Improvements and Extensions of Two Theorems of Sárközy

by

Alex Joseph Rice

(Under the Direction of Neil Lyall)

Abstract

We explore quantitative improvements and extensions of two theorems of Sárközy, the qualitative versions of which state that any set of natural numbers of positive upper density necessarily contains two distinct elements which differ by a perfect square, as well as two elements which differ by one less than a prime number.

Index words: Arithmetic combinatorics, Additive combinatorics, Discrete Fourier analysis, Hardy-Littlewood circle method, Difference set, Sárközy's theorem, Intersective polynomials, $\mathcal{P}$-intersective polynomials

Improvements and Extensions of Two Theorems of Sárközy

by

Alex Joseph Rice

B.S., University of Georgia, 2008

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2012

Improvements and Extensions of Two Theorems of Sárközy

by

Alex Joseph Rice

Approved:

Major Professor:	Neil Lyall
Committee:	Malcolm Adams Ernest S. Croot III Robert Rumely

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
August 2012

Acknowledgements

I would like to thank my advisor and friend, Neil Lyall, without whom none of this work would be possible, and my fiancée, Whitney George, without whom nothing in my life would be possible.

I would like to thank Mariah Hamel and Ernie Croot for their collaboration and support, and I would like to thank Andrew Granville, whose questions inspired Chapter 8 of this thesis.

I would like to thank my parents for their unconditional love and support, as well as all of my friends, students and faculty alike, in the University of Georgia Mathematics Department.

Contents

1 Introduction

1.1 Background and Previous Results

A set $A \subseteq \mathbb{N}$ is said to have *positive upper density* if

$$\limsup_{N\to\infty} \frac{|A \cap [1,N]|}{N} > 0,$$

where $[1,N]$ always denotes $\{1,2,\ldots,N\}$. It is a central concern of the field of arithmetic combinatorics to determine which structures sets of positive upper density are guaranteed to contain.

Two Theorems of Sárközy

In the late 1970s, Sárközy and Furstenberg independently confirmed a conjecture of Lovász that any set of positive upper density necessarily contains two distinct elements which differ by a perfect square. Furstenberg [4] used ergodic theory and obtained a purely qualitative result, proving the conjecture in its qualitative form as stated above. Sárközy, however, employed Fourier analysis, specifically a density increment strategy inspired by Roth's proof of the analogous conjecture for three-term arithmetic progressions [20], to prove the following quantitative strengthening.

Theorem A (Sárközy, [22]). *If $A \subseteq [1,N]$ and $n^2 \notin A - A$ for all $n \in \mathbb{N}$, then*

$$\frac{|A|}{N} \ll \Big(\frac{(\log\log N)^2}{\log N}\Big)^{1/3}.$$

In this and the following theorems, $A - A$ denotes the difference set $\{a - a' : a, a' \in A\}$, the symbol $\ll$ denotes "less than a constant times", and we implicitly assume that N is large enough to make the right hand side of the inequalities defined and positive.

An extensive literature has developed on improvements and extensions of Theorem A, and simpler Fourier analytic proofs with weaker bounds can be found in [5] and [12]. In the same series of papers, Sárközy answered a similar question of Erdős, proving in particular that a set of positive upper density necessarily contains two elements which differ by one less than a prime number.

Theorem B (Sárközy, [23]). *If $A \subseteq [1, N]$ and $p - 1 \notin A - A$ for all primes p, then*

$$\frac{|A|}{N} \ll \frac{(\log\log\log N)^3 \log\log\log\log N}{(\log\log N)^2}. \tag{1.1}$$

An identical argument yields Theorem B with $p+1$ in place of $p-1$, but simple local considerations reveal that these are the only shifts admissible for such a result, as ± 1 are the only congruence classes which admit primes at every modulus. The bounds in Theorem B have been improved, first by Lucier [10] and later by Ruzsa and Sanders [21], who replaced (1.1) with $|A|/N \ll e^{-c(\log N)^{1/4}}$ for an absolute constant $c > 0$.

Improved Bounds for Squares

The best bound for the density of a set $A \subseteq [1, N]$ with no square differences, up to improvements of the constant μ in the exponent below, was obtained by Pintz, Steiger, and Szemerédi [18].

Theorem C (Pintz, Steiger, Szemerédi, [18]). *If $A \subseteq [1, N]$ and $n^2 \notin A - A$ for all $n \in \mathbb{N}$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu \log\log\log\log N}, \tag{1.2}$$

with $\mu = 1/12$.

Extensions to Polynomials

A natural generalization of Theorem A is the replacement of the squares with the image of a more general polynomial. For example, Balog, Pelikán, Pintz, and Szemerédi [1] modified the argument used in [18] to establish the bound from Theorem C with squares replaced by perfect k^{th}-powers for an arbitrary fixed $k \in \mathbb{N}$. In fact, they improved the constant μ in the exponent from $1/12$ to

1/4. However, to hope for such a result for a given polynomial $h \in \mathbb{Z}[x]$, it is clearly necessary that h has a root modulo q for every $q \in \mathbb{N}$, as otherwise there would exist q such that $q\mathbb{N}$, clearly a set of positive upper density, has no differences in the image of h. It follows from a theorem of Kamae and Mendès France [8] that this condition is also sufficient, in a qualitative sense, which leads to the following definition.

Definition 1.1. A polynomial $h \in \mathbb{Z}[x]$ is called *intersective* if for every $q \in \mathbb{N}$, there exists $r \in \mathbb{Z}$ such that $q \mid h(r)$. Equivalently, a polynomial $h \in \mathbb{Z}[x]$ is intersective if it has a root in the p-adic integers for every prime p.

Examples of intersective polynomials include any polynomial with an integer root and any polynomial with two rational roots with coprime denominators. However, there are also intersective polynomials with no rational roots, for example $(x^3-19)(x^2+x+1)$. Berend and Bilu [2] developed an algorithm to determine if a given polynomial is intersective.

The first broad quantitative generalization of Theorem A was obtained by Slijepčević [24], who showed triple logarithmic decay in the case of polynomials with an integer root. Lyall and Magyar [13] obtained a stronger, single logarithmic bound in the integer root case as a corollary of a higher dimensional result (see also [14]). The best current bounds for an arbitrary intersective polynomial are due to Lucier [11], who successfully adapted Sárközy's density increment procedure by utilizing p-adic roots and allowing the polynomial to change at each step of the iteration.

Theorem D (Lucier, [11])**.** *Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree $k \geq 2$. If $A \subseteq [1, N]$ and $h(n) \notin A - A$ for all $n \in \mathbb{N}$ with $h(n) > 0$, then*

$$\frac{|A|}{N} \ll \Big(\frac{(\log\log N)^{\mu}}{\log N}\Big)^{1/(k-1)}, \quad \mu = \begin{cases} 3 & \text{if } k = 2 \\ 2 & \text{if } k > 2 \end{cases},$$

where the implied constant depends only on h.

Here we provide an extremely mild improvement of this bound, showing that one can in fact take $\mu = 1$. By the symmetry of difference sets, Theorem D and all the following theorems clearly imply the analogous results for the negative values of a polynomial with negative leading term.

A Hybrid Result

Some work has also been done to combine extensions of Theorem A with Theorem B. Li and Pan [9] established the following quantitative result.

Theorem E (Li, Pan, [9])**.** *Suppose $h \in \mathbb{Z}[x]$ has positive leading term and $h(1) = 0$. If $A \subseteq [1, N]$ and $h(p) \notin A - A$ for all primes p with $h(p) > 0$, then*

$$\frac{|A|}{N} \ll 1/\log\log\log N.$$

The condition $h(1) = 0$ is needed to exploit, as in Theorem B, that there are primes congruent to 1 at every modulus, and again an identical argument yields the result under the condition $h(-1) = 0$.

1.2 New Results

$\mathcal{P}$-intersective Polynomials

Just as there are intersective polynomials without integer roots, it is natural to think that a result like Theorem E should hold for a larger class of polynomials. Also, due to the huge leap made by Ruzsa and Sanders [21] for the original $p - 1$ problem, we expect that the prime input restriction should not have a large impact on the quality of the bound, so the triple logarithmic decay in Theorem E should give way to a single logarithmic bound like in Theorem D.

A moment's consideration reveals that the correct analog to the intersective condition on a polynomial h when looking for differences of the form $h(p)$ is to insist that h not only has a root modulo q for every $q \in \mathbb{N}$, but has a root at a congruence class that admits infinitely many primes, leading to the following definition.

Definition 1.2. A polynomial $h \in \mathbb{Z}[x]$ is called *$\mathcal{P}$-intersective* if for every $q \in \mathbb{N}$, there exists $r \in \mathbb{Z}$ such that $(r, q) = 1$ and $q \mid h(r)$. Equivalently, for every prime p, there exists a p-adic integer z_p such that $h(z_p) = 0$ and $z_p \not\equiv 0 \mod p$.

Examples of $\mathcal{P}$-intersective polynomials include any polynomial with a root at 1 or -1 and any polynomial with two rational roots a/b and c/d such that $(ab, cd) = 1$. Again, there are also $\mathcal{P}$-intersective polynomials with no rational roots, in fact the same example, $(x^3 - 19)(x^2 + x + 1)$, still qualifies. The necessity of this condition is almost as clear as that of the original intersective condition. To exhibit this, suppose we have $h \in \mathbb{Z}[x]$ and $q \in \mathbb{N}$ such that the only roots of h modulo q share common factors with q. In particular, there are finitely many primes p such that $q \mid h(p)$. Letting $m = \max\{h(p)/q : p \in \mathcal{P},\ q \mid h(p)\}$ if such primes exist and $m = 0$ otherwise, we see that $q(m+1)\mathbb{N}$ is a set of positive upper density which contains no differences of the form $h(p)$.

Wierdl [26] observed in his thesis that one can again deduce the sufficiency of this condition, in a qualitative sense, from the aforementioned theorem of Kamae and Mendés France [8], and the following quantitative estimate is the first of our new results.

Theorem F (Rice, [19]). *Suppose $h \in \mathbb{Z}[x]$ is a $\mathcal{P}$-intersective polynomial of degree $k \geq 2$ with positive leading term. If $A \subseteq [1, N]$ and $h(p) \notin A - A$ for all $p \in \mathcal{P}$ with $h(p) > 0$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu} \tag{1.3}$$

for any $\mu < 1/(2k-2)$, where the implied constant depends only on h and μ.

In fact, with a few careful modifications one can sharpen (1.3) to

$$\frac{|A|}{N} \ll \Big(\frac{(\log\log N)^2(\log\log\log N)^{2k}}{\log N}\Big)^{1/(2k-2)},$$

but here we stick to the slightly less precise version for a more pleasing exposition.

Improved Bounds for Quadratic Polynomials

The method employed by Pintz et al. [18] and Balog et al. [1] to establish superior bounds for squares and k^{th}-powers, respectively, also utilizes a density increment iteration as a component of the argument. This suggests a potential marriage between this method and Lucier's modified density increment procedure to establish these improved bounds for an arbitrary intersective polynomial. Here we achieve this goal for degree $k = 2$ and briefly discuss the difficulties for higher

degrees. We also improve the constant μ in the exponent from $1/4$ to $1/\log 3$, the natural limit of the method as remarked in [1].

Theorem G (Hamel, Lyall, Rice, [6]). *Suppose $h \in \mathbb{Z}[x]$ is an intersective quadratic polynomial with positive leading term. If $A \subseteq [1, N]$ and $h(n) \notin A - A$ for all $n \in \mathbb{N}$ with $h(n) > 0$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu \log\log\log\log N}$$

for any $\mu < 1/\log 3$, where the implied constant depends only on h and μ.

It is worth pointing out that while the intersective condition can be somewhat mysterious and difficult to check for a general polynomial, this is not the case when restricted to degree 2, as a quadratic polynomial is intersective if and only if it has two rational roots with coprime denominators. While it follows from Theorem 1 of [2] that an intersective polynomial with no rational roots must have degree at least 5, the quadratic case can be shown rather easily by applying the quadratic formula over an appropriate field of p-adic numbers, and we provide a proof in Section 10.6.

Additionally, we adapt the method used to prove Theorem G and establish the analogous result for $\mathcal{P}$-intersective quadratic polynomials, in which the prime input restriction again accounts for a factor of 2 loss in the exponent.

Theorem H (Rice, [19]). *Suppose $h \in \mathbb{Z}[x]$ is a $\mathcal{P}$-intersective quadratic polynomial with positive leading term. If $A \subseteq [1, N]$ and $h(p) \notin A - A$ for all primes p with $h(p) > 0$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu \log\log\log\log N}$$

for any $\mu < 1/2\log 3$, where the implied constant depends only on h and μ.

It follows immediately from the aforementioned classification of intersective quadratic polynomials, combined with the requirement of p-adic integer roots which do not reduce to 0 mod p, that a quadratic polynomial is $\mathcal{P}$-intersective if and only if it has rational roots a/b and c/d with $(ab, cd) = 1$.

Remark on the Generalized Riemann Hypothesis

The reason for the discrepancy in the quality of bounds between Theorems D and G and their prime input analogs, Theorems F and H, is our limited knowledge of the distribution of primes in arithmetic progressions. Assuming the Generalized Riemann Hypothesis, one can considerably simplify the methods used to prove Theorems F and H and obtain the bounds without the factor of 2 loss in the exponent. Also assuming GRH, as remarked by Ruzsa and Sanders, one can simplify the method of [21] and improve the bound for the original $p-1$ problem to $|A|/N \ll e^{-c\sqrt{\log N}}$ for an absolute constant $c > 0$.

1.3 Brief Outline of Thesis

Part I (Chapters 2-8): Sarközy's Method via Lyall and Magyar

We begin in Chapter 2 by defining some preliminary notation regarding discrete Fourier analysis and the Hardy-Littlewood circle method, as well as proving the key density increment lemma which lies at the heart of each of the subsequent arguments. In Chapters 3, 4, and 6, we provide simplified, streamlined versions of the methods used to prove Theorems A, B, and D, respectively, and in each case we establish a stronger bound than the original. Additionally, we provide an exposition of Rusza and Sanders' [21] improvement of Theorem B in Chapter 5. In Chapter 7 we prove Theorem F, our first new result, and in Chapter 8 we give a template for further extensions of the common general method of the preceeding chapters. Without exception, the arguments in these chapters closely follow the approach of Lyall and Magyar [13].

Part II (Chapters 9-11): Improved Bounds for Quadratic Polynomials

We begin Part II in Chapter 9 by providing some slightly modified definitions and a new density increment lemma, analogous to those in Chapter 2. In Chapter 10 we streamline and extend the method of Pintz et al. [18] and Balog et al. [1] to prove Theorem G, and we make a brief remark on the limitations of the method with regard to non-monomials of higher degree. Finally, in Chapter 11, we make the minor modifications required to establish Theorem H.

2 Preliminaries

2.1 Notation for Explicit and Implied Constants

Vinogradov Symbols

As indicated in the introduction, we write $f(x) \ll g(x)$ if f and g are nonnegative functions and $f(x) \leq Cg(x)$ for some constant C and all x in the common domain of f and g. We also write $f(x) \gg g(x)$ if $g(x) \ll f(x)$.

Big-Oh Notation

As is standard, if f and g are complex-valued functions and h is a nonnegative function, we write $f(x) = g(x) + O(h(x))$ if $|f(x) - g(x)| \leq Ch(x)$ for some constant C and all x in the common domain of f and g. In particular, $f(x) = O(h(x))$ means exactly the same as $|f(x)| \ll h(x)$.

Technical Remark

At the expense of the implied constants in our theorems, we are free to insist that the main parameter N is sufficiently large, even with respect to a fixed polynomial h or exponent μ should they be involved. For convenience, we take this as a perpetual hypothesis and abstain from including it further. We use the letters C and c to denote appropriately large and small positive constants, respectively, which change from step to step and we allow, along with any implied constants, to depend on a fixed polynomial h and exponent μ if needed. The implied constants in the notation defined above do not depend on any other parameters unless otherwise stated.

2.2 Summation By Parts

We make frequent use of the following standard formula, which is simply integration by parts applied to an appropriate Riemann-Stieltjes integral.

