sum_{M-uv<n\le M}\chi(n+uv)\\ &\quad -\sum_{M+N-uv<n\le M+N}\chi(n+uv).\end{aligned}$$

By (6.3.3) and our induction hypothesis we have

$$\left|\sum_{M-uv<n\le M}\chi(n+uv)\right| \le \frac{c_1}{4}N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r},$$

and

$$\left|\sum_{M+N-uv<n\le M+N}\chi(n+uv)\right| \le \frac{c_1}{4}N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r},$$

which combined with the above implies that

$$\left|\sum_{M<n\le M+N}\chi(n)-\sum_{M<n\le M+N}\chi(n+uv)\right| \le \frac{c_1}{2}N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r}.$$

Set

$$z = \exp\left((\log U)^{1/2}\right), \tag{6.3.5}$$

and let $P(z)$ and $\mathcal{U}_z(U)$ be defined by (6.2.1) and (6.2.3), respectively.

Averaging over $u \in \mathcal{U}_z(U)$ and $1 \le v \le V$ we see that

$$\left|\sum_{M<n\le M+N}\chi(n)\right| \le \frac{W}{\#\mathcal{U}_z(U)V}+\frac{c_1}{2}N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r}, \tag{6.3.6}$$

where

$$W = \sum_{M<n\le M+N}\sum_{u\in\mathcal{U}_z(U)}\left|\sum_{1\le v\le V}\chi(n+uv)\right|. \tag{6.3.7}$$

By multiplying the innermost summation in (6.3.7) by $\chi(u^{-1})$ and collecting the values of $nu^{-1} \pmod q$, we arrive at

$$W = \sum_{\lambda=1}^{q} I(\lambda)\left|\sum_{1\le v\le V}\chi(\lambda+v)\right|,$$

where $I(\lambda)$ counts the number of solutions to the congruence

$$n \equiv \lambda u \pmod{q}, \qquad M < n \leq M + N,\ u \in \mathcal{U}_z(U).$$

Writing

$$W = \sum_{\lambda=1}^{q} I(\lambda)^{(r-1)/r} \left(I(\lambda)^2\right)^{1/2r} \left| \sum_{1 \leq v \leq V} \chi(\lambda + v) \right|,$$

and applying the Hölder inequality give

$$W^{2r} \leq \left(\sum_{\lambda=1}^{q} I(\lambda) \right)^{2r-2} \left(\sum_{\lambda=1}^{q} I(\lambda)^2 \right) \left(\sum_{\lambda=1}^{q} \left| \sum_{1 \leq v \leq V} \chi(\lambda + v) \right|^{2r} \right).$$

From Lemma 6.2.2 we have

$$\begin{aligned} \sum_{\lambda=1}^{q} I(\lambda) &= \sum_{M < n \leq M+N} \sum_{u \in \mathcal{U}_z(U)} 1 \\ &= \#\mathcal{U}_z(U) N \\ &\ll \frac{NU}{\log z}. \end{aligned} \tag{6.3.8}$$

We have

$$\sum_{\lambda=1}^{q} I(\lambda)^2 = I(z, M, N, U),$$

where $I(z, M, N, U)$ is as in Lemma 6.2.4. Since $N < q^{1/2+1/4r}$ the conditions of Lemma 6.2.4 are satisfied, hence recalling (6.3.5) we have

$$\begin{aligned} \sum_{\lambda=1}^{q} I(\lambda)^2 &\ll \frac{NU}{\log z} \left(1 + \frac{\log U}{(\log z)^2}\right) \\ &\ll \frac{NU}{\log z}. \end{aligned} \tag{6.3.9}$$

Combining (6.3.4), (6.3.8), and (6.3.9) gives

$$W^{2r} \ll (2r)^{2r} q^{3/2} \left(\frac{NU}{\log z}\right)^{2r-1},$$

which using Lemma 6.2.2 we rewrite as

$$\left(\frac{W}{\#\mathcal{U}_z(U)}\right)^{2r} \ll (2r)^{2r} q^{3/2} N^{2r-1} \frac{\log z}{U}.$$

Hence

$$\frac{W}{\#\mathcal{U}_z(U)V} \ll r\frac{(\log z)^{1/2r}}{VU^{1/2r}}N^{1-1/2r}q^{3/4r}. \tag{6.3.10}$$