Proposition 2.1 (Summation By Parts)**.** *If $a, b \geq 0$, $f : \mathbb{N} \to \mathbb{C}$, and $g : [a, b] \to \mathbb{C}$ is continuously differentiable, then*

$$\sum_{a<n\leq b} f(n)g(n) = S(b)g(b) - S(a)g(a) - \int_a^b S(x)g'(x)\mathrm{d}x,$$

where

$$S(x) = \sum_{1\leq n\leq x} f(n).$$

2.3 Fourier Analysis on $\mathbb{Z}$

For the majority of our discussions, we embed our finite sets in $\mathbb{Z}$, on which we utilize the discrete Fourier transform. Specifically, for a function $F : \mathbb{Z} \to \mathbb{C}$ with finite support, we define $\widehat{F} : \mathbb{T} \to \mathbb{C}$, where $\mathbb{T}$ denotes the circle parametrized by the interval $[0, 1]$ with 0 and 1 identified, by

$$\widehat{F}(\alpha) = \sum_{n\in\mathbb{Z}} F(n)e^{-2\pi in\alpha}.$$

Under the finite support assumption, standard properties like Plancherel's Identity

$$\int_0^1 |\widehat{F}(\alpha)|^2\mathrm{d}\alpha = \sum_{n\in\mathbb{Z}} |F(n)|^2$$

follow easily from the orthogonality relation

$$\int_0^1 e^{2\pi in\alpha}\mathrm{d}\alpha = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n \in \mathbb{Z} \setminus \{0\} \end{cases}. \tag{2.1}$$

Expressing Counts on the Transform Side

Given $N \in \mathbb{N}$ and a set $A \subseteq [1, N]$ with $|A| = \delta N$, we examine the Fourier analytic behavior of A by considering the *balance function*, f_A, defined by

$$f_A = 1_A - \delta 1_{[1,N]}.$$

The balance function can be used to detect deviations from the expected count of a prescribed arithmetic structure. Specifically, given a function $h : \mathbb{N} \to \mathbb{Z}$ and a weight $\nu : \mathbb{N} \to [0, \infty)$, if

$$H = \{n \in \mathbb{N} : 0 < h(n) < N/9\}$$

and $(A - A) \cap h(H) = \emptyset$, then

$$\begin{aligned}
\sum_{\substack{n\in\mathbb{Z}\\ m\in H}} f_A(n) f_A(n + h(m))\nu(m) = &\sum_{\substack{n\in\mathbb{Z}\\ m\in H}} 1_A(n)1_A(n + h(m))\nu(m) \\
&- \delta \sum_{\substack{n\in\mathbb{Z}\\ m\in H}} 1_A(n)1_{[1,N]}(n + h(m))\nu(m) \\
&- \delta \sum_{\substack{n\in\mathbb{Z}\\ m\in H}} 1_{[1,N]}(n - h(m))1_A(n)\nu(m) \\
&+ \delta^2 \sum_{\substack{n\in\mathbb{Z}\\ m\in H}} 1_{[1,N]}(n)1_{[1,N]}(n + h(m))\nu(m) \\
&\leq \Big(0 - \delta\big(|A \cap [1, 8N/9)| + |A \cap (N/9, N]|\big) + \delta^2 N\Big) \sum_{m\in H} \nu(m).
\end{aligned}$$

In particular, if $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, we have

$$\sum_{\substack{n\in\mathbb{Z}\\ m\in H}} f_A(n) f_A(n+h(m))\nu(m) \leq -\frac{\delta^2 N}{2} \sum_{m\in H} \nu(m). \tag{2.2}$$

Further, the orthogonality relation (2.1) allows us to express the form on the left hand side as an integral over the circle. Specifically, for any finite set $H \subseteq \mathbb{N}$ we have

$$\sum_{\substack{n\in\mathbb{Z}\\ m\in H}} f_A(n) f_A(n+h(m))\nu(m) = \sum_{\substack{x,y\in\mathbb{Z}\\ m\in H}} f_A(x) f_A(y)\nu(m) \int_0^1 e^{2\pi i(x-y+h(m))\alpha} \mathrm{d}\alpha$$

$$= \int_0^1 |\widehat{f_A}(\alpha)|^2 S(\alpha) \mathrm{d}\alpha,$$

where

$$S(\alpha) = \sum_{m\in H} \nu(m) e^{2\pi i h(m)\alpha}.$$

In particular, in the case of (2.2) we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |S(\alpha)| \mathrm{d}\alpha \geq \frac{\delta^2 N}{2} \sum_{m\in H} \nu(m). \tag{2.3}$$

In practice, the weight ν is either identically 1 or an appropriate weighting of shifted primes with a logarithm.

The Hardy-Littlewood Circle Method

We exploit information such as (2.3) using known estimates, which roughly assert that certain exponential sums shaped like $S(\alpha)$ above are concentrated near rationals with small denominator. To make this analysis precise, we employ the Hardy-Littlewood Circle Method, decomposing the circle into two pieces: the frequencies which are close to rationals with small denominator, and those which are not.

Definition 2.2. Given $N \in \mathbb{N}$ and $K > 0$, we define, for each $q \in \mathbb{N}$ and $a \in [1, q]$,

$$\mathbf{M}_{a/q}(K) = \mathbf{M}_{a/q}(K, N) = \left\{ \alpha \in \mathbb{T} : \left| \alpha - \frac{a}{q} \right| < \frac{K}{N} \right\},$$

$$\mathbf{M}_q(K) = \bigcup_{(a,q)=1} \mathbf{M}_{a/q}(K),$$

and

$$\mathbf{M}'_q(K) = \bigcup_{r|q} \mathbf{M}_r(K) = \bigcup_{a=1}^{q} \mathbf{M}_{a/q}(K).$$

We then define $\mathfrak{M}(K)$, the *major arcs*, by

$$\mathfrak{M}(K) = \bigcup_{q=1}^{K} \mathbf{M}_q(K),$$

and $\mathfrak{m}(K)$, the *minor arcs*, by

$$\mathfrak{m}(K) = \mathbb{T} \setminus \mathfrak{M}(K).$$

The parameter N, which is usually suppressed in this notation, should always be replaced with the size of the ambient interval in consideration. It is important to note that if $2K^3 < N$, then

$$\mathbf{M}_{a/q}(K) \cap \mathbf{M}_{b/r}(K) = \emptyset \tag{2.4}$$

whenever $a/q \neq b/r$ and $q, r \leq K$.

Density Increment Lemma

After applying the circle method and known exponential sum estimates, one can often conclude that the transform of the balanced function has significant concentration of L^2 mass around rationals with a single small denominator q. However, if the set A is uniformly distributed over congruence classes modulo q, then $\widehat{f_A}(a/q)$ is basically a sum over a full collection of roots of unity, with each root counted an equal number of times, which is zero. As a result, we expect $\widehat{f_A}(\alpha)$ to be small if A is roughly uniformly distributed modulo q and α is near a rational with denominator q.

Therefore, the L^2 concentration should indicate that A is significantly "biased" with respect to congruence modulo q, and in particular has noticeably increased density on a long arithmetic progression of step size q. We make this last idea precise with the following standard lemma.

Lemma 2.3. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$. If $\sigma \leq 1$ and*

$$\int_{\mathbf{M}'_q(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \geq \sigma\delta^2 N,$$

then there exists an arithmetic progression

$$P = \{x + \ell q : 1 \leq \ell \leq L\}$$

with $qL \gg \min\{\sigma, K^{-1}\}N$ and $|A \cap P| \geq \delta(1 + \sigma/32)L$.

Proof. Suppose $A \subseteq [1, N]$ with $|A| = \delta N$. Suppose further that

$$\int_{\mathbf{M}'_q(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \geq \sigma\delta^2 N \tag{2.5}$$

and let $P = \{q, 2q, \ldots, Lq\}$ with $L = \lfloor \min\{\sigma, K^{-1}\}N/128q \rfloor$. We will show that some translate of P satisfies the conclusion of Lemma 2.3. We note that for $\alpha \in [0, 1]$,

$$|\widehat{1_P}(\alpha)| = \Big| \sum_{\ell=1}^{L} e^{-2\pi i \ell q \alpha} \Big| \geq L - \sum_{\ell=1}^{L} |1 - e^{-2\pi i \ell q \alpha}| \geq L - 2\pi L^2 \|q\alpha\|, \tag{2.6}$$

where $\|\cdot\|$ denotes the distance to the nearest integer. Further, if $\alpha \in \mathbf{M}'_q(K)$, then

$$\|q\alpha\| \leq qK/N \leq 1/4\pi L. \tag{2.7}$$

Therefore, by (2.6) and (2.7) we have

$$|\widehat{1_P}(\alpha)| \geq L/2 \quad \text{for all} \quad \alpha \in \mathbf{M}_q(K). \tag{2.8}$$

By (2.5), (2.8), Plancherel's Identity, and the standard fact that the Fourier transform takes con-

volutions to products, we see

$$\sigma\delta^2 N \le \int_{\mathbf{M}_q'(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \le \frac{4}{L^2}\int_0^1 |\widehat{f_A}(\alpha)|^2 |\widehat{1_P}(\alpha)|^2 \mathrm{d}\alpha = \frac{4}{L^2}\sum_{n\in\mathbb{Z}} |f_A * \widetilde{1_P}(n)|^2, \tag{2.9}$$

where $\widetilde{1_P}(n) = 1_P(-n)$ and

$$f_A * \widetilde{1_P}(n) = \sum_{m\in\mathbb{Z}} f_A(m) 1_P(m-n) = |A\cap(P+n)| - \delta|(P+n)\cap[1,N]|. \tag{2.10}$$

We now take advantage of the fact that f_A, and consequently $f_A * \widetilde{1_P}$, has mean value zero. In other words,

$$\sum_{n\in\mathbb{Z}} f_A * \widetilde{1_P}(n) = 0. \tag{2.11}$$

As with any real valued function, we can write

$$|f_A * \widetilde{1_P}| = 2(f_A * \widetilde{1_P})_+ - f_A * \widetilde{1_P}, \tag{2.12}$$

where $(f_A * \widetilde{1_P})_+ = \max\{f_A * \widetilde{1_P}, 0\}$. For the purposes of proving Lemma 2.3, we can assume that $f_A * \widetilde{1_P}(n) \le 2\delta L$ for all $n \in \mathbb{Z}$, as otherwise the progression $P + n$ would more than satisfy the conclusion. Combined with the trivial upper bound $f_A * \widetilde{1_P}(n) \ge -\delta L$, we can assume

$$|f_A * \widetilde{1_P}(n)| \le 2\delta L \quad \text{for all} \quad n \in \mathbb{Z}. \tag{2.13}$$

By (2.9), (2.11), (2.12), and (2.13), we have

$$\sum_{n\in\mathbb{Z}} (f_A * \widetilde{1_P})_+(n) = \frac{1}{2}\sum_{n\in\mathbb{Z}} |f_A * \widetilde{1_P}| \ge \frac{1}{4\delta L}\sum_{n\in\mathbb{Z}} |f_A * \widetilde{1_P}|^2 \ge \frac{\sigma\delta N L}{16}. \tag{2.14}$$

By (2.10), we see that $f_A * \widetilde{1_P}(n) = 0$ if $n \notin [-qL, N]$. Letting $E = \{n \in \mathbb{Z} : P + n \subseteq [1, N]\}$ and $F = [-qL, N] \setminus E$, we see that $|F| \le 2qL$.

Therefore, by (2.13) and (2.14) we have

$$\sum_{n\in E}(f_A * \widetilde{1_P})_+(n) \geq \frac{\sigma\delta NL}{16} - 4q\delta L^2 \geq \frac{\sigma\delta NL}{32}. \tag{2.15}$$

Noting that $|E| \leq N$ and $f_A * \widetilde{1_P}(n) = |A \cap (P+n)| - \delta L$ for all $n \in E$, we have that there exists $n \in \mathbb{Z}$ with

$$|A \cap (P+n)| \geq \delta(1+\sigma/32)L,$$

as required. □

3 Sárközy's Method for Squares

In this chapter we provide a streamlined exposition of the method used by Sárközy [22] to prove Theorem A. We establish the following bound, which is noticeably better than the original.

Theorem 3.1. *If $A \subseteq [1, N]$ and $n^2 \notin A - A$ for all $n \in \mathbb{N}$, then*

$$\frac{|A|}{N} \ll \frac{\log\log N}{\log N}.$$

3.1 Main Iteration Lemma: Deducing Theorem 3.1

We deduce Theorem 3.1 using a density increment iteration, which roughly says that a set with no square differences spawns a new, denser subset of a slightly smaller interval with an inherited lack of square differences.

Lemma 3.2. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $\delta \geq N^{-1/20}$. If $n^2 \notin A - A$ for all $n \in \mathbb{N}$, then there exists $A' \subseteq [1, N']$ with*

$$N' \gg \delta^6 N, \quad |A'| \geq (\delta + c\delta^2)N', \quad \text{and} \quad n^2 \notin A' - A' \text{ for all } n \in \mathbb{N}.$$

Proof of Theorem 3.1

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $n^2 \notin A - A$ for all $n \in \mathbb{N}$. Setting $A_0 = A$, $N_0 = N$, and $\delta_0 = \delta$, Lemma 3.2 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $n^2 \notin A_m - A_m$ for all $n \in \mathbb{N}$ satisfying

$$N_m \geq c\delta^6 N_{m-1} \geq (c\delta^6)^m N \tag{3.1}$$

and

$$\delta_m \geq \delta_{m-1} + c\delta_{m-1}^2, \tag{3.2}$$

as long as

$$\delta_m \geq N_m^{-1/20}. \tag{3.3}$$

By (3.2) we see that the density δ_m will surpass 1, and hence (3.3) must fail, for $m = C\delta^{-1}$. In particular, by (3.1) we have

$$\delta \leq (c\delta^6)^{-C\delta^{-1}} N^{-1/20},$$

which can be rearranged to

$$N \leq (c\delta)^{-C\delta^{-1}}$$

and seen to imply

$$\delta \ll \frac{\log\log N}{\log N},$$

as required. □

3.2 L^2 Concentration for Squares

As indicated in Section 2.3, we establish Lemma 3.2 by observing that if a set has no square differences, the transform of its balance function has concentrated L^2 mass around rationals with a single small denominator q.

Lemma 3.3. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and let $\eta = c_0\delta$ for a sufficiently small constant $c_0 > 0$. If $n^2 \notin A - A$ for all $n \in \mathbb{N}$, $\delta \geq N^{-1/20}$, and $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then there exists $q \leq \eta^{-2}$ such that*

$$\int_{\mathbf{M}_q(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^3 N.$$

Proof of Lemma 3.2

Suppose $A \subseteq [1, N]$, $|A| = \delta N$, $\delta \geq N^{-1/20}$, and $n^2 \notin A - A$ for all $n \in \mathbb{N}$. If $|A \cap (N/9, 8N/9)| < 3\delta N/4$, then $\max\{|A \cap [1, N/9]|, |A \cap [8N/9, N]|\} > \delta N/8$. In other words, A has density at least

$9\delta/8$ on one of these intervals. Otherwise, Lemmas 3.3 and 2.3 apply, so in either case, letting $\eta = c_0\delta$, there exists $q \leq \eta^{-2}$ and an arithmetic progression

$$P = \{x + \ell q : 1 \leq \ell \leq L\}$$

with $qL \gg \delta^2 N$ and $|A \cap P|/L \geq \delta + c\delta^2$. Partitioning P into subprogressions of step size q^2, the pigeonhole principle yields a progression

$$P' = \{y + \ell q^2 : 1 \leq \ell \leq N'\} \subseteq P$$

with $N' \geq L/2q$ and $|A \cap P'|/N' \geq \delta + c\delta^2$. This allows us to define a set $A' \subseteq [1, N']$ by

$$A' = \{\ell \in [1, N'] : y + \ell q^2 \in A\},$$

which satisfies $|A'| \geq (\delta + c\delta^2)N'$ and $N' \gg \delta^2 N/q^2 \gg \delta^6 N$. Moreover, due to our choice of a perfect square step size, A' inherits the lack of square differences from A. □

Proof of Lemma 3.3

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, let $\eta = c_0\delta$, and let $M = \lfloor \sqrt{N}/3 \rfloor$. If $n^2 \notin A - A$ for all $n \in \mathbb{N}$ and $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then on the transform side, as in Section 2.3, we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |S_M(\alpha)| \mathrm{d}\alpha \geq \Big| \sum_{\substack{n \in \mathbb{Z} \\ 1 \leq m \leq M}} f_A(n) f_A(n + m^2) \Big| \geq \delta^2 NM/2, \tag{3.4}$$

where

$$S_x(\alpha) = \sum_{1 \leq m \leq x} e^{2\pi i m^2 \alpha}.$$

It follows from traditional Weyl sum estimates that if $\delta \geq N^{-1/20}$, then

$$|S_M(\alpha)| \ll q^{-1/2} M \quad \text{if} \quad \alpha \in \mathbf{M}_q(\eta^{-2}),\ q \leq \eta^{-2} \tag{3.5}$$

and

$$|S_M(\alpha)| \le C\eta M \le \delta M/4 \quad \text{for all} \quad \alpha \in \mathfrak{m}(\eta^{-2}), \tag{3.6}$$

provided we choose $c_0 \le 1/4C$. We discuss these estimates in more detail in Section 3.3.

By (3.6) and Plancherel's Identity, we have

$$\int_{\mathfrak{m}(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 |S_M(\alpha)| \mathrm{d}\alpha \le \delta^2 NM/4,$$

which by (3.4) yields

$$\int_{\mathfrak{M}(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 |S_M(\alpha)| \mathrm{d}\alpha \ge \delta^2 NM/4. \tag{3.7}$$

Finally, by (3.5) and (3.7) we have

$$\delta^2 N \ll \Big(\sum_{1 \le q \le \eta^{-2}} q^{-1/2} \Big) \max_{q \le \eta^{-2}} \int_{\mathbf{M}_q(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha$$

$$\ll \eta^{-1} \max_{q \le \eta^{-2}} \int_{\mathbf{M}_q(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha,$$

and the lemma follows. □

The remainder of the chapter is dedicated to establishing the Weyl sum estimates (3.5) and (3.6).

3.3 Exponential Sum Estimates for Squares

The following lemma exhibits that if α is on a major arc, then the Weyl sum $S_M(\alpha)$ decomposes as the product of an "arithmetic part" and a "continuous part", up to a manageable error term.

Lemma 3.4. *If $a, q \in \mathbb{N}$ and $\alpha = a/q + \beta$, then*

$$S_M(\alpha) = q^{-1} G(a,q) \int_0^M e^{2\pi i x^2 \beta} \mathrm{d}x + O(q(1 + M^2|\beta|)),$$

where

$$G(a,q) = \sum_{r=0}^{q-1} e^{2\pi i r^2 a/q}.$$

Proof. First we see that for any $a, q \in \mathbb{N}$ and $x \geq 0$ we have

$$S_x(a/q) = \sum_{1 \leq m \leq x} e^{2\pi i m^2 a/q} = \sum_{r=0}^{q-1} e^{2\pi i r^2 a/q} \Big| \{1 \leq m \leq x \ : \ m \equiv r \bmod q\} \Big| = q^{-1} G(a,q) x + O(q).$$

Then, letting $\alpha = a/q + \beta$, successive applications of summation and integration by parts yield

$$S_M(\alpha) = \sum_{m=1}^{M} e^{2\pi i m^2 a/q} e^{2\pi i m^2 \beta} = S_M(a/q) e^{2\pi i M^2 \beta} - \int_0^M S_x(a/q)(4\pi i x \beta) e^{2\pi i x^2 \beta} \mathrm{d}x$$

$$= q^{-1} G(a,q) \Big(M e^{2\pi i M^2 \beta} - \int_0^M x(4\pi i x \beta) e^{2\pi i x^2 \beta} \mathrm{d}x \Big) + O(q(1 + M^2 \beta))$$

$$= q^{-1} G(a,q) \int_0^M e^{2\pi i x^2 \beta} \mathrm{d}x + O(q(1 + M^2 \beta)),$$

as required. □

To establish the cancellation on the major arcs promised in (3.5), we need the following standard estimate on the Gauss sum $G(a,q)$.

Lemma 3.5. *If $(a,q) = 1$, then $|G(a,q)| \leq \sqrt{2q}$.*

Proof. Using a change of variables ($r = s + h$) and the orthogonality relation

$$\sum_{s=0}^{q-1} e^{2\pi i s t/q} = \begin{cases} q & \text{if } q \mid t \\ 0 & \text{else} \end{cases}, \tag{3.8}$$

we see

$$|G(a,q)|^2 = \sum_{r,s=0}^{q-1} e^{2\pi i (r^2 - s^2) a/q} = \sum_{s,h=0}^{q-1} e^{2\pi i (2sh + h^2) a/q} = \sum_{h=0}^{q-1} e^{2\pi i h^2 a/q} \begin{cases} q & \text{if } q \mid 2ha \\ 0 & \text{else} \end{cases}.$$

In particular, if $(a,q) = 1$, then $|G(a,q)|^2 \leq 2q$. □

Proof of (3.5)

Since $\delta \gg M^{-1/10}$, Lemma 3.4 yields

$$|S_M(\alpha)| \leq q^{-1}|G(a,q)|M + O(M^{2/5})$$

provided $\alpha \in \mathbf{M}_q(\eta^{-2})$, $q \leq \eta^{-2}$. Applying Lemma 3.5, the estimate follows. □

For the minor arcs, we make further use of Lemma 3.4 as well as the following well-known result, which roughly says that being close to a rational with small denominator is the only obstruction to a great deal of cancellation in an exponential sum over the squares.

Lemma 3.6 (Weyl Inequality for Squares)**.** *If $(a,q) = 1$ and $|\alpha - a/q| \leq q^{-2}$, then*

$$|S_M(\alpha)| \ll \log M (q + M + M^2/q)^{1/2}.$$

This particular formulation of the Weyl Inequality follows from Theorem 1, Chapter 3, of [15]. To complete the re-purposing of Lemma 3.4, we need a nontrivial estimate on the oscillatory integral in the asymptotic formula.

Lemma 3.7. *If $k \geq 1$, then*

$$\Big| \int_0^M e^{2\pi i x^k \beta} \mathrm{d}x \Big| \leq 2|\beta|^{-1/k}.$$

Proof. By trivially bounding the integral we can assume that $|\beta|^{-1/k} \leq M$, in which case we can break up the interval and integrate by parts to see

$$\Big| \int_0^M e^{2\pi i x^k \beta} \mathrm{d}x \Big| = \Big| \int_0^{|\beta|^{-1/k}} e^{2\pi i x^k \beta} \mathrm{d}x + \int_{|\beta|^{-1/k}}^M \frac{1}{2k\pi i x^{k-1}\beta} \frac{\mathrm{d}}{\mathrm{dx}} (e^{2\pi i x^k \beta}) \mathrm{d}x \Big|$$

$$\leq |\beta|^{-1/k} + \frac{1}{2k\pi|\beta|} \left| \Big[\frac{e^{2\pi i x^2 \beta}}{x^{k-1}} \Big]_{|\beta|^{-1/k}}^M + (k-1) \int_{|\beta|^{-1/k}}^M \frac{e^{2\pi i x^k \beta}}{x^k} \mathrm{d}x \right| \leq 2|\beta|^{-1/k},$$

as required. □

Proof of (3.6)

For a fixed $\alpha \in \mathfrak{m}(\eta^{-2})$, we have by the pigeonhole principle that there exist

$$1 \leq q \leq M^{7/4}$$

and $(a,q) = 1$ with

$$|\alpha - a/q| < 1/qM^{7/4}.$$

If $\eta^{-2} \leq q \leq M^{1/4}$, then Lemmas 3.4 and 3.5 imply

$$|S_M(\alpha)| \leq q^{-1}|G(a,q)|M + O(M^{1/2}) \ll q^{-1/2}M \leq \eta M.$$

If $M^{1/4} \leq q \leq M^{7/4}$, then Lemma 3.6 and the bound $\delta \geq N^{-1/20} \gg M^{-1/10}$ imply

$$|S_M(\alpha)| \ll M^{9/10} \ll \eta M.$$

If $1 \leq q \leq \eta^{-2}$, then, letting $\beta = \alpha - a/q$, it must be the case that

$$|\beta| > 1/\eta^2 N \gg 1/\eta^2 M^2, \tag{3.9}$$

as otherwise we would have $\alpha \in \mathfrak{M}(\eta^{-2})$. Combining Lemma 3.4 and (3.9) with Lemma 3.7, the minor arc estimate is established. □

4 Sárközy's Method for $p-1$

In this chapter we provide a streamlined exposition of the method used by Sárközy [23] to prove Theorem B. We establish the following bound, which is quite significantly better than the original and even better than an improvement of Lucier [10] that requires heavier machinery.

Theorem 4.1. *If $A \subseteq [1,N]$ and $p-1 \notin A-A$ for all primes p, then*

$$\frac{|A|}{N} \ll e^{-c\sqrt{\log\log N}}$$

for some absolute constant $c>0$.

4.1 Main Iteration Lemma: Deducing Theorem 4.1

We deduce Theorem 4.1 from an iteration lemma which states that a set without the desired arithmetic structure spawns a denser set with an inherited lack of structure. In the case of squares we saw that the new set inherited the identical property, but here this is not the case, as shifted primes are not invariant under any scaling, and we need to keep track of the lack of structure at each step of the iteration. To this end, we let $\mathcal{P}$ denote the primes and we define, for each $d \in \mathbb{N}$,

$$\Lambda_d = \{n \in \mathbb{N} : dn+1 \in \mathcal{P}\}.$$

Lemma 4.2. *Suppose $A \subseteq [1,N]$ with $|A| = \delta N$. If $(A-A)\cap \Lambda_d = \emptyset$ and $d, \delta^{-1} \leq \log N$, then there exists $A' \subseteq [1,N']$ and $q \ll \delta^{-2}$ with*

$$N' \gg \delta^4 N, \quad |A'| \geq \delta(1+c)N', \quad \text{and} \quad (A'-A')\cap \Lambda_{qd} = \emptyset.$$

Proof of Theorem 4.1

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $p - 1 \notin A - A$ for all $p \in \mathcal{P}$. Setting $A_0 = A$, $N_0 = N$, $\delta_0 = \delta$, and $d_0 = 1$, Lemma 4.2 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $(A_m - A_m) \cap \Lambda_{d_m} = \emptyset$ satisfying

$$N_m \geq c\delta^4 N_{m-1} \geq (c\delta^4)^m N, \tag{4.1}$$

$$\delta_m \geq \delta_{m-1}(1 + c), \tag{4.2}$$

and

$$d_m \leq C\delta^{-2} d_{m-1} \leq (C\delta^{-2})^m, \tag{4.3}$$

as long as

$$d_m, \delta_m^{-1} \leq \log N_m. \tag{4.4}$$

By (4.2), we see that the density δ_m will surpass 1 for $m = C(\log(\delta^{-1}))$. Therefore, if

$$\delta \geq e^{-c\sqrt{\log\log N}} \tag{4.5}$$

for an absolute constant $c > 0$, then (4.4) must fail for

$$m = C\sqrt{\log\log N}. \tag{4.6}$$

However, we see that if c is sufficiently small, then (4.3), (4.5), and (4.6) imply

$$d_m \leq e^{3cm\sqrt{\log\log N}} \leq e^{\log\log N/2} = \sqrt{\log N},$$

and similarly (4.1), (4.5), and (4.6) imply $N_m \geq N/\log N$. In particular (4.4) holds, yielding a contradiction, and the theorem follows. □

4.2 Counting Primes in Arithmetic Progressions I

As indicated by the definition of Λ_d, we need some information about the distribution of primes in certain congruence classes. Classical estimates of this type come from the famous Siegel-Walfisz Theorem, which can be found for example in Corollary 11.19 of [16].

Lemma 4.3 (Siegel-Walfisz Theorem)**.** *If $D > 0$, $q \leq (\log x)^D$, and $(a, q) = 1$, then*

$$\psi(x, a, q) := \sum_{\substack{p \in \mathcal{P}_x \\ p \equiv a \bmod q}} \log p = x/\phi(q) + O(xe^{-c\sqrt{\log x}})$$

for some constant $c = c(D) > 0$, where ϕ is the Euler totient function and $\mathcal{P}_x = \mathcal{P} \cap [1, x]$.

4.3 L^2 Concentration for Shifted Primes I

We establish Lemma 4.2 from the following two observations, which combine to a sharper analog of Lemma 3.3.

Lemma 4.4. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, and let $\eta = c_0\delta$ for a sufficiently small constant $c_0 > 0$. If $d, \delta^{-1} \leq \log N$, $(A - A) \cap \Lambda_d = \emptyset$, and $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then*

$$\sum_{1 \leq q \leq \eta^{-2}} \frac{1}{\phi(q)} \int_{\mathbf{M}_q(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^2 N.$$

Lemma 4.5. *If $A \subseteq [1, N]$, then for any $0 < Q, K < N^{1/4}$,*

$$\max_{q \leq Q} \int_{\mathbf{M}'_q(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \sum_{1 \leq q \leq Q} \frac{1}{\phi(q)} \int_{\mathbf{M}_q(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha.$$

Proof. Using (2.4) and the fact

$$\sum_{1 \leq q \leq Q} \frac{q}{\phi(q)} \ll Q,$$

we see

$$Q \max_{q\le Q} \int_{\mathbf{M}'_q(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \sum_{1\le q\le Q} \frac{q}{\phi(q)} \int_{\mathbf{M}'_q(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha$$

$$= \sum_{1\le q\le Q} \frac{q}{\phi(q)} \sum_{r|q} \int_{\mathbf{M}_r(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha$$

$$= \sum_{1\le r\le Q} \int_{\mathbf{M}_r(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \Big(r \sum_{1\le q\le Q/r} \frac{q}{\phi(rq)} \Big)$$

$$\gg Q \sum_{1\le r\le Q} \frac{1}{\phi(r)} \int_{\mathbf{M}_r(K)} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha,$$

and the lemma follows. □

Proof of Lemma 4.2

Suppose $A \subseteq [1, N]$, $|A| = \delta N$, $d, \delta^{-1} \le \log N$, and $(A-A)\cap\Lambda_d = \emptyset$. If $|A\cap(N/9, 8N/9)| < 3\delta N/4$, then $\max\{|A \cap [1, N/9]|, |A \cap [8N/9, N]|\} > \delta N/8$. In other words, A has density at least $9\delta/8$ on one of these intervals. Otherwise, Lemmas 4.4, 4.5, and 2.3 apply, so in either case, letting $\eta = c_0\delta$, there exists $q \le \eta^{-2}$ and an arithmetic progression

$$P = \{x + \ell q : 1 \le \ell \le N'\}$$

with $qN' \gg \delta^2 N$ and $|A \cap P|/N' \ge \delta(1 + c)$. This allows us to define a set $A' \subseteq [1, N']$ by

$$A' = \{\ell \in [1, N'] : y + \ell q \in A\},$$

which clearly satisfies $|A'| \ge \delta(1 + c)N'$ and $N' \gg \delta^2 N/q \gg \delta^4 N$. Moreover, we defined the set Λ_d so that $(A - A) \cap \Lambda_d = \emptyset$ implies $(A' - A') \cap \Lambda_{qd} = \emptyset$. □

Proof of Lemma 4.4

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, let $\eta = c_0\delta$, and let $M = \lfloor N/9 \rfloor$. We define a function ν_d on $\mathbb{Z}$ by

$$\nu_d(m) = \frac{\phi(d)}{d} \log(dm + 1) 1_{\Lambda_d}(m).$$

If $(A - A) \cap \Lambda_d = \emptyset$ and $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then on the transform side, as in Section 2.3, we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |W_{d,M}(\alpha)| \mathrm{d}\alpha \geq \Big| \sum_{\substack{n \in \mathbb{Z} \\ 1 \leq m \leq M}} f_A(n) f_A(n+m) \nu_d(m) \Big| \geq \frac{\delta^2 N}{2} \sum_{m=1}^{M} \nu_d(m), \tag{4.7}$$

where

$$W_{d,x}(\alpha) = \sum_{1 \leq m \leq x} \nu_d(m) e^{2\pi i m\alpha}.$$

If $d \leq \log N$, then it follows from Lemma 4.3 that

$$\sum_{m=1}^{M} \nu_d(m) = \phi(d)\psi(dM + 1, 1, d)/d \geq M/2.$$

and hence by (4.7) we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |W_{d,M}(\alpha)| \mathrm{d}\alpha \geq \delta^2 NM/4. \tag{4.8}$$

It follows from Lemma 4.3 and work of Vinogradov that if $\delta \geq 1/\log N$, then

$$|W_{d,M}(\alpha)| \ll M/\phi(q) \quad \text{if} \quad \alpha \in \mathbf{M}_q(\eta^{-2}),\ q \leq \eta^{-2} \tag{4.9}$$

and

$$|W_{d,M}(\alpha)| \leq C\eta M \leq \delta M/8 \quad \text{for all} \quad \alpha \in \mathfrak{m}(\eta^{-2}), \tag{4.10}$$

provided we choose $c_0 \leq 1/8C$. We discuss these estimates in more detail in Section 4.4.

From (4.8), (4.10), and Plancherel's Identity, we conclude

$$\int_{\mathfrak{M}(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 |W_{d,M}(\alpha)| \mathrm{d}\alpha \geq \delta^2 NM/8, \tag{4.11}$$

which by (4.9) implies

$$\sum_{1 \leq q \leq \eta^{-2}} \frac{1}{\phi(q)} \int_{\mathbf{M}_q(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^2 N,$$

as required. □

The remainder of the chapter is dedicated to establishing estimates (4.9) and (4.10).

4.4 Exponential Sum Estimates for Shifted Primes I

Analogous to Lemma 3.4, the following lemma exhibits if α is on a major arc, $W_{d,M}(\alpha)$ decomposes as the product of an "arithmetic part" and a "continuous part", up to a manageable error term.

Lemma 4.6. *If $d \leq (\log M)^D$, $a, q \in \mathbb{N}$, and $\alpha = a/q + \beta$, then*

$$W_{d,M}(\alpha) = \frac{r(d,a,q)\phi(d)}{\phi(qd)} \int_0^M e^{2\pi i x\beta} \mathrm{d}x + O(qM(1+M\beta)e^{-c\sqrt{\log M}})$$

for some constant $c = c(D) > 0$, where

$$r(d,a,q) = \sum_{\substack{r=0 \\ (dr+1,q)=1}}^{q-1} e^{2\pi i r a/q}.$$

Proof. First we see that for any $a, q \in \mathbb{N}$ and $x \geq 0$ we have

$$W_{d,x}(a/q) = \sum_{1 \leq m \leq x} \nu_d(x) e^{2\pi i m a/q} = \frac{\phi(d)}{d} \sum_{r=0}^{q-1} e^{2\pi i r a/q} \psi(dx+1, dr+1, qd). \tag{4.12}$$

Noting that $(dr+1, qd) = 1$ if and only if $(dr+1, q) = 1$, we have by (4.12) and Lemma 4.3 that

$$W_{d,x}(a/q) = \frac{r(d,a,q)\phi(d)}{\phi(qd)} x + O(qMe^{-c\sqrt{\log M}})$$

for all $x \leq M$. Then, letting $\alpha = a/q + \beta$, successive applications of summation and integration by parts yield

$$\begin{aligned} W_{d,M}(\alpha) &= \sum_{m=1}^{M} \nu_d(m) e^{2\pi i m a/q} e^{2\pi i m\beta} \\ &= W_{d,M}(a/q) e^{2\pi i M\beta} - \int_0^M W_{d,x}(a/q)(2\pi i\beta) e^{2\pi i x\beta} \mathrm{d}x \\ &= \frac{r(d,a,q)\phi(d)}{\phi(qd)} \Big(M e^{2\pi i M\beta} - \int_0^M x(2\pi i\beta) e^{2\pi i x\beta} \mathrm{d}x \Big) + O(qM(1+M\beta)e^{-c\sqrt{\log M}}) \\ &= \frac{r(d,a,q)\phi(d)}{\phi(qd)} \int_0^M e^{2\pi i x\beta} \mathrm{d}x + O(qM(1+M\beta)e^{-c\sqrt{\log M}}), \end{aligned}$$

as required. □

Lemma 4.7. *If $(a,q) = 1$, then*

$$r(d,a,q) = \begin{cases} \mu(q) e^{-2\pi i \ell a/q} & \text{if } (d,q) = 1, \text{ where } \ell \equiv d^{-1} \bmod q \\ 0 & \text{else} \end{cases},$$

where μ is the Möbius function.