Using that $r^{1/r} \leq 2$ and recalling (6.3.2) and (6.3.5), we see that

$$V/r \gg q^{1/2r}, \qquad U^{1/2r} \gg N^{1/2r}q^{-1/4r^2}, \qquad \log z \ll (\log q)^{1/2},$$

where all implied constants are absolute. Therefore we now derive from (6.3.10) that

$$\frac{W}{\#\mathcal{U}_z(U)V} \leq c_0 N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r}$$

for some absolute constant c_0. Substituting the above into (6.3.6) gives

$$\left|\sum_{M<n\leq M+N}\chi(n)\right| \leq c_0 N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r} + \frac{c_1}{2}N^{1-1/r}q^{(r+1)/4r^2}(\log q)^{1/4r},$$

from which (6.3.1) follows on taking $c_1 = 2c_0$.

References

[1] N. C. Ankeny, *The least quadratic non residue.* Ann. of Math. (2) **55** (1952), 65–72. 44

[2] A. Ayyad, T. Cochrane, Z. Zheng, *The congruence $x_1x_2 \equiv x_3x_4 \bmod p$, the equation $x_1x_2 = x_3x_4$ and mean values of character sums.* J. Number Theory **59** (2) (1996), 398–413. 46

[3] R. C. Baker, *Diophantine Inequalities.* London Mathematical Society Monographs. New Series, 1. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1986. 4

[4] R. C. Baker, *Kloosterman sums with prime variable.* Acta Arith. **156** (4) (2012), 351–372. 33

[5] R. C. Baker, G. Harman, *On the distribution of αp^k modulo one.* Mathematika **38** (1) (1991), 170–184. 2

[6] A. Balog, A. Perelli, *Diophantine approximation by square-free numbers.* Ann. Sc. Norm. Super. Pisa Cl. Sci. (4) **11** (3) (1984), 353–359. 2

[7] A. Balog, C. Pomerance, *The distribution of smooth numbers in arithmetic progressions.* Proc. Amer. Math. Soc. **115** (1) (1992), 33–43. x, 41, 42, 43

[8] W. D. Banks, M. Z. Garaev, R. Heath-Brown, I. E. Shparlinski, *Density of non-residues in Burgess-type intervals and applications.* Bull. London Math. Soc. **40** (1) (2008), 88–96. 46

[9] J. W. Bober, L. Goldmakher, *Pólya–Vinogradov and the least quadratic non-residue.* Math. Ann. **366** (1–2) (2016), 853–863. 94

[10] A. R. Booker, *Quadratic class numbers and character sums.* Math. Comp. **75** (255) (2006), 1481–1492. 95

[11] A. Booker, C. Pomerance, *Squarefree smooth numbers and Euclidean prime generators.* Proc. Amer. Math. Soc. **145** (12) (2017), 5035–5042. 41

[12] J. Brüdern, A. Perelli, *Exponential sums of additive problems involving square-free numbers.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 28 (4) (1999), 591–613. 62

[13] V. Brun, *Le crible d'Eratosthene et le théorème de Goldbach.* Skr. Norske Vid.-Akad. Kristiana (1920), no. 3, 36. 59

[14] D. A. Burgess, *The distribution of quadratic residues and non-residues.* Mathematika, **4** (1957), 106–112. 43, 94

[15] D. A. Burgess, *On character sums and L-series.* Proc. Lond. Math. Soc. (3) **12** (1962), 193–206. 94

[16] D. A. Burgess, *On character sums and L-series.* II. Proc. Lond. Math. Soc. (3) **13** (1963), 524–536. 94

[17] D. A. Burgess, *A note on the distribution of quadratic residues and non-residues.* J. London Math. Soc. **38** (1963), 253–256. 94

[18] T. H. Chan, *Squarefull numbers in arithmetic progression* II. J. Number Theory **152** (2015), 90–104. 42

[19] J.-R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes.* Sci. Sinica **16** (1973), 157–176. 59

[20] H. Davenport, *Multiplicative number theory.* Springer-Velag, New York, 1980. 23, 33, 60

[21] R. de la Bretèche, M. Munsch, *Minimizing GCD sums and applications to non-vanishing of theta functions and to Burgess' inequality.* To appear, preprint available at arXiv:1812.03788, 2019. x, 95

[22] R. de la Bretèche, M. Munsch, G. Tenenbaum, *Small Gál sums and applications.* To appear, preprint available at arXiv:1906.12203, 2019. x, 95