Proof. As is often the case with this type of sum, we take advantage of multiplicativity. Specifically, it is not difficult to show using the Chinese Remainder Theorem that if $(a,q) = 1$ and $q = q_1 q_2$ with $(q_1, q_2) = 1$, then

$$r(d,a,q) = \sum_{\substack{r=0 \\ (dr+1,q)=1}}^{q-1} e^{2\pi i r a/q} = \sum_{\substack{r_1=0 \\ (dr_1+1,q_1)=1}}^{q_1-1} e^{2\pi i r_1 a_1/q_1} \cdot \sum_{\substack{r_2=0 \\ (dr_2+1,q_2)=1}}^{q_2-1} e^{2\pi i r_2 a_2/q_2},$$

where $a/q = a_1/q_1 + a_2/q_2$. Therefore, we can assume $q = p^j$ for $p \in \mathcal{P}$ and $j \in \mathbb{N}$. If $p \mid d$, then we always have $(dr+1, p^j) = 1$, so the exponential sum is complete and equal to 0 by (3.8).

If $p \nmid d$, then we can change variables in the sum setting $s = dr + 1$, which yields

$$r(d, a, p^j) = \sum_{\substack{s=0 \\ p \nmid s}}^{p^j - 1} e^{2\pi i (s-1)\ell a / p^j},$$

where $\ell \equiv d^{-1} \bmod p^j$, so the lemma follows from the identity

$$\sum_{\substack{s=0 \\ p \nmid s}}^{p^j - 1} e^{2\pi i s a / p^j} = \begin{cases} -1 & \text{if } j = 1 \\ 0 & \text{else} \end{cases},$$

which follows quickly from (3.8). □

Proof of (4.9)

Since $\delta^{-1} \ll \log M$, Lemma 4.6 yields

$$|W_{d,M}(\alpha)| \leq \frac{|r(d, a, q)|\phi(d)}{\phi(qd)} M + O(M e^{-c\sqrt{\log M}})$$

provided $\alpha \in \mathbf{M}_q(\eta^{-2})$, $q \leq \eta^{-2}$. Applying Lemma 4.7 we see that $|r(d, a, q)| \leq 1$, and since $\phi(qd) \geq \phi(q)\phi(d)$, the estimate follows. □

For the minor arcs, we make further use of Lemma 4.6 as well as the following estimate of Vinogradov, a suitable analog to the Weyl Inequality used famously in his solution to the ternary Goldbach problem, which can be found in Theorem 3.1 of [25].

Lemma 4.8 (Vinogradov)**.** *If $(a, q) = 1$ and $|\alpha - a/q| \leq q^{-2}$, then*

$$|V_x(\alpha)| \ll (\log x)^4 (\sqrt{qx} + x^{4/5} + x/\sqrt{q}),$$

where

$$V_x(\alpha) = \sum_{p \in \mathcal{P}_x} \log p \; e^{2\pi i p \alpha}.$$

Corollary 4.9. *If $(a,q)=1$ and $|\alpha - a/q| \le q^{-2}$, then*

$$|W_{d,M}(\alpha)| \ll d(\log M)^4(\sqrt{qM} + M^{4/5} + M/\sqrt{q}).$$

Proof. Exploiting (3.8), we see

$$\begin{aligned}
\frac{d}{\phi(d)}|W_{d,M}(\alpha)| &= \Big| \sum_{\substack{p\in\mathcal{P}_{dM+1}\\ p\equiv 1 \bmod d}} \log p \; e^{2\pi i(p-1)\alpha/d}\Big| \\
&= \Big| \sum_{p\in\mathcal{P}_{dM+1}} \log p \; e^{2\pi i(p-1)\alpha/d} \; \frac{1}{d}\sum_{r=0}^{d-1} e^{2\pi i(p-1)r/d}\Big| \\
&\le \frac{1}{d}\sum_{r=0}^{d-1}\Big| \sum_{p\in\mathcal{P}_{dM+1}} \log p \; e^{2\pi i(p-1)(\alpha+r)/d}\Big| \\
&= \frac{1}{d}\sum_{r=0}^{d-1}\Big|V_{dM+1}\Big(\frac{\alpha+r}{d}\Big)\Big|.
\end{aligned}$$

If $(a,q)=1$ and $|\alpha - a/q| \le q^{-2}$, then for any fixed $0 \le r \le d-1$, the pigeonhole principle yields $1 \le q' \le 2dq$ and $(a',q')=1$ with $|(\alpha+r)/d - a'/q'| < 1/2dqq'$. We also know that $|(\alpha+r)/d - (a+rq)/qd| < 1/dq^2$, so in particular we have

$$\Big|\frac{a'}{q'} - \frac{a+rq}{qd}\Big| < \frac{1}{2dqq'} + \frac{1}{dq^2}. \tag{4.13}$$

If $q' < q$, then since $(a,q)=1$ the two fractions on the left hand side above cannot be equal, hence

$$\frac{1}{2dqq'} + \frac{1}{dq^2} > \frac{1}{dqq'},$$

which implies $q' \geq q/2$. In any case $q/2 \leq q' \leq 2dq$, so by Lemma 4.8 we have

$$\begin{aligned}\Big|V_{dM+1}\Big(\frac{\alpha+r}{d}\Big)\Big| &\ll (\log(dM+1))^4(\sqrt{q'(dM+1)}+(dM+1)^{4/5}+(dM+1)/\sqrt{q'}) \\ &\ll d(\log M)^4(\sqrt{qM}+M^{4/5}+M/\sqrt{q}),\end{aligned}$$

and the corollary follows. □

Proof of (4.10)

For a fixed $\alpha \in \mathfrak{m}(\eta^{-2})$ we have by the pigeonhole principle that there exist $1 \leq q \leq M/(\log M)^{20}$ and $(a,q)=1$ with $|\alpha - a/q| < (\log M)^{20}/qM$.

If $\eta^{-2} \leq q \leq (\log M)^{20}$, then Lemmas 4.6 and 4.7 imply

$$|W_M(\alpha)| \leq \frac{|r(d,a,q)|\phi(d)}{\phi(qd)}M + O(Me^{-c\sqrt{\log M}}) \ll M/\phi(q) \ll \eta M,$$

where the last inequality follows from the fact that $\phi(q) \gg \sqrt{q}$.

If $(\log M)^{20} \leq q \leq M/(\log M)^{20}$, then Corollary 4.9 and the bound $d, \delta^{-1} \ll \log M$ imply

$$|W_M(\alpha)| \ll M/(\log M)^5 \leq \eta M.$$

If $1 \leq q \leq \eta^{-2}$, then, letting $\beta = \alpha - a/q$, it must be the case that

$$|\beta| > 1/\eta^2 N \gg 1/\eta^2 M, \tag{4.14}$$

as otherwise we would have $\alpha \in \mathfrak{M}(\eta^{-2})$. Combining Lemma 4.6 and (4.14) with the bound

$$\Big|\int_0^M e^{2\pi i x\beta}\mathrm{d}x\Big| = \Big|\frac{e^{2\pi i M\beta}-1}{2\pi i\beta}\Big| < |\beta|^{-1},$$

the minor arc estimate is established. □

5 Ruzsa-Sanders' Improvement for $p-1$

In this chapter, we provide an exposition of the method used by Ruzsa and Sanders [21] to drastically improve the bound in Theorem B.

Theorem 5.1 (Ruzsa, Sanders, [21]). *If $A \subseteq [1,N]$ and $p-1 \notin A-A$ for all primes p, then*

$$\frac{|A|}{N} \ll e^{-c(\log N)^{1/4}}$$

for an absolute constant $c>0$.

5.1 Counting Primes in Arithmetic Progressions II

Ruzsa and Sanders [21] established asymptotics for $\psi(x,a,q)$ for certain moduli q beyond the limitations of Lemma 4.3 by exploiting a dichotomy based on exceptional zeros, or lack thereof, of Dirichlet L-functions. In particular, the following result follows from their work.

Lemma 5.2. *For any $Q, D>0$, there exist $q_0 \le Q^D$ and $\rho \in [1/2,1)$ with $(1-\rho)^{-1} \ll q_0$ such that*

$$\psi(x,a,q) = \frac{x}{\phi(q)} - \frac{\chi(a)x^\rho}{\phi(q)\rho} + O\Big(x\exp\Big(-\frac{c\log x}{\sqrt{\log x}+D^2\log Q}\Big)D^2\log Q\Big), \tag{5.1}$$

where χ is a Dirichlet character modulo q_0, provided $q_0 \mid q$, $(a,q)=1$, and $q \le (q_0 Q)^D$.

Lemma 5.2 is a purpose-built special case of Proposition 4.7 of [21], which in the language of that paper can be deduced by considering the pair (Q^{D^2+D}, Q^D), where q_0 is the modulus of the exceptional Dirichlet character if the pair is exceptional and $q_0=1$ if the pair is unexceptional.

It is a calculus exercise to verify that if $\epsilon \in [0, 1/2]$ and $x \geq 16$, then $1 - x^{-\epsilon}/(1-\epsilon) \geq \epsilon$, which implies that the main term in Lemma 5.2 satisfies

$$\Re\Big((x - \chi(a)x^{\rho}/\rho)/\phi(q)\Big) \geq (1-\rho)x/\phi(q) \gg x/q_0\phi(q). \tag{5.2}$$

5.2 Main Iteration Lemma: Deducing Theorem 5.1

For the remainder of the argument, we fix a natural number N, and we set $Q = e^{c\sqrt{\log N}}$ for a sufficiently small constant $c > 0$. Applying Lemma 5.2 with $D = 6$, we let $q_0 \leq Q^6$, $\rho \in [1/2, 1)$, and the Dirichlet character χ be as in the conclusion. We see that if c is sufficiently small and $X \geq N^{1/3}$, then

$$\psi(x, a, q) = \frac{x}{\phi(q)} - \frac{\chi(a)x^{\rho}}{\phi(q)\rho} + O(XQ^{-100}) \tag{5.3}$$

for all $x \leq X$, provided $q_0 \mid q$, $(a, q) = 1$, and $q \leq (q_0 Q)^6$. After passing to a subprogression of step size q_0, we deduce Theorem 5.1 from an iteration lemma analogous to Lemma 4.2.

Lemma 5.3. *Suppose $A \subseteq [1, L]$ with $|A| = \delta L$ and $L \geq \sqrt{N}$. If $q_0 \mid d$, $(A - A) \cap \Lambda_d = \emptyset$, and $d/q_0, \delta^{-1} \leq Q$, then there exists $q \ll \delta^{-2}$ and $A' \subseteq [1, L']$ with*

$$L' \gg \delta^4 L, \quad |A'| \geq \delta(1+c)L', \quad \text{and} \quad (A' - A') \cap \Lambda_{qd} = \emptyset.$$

Proof of Theorem 5.1

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $p - 1 \notin A - A$ for all primes p. Partitioning $[1, N]$, the pigeonhole principle guarantees the existence of an arithmetic progression

$$P = \{x + \ell q_0 : 1 \leq \ell \leq N_0\} \subseteq [1, N]$$

with $N_0 \geq N/2q_0$ and $|A \cap P| \geq \delta N_0$. Defining $A_0 \subseteq [1, N_0]$ by

$$A' = \{\ell \in [1, N_0] : x + \ell q_0 \in A\},$$

we see that $|A_0| \geq \delta N_0$ and $(A - A) \cap \Lambda_{q_0} = \emptyset$. If $\delta \geq Q^{-1}$, then Lemma 5.3 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $(A_m - A_m) \cap \Lambda_{d_m} = \emptyset$ satisfying $q_0 \mid d$,

$$N_m \geq c\delta^4 N_{m-1} \geq (c\delta^4)^m N/q_0, \tag{5.4}$$

$$\delta_m \geq \delta_{m-1}(1 + c), \tag{5.5}$$

and

$$d_m \leq C\delta^{-2} d_{m-1} \leq (C\delta^{-2})^m q_0, \tag{5.6}$$

as long as

$$d_m/q_0 \leq Q. \tag{5.7}$$

and

$$N_m \geq \sqrt{N}. \tag{5.8}$$

By (4.2), we see that the density δ_m will surpass 1 for $m = C(\log(\delta^{-1}))$. Therefore, if

$$\delta \geq e^{-c(\log N)^{1/4}} \tag{5.9}$$

for an absolute constant $c > 0$, then (5.7) or (5.8) must fail for

$$m = C(\log N)^{1/4}. \tag{5.10}$$

However, we see that if c is sufficiently small, then (5.6), (5.9), and (5.10) imply

$$d_m/q_0 \leq e^{3cm(\log N)^{1/4}} \leq e^{c_1\sqrt{\log N}/2} = Q^{1/2},$$

and similarly (5.4), (5.9), and (5.10) imply $N_m \geq N/Q^{20}$. In particular (5.7) and (5.8) hold, yielding a contradiction, and the theorem follows. □

5.3 L^2 Concentration for Shifted Primes II

We establish Lemma 5.3 from the following analog of Lemma 4.4.

Lemma 5.4. *Suppose $A \subseteq [1, L]$ with $|A| = \delta L$ and $L \geq \sqrt{N}$, and let $\eta = c_0\delta$. If $q_0 \mid d$, $d/q_0, \delta^{-1} \leq Q$, $(A - A) \cap \Lambda_d = \emptyset$, and $|A \cap (L/9, 8L/9)| \geq 3\delta L/4$, then*

$$\sum_{1 \leq q \leq \eta^{-2}} \frac{1}{\phi(q)} \int_{\mathbf{M}_q(\eta^{-2})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^2 L.$$

The deduction of Lemma 5.3 from Lemma 5.4 and Lemma 4.5 is completely identical to the deduction of Lemma 4.2 from Lemma 4.4 and Lemma 4.5.

Proof of Lemma 5.4

Suppose $A \subseteq [1, L]$ with $|A| = \delta L$ and $(A - A) \cap \Lambda_d = \emptyset$. Let $\eta = c_0\delta$, let $M = \lfloor L/9 \rfloor$, and let ν_d and $W_{x,d}$ be as in the proof of Lemma 4.4. If $|A \cap (L/9, 8L/9)| \geq 3\delta L/4$, then just as before we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |W_{d,M}(\alpha)| \mathrm{d}\alpha \geq \Big| \sum_{\substack{n \in \mathbb{Z} \\ 1 \leq m \leq M}} f_A(n) f_A(n+m) \nu_d(m) \Big| \geq \frac{\delta^2 L}{2} \sum_{m=1}^{M} \nu_d(m) = -\delta^2 L \Psi/2,$$

where $\Psi = \phi(d)\psi(dM + 1, 1, d)/d$. It follows from Lemma 4.7, Lemma 4.9, and (5.3) that if $q_0 \mid d$ and $d/q_0, \delta^{-1} \leq Q$, then

$$|W_{d,M}(\alpha)| \ll \Psi/\phi(q) \quad \text{if} \quad \alpha \in \mathbf{M}_q(\eta^{-2}),\ q \leq \eta^{-2} \tag{5.11}$$

and

$$|W_{d,M}(\alpha)| \leq C\eta\Psi \leq \delta\Psi/8 \quad \text{for all} \quad \alpha \in \mathfrak{m}(\eta^{-2}). \tag{5.12}$$

We discuss these estimates in more detail in Section 5.4, and the remainder of the proof is identical to that of Lemma 4.4. □

The remainder of the chapter is dedicated to establishing estimates (5.11) and (5.12).

5.4 Exponential Sum Estimates for Shifted Primes II

The following lemma is nearly identical to Lemma 4.6, just applying (5.3) in place of Lemma 4.3.

Lemma 5.5. *If $q_0 \mid d$, $d/q_0 \le Q$, $a, q \in \mathbb{N}$, $q \le (q_0 Q)^5$, and $\alpha = a/q + \beta$, then*

$$W_{d,M}(\alpha) = \frac{r(d,a,q)\phi(d)}{\phi(qd)} \int_0^M (1 - (dx)^{\rho-1}) e^{2\pi i x\beta} \mathrm{d}x + O(qM(1+M\beta)Q^{-90}),$$

where $r(d,a,q)$ is as in Lemma 4.6.

Proof. Just as in the proof of Lemma 4.6, we see

$$W_{d,x}(a/q) = \frac{\phi(d)}{d} \sum_{r=0}^{q-1} e^{2\pi i r a/q} \psi(dx+1, dr+1, qd) \tag{5.13}$$

for any $x \ge 0$. Noting that $(dr+1, qd) = 1$ if and only if $(dr+1, q) = 1$, we have by (5.13), (5.3), and the observation that $\chi(dr+1) = \chi(1) = 1$ because $q_0 \mid d$, that

$$W_{d,x}(a/q) = \frac{r(d,a,q)\phi(d)}{\phi(qd)} (x - (dx)^\rho/\rho d) + O(qMQ^{-90})$$

for all $x \le M$. Observing that

$$\frac{\mathrm{d}}{\mathrm{d}x}\Big(x - (dx)^\rho/\rho d\Big) = 1 - (dx)^{\rho-1},$$

the remainder of the proof is identical to that of Lemma 4.6. □

Proof of (5.11)

Since $\delta^{-1} \le Q$, Lemmas 5.5 and 4.7 yield

$$|W_{d,M}(\alpha)| \le \frac{|r(d,a,q)|\phi(d)}{\phi(qd)} (M - (dM)^\rho/\rho d) + O(MQ^{-80})$$

$$\le \Psi/\phi(q) + O(MQ^{-80}),$$

provided $\alpha \in \mathbf{M}_q(\eta^{-2})$, $q \leq \eta^{-2}$. By (5.3) and (5.2) we know that

$$\Psi \gg (1-\rho)M \gg M/q_0 \geq M/Q^6, \tag{5.14}$$

so the error term is negligible and the estimate follows. □

Proof of (5.12)

For a fixed $\alpha \in \mathfrak{m}(\eta^{-2})$ we have by the pigeonhole principle that there exist

$$1 \leq q \leq M/(q_0 Q)^5$$

and $(a,q) = 1$ with

$$|\alpha - a/q| < (q_0 Q)^5/qM.$$

If $\eta^{-2} \leq q \leq (q_0 Q)^5$, then Lemma 5.5, Lemma 4.7, and (5.14) imply

$$|W_M(\alpha)| \leq \frac{|r(d,a,q)|\phi(d)}{\phi(qd)}(M + (dM)^\rho/\rho d) + O(MQ^{-10}) \ll \Psi/\phi(q) \ll \eta\Psi,$$

where the last inequality follows from the fact that $\phi(q) \gg \sqrt{q}$.
If $(q_0 Q)^5 \leq q \leq M/(q_0 Q)^5$, then Corollary 4.9, (5.14), and the bound $d/q_0, \delta^{-1} \ll Q$ imply

$$|W_M(\alpha)| \ll M/q_0 Q \ll \eta\Psi.$$

If $1 \leq q \leq \eta^{-2}$, then, letting $\beta = \alpha - a/q$, it must be the case that

$$|\beta| > 1/\eta^2 L \gg 1/\eta^2 M, \tag{5.15}$$

as otherwise we would have $\alpha \in \mathfrak{M}(\eta^{-2})$.

By Lemma 5.5, (5.14), (5.15), and integration by parts, we have

$$|W_M(\alpha)| \leq \Big| \int_0^M (1-(dx)^{\rho-1}) e^{2\pi i x\beta} \mathrm{d}x \Big| + O(MQ^{-50})$$

$$\leq |\beta|^{-1}(1-(dM)^{\rho-1}) + O(MQ^{-50})$$

$$\ll \eta^2(M-(dM)^{\rho}/\rho d + 2(1-\rho)M)$$

$$\ll \eta\Psi,$$

and the minor arc estimate is established. □

6 Lucier's Extension to Intersective Polynomials

In this chapter we provide a streamlined exposition of the method used by Lucier [11] to prove Theorem D. We establish the following bound, which is very slightly better than the original.

Theorem 6.1. *Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree $k \geq 2$ with positive leading term. If $A \subseteq [1, N]$ and $h(n) \notin A - A$ for all $n \in \mathbb{N}$ with $h(n) > 0$, then*

$$\frac{|A|}{N} \ll \Big(\frac{\log\log N}{\log N}\Big)^{1/(k-1)},$$

where the implied constant depends only on h.

6.1 Auxiliary Polynomials and Related Definitions

For the remainder of the argument, we fix an intersective polynomial $h \in \mathbb{Z}[x]$ of degree $k \geq 2$ with positive leading term, and we set $\rho = 2^{-10k}$. We apply the same type of density increment strategy as in the previous chapters, and as in Chapters 4 and 5, we need to keep track of the inherited lack of arithmetic structure at each step of the iteration. Specifically, if we start with a set free of differences in the image of h, it spawns denser sets free of differences in the image of new polynomials. The following definitions describe all of the polynomials that we could potentially encounter.

Definition 6.2. For each $p \in \mathcal{P}$, we fix p-adic integers z_p with $h(z_p) = 0$. By reducing and applying the Chinese Remainder Theorem, the choices of z_p determine, for each natural number d, a unique integer $r_d \in (-d, 0]$, which consequently satisfies $d \mid h(r_d)$. We define the function λ on $\mathbb{N}$ by letting $\lambda(p) = p^m$ for each $p \in \mathcal{P}$, where m is the multiplicity of z_p as a root of h, and then extending it to be completely multiplicative.

For each $d \in \mathbb{N}$, we define the *auxiliary polynomial* h_d by

$$h_d(x) = h(r_d + dx)/\lambda(d).$$

If $p^j \mid d$ for $p \in \mathcal{P}$ and $j \in \mathbb{N}$, then since $r_d \equiv z_p \bmod p^j$, we see by factoring h over $\mathbb{Z}_p$ that all the coefficients of $h(r_d + dx)$ are divisible by p^{jm}, hence each auxiliary polynomial has integer coefficients. It is important to note that the leading coefficients of the auxiliary polynomials grow at least as quickly, up to a constant depending only on h, as the other coefficients. In particular, if b_d is the leading coefficient of h_d, then for any $x > 0$ we have

$$\left|\left\{n \in \mathbb{N} : 0 < h_d(n) < x\right\} \triangle [1, (x/b_d)^{1/k}]\right| \ll 1, \tag{6.1}$$

where $\triangle$ denotes the symmetric difference. We define these auxiliary polynomials to keep track of the inherited lack of arithmetic structure at each step of a density increment iteration, and letting

$$I(f) = \{f(n) > 0 : n \in \mathbb{N}\}$$

for a polynomial $f \in \mathbb{Z}[x]$, the following proposition makes this inheritance precise.

Proposition 6.3. *If $A \subseteq \mathbb{N}$, $(A - A) \cap I(h_d) = \emptyset$, and $A' \subseteq \{\ell \in \mathbb{N} : x + \lambda(q)\ell \in A\}$, then $(A' - A') \cap I(h_{qd}) = \emptyset$.*

Proof. Suppose that $A \subseteq \mathbb{N}$, $A' \subseteq \{\ell \in \mathbb{N} : x + \lambda(q)\ell \in A\}$, and

$$\ell - \ell' = h_{qd}(n) = h(r_{qd} + qdn)/\lambda(qd) > 0$$

for some $n \in \mathbb{N}$, $\ell, \ell' \in A'$. By construction we see that $r_{qd} \equiv r_d \bmod d$, so there exists $s \in \mathbb{Z}$ such that $r_{qd} = r_d + ds$, and therefore

$$0 < h_d(s + qn) = \frac{h(r_d + d(s + qn))}{\lambda(d)} = \lambda(q)h_{qd}(n) = \lambda(q)\ell - \lambda(q)\ell' \in A - A,$$

hence $(A - A) \cap I(h_d) \neq \emptyset$ and the contrapositive is established. □

6.2 Main Iteration Lemma: Deducing Theorem 6.1

We deduce Theorem 6.1 from the following iteration lemma.

Lemma 6.4. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$. If $(A - A) \cap I(h_d) = \emptyset$ and $d, \delta^{-1} \leq N^{\rho}$, then there exist $q \ll \delta^{-k}$ and $A' \subseteq [1, N']$ with*

$$N' \gg \delta^{k(k+1)} N, \quad |A'| \geq (\delta + c\delta^k) N', \quad \text{and} \quad (A' - A') \cap I(h_{qd}) = \emptyset.$$

Proof of Theorem 6.1

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $(A - A) \cap I(h) = \emptyset$. Setting $A_0 = A$, $N_0 = N$, $d_0 = 1$, and $\delta_0 = \delta$, Lemma 6.4 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $(A - A) \cap I(h_{d_m}) = \emptyset$ satisfying

$$N_m \geq c\delta^{k(k+1)} N_{m-1} \geq (c\delta)^{k(k+1)m} N, \tag{6.2}$$

$$\delta_m \geq \delta_{m-1} + c\delta_{m-1}^k, \tag{6.3}$$

and

$$d_m \leq (c\delta)^{-k} d_{m-1} \leq (c\delta)^{-km}, \tag{6.4}$$

as long as

$$d_m, \delta_m^{-1} \leq N_m^{\rho}. \tag{6.5}$$

By (6.3), we see that the density δ_m will surpass 1, and hence (6.5) must fail, for $m = C\delta^{-(k-1)}$. In particular, by (6.2) and (6.4) we must have $(c\delta)^{-C\delta^{-(k-1)}} \geq N$, which implies

$$\delta \ll \Big(\frac{\log \log N}{\log N} \Big)^{1/(k-1)},$$

as required. □

6.3 L^2 Concentration for Auxiliary Polynomials

We establish Lemma 6.4 from the following analog of Lemma 3.3.

Lemma 6.5. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, and let $\eta = c_0\delta$ for a sufficiently small constant $c_0 > 0$. If $(A - A) \cap I(h_d) = \emptyset$, $d, \delta^{-1} \leq N^\rho$, and $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then there exists $q \leq \eta^{-k}$ such that*

$$\int_{\mathbf{M}_q(\eta^{-k})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^{k+1} N.$$

Proof of Lemma 6.4

Suppose $A \subseteq [1, N]$, $|A| = \delta N$, $(A-A)\cap I(h_d) = \emptyset$, and $d, \delta^{-1} \leq N^\rho$. If $|A\cap(N/9, 8N/9)| < 3\delta N/4$, then $\max\{|A \cap [1, N/9]|, |A \cap [8N/9, N]|\} > \delta N/8$. In other words, A has density at least $9\delta/8$ on one of these intervals. Otherwise, Lemmas 6.5 and 2.3 apply, so in either case, letting $\eta = c_0\delta$, there exists $q \leq \eta^{-k}$ and an arithmetic progression

$$P = \{x + \ell q : 1 \leq \ell \leq L\}$$

with $qL \gg \delta^k N$ and $|A \cap P|/L \geq \delta + c\delta^k$. Partitioning P into subprogressions of step size $\lambda(q)$, the pigeonhole principle yields a progression

$$P' = \{y + \ell\lambda(q) : 1 \leq \ell \leq N'\} \subseteq P$$

with $N' \geq qL/2\lambda(q)$ and $|A \cap P'|/N' \geq \delta + c\delta^k$. This allows us to define a set $A' \subseteq [1, N']$ by

$$A' = \{\ell \in [1, N'] : y + \ell\lambda(q) \in A\},$$

which satisfies $|A'| \geq (\delta + c\delta^k)N'$ and $N' \gg \delta^k N/\lambda(q) \gg \delta^{k(k+1)}N$. Moreover, by Proposition 6.3, $(A - A) \cap I(h_d) = \emptyset$ implies $(A' - A') \cap I(h_{qd}) = \emptyset$. □

Proof of Lemma 6.5

Suppose $A \subseteq [1,N]$ with $|A| = \delta N$ and $(A-A) \cap I(h_d) = \emptyset$. Let $\eta = c_0\delta$ and let $M = \lfloor (N/9b_d)^{1/k} \rfloor$, where b_d is the leading coefficient of h_d. Letting $H_d = \{n \in \mathbb{N} : 0 < h_d(n) < N/9\}$, we note by (6.1) that

$$|H_d \triangle [1,M]| \ll 1. \tag{6.6}$$

If $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then on the transform side, as in Section 2.3, we have by (6.6) that

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |S_{d,M}(\alpha)| \mathrm{d}\alpha \geq \Big| \sum_{\substack{n \in \mathbb{Z} \\ m \in H_d}} f_A(n) f_A(n + h_d(m)) \Big| + O(N) \geq \delta^2 NM/4, \tag{6.7}$$

where

$$S_{d,x}(\alpha) = \sum_{1 \leq m \leq x} e^{2\pi i h_d(m)\alpha}.$$

It follows from traditional Weyl sum estimates and observations of Lucier on auxiliary polynomials that if $d, \delta^{-1} \leq N^\rho$, then

$$|S_{d,M}(\alpha)| \ll q^{-1/k} M \quad \text{if} \quad \alpha \in \mathbf{M}_q(\eta^{-k}),\ q \leq \eta^{-k} \tag{6.8}$$

and

$$|S_{d,M}(\alpha)| \leq C\eta M \leq \delta M/8 \quad \text{for all} \quad \alpha \in \mathfrak{m}(\eta^{-k}), \tag{6.9}$$

provided we choose $c_0 \leq 1/8C$. We will discuss these estimates in more detail in Section 6.4. By (6.9) and Plancherel's Identity, we have

$$\int_{\mathfrak{M}(\eta^{-k})} |\widehat{f_A}(\alpha)|^2 |S_{d,M}(\alpha)| \mathrm{d}\alpha \geq \delta^2 NM/8,$$

which by (6.7) and (6.8) implies

$$\delta^2 N \ll \Big(\sum_{1\le q\le \eta^{-k}} q^{-1/k} \Big) \max_{q\le \eta^{-k}} \int_{\mathbf{M}_q(\eta^{-k})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha$$

$$\ll \eta^{-(k-1)} \max_{q\le \eta^{-k}} \int_{\mathbf{M}_q(\eta^{-k})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha,$$

and the lemma follows. □

The remainder of the chapter is dedicated to establishing estimates (6.8) and (6.9).

6.4 Exponential Sum Estimates over Polynomials

The following lemma generalizes Lemma 3.4 to arbitrary polynomials.

Lemma 6.6. *Suppose $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{Z}[x]$ and let $J = |a_0| + \cdots + |a_k|$. If $a, q \in \mathbb{N}$ and $\alpha = a/q + \beta$, then*

$$\sum_{m=1}^{M} e^{2\pi i f(m)\alpha} = q^{-1} G_f(a,q) \int_0^M e^{2\pi i f(x)\beta} \mathrm{d}x + O(q(1 + JM^k\beta)),$$

where

$$G_f(a,q) = \sum_{r=0}^{q-1} e^{2\pi i h(r) a/q}.$$

Proof. We begin by noting that for any $a, q \in \mathbb{N}$ and $x \ge 0$,

$$\sum_{1\le m\le x} e^{2\pi i f(m)a/q} = \sum_{r=0}^{q-1} \sum_{\substack{1\le m\le x \\ m\equiv r \bmod q}} e^{2\pi i f(r)a/q} = q^{-1} G_f(a,q) x + O(q), \tag{6.10}$$

since $\#\{1 \le m \le x : m \equiv r \bmod q\} = x/q + O(1)$.

Using (6.10) and successive applications of summation and integration by parts, we have that if $\alpha = a/q + \beta$, then

$$\sum_{m=1}^{M} e^{2\pi i f(m)\alpha} = q^{-1}G_f(a,q)\Big(Me^{2\pi i f(M)\beta} - \int_0^M x(2\pi i\beta f'(x))e^{2\pi i f(x)\beta}\mathrm{d}x\Big) + O(q(1+JM^k\beta))$$

$$= q^{-1}G_f(a,q)\int_0^M e^{2\pi i f(x)\beta}\mathrm{d}x + O(q(1+JM^k\beta)),$$

as required. □

To establish the cancellation on the major arcs promised in (6.8), we need the following generalization of Lemma 3.5, obtained independently by Chen [3] and Nechaev [17].

Lemma 6.7. *If $f(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathbb{Z}[x]$ and $(a,q) = 1$, then*

$$|G_f(a,q)| \ll \gcd(\mathrm{cont}(f), q)^{1/k}q^{1-1/k},$$

where

$$\mathrm{cont}(f) = \gcd(a_1, \ldots, a_k).$$

The conclusion of Lemma 6.7 indicates that we could lose control of the sum $G(a,q)$ if the coefficients of the auxiliary polynomials h_d share larger and larger common factors. The following observation of Lucier ensures that this does not occur.

Lemma 6.8 (Lemma 28, [11])**.** *For every $d \in \mathbb{N}$,*

$$\mathrm{cont}(h_d) \leq |\Delta(h)|^{(k-1)/2}\mathrm{cont}(h),$$

where $\Delta(h) = a^{2k-2}\prod_{i\neq j}(\alpha_i - \alpha_j)^{e_ie_j}$ if h factors over the complex numbers as

$$h(x) = a(x-\alpha_1)^{e_1}\ldots(x-\alpha_r)^{e_r}$$

with all the α_i's distinct.

While the statement of Lemma 6.8 is pleasingly precise, we only use that $\mathrm{cont}(h_d)$ is uniformly bounded in terms of the original polynomial h.

Proof of (6.8)

Since

$$d, \delta^{-1} \ll N^{\rho} \ll M^{2k\rho}, \tag{6.11}$$

and all of the coefficients of h_d are bounded by a constant times d^{k-1}, Lemma 3.4 yields

$$|S_M(\alpha)| \leq q^{-1}|G_{h_d}(a,q)|M + O(M^{6k^2\rho})$$

provided $\alpha \in \mathbf{M}_q(\eta^{-k})$, $q \leq \eta^{-k}$. Applying Lemmas 6.7 and 6.8, the estimate follows. □

For the minor arcs we now require the full Weyl inequality, which says that when taking an exponential sum over a polynomial, the only obstruction to cancellation is if the leading coefficient is close to a rational with small denominator.