[23] H. G. Diamond, H. Halberstam, W. F. Galway, *A Higher-dimensional sieve method: With Procedures for Computing Sieve Functions.* Cambridge Tracts in Math. **177**, Cambridge Univ. Press, Cambridge, 2008. 96, 98

[24] S. Drappeau, *Théorémes de type Fouvry-Iwaniec pour les entiers friables.* Compos. Math. **151** (5) (2015), 828–862. 41

[25] M. Drmota, R. Tichy, *Sequences, discrepancies and applications.* SpringerVerlag, Berlin, 1997. 36

[26] A. W. Dudek, *Explicit estimates in the theory of prime numbers.* Ph.D. thesis, The Australian National University, 2016. 60

[27] A. W. Dudek, *On the sum of a prime and a square-free number.* Ramanujan J. **42** (1) (2017), 233–240. 23, 33, 60

[28] P. D. T. A. Elliott, *Some remarks about multiplicative functions of modulus* ≤ 1. Analytic number theory, Progr. Math. **85**, Birkhäuser Boston, 1990, 159–164. 94

[29] P. Erdós, A. M. Odlyzko, A. Sárközy, *On the residues of products of prime numbers.* Period. Math. Hungar. **18** (3) (1987), 229–239. ix, 19, 33

[30] T. Estermann, *On the representations of a number as the sum of a prime and a quadratfrei number.* J. Lond. Math. Soc. **6** (3) (1931), 219–221. 33, 60

[31] T. Estermann, *On the representations of a number as the sum of two numbers not divisible by* k*-th powers.* J. Lond. Math. Soc. **6** (1) (1931), 37–40. 62

[32] C. J. A. Evelyn, E. H. Linfoot, *On a problem in the additive theory of numbers.* Math. Z. **34** (1) (1932), 637–644. 62

[33] E. Fouvry, I. E. Shparlinski, *On a ternary quadratic form over primes.* Acta Arith. **150** (3) (2011), 285–314. x, 33, 35

[34] J. Friedlander, *Integers free from large and small primes.* Proc. Lond. Math. Soc. (3) **33** (3) (1976), 565–576. 4

[35] J. B. Friedlander, H. Iwaniec, *Estimates for character sums.* Proc. Amer. Math. Soc. **119** (2) (1993), 365–372. 94, 95

[36] J. Friedlander, H. Iwaniec, *Opera de cribro.* AMS Colloquium Publications, **57**. American Math. Soc., Providence, RI., 2010. 60, 96

[37] J. B. Friedlander, P. Kurlberg, I. E. Shparlinski, *Products in residue classes.* Math. Res. Lett. **15** (6) (2008), 1133–1147. 19, 20, 33

[38] E. Fromm, L. Goldmakher, *Improving the Burgess bound via Pólya-Vinogradov.* Proc. Amer. Math. Soc. **147** (2) (2019), 461–466. 93

[39] M. Z. Garaev, *Estimation of Kloosterman Sums with Primes and Its Application.* Mat. Zametki **88** (3) (2010), 365–373. 20, 33, 35, 45

[40] M. Z. Garaev, *On multiplicative congruences.* Math. Z. **272** (1–2) (2012), 473–482. 33

[41] A. Ghosh, *The distribution of αp^2 modulo* 1. Proc. Lond. Math. Soc. **3** (2) (1981), 252–269. 2

[42] L. Goldmakher, Y. Lamzouri, *Large even order character sums.* Proc. Amer. Math. Soc. **142** (8) (2014), 2609–2614. 93

[43] S. W. Graham, C. J. Ringrose, *Lower bounds for least quadratic nonresidues.* Analytic number theory, Progr. Math. **85** (1990), 269–309. 44

[44] A. Granville, K. Soundararajan, *Large character sums.* J. Amer. Math. Soc. **14** (2) (2001), 365–397. 94

[45] G. Greaves, *Sieves in number theory.* Springer-Verlag, Berlin, 2001. 19

[46] A. Granville, K. Soundararajan, *Decay of mean values of multiplicative functions.* Canad. J. Math. **55** (6) (2003), 1191–1230. 94

[47] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers.* 6th ed., Oxford University Press, Oxford (2008). Revised by D. R. Heath-Brown and J. Silverman; With a foreword by Andrew Wiles. 1

[48] G. Harman, *On the distribution of αp modulo one.* J. Lond. Math. Soc. (2) **27** (1) (1983), 9–18. 2

[49] G. Harman, *Diophantine approximation with square-free integers.* Math. Proc. Cambridge Philos. Soc. **95** (3) (1984), 381–388. 2

[50] G. Harman, *On the distribution of αp modulo one.* II. Proc. Lond. Math. Soc. (3) **72** (2) (1996), 241–260. 2, 11, 15

[51] G. Harman, *Prime-Detecting Sieves.* London Math. Soc. Monogr. Ser. 33 (2007). ix, 2, 4, 5, 25

[52] A. J. Harper, *On a paper of K. Soundararajan on smooth numbers in arithmetic progressions.* J. Number Theory **132** (1) (2012), 182–199. 41

[53] D. R. Heath-Brown, *Diophantine approximation with square-free numbers.* Math. Z. **187** (3) (1984), 335–344. 2

[54] D. R. Heath-Brown, *The ternary Goldbach problem.* Rev. Mat. Iberoamericana **1** (1) (1985), 45–59. 60

[55] D. R. Heath-Brown, J.-C. Puchta, *Integers represented as a sum of primes and powers of two.* Asian J. Math. **6** (3) (2002), 535–565. 59

[56] D. R. Heath-Brown, C. Jia, *The distribution of αp modulo one.* Proc. Lond. Math. Soc. (3) **84** (1) (2002), 79–104. 2

[57] H. A. Helfgott, *The ternary Goldbach conjecture is true.* Too appear, preprint available at arXiv:1312.7748, 2014. 60

[58] A. Hildebrand, *A note on Burgess' character sum estimate.* C. R. Math. Rep. Acad. Sci. Canada **8** (1) (1986), 35–37. 94

[59] H. Iwaniec, E. Kowalski, *Analytic number theory,* Amer. Math. Soc. Colloq. Publ. **53** (2004). x, 5, 7, 22, 25, 44, 65, 94, 96

[60] C. Jia, *On the distribution of αp modulo one.* II. Sci. China Ser. A **43** (7) (2000), 703–721. 2

[61] G. A. Jones, J. M. Jones, *Elementary number theory.* Springer Undergraduate Mathematics Series. Springer-Verlag London, 1998. 64

[62] B. Kerr, *On the congruence $x_1x_2 \equiv x_3x_4 \bmod q$.* J. Number Theory **180** (2017), 154–168. 46

[63] B. Kerr, I. E. Shparlinski, K. H. Yau, *A Refinement of the Burgess Bound for Character Sums.* Michigan Math. J. **69** (2) (2020), 227–240. x, 95

[64] J. M. De Koninck, F. Luca, *Sur la proximité des nombres puissants.* Acta Arith. **114** (2) (2004), 149–157. 42

[65] J. M. De Koninck, F. Luca, I. E. Shparlinski, *Powerful numbers in short intervals.* Bull. Austral. Math. Soc. **71** (1) (2005), 11–16. 42

[66] Y. Lamzouri, A. P. Mangerel, *Large odd order character sums and improvements of the Pólya-Vinogradov inequality.* Too appear, preprint available at arXiv:1701.01042, 2017. 93

[67] Yu. V. Linnik, *Addition of primes numbers with powers of one and the same number.* Mat. Sbornik N.S. **32** (74), (1953), 3–60. 59

[68] Yu. V. Linnik, *The dispersion method in binary additive problems.* American Mathematical Society, RI 1963. 60

[69] Z. Liu, G. Lü, *Density of two squares of primes and powers of 2.* Int. J. Number Theory **7** (5) (2011), 1317–1329. 59

[70] K. Matomäki, *The distribution of αp modulo one.* Math. Proc. Cambridge Philos. Soc. **147** (2) (2009), 267–283. 2

[71] L. Mirsky, *The number of representations of an integer as the sum of a prime and a k-free integer.* Amer. Math. Monthly **56** (1949), 17–19. 33, 60, 61

[72] H. L. Montgomery, *Topics in multiplicative number theory.* Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, 1971. 44

[73] H. L. Montgomery, R. C. Vaughan, *Exponential sums with multiplicative coefficients.* Invent. Math. **43** (1) (1977), 69–82. 93, 94

[74] H. L. Montgomery, R. C. Vaughan, *Multiplicative number theory.* I. *Classical theory.* Cambridge Studies in Advanced Mathematics, 97. Cambridge University Press, Cambridge, 2007. 64