Lemma 6.9 (Weyl Inequality)**.** *If $\alpha_1, \dots, \alpha_k \in \mathbb{R}$, $t \geq 1$, $(a,q) = 1$ and $|\alpha_k - a/q| \leq t/q^2$, then*

$$\Big| \sum_{m=1}^{M} e^{2\pi i(\alpha_1 m + \cdots + \alpha_k m^k)} \Big| \ll M^{1+\epsilon}(t/q + 1/M + t/M^{k-1} + q/M^k)^{2^{1-k}}$$

for any $\epsilon > 0$, where the implied constant depends only on k and ϵ.

This result is completely standard, and although most treatments, such as Lemma 2.4 of [25], restrict to the case of $t = 1$, this version follows from a trivial modification of the proof.

Corollary 6.10. *Suppose $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ with $a_k \in \mathbb{N}$. If $(a,q) = 1$ and $|\alpha - a/q| \leq q^{-2}$, then*

$$\Big| \sum_{m=1}^{M} e^{2\pi i f(m)\alpha} \Big| \ll M^{1+\epsilon}(a_k/q + 1/M + a_k/M^{k-1} + q/M^k)^{2^{1-k}}$$

for any $\epsilon > 0$, where the implied constant depends only on k and ϵ.

Proof. Suppose $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ with $a_k \in \mathbb{N}$, $(a,q) = 1$, and $|\alpha - a/q| \le q^{-2}$. Letting $D = \gcd(a_k, q)$, we see that

$$\Big| a_k \alpha - \frac{a_k a/D}{q/D} \Big| \le \frac{a_k/D}{(q/D)^2},$$

so by Lemma 6.9 we have

$$\Big| \sum_{m=1}^{M} e^{2\pi i f(m)\alpha} \Big| \ll M^{1+\epsilon} \Big(\frac{a_k/D}{q/D} + \frac{1}{M} + \frac{a_k/D}{M^{k+1}} + \frac{q/D}{M^k} \Big)^{2^{1-k}},$$

and the corollary follows. □

Proof of (6.9)

For a fixed $\alpha \in \mathfrak{m}(\eta^{-k})$, we have by the pigeonhole principle that there exist

$$1 \le q \le M^{k-1/4}$$

and $(a,q) = 1$ with

$$|\alpha - a/q| < 1/qM^{k-1/4}.$$

If $\eta^{-k} \le q \le M^{1/4}$, then Lemmas 6.6, 6.7, and 6.8 combine with (6.11) to imply

$$|S_M(\alpha)| \le q^{-1} |G_{h_d}(a,q)| M + O(M^{2/3}) \ll q^{-1/k} M \le \eta M.$$

If $M^{1/4} \le q \le M^{k-1/4}$, then Corollary 6.10 and (6.11) imply

$$|S_M(\alpha)| \ll M^{1-2^{-2k}} \le M^{1-2k\rho} \le \eta M.$$

If $1 \le q \le \eta^{-k}$, then, letting $\beta = \alpha - a/q$, it must be the case that

$$|\beta| > 1/\eta^k N \gg 1/\eta^k b_d M^k, \tag{6.12}$$

where again b_d is the leading coefficient of h_d, as otherwise we would have $\alpha \in \mathfrak{M}(\eta^{-k})$.

By Lemma 3.7 we have

$$\Big| \int_0^M e^{2\pi i b_d x^k \beta} \Big| \ll |b_d \beta|^{-1/k}. \tag{6.13}$$

Combining Lemma 6.6 and (6.12) with (6.13) and the fact that

$$\Big| \int_0^M e^{2\pi i b_d x^k \beta} - e^{2\pi i h_d(x)\beta} \mathrm{d}x \Big| \ll d^k M^k \beta \leq M^{1/2}, \tag{6.14}$$

the minor arc estimate is established. □

7 $\mathcal{P}$-intersective Polynomials

In this chapter we establish one of our main new results which improves Theorem E in two ways, expanding the class of polynomials and improving the bound from triple to single logarithmic.

Theorem 7.1. *Suppose $h \in \mathbb{Z}[x]$ is a $\mathcal{P}$-intersective polynomial of degree $k \geq 2$ with positive leading term. If $A \subseteq [1, N]$ and $h(p) \notin A - A$ for all $p \in \mathcal{P}$ with $h(p) > 0$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu} \tag{7.1}$$

for any $\mu < 1/(2k-2)$, where the implied constant depends only on h and μ.

7.1 Main Iteration Lemma: Deducing Theorem 7.1

For the remainder of the argument, we fix a $\mathcal{P}$-intersective polynomial h of degree $k \geq 2$ with positive leading term, and we set $K = 2^{10k}$. We also fix an arbitrary $\epsilon > 0$, we set $\gamma = k + \epsilon$, and we prove Theorem 7.1 with $\mu = 1/2(\gamma - 1) + \epsilon$. For each $p \in \mathcal{P}$ we fix a p-adic integer z_p such that $h(z_p) = 0$ and $z_p \not\equiv 0 \bmod p$. By reducing and applying the Chinese Remainder Theorem, the choices of z_p determine, for each natural number d, a unique integer $r_d \in (-d, 0]$, which consequently satisfies $d \mid h(r_d)$ and $(r_d, d) = 1$. We let the function λ and the auxiliary polynomials h_d be as in Definition 6.2, we let

$$\Lambda_d = \{n \in \mathbb{N} : r_d + dn \in \mathcal{P}\},$$

and we let

$$\mathcal{V}_d(h) = \{h_d(n) > 0 : n \in \Lambda_d\}.$$

The following proposition, analogous to Proposition 6.3, shows that the definition of $\mathcal{V}_d(h)$ is appropriate for keeping track of the inherited lack of arithmetic structure in our density increment iteration.

Proposition 7.2. *If $A \subseteq \mathbb{N}$, $(A-A) \cap \mathcal{V}_d(h) = \emptyset$, and $A' \subseteq \{\ell \in \mathbb{N} : x + \lambda(q)\ell \in A\}$, then $(A'-A') \cap \mathcal{V}_{qd}(h) = \emptyset$.*

Proof. The proof is identical to that of Proposition 6.3, with the added observation that if $n \in \Lambda_{qd}$ and $r_{qd} = r_d + ds$, then $s + qn \in \Lambda_d$. □

We also fix a natural number N, and we set $Q = e^{c\sqrt{\log N}}$for a sufficiently small constant $c > 0$. Applying Lemma 5.2 with $D = 10K$, we let $q_0 \leq Q^{10K}$, $\rho \in [1/2, 1)$, and the Dirichlet character χ be as in the conclusion. We see that if c is sufficiently small and $X \geq N^{1/10k}$, then

$$\psi(x, a, q) = \frac{x}{\phi(q)} - \frac{\chi(a)x^\rho}{\phi(q)\rho} + O(XQ^{-1000K^2}) \tag{7.2}$$

for all $x \leq X$, provided $q_0 \mid q$, $(a, q) = 1$, and $q \leq (q_0 Q)^{10K}$.

Lemma 7.3. *Suppose $A \subseteq [1, L]$ with $|A| = \delta L$ and $L \geq \sqrt{N}$. If $q_0 \mid d$, $(A-A) \cap \mathcal{V}_d(h) = \emptyset$, and $d/q_0, \delta^{-1} \leq Q$, then there exists $q \ll \delta^{-\gamma}$ and $A' \subseteq [1, L']$ with*

$$L' \gg \delta^{\gamma(k+1)} L, \quad |A'| \geq (\delta + c\delta^\gamma)L', \quad \text{and} \quad (A'-A') \cap \mathcal{V}_{qd}(h) = \emptyset.$$

Proof of Theorem 7.1

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $h(p) \notin A - A$ for all $p \in \mathcal{P}$ with $h(p) > 0$, that is to say $(A-A) \cap \mathcal{V}_1(h) = \emptyset$. Partitioning $[1, N]$, the pigeonhole principle guarantees the existence of an arithmetic progression

$$P = \{x + \ell\lambda(q_0) : 1 \leq \ell \leq N_0\} \subseteq [1, N]$$

with $N_0 \geq N/2\lambda(q_0)$ and $|A \cap P| \geq \delta N_0$. Defining $A_0 \subseteq [1, N_0]$ by

$$A' = \{\ell \in [1, N_0] : x + \ell\lambda(q_0) \in A\},$$

we see that $|A_0| \geq \delta N_0$ and $(A-A) \cap \mathcal{V}_{q_0}(h) = \emptyset$. If $\delta \geq Q^{-1}$, then Lemma 7.3 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $(A-A) \cap \mathcal{V}_{d_m}(h) = \emptyset$ satisfying $q_0 \mid d$,

$$N_m \geq c\delta^{\gamma(k+1)} N_{m-1} \geq (c\delta)^{\gamma(k+1)m} N/q_0^k, \tag{7.3}$$

$$\delta_m \geq \delta_{m-1} + c\delta_{m-1}^{\gamma}, \tag{7.4}$$

and

$$d_m \leq (c\delta)^{-\gamma} d_{m-1} \leq (c\delta)^{-\gamma m} q_0, \tag{7.5}$$

as long as

$$d_m/q_0, \delta_m^{-1} \leq Q \tag{7.6}$$

and

$$N_m \geq \sqrt{N} \tag{7.7}$$

By (7.4), we see that the density δ_m will surpass 1, and hence (7.6) must fail, for $m = C\delta^{-(\gamma-1)}$. Therefore, if

$$\delta \geq (\log N)^{-1/2(\gamma-1)+\epsilon}, \tag{7.8}$$

then (7.6) or (7.7) must fail for

$$m = C(\log N)^{1/2-\epsilon}. \tag{7.9}$$

However, we see that (7.5), (7.8), and (7.9) imply

$$d_m/q_0 \leq e^{(\log N)^{1/2-\epsilon/2}} \leq Q,$$

and similarly (7.3), (7.8), and (7.9) imply $N_m \geq N/Q^C$. In particular (7.6) and (7.7) hold, yielding a contradiction, and the theorem follows. □

7.2 L^2 Concentration for $\mathcal{P}$-Intersective Polynomials

We establish Lemma 7.3 from the following analog of Lemma 6.5.

Lemma 7.4. *Suppose $A \subseteq [1, L]$ with $|A| = \delta L$ and $L \geq \sqrt{N}$, and let $\eta = c_0\delta$ for a sufficiently small constant $c_0 > 0$. If $q_0 \mid d$, $d/q_0, \delta^{-1} \leq Q$, $(A-A)\cap \mathcal{V}_d(h) = \emptyset$, and $|A\cap(L/9, 8L/9)| \geq 3\delta L/4$, then there exists $q \leq \eta^{-\gamma}$ such that*

$$\int_{\mathbf{M}_q(\eta^{-\gamma})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^{\gamma+1} L.$$

The deduction of Lemma 7.3 from Lemma 7.4 is completely identical to the deduction of Lemma 6.4 from Lemma 6.5.

Proof of Lemma 7.4

Suppose $A \subseteq [1, L]$ with $|A| = \delta L$, $L \geq \sqrt{N}$, $(A - A) \cap \mathcal{V}_d(h) = \emptyset$, $q_0 \mid d$, and $d/q_0, \delta^{-1} \leq Q$. Let $\eta = c_0\delta$, let ν_d be as in the proof of Lemma 4.4, and let $M = \lfloor (L/9b_d)^{1/k} \rfloor$, where b_d is the leading coefficient of h_d. Letting $H_d = \{n \in \mathbb{N} : 0 < h_d(n) < L/9\}$, we again note by (6.1) that

$$|H_d \triangle [1, M]| \ll 1. \tag{7.10}$$

If $|A \cap (L/9, 8L/9)| \geq 3\delta L/4$, then on the transform side, as in Section 2.3, we have by (7.10) that

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |\mathcal{W}_{d,M}(\alpha)| \mathrm{d}\alpha \geq \Big| \sum_{\substack{n\in\mathbb{Z} \\ m\in H_d}} f_A(n) f_A(n + h_d(m))\nu_d(m) \Big| + O(L \log L) \geq \delta^2 L\Psi/2 + O(L \log L), \tag{7.11}$$

where

$$\Psi = \sum_{m=1}^{M} \nu_d(m) = \phi(d)\psi(dM + r_d, r_d, d)/d$$

and

$$\mathcal{W}_{d,x}(\alpha) = \sum_{1\leq m\leq x} \nu_d(m) e^{2\pi i h_d(m)\alpha}.$$

From (7.2) and (5.2), we know that

$$\Psi \gg (1-\rho)M \gg M/q_0 \geq M/Q^{3K}, \tag{7.12}$$

which combined with (7.11) implies

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |\mathcal{W}_{d,M}(\alpha)| \mathrm{d}\alpha \geq \delta^2 L\Psi/4. \tag{7.13}$$

It follows from (7.2), Lemma 6.8, and Theorem 4.1 of [9] that

$$|\mathcal{W}_{d,M}(\alpha)| \ll q^{-1/\gamma}\Psi \quad \text{if} \quad \alpha \in \mathbf{M}_q(\eta^{-\gamma}),\ q \leq \eta^{-\gamma} \tag{7.14}$$

and

$$|\mathcal{W}_{d,M}(\alpha)| \leq C\eta\Psi \leq \delta\Psi/8 \quad \text{for all} \quad \alpha \in \mathfrak{m}(\eta^{-\gamma}), \tag{7.15}$$

provided we choose $c_0 \leq 1/8C$. We discuss these estimates in more detail in Section 7.3. By (7.13), (7.15) and Plancherel's Identity, we have

$$\int_{\mathfrak{M}(\eta^{-\gamma})} |\widehat{f_A}(\alpha)|^2 |\mathcal{W}_{d,M}(\alpha)| \mathrm{d}\alpha \geq \delta^2 N\Psi/8,$$

which by (7.14) implies

$$\delta^2 N \ll \Big(\sum_{1 \leq q \leq \eta^{-\gamma}} q^{-1/\gamma} \Big) \max_{q \leq \eta^{-\gamma}} \int_{\mathbf{M}_q(\eta^{-\gamma})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha$$

$$\ll \eta^{-(\gamma-1)} \max_{q \leq \eta^{-\gamma}} \int_{\mathbf{M}_q(\eta^{-\gamma})} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha,$$

and the lemma follows. □

The remainder of the chapter is dedicated to establishing estimates (7.14) and (7.15).

7.3 Exponential Sum Estimates for Polynomials in Shifted Primes

The following is the analog of Lemma 6.6 for polynomials in shifted primes.

Lemma 7.5. *Suppose $f(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathbb{Z}[x]$ and let $J = |a_0| + \cdots + |a_k|$. If $q_0 \mid d$, $d/q_0 \le Q$, $a, q \in \mathbb{N}$, $q \le (q_0Q)^{8K}$, and $\alpha = a/q + \beta$, then*

$$\sum_{m=1}^{M} \nu_d(m) e^{2\pi i f(m)\alpha} = \frac{\phi(d)}{\phi(qd)} \mathcal{G}_f(a,q) \int_0^M (1 - \chi(r_d)(dx)^{\rho-1}) e^{2\pi i f(x)\beta} \mathrm{d}x$$

$$+ O(qM(1 + JM^k\beta)Q^{-900K^2}),$$

where

$$\mathcal{G}_f(a,q) = \sum_{\substack{\ell=0 \\ (r_d + d\ell, q) = 1}}^{q-1} e^{2\pi i f(\ell) a/q}.$$

Proof. First we see that for any $x \ge 0$,

$$\sum_{1 \le m \le x} \nu_d(m) e^{2\pi i f(m)a/q} = \frac{\phi(d)}{d} \sum_{\ell=0}^{q-1} e^{2\pi i f(\ell)a/q} \psi(dx + r_d, d\ell + r_d, qd). \tag{7.16}$$

Noting that $(d\ell + r_d, qd) = 1$ if and only if $(d\ell + r_d, q) = 1$, we have by (7.16), (7.2), and the observation that $\chi(d\ell + r_d) = \chi(r_d)$ since $q_0 \mid d$, that

$$\sum_{1 \le m \le x} \nu_d(m) e^{2\pi i f(m)a/q} = \frac{\phi(d)}{\phi(qd)} \mathcal{G}_f(a,q)(x - \chi(r_d)(dx)^\rho/\rho d) + O(qMQ^{-900K^2})$$

for all $x \le M$. The result then follows from successive applications of summation and integration by parts, just as in the proofs of Lemmas 5.5 and 6.6. □

Since $\mathcal{G}_f(a,q)$ is not a typical Gauss sum, we need to do a bit more work to get the cancellation on the major arcs promised in (7.14).