[75] M. Munsch, *Character sums over squarefree and squarefull numbers.* Arch. Math. **102** (6) (2014), 555–563. 42

[76] M. Munsch, I. E. Shparlinski, *On smooth square-free numbers in arithmetic progressions.* Too appear, preprint available at arXiv:1710.04705, 2018. 41, 45, 46, 47, 48

[77] M. Munsch, I. E. Shparlinski, K. H. Yau, *Smooth squarefree and squarefull integers in arithmetic progressions.* Mathematika **66** (1) (2020), 56–70. x, 42

[78] M. Munsch, T. Trudgian, *Square-full primitive roots.* Int. J. Number Theory **14** (4) (2018), 1013–1021. 42

[79] A. Page, *On the number of primes in an arithmetic progression.* Proc. London Math. Soc. (2) **39** (2) (1935), 116–141. 33, 60

[80] G. Pólya, *Ueber die Verteilung der quadratischen Reste und Nichtreste.* Königl. Ges. Wiss. Göttingen Nachr. (1918), 21–29. 93

[81] O. Ramaré, *Arithmetical aspects of the large sieve inequality.* Harish-Chandra Research Institute Lecture Notes 1, Hindustan Book Agency 2009. x, 60, 62, 63, 64, 65, 66, 70, 88

[82] O. Ramaré, A. Walker, *Products of primes in arithmetic progressions: a footnote in parity breaking.* J. Théor. Nombres Bordeaux **30** (1) (2018), 219–225. 19, 33

[83] É. Saias, *Entiers sans grand ni petit facteur premier.* I. Acta Arith. **61** (4) (1992), 347–374. 4

[84] É. Saias, *Entiers sans grand ni petit facteur premier.* II. Acta Arith. **63** (4) (1993), 287–312. 4

[85] É. Saias, *Entiers sans grand ni petit facteur premier.* III. Acta Arith. **71** (4) (1995), 351–379. 4

[86] W. Schmidt, *Diophantine Approximation.* Lecture Notes in Mathematics, Vol. 785, Springer-Verlag, 1980. 56

[87] I. E. Shparlinski, *On products of primes and almost primes in arithmetic progressions.* Period. Math. Hungar. **67** (1) (2013), 55–61. 19, 33

[88] I. E. Shparlinski, *On short products of primes in arithmetic progressions.* Proc. Amer. Math. Soc. **147** (3) (2019), 977–986. 19, 33

[89] K. Soundararajan, *The distribution of smooth numbers in arithmetic progressions.* Anatomy of integers, CRM Proc. Lecture Notes 46, Amer. Math. Soc., 2008, 115–128. 41

[90] D. Suryanarayana, R. Sitaramachandra Rao, *The distribution of square-full integers.* Ark. Mat. **11** (1973), 195–201. 44

[91] T. Tao, *The Elliott-Halberstam conjecture implies the Vinogradov least quadratic nonresidue conjecture.* Algebra Number Theory **9** (4) (2015), 1005–1034. 94

[92] E. Treviño, *The Burgess inequality and the least kth power non-residue.* Int. J. Number Theory **11** (5) (2015), 1653–1678. 95

[93] R. C. Vaughan, *On the distribution of αp modulo* 1. Mathematika **24** (2) (1977), 135–141. 2, 16

[94] R. C. Vaughan, *Sommes trigonométriques sur les nombres premiers.* C. R. Acad. Sci. Paris Sér. A–B **285** (16) (1977), A981–A983. 2

[95] R. C. Vaughan, *The Hardy-Littlewood method.* Second edition. Cambridge Tracts in Mathematics, 125. Cambridge University Press, Cambridge, 1997. 60

[96] I. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances.* J. Soc. Phys.-Math. Soc. Pwem. **1** (1919), 94–98. 93

[97] I. M. Vinogradov, *Representation of an odd number as a sum of three primes.* Dokl. Akad. Nauk SSR **15** (1937), 291–294. 59, 60

[98] A. Walker, *A multiplicative analogue of Schnirelmann's theorem.* Bull. Lond. Math. Soc. **48** (6) (2016), 1018–1028. 33

[99] K. C. Wong, *On the distribution of αp^k modulo* 1. Glasgow Math. J. **39** (2) (1997), 121–130. 2

[100] K. H. Yau, *Distribution of $\alpha n+\beta$ modulo* 1 *over integers free from large and small primes.* Acta Arith. **189** (1) (2019), 95–107. ix, 3