Lemma 7.6. *Suppose $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{Z}[x]$. If $W, b \in \mathbb{Z}$ and $(a, q) = 1$, then*

$$\Big| \sum_{\substack{\ell=0 \\ (W\ell+b,q)=1}}^{q-1} e^{2\pi i f(\ell)a/q} \Big| \ll \Big(\gcd(\mathrm{cont}(f), q_1) \gcd(a_k, q_2) \Big)^{1/k} q^{1-1/k}, \tag{7.17}$$

where $q = q_1 q_2$, q_2 is the maximal divisor of q which is coprime to W, and

$$\mathrm{cont}(f) = \gcd(a_1, \ldots, a_k).$$

Proof. Fix f, W, b, a, q as in Lemma 7.6. As is often the case with this type of sum, we can simplify our argument by taking advantage of multiplicativity. Specifically, it is not difficult to show that if $q = q_1 q_2$ with $(q_1, q_2) = 1$, then

$$\sum_{\substack{\ell=0 \\ (W\ell+b,q)=1}}^{q-1} e^{2\pi i f(\ell)a/q} = \Bigg(\sum_{\substack{\ell_1=0 \\ (W\ell_1+b,q_1)=1}}^{q_1-1} e^{2\pi i f(\ell_1)a_1/q_1} \Bigg) \Bigg(\sum_{\substack{\ell_2=0 \\ (W\ell_2+b,q_2)=1}}^{q_2-1} e^{2\pi i f(\ell_2)a_2/q_2} \Bigg),$$

where $a/q = a_1/q_1 + a_2/q_2$, so we can assume $q = p^j$ for some $p \in \mathcal{P}$, $j \in \mathbb{N}$. If $p \mid W$ and $p \mid b$, then $W\ell + b$ is never coprime to p^j, so the sum is clearly zero. If $p \mid W$ and $p \nmid b$, then $W\ell + b$ is always coprime to p^j, so the sum is complete and the result follows from Lemma 6.7. If $p \nmid W$, then $p \mid W\ell + b$ if and only if $\ell \equiv -bW^{-1} \bmod p$. Therefore,

$$\sum_{\substack{\ell=0 \\ p \nmid W\ell+b}}^{p^j-1} e^{2\pi i g(\ell)a/p^j} = \sum_{\ell=0}^{p^j-1} e^{2\pi i f(\ell)a/p^j} - \sum_{r=0}^{p^{j-1}-1} e^{2\pi i f(pr+m)a/p^j}, \tag{7.18}$$

where $m \equiv -bW^{-1} \bmod p$, and by Lemma 6.7 we need only obtain the estimate for the second sum. Setting

$$\tilde{f}(r) = \frac{f(pr+m) - f(m)}{p},$$

we see that $\tilde{f}$ is a polynomial with integer coefficients and leading coefficient $a_k p^{k-1}$. In particular,

$$\gcd(\mathrm{cont}(\tilde{f}), p^{j-1}) \le p^{k-1} \gcd(a_k, p^{j-1}).$$

Therefore, by Lemma 6.7 we have

$$\Big|\sum_{r=0}^{p^{j-1}-1} e^{2\pi i f(pr+m)a/p^j}\Big| = \Big|\sum_{r=0}^{p^{j-1}-1} e^{2\pi i (f(pr+m)-f(m))a/p^j}\Big|$$

$$= \Big|\sum_{r=0}^{p^{j-1}-1} e^{2\pi i \tilde{f}(r)a/p^{j-1}}\Big|$$

$$\ll \Big(p^{k-1}\gcd(a_k, p^{j-1})\Big)^{1/k} p^{(j-1)(1-1/k)}$$

$$\leq \gcd(a_k, p^j)^{1/k} p^{j(1-1/k)},$$

as required. □

Corollary 7.7. *If $(a,q)=1$, then*

$$|\mathcal{G}_{h_d}(a,q)| \ll q^{1-1/k}$$

for all $d \in \mathbb{N}$, where the implied constant depends only on h.

Proof. From its definition, we see that the leading coefficient of h_d is $d^k b/\lambda(d)$, where b is the leading coefficient of h. Given $q \in \mathbb{N}$ and $(a,q)=1$, we write $q = q_1 q_2$, where q_2 is the maximal divisor of q which is coprime to d. In particular,

$$\gcd(d^k b/\lambda(d), q_2) \leq b. \tag{7.19}$$

Therefore, by Lemma 7.6, Lemma 6.8, and (7.19) we have

$$|\mathcal{G}_{h_d}(a,q)| = \Big|\sum_{\substack{\ell=0 \\ (r_d+d\ell,q)=1}}^{q-1} e^{2\pi i h_d(\ell)a/q}\Big| \ll \Big(\gcd(\mathrm{cont}(h_d), q_1)b\Big)^{1/k} q^{1-1/k} \ll q^{1-1/k},$$

as required. □

Proof of (7.14)

Since $q_0 \mid d$ and $d, \delta^{-1} \leq Q$, Lemma 7.5 and Corollary 7.7 yield

$$|\mathcal{W}_{d,M}(\alpha)| \ll \frac{q^{1-1/k}\phi(d)}{\phi(qd)}(M - \chi(r_d)(dM)^\rho/\rho d) + O(MQ^{-800K^2})$$

$$\ll q^{-1/\gamma}\Psi + O(MQ^{-800K^2})$$

provided $\alpha \in \mathbf{M}_q(\eta^{-\gamma})$, $q \leq \eta^{-\gamma}$, where the last inequality uses that $\phi(qd) \geq \phi(q)\phi(d)$ and $\phi(q) \gg q/\log\log q$. By (7.12) the error term is negligible, and the estimate follows. □

For our minor arc estimate we need the following analog of Weyl's Inequality, due to Li and Pan, which generalizes work of Vinogradov.

Lemma 7.8. *Suppose $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{Z}[x]$ with $a_k > 0$, $D, W \in \mathbb{N}$, and $b \in \mathbb{Z}$. If $U \geq \log D$, $a_k \gg |a_0| + \cdots + |a_{k-1}|$, and $W, |b|, a_k \leq U^k$, then*

$$\sum_{\substack{x=1 \\ Wx+b\in\mathcal{P}}}^{D} \log(Wx+b)e^{2\pi i f(x)\alpha} \ll \frac{D}{U} + U^C D^{1-c}$$

for some constants $C = C(k)$ and $c = c(k) > 0$, provided

$$|\alpha - a/q| \leq q^{-2} \quad \text{for some} \quad U^K \leq q \leq f(D)/U^K \quad \text{and} \quad (a,q) = 1.$$

Lemma 7.8 is a rougher, only nominally generalized version of Theorem 4.1 of [9]. That result restricts to the case where U is a power of $\log D$, and provides a more precise bound in place of K, but the main achievement of the theorem is that one can take U to be that small. Larger values of U, and hence stricter conditions on q, actually make the proof, which can be found in the appendix of that paper, slightly easier. Specifically, one can observe that the precise condition on q is not utilized until Lemmas 4.11 and 4.12, and adaptations of those lemmas are sufficient to adapt the proof of Theorem 4.1.

Proof of (7.15)

For a fixed $\alpha \in \mathfrak{m}(\eta^{-\gamma})$ we have by the pigeonhole principle that there exist

$$1 \leq q \leq L/(q_0 Q)^K$$

and $(a, q) = 1$ with

$$|\alpha - a/q| < (q_0 Q)^K / qL.$$

If $\eta^{-\gamma} \leq q \leq (q_0 Q)^K$, then Lemma 7.5, Corollary 7.7, and (7.12) imply

$$|\mathcal{W}_{d,M}(\alpha)| \ll q^{-1/\gamma}\Psi + O(MQ^{-800K^2}) \ll \eta\Psi.$$

If $(q_0 Q)^K \leq q \leq L/(q_0 Q)^K$, then we can apply Lemma 7.8 with $U = q_0 Q$, which combined with (7.12) and the bound $\delta^{-1} \leq Q$ yields

$$|\mathcal{W}_{d,M}\alpha)| \ll M/q_0 Q \ll \eta\Psi.$$

If $1 \leq q \leq \eta^{-2}$, then, letting $\beta = \alpha - a/q$, it must be the case that

$$|\beta| > 1/\eta^{\gamma} L \gg 1/\eta^{\gamma} b_d M^k, \tag{7.20}$$

where b_d is the leading coefficient of h_d, as otherwise we would have $\alpha \in \mathfrak{M}(\eta^{-\gamma})$. By (6.13), (6.14), and (7.20), we have

$$\Big| \int_0^M e^{2\pi i h_d(x)\beta} \mathrm{d}x \Big| \ll \eta M,$$

which combined with Lemma 7.5, (7.12), and integration by parts yields

$$|\mathcal{W}_{d,M}(\alpha)| \leq \Big| \int_0^M (1-(dx)^{\rho-1}) e^{2\pi i h_d(x)\beta} \mathrm{d}x \Big| + O(MQ^{-800K^2})$$

$$\leq \eta M(1-(dM)^{\rho-1}) + O(MQ^{-800K^2})$$

$$\ll \eta(M-(dM)^{\rho}/\rho d + 2(1-\rho)M)$$

$$\ll \eta\Psi,$$

and the minor arc estimate is established. □

8 A Template for Sárközy's Method

As the attentive reader has surely realized, the methods used in the preceeding chapters are all morally the same. The main distinguishing characteristic is the type of exponential sum estimates required to obtain the L^2 concentration of the transform of the balance function. In this chapter we provide a template for this method, which allows one to plug in appropriate major and minor arc exponential sum estimates over a set $H \subseteq \mathbb{N}$ and extract a bound on the largest subset of $[1, N]$ with no differences in H.

Theorem 8.1. *Suppose that $H \subseteq \mathbb{N}$, increasing functions $B_1, B_2, B_3 : \mathbb{N} \to [0, \infty]$, a decreasing function $D : (0, 1] \to [1, \infty)$, a completely multiplicative function $\lambda : \mathbb{N} \to \mathbb{N}$ satisfying $q \mid \lambda(q)$, and $b : \mathbb{N} \to [0, 1]$ are such that the following implication holds:*

If $\delta^{-1} \leq B_1(N)$, $d \leq B_2(N)$, $L \geq B_3(N)$, and N is sufficiently large, then there exists a not identically zero function $\nu = \nu(d, L) : \mathbb{Z} \to [0, \infty)$ supported on $H_d \cap [1, L/9]$, where

$$H_d = \{h \in \mathbb{N} : \lambda(d)h \in H\},$$

such that

$$|\widehat{\nu}(\alpha)| \leq b(q)M \quad \text{if} \quad \alpha \in \mathbf{M}_q(D(\delta), L),\ q \leq D(\delta) \tag{8.1}$$

and

$$|\widehat{\nu}(\alpha)| \leq \delta M/4 \quad \text{if} \quad \alpha \in \mathfrak{m}(D(\delta), L), \tag{8.2}$$

where $M = \widehat{\nu}(0) = \sum_{x \in \mathbb{Z}} \nu(x)$.

Then, if $A \subseteq [1,N]$ with $|A| = \delta N$ and $(A-A) \cap H = \emptyset$, one of the following holds:

1. $\delta < C/B_1(N)$.

2. $C(D(\delta))^m > B_2(N)$

3. $\Big(C \max\{D(\delta), E(\delta)\} \max_{q \le D(\delta)} \lambda(q)\Big)^{-m} N < B_3(N)$,

where C is a sufficiently large absolute constant,

$$E(\delta) = \begin{cases} \displaystyle\sum_{1 \le q \le D(\delta)} b(q) & \text{in general} \\ 1 & \text{if } b(rq) \ge b(r)/q \text{ and } \displaystyle\sum_{1 \le q \le Q} qb(q) \ll Q \end{cases},$$

and

$$m = \begin{cases} CE(\delta) & \text{if } E(2x) \le cE(x) \text{ for some } c < 1 \\ CE(\delta)\log(\delta^{-1}) & \text{else} \end{cases}.$$

8.1 Main Iteration Lemma: Deducing Theorem 8.1

For the remainder of this note we fix a sufficiently large natural number N, a set $H \subseteq \mathbb{N}$ and functions $B_1, B_2, B_3, D, \lambda, b$ meeting the hypotheses of Theorem 8.1. The theorem follows quickly from the following iteration lemma.

Lemma 8.2. *Suppose that $A \subseteq [1,L]$ with $|A| = \delta L$, $\delta^{-1} \le B_1(N)$, and $L \ge B_3(N)$. If $d \le B_2(N)$ and $(A-A) \cap H_d = \emptyset$, then there exists $q \le D(\delta)$ and a set $A' \subseteq [1,L']$ satisfying*

$$L' \gg (\max\{D(\delta), E(\delta)\} \max_{q \le D(\delta)} \lambda(q))^{-1} L, \quad |A'| \ge \delta(1 + c/E(\delta))L', \quad \text{and} \quad (A'-A') \cap H_{qd} = \emptyset.$$

Proof of Theorem 8.1

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $(A-A) \cap H = \emptyset$. If $\delta^{-1} \leq B_1(N)$ and N is sufficiently large, then Lemma 8.2 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $(A_m - A_m) \cap H_{d_m} = \emptyset$ satisfying

$$N_m \gg (\max\{D(\delta), E(\delta)\} \max_{q \leq D(\delta)} \lambda(q))^{-m} N, \quad \delta_m \geq \delta_{m-1}(1 + c/E(\delta_{m-1})), \tag{8.3}$$

and

$$d_m \leq (D(\delta))^m$$

as long as

$$d_m \leq B_2(N) \tag{8.4}$$

and

$$N_m \geq B_3(N). \tag{8.5}$$

However, we see by (8.3) that the density δ_m will exceed 1, and hence (8.4) or (8.5) must fail, with

$$m = \begin{cases} CE(\delta) & \text{if } E(2x) \leq cE(x) \text{ for some } c < 1 \\ CE(\delta)\log(\delta^{-1}) & \text{else} \end{cases},$$

and the theorem follows. □

8.2 L^2 Concentration

We deduce Lemma 8.2 from the following analog of Lemma 3.3.

Lemma 8.3. *Suppose $A \subseteq [1, L]$ with $|A| = \delta L$, $\delta^{-1} \leq B_1(N)$, and $L \geq B_3(N)$. Suppose further that $d \leq B_2(N)$ and $(A - A) \cap H_d = \emptyset$. If $|A \cap (L/9, 8L/9)| \geq 3\delta L/4$, then there exists $q \leq D(\delta)$ with*

$$\int_{\mathbf{M}'_q(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \gg \delta^2 L/E(\delta).$$

Proof of Lemma 8.2

Suppose $A \subseteq [1, L]$ meets the hypotheses of Lemma 8.2. If $|A \cap (L/9, 8L/9)| < 3\delta L/4$, then $\max\{|A \cap [1, L/9]|, |A \cap [8L/9, L]\} \geq \delta L/8$. In other words, A has density at least $9\delta/8$ on one of these intervals. Otherwise, Lemmas 8.3 and 2.3 apply, so in either case there exists $q \leq D(\delta)$ and an arithmetic progression

$$P = \{x + \ell q : 1 \leq \ell \leq J\}$$

with $J \gg (\max\{D(\delta), E(\delta)\}q)^{-1}L$ and $|A \cap P| \geq \delta(1 + c/E(\delta))J$. Partitioning P into subprogressions of step size $\lambda(q)$, the pigeonhole principle yields a progression

$$P' = \{y + \ell\lambda(q) : 1 \leq \ell \leq L'\} \subseteq P$$

with $L' \geq qJ/2\lambda(q)$ and $|A \cap P'| \geq \delta(1 + c/E(\delta))L'$. This allows us to define a set $A' \subseteq [1, L']$ by

$$A' = \{\ell \in [1, L'] : y + \ell\lambda(q) \in A\},$$

which satisfies $|A'| \geq \delta(1 + c/E(\delta))L'$ and $L' \gg (\max\{D(\delta), E(\delta)\} \max_{q \leq D(\delta)} \lambda(q))^{-1}L$. Moreover, $(A - A) \cap H_d = \emptyset$ implies $(A' - A') \cap H_{qd} = \emptyset$, as $\lambda(q)h \in H_d$ whenever $h \in H_{qd}$. □

Proof of Lemma 8.3

Suppose $A \subseteq [1, L]$ meets the hypotheses of Lemma 8.3, and let ν be the function guaranteed in the hypotheses of Theorem 8.1. Since $(A - A) \cap H_d = \emptyset$, ν is supported on $H_d \cap [1, L/9]$, and $|A \cap (L/9, 8L/9)| \geq 3\delta L/4$, we have on the transform side, as in Section 2.3, that

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |\widehat{\nu}(\alpha)| \mathrm{d}\alpha \geq \delta^2 NM/2, \tag{8.6}$$

where

$$M = \sum_{x \in \mathbb{Z}} \nu(x).$$

From (8.2) and Plancherel's Identity we see

$$\int_{\mathfrak{M}(D(\delta))} |\widehat{f_A}(\alpha)|^2 |\widehat{\nu}(\alpha)| \mathrm{d}\alpha \geq \delta^2 NM/4. \tag{8.7}$$

By (8.1) and (8.7), we have

$$\delta^2 N \ll \sum_{1\leq q\leq D(\delta)} b(q) \int_{\mathbf{M}_q(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \leq \Big(\sum_{1\leq q\leq D(\delta)} b(q)\Big) \max_{q\leq D(\delta)} \int_{\mathbf{M}_q(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha, \tag{8.8}$$

establishing the result in the general case since $\mathbf{M}_q(D(\delta)) \subseteq \mathbf{M}'_q(D(\delta))$. Further, if b satisfies $b(rq) \geq b(r)/q$ and

$$\sum_{1\leq q\leq Q} qb(q) \ll Q,$$

then by (8.8) we see

$$\begin{aligned}
D(\delta) \max_{q\leq D(\delta)} \int_{\mathbf{M}'_q(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha &\gg \sum_{1\leq q\leq D(\delta)} qb(q) \int_{\mathbf{M}'_q(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \\
&= \sum_{1\leq q\leq D(\delta)} qb(q) \sum_{r|q} \int_{\mathbf{M}_r(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \\
&= \sum_{1\leq r\leq D(\delta)} \int_{\mathbf{M}_r(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \Big(r \sum_{1\leq q\leq D(\delta)/r} qb(rq)\Big) \\
&\gg D(\delta) \sum_{1\leq r\leq D(\delta)} b(r) \int_{\mathbf{M}_r(D(\delta))} |\widehat{f_A}(\alpha)|^2 \mathrm{d}\alpha \\
&\gg D(\delta)\delta^2 N,
\end{aligned}$$

which establishes the lemma in the case that $E(\delta) = 1$. □

9 Fourier Analysis on $\mathbb{Z}/N\mathbb{Z}$

For the remainder of our discussions, it is convenient, if not necessary, for us to identify the interval $[1, N]$ with the finite cyclic group $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$, on which we utilize a normalized discrete Fourier transform. Specifically, for a function $F : \mathbb{Z}_N \to \mathbb{C}$, we define $\widehat{F} : \mathbb{Z}_N \to \mathbb{C}$ by

$$\widehat{F}(t) = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} F(x) e^{-2\pi i x t/N}.$$

In this finite setting, standard properties like Plancherel's Identity

$$\sum_{t \in \mathbb{Z}_N} |\widehat{F}(t)|^2 = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} |F(x)|^2$$

follow easily from the orthogonality relation

$$\frac{1}{N} \sum_{t \in \mathbb{Z}_N} e^{2\pi i x t/N} = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \in \mathbb{Z}_N \setminus \{0\} \end{cases}. \tag{9.1}$$

9.1 Expressing Counts on the Transform Side

In the $\mathbb{Z}_N$ setting, when analyzing the Fourier analytic behavior of a set $A \subseteq [1, N]$, we carefully distinguish the frequency at 0 and directly analyze the transform of the characteristic function of A. By (9.1), this is completely equivalent to considering the balance function like we did previously, as the balance function has mean value 0 and the transforms of the characteristic function and balance function are identical away from 0.

For the purposes of the subsequent chapters, it will be useful for us to explore a slightly more general version of expressing counts on the transform side, which exploits the fact that the Fourier transform takes translations to modulations. For a set A we use the common abuse of notation $A(x) := 1_A(x)$, and for two sets $A, B \subseteq [1, N]$ with $|A| = \delta N$, a function $h : [1, N] \to \mathbb{Z}$, a weight $\nu : [1, N] \to [0, \infty)$, and $s \in \mathbb{Z}_N$, we see by (9.1) that

$$\frac{1}{N} \sum_{n,m \in \mathbb{Z}_N} A(n + h(m))B(n)\nu(m)e^{2\pi ins/N}$$

$$= \frac{1}{N^2} \sum_{x,y,m \in \mathbb{Z}_N} A(x)B(y)\nu(m)e^{2\pi iys/N} \sum_{t \in \mathbb{Z}_N} e^{2\pi i(y-x+h(m))t/N}$$

$$= \sum_{t \in \mathbb{Z}_N} \widehat{A}(t)\overline{\widehat{B}(s+t)}S(t),$$

where

$$S(t) = \sum_{m \in \mathbb{Z}_N} \nu(m)e^{2\pi ih(m)t/N}.$$

In particular, if there are no solutions to

$$x - y \equiv h(m) \bmod N$$

with $x \in A$, $y \in B$, and m in the support of ν, then

$$\sum_{t \in \mathbb{Z}_N} \widehat{A}(t)\overline{\widehat{B}(s+t)}S(t) = 0$$

and hence

$$\sum_{t \in \mathbb{Z}_N \backslash \{0\}} |\widehat{A}(t)||\widehat{B}(s+t)||S(t)| \geq |\widehat{A}(0)||\widehat{B}(s)||S(0)| = \delta|\widehat{B}(s)| \sum_{m \in \mathbb{Z}_N} \nu(m).$$

9.2 The Hardy-Littlewood Circle Method

Morally, the application of the circle method in the $\mathbb{Z}_N$ setting is the same as in the previous chapters, but the discrete frequency domain and the "separation" of the 0 frequency from the nonzero frequencies lead to the following, slightly modified definition of the major and minor arcs.

Definition 9.1. Given $N \in \mathbb{N}$ and $K > 0$, we define, for each $q \in \mathbb{N}$ and $a \in [1, q]$,

$$\mathbf{M}_{a/q}(K) = \mathbf{M}_{a/q}(K, N) = \left\{ t \in \mathbb{Z}_N : \left| \frac{t}{N} - \frac{a}{q} \right| < \frac{K}{N} \right\},$$

$$\mathbf{M}_q(K) = \bigcup_{(a,q)=1} \mathbf{M}_{a/q}(K) \setminus \{0\},$$

and

$$\mathbf{M}'_q(K) = \bigcup_{r|q} \mathbf{M}_r(K) = \bigcup_{a=1}^{q} \mathbf{M}_{a/q}(K) \setminus \{0\}.$$

We then define $\mathfrak{M}(K)$, the *major arcs*, by

$$\mathfrak{M}(K) = \bigcup_{q=1}^{K} \mathbf{M}_q(K),$$

and $\mathfrak{m}(K)$, the *minor arcs*, by

$$\mathfrak{m}(K) = \mathbb{Z}_N \setminus (\mathfrak{M}(K) \cup \{0\}).$$

Again we note that if $2K^3 < N$, then

$$\mathbf{M}_{a/q}(K) \cap \mathbf{M}_{b/r}(K) = \emptyset \tag{9.2}$$

whenever $a/q \neq b/r$ and $q, r \leq K$.

9.3 Density Increment Lemma

We make use of the following density increment lemma, which is analogous to Lemma 2.3 and proven in much the same way, so we omit the details here.

Lemma 9.2 (Lemma 20, [11]). *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$. If $2\pi qK \leq N$ and*

$$\sum_{t \in \mathbf{M}'_q(K)} |\widehat{A}(t)|^2 \geq \theta\delta^2,$$

then there exists an arithmetic progression

$$P = \{x + \ell q : 1 \leq \ell \leq L\}$$

with $L \geq \theta\delta N/32\pi qK$ and $|A \cap P| \geq \delta(1 + \theta/8)L$.

10 Improved Bounds for Intersective Quadratic Polynomials

In this chapter we extend, and mildly improve, the method of Pintz et al. [18] and Balog et al. [1] to establish the following bound for intersective polynomials of degree 2.

Theorem 10.1. *Suppose $h \in \mathbb{Z}[x]$ is an intersective quadratic polynomial with positive leading term. If $A \subseteq [1, N]$ and $h(n) \notin A - A$ for all $n \in \mathbb{N}$ with $h(n) > 0$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu \log\log\log\log N}$$

for any $\mu < 1/\log 3$, where the implied constant depends only on h and μ.

10.1 Overview of the argument

The underlying philosophy of this and many related results is that certain types of non-random phenomena in a set of integers should be detectable in the Fourier transform of the characteristic function of the set. That information about the transform can then be used to obtain some more explicit structural information about the set, such as increased density on a long arithmetic progression, and eventually provide an upper bound on its size.

More specifically, we define

$$I(h) = \{h(n) > 0 : n \in \mathbb{N}\}$$

for a polynomial $h \in \mathbb{Z}[x]$ with positive leading term. If $(A - A) \cap I(h) = \emptyset$ for a set $A \subseteq [1, N]$, one can apply the circle method and Weyl sum estimates to show that this unexpected behavior implies substantial L^2 mass of $\widehat{A}$ over nonzero frequencies near rationals with small denominator. At this point, there are multiple paths to take in order to obtain the desired structural information.

The method of the previous chapters, rephrased in the $\mathbb{Z}_N$ setting, is to use the pigeonhole principle to conclude that there is one single denominator q such that $\widehat{A}$ has L^2 concentration around rationals with denominator q. From this information, one can conclude that A has increased density on a long arithmetic progression with step size an appropriate multiple of q, for example q^2 in the classical squares case. By translating and scaling the intersection of A with this progression, one obtains a new subset A' of a slightly smaller interval with significantly greater density. In addition, if h is an intersective polynomial, A' inherits non-random behavior from the fact that $(A-A) \cap I(h) = \emptyset$. In the case that h is a monomial, A' actually inherits the identical property, but more generally one sees that $(A'-A') \cap I(h_q) = \emptyset$ for the auxiliary polynomial h_q as defined in Definition 6.2. One then shows that if the density of the original set A was too large, then this process could be iterated enough times for the density to surpass 1, obtaining a contradiction.

Pintz, Steiger, and Szemerédi [18] observed that pigeonholing to obtain a single denominator q is a potentially wasteful step. We follow their approach, observing the following dichotomy:

> **Case 1.** There is a single denominator q such that $\widehat{A}$ has extremely high L^2 concentration, greater than yielded by the pigeonhole principle, around rationals with denominator q. This leads to a large density increment on a long arithmetic progression.

> **Case 2.** The L^2 mass of $\widehat{A}$ on the major arcs is spread over many denominators. In this case, an iteration procedure using the "combinatorics of rational numbers" can be employed to build a large collection of frequencies at which $\widehat{A}$ is large, then Plancherel's identity is applied to bound the density of A.

Philosophically, Case 1 provides more structural information about the original set A than Case 2 does. The downside is that the density increment procedure yields a new set and potentially a new polynomial, while the iteration in Case 2 leaves these objects fixed. With these cases in mind, we can now outline the argument, separated into two distinct phases.

> **Phase 1** (The Outer Iteration): Given a set A and an intersective quadratic polynomial h with $(A-A) \cap I(h) = \emptyset$, we ask if the set falls into Case 1 or Case 2 described above.

If it falls into Case 2, then we proceed to Phase 2.

If it falls into Case 1, then the density increment procedure yields a new subset A' of a slightly smaller interval with significantly greater density, and an intersective quadratic h_q with slightly larger coefficients and $(A' - A') \cap I(h_q) = \emptyset$. We can then iterate this process as long as the resulting interval is not too small, and the dichotomy holds as long as the coefficients of the corresponding polynomial are not too large.

One can show that if the resulting sets remain in Case 1, and the process iterates until the interval shrinks down or the coefficients grow to the limit, then the density of the original set A must have satisfied a bound stronger than the one purported in Theorem 10.1.

Contrapositively, we assume that the original density does not satisfy this stricter bound, and we conclude that one of the sets yielded by the density increment procedure must lie in a large interval, have no differences in the image of a polynomial with small coefficients, and fall into Case 2. We call that set $B \subseteq [1, L]$ and the corresponding polynomial h_d.

We now have a set $B \subseteq [1, L]$ and a quadratic polynomial h_d with $(B - B) \cap I(h_d) = \emptyset$ which fall into Case 2, so we can adapt the strategy of [18] and [1].

Phase 2 (The Inner Iteration): We prove that given a frequency $s \in \mathbb{Z}_L$ with s/L close to a rational a/q such that $\widehat{B}(s)$ is large, there are lots of nonzero frequencies $t \in \mathbb{Z}_L$ with t/L close to rationals b/r such that $\widehat{B}(s + t)$ is almost as large. This intuitively indicates that a set P of frequencies associated with large Fourier coefficients can be blown up to a much larger set P' of frequencies associated with nearly as large Fourier coefficients.

The only obstruction to this intuition is the possibility that there are many pairs $(a/q, b/r)$ and $(a'/q', b'/r')$ with $a/q + b/r = a'/q' + b'/r'$. Observations made in [18] and [1] on the combinatorics of rational numbers demonstrate that this potentially harmful phenomenon can not occur terribly often.

Starting with the trivially large Fourier coefficient at 0, this process is applied as long as certain parameters are not too large, and the number of iterations is ultimately limited by the growth of the divisor function. Once the iteration is exhausted, we use the resulting set of large Fourier coefficients and Plancherel's Identity to get the upper bound on the density of B, which is by construction larger than the density of the original set A, claimed in Theorem 10.1.

10.2 Reduction of Theorem 10.1 to Two Lemmas

To make the strategy outlined in Section 10.1 precise, we fix a natural number N, an intersective quadratic polynomial $h \in \mathbb{Z}[x]$ with positive leading term, and a set $A \subseteq [1, N]$ with $|A| = \delta N$ and $(A - A) \cap I(h) = \emptyset$. We fix p-adic integer roots z_p of h for each prime p, which determine roots $r_d \in (-d, 0]$ of h modulo each $d \in \mathbb{N}$, and we let the function λ and the auxiliary polynomials h_d be as in Definition 6.2. We also fix an arbitrary $\epsilon > 0$, set $Z = (\log N)^{\epsilon \log\log\log N}$, and we prove Theorem 10.1 with $\mu = (1 - 11\epsilon)/\log 3$.

Lemma 10.2. *If*

$$\delta \geq e^{-(\log N)^{\epsilon/8}}, \tag{10.1}$$

then there exists $B \subseteq [1, L]$ satisfying $L \geq N^{.99}$, $|B|/L = \sigma \geq \delta$, and $(B - B) \cap I(h_d) = \emptyset$ with $d \leq N^{.01}$. Further, B satisfies $|B \cap [1, L/2]| \geq \sigma L/3$ and

$$\max_{q \leq Z} \sum_{t \in \mathbf{M}_q(Z)} |\widehat{B}(t)|^2 \leq \sigma^2 (\log N)^{-1+\epsilon}. \tag{10.2}$$

We note that $e^{-(\log N)^{\epsilon/8}} \ll (\log N)^{-\log\log\log\log N}$. In particular, if hypothesis (10.1) is not satisfied, then Theorem 10.1 is already more than true. The next lemma corresponds to the iteration scheme in which a set of large Fourier coefficients from distinct major arcs is blown up in such a way that the relative growth of the size of the set is much greater than the relative loss of pointwise mass.

Lemma 10.3. *Suppose $B \subseteq [1, L]$ with $|B| = \sigma L$ is as in the conclusion of Lemma 10.2, let $B_1 = B \cap [1, L/2]$, and suppose $\sigma \geq Z^{-1/6}$. Given $U, V, K \in \mathbb{N}$ with $\max\{U, V, K\} \leq Z^{1/6}$ and a set*

$$P \subseteq \left\{ t \in \bigcup_{q=1}^{V} \mathbf{M}_q(K) \cup \{0\} : |\widehat{B_1}(t)| \geq \frac{\sigma}{U} \right\}$$

satisfying

$$|P \cap \mathbf{M}_{a,q}(K)| \leq 1 \quad \textit{whenever} \quad q \leq V, \tag{10.3}$$

there exist $U', V', K' \in \mathbb{N}$ with $\max\{U', V', K'\} \ll (\max\{U, V, K\})^3 \sigma^{-5/2}$ and a set

$$P' \subseteq \left\{ t \in \bigcup_{q=1}^{V'} \mathbf{M}_q(K') \cup \{0\} : |\widehat{B_1}(t)| \geq \frac{\sigma}{U'} \right\} \tag{10.4}$$

satisfying

$$|P' \cap \mathbf{M}_{a,q}(K')| \leq 1 \quad \textit{whenever} \quad q \leq V' \tag{10.5}$$

and

$$\frac{|P'|}{(U')^2} \geq \frac{|P|}{U^2} (\log N)^{1-10\epsilon}. \tag{10.6}$$

Proof of Theorem 10.1

In order to prove Theorem 10.1, we can assume that

$$\delta \geq (\log N)^{-\log\log\log\log N}.$$

Therefore, Lemma 10.2 produces a set B of density $\sigma \geq \delta$ with the stipulated properties, and we set $P_0 = \{0\}$, $U_0 = 3$, and $V_0 = K_0 = 1$. Lemma 10.3 then yields, for each n, a set P_n with parameters U_n, V_n, K_n such that

$$\max\{U_n, V_n, K_n\} \leq (\log N)^{3^{n+1} \log\log\log\log N}$$

and

$$\frac{1}{\sigma} \geq \frac{1}{\sigma^2} \sum_{t \in P_n} |\widehat{B_1}(t)|^2 \geq \frac{|P_n|}{U_n^2} \gg (\log N)^{n(1-10\epsilon)},$$

where the left-hand inequality comes from Plancherel's Identity, as long as $\max\{U_n, V_n, K_n\} \le Z^{1/6}$. This holds with $n = (1-\epsilon)(\log\log\log\log N)/\log 3$, as $3^{n+1} \le (\log\log\log N)^{1-\epsilon/2}$, and Theorem 10.1 follows. □

10.3 The Outer Iteration I

We deduce Lemma 10.2 from the following density increment lemma which, after partitioning a progression of step size q into progressions of step size $\lambda(q)$, follows immediately from Lemma 9.2 and Proposition 6.3.

Lemma 10.4. *Suppose $B \subseteq [1, L]$ with $|B| = \sigma L$ and $(B - B) \cap I(h_d) = \emptyset$. If $L \ge Z^4$ and*

$$\sum_{t \in \mathbf{M}_q(Z)} |\widehat{B}(t)|^2 \ge \sigma^2 (\log N)^{-1+\epsilon}, \tag{10.7}$$

for some $q \le Z$, then there exists $B' \subseteq [1, L']$ satisfying $L' \gg \sigma L/Z^4$, $(B' - B') \cap I(h_{qd}) = \emptyset$, and

$$|B'|/L' \ge \sigma(1 + (\log N)^{-1+\epsilon}/8).$$

Proof of Lemma 10.2

Setting A_0=A, $N_0 = N$, $\delta_0 = \delta$, and $d_0 = 1$, we iteratively apply Lemma 10.4. This yields, for each k, a set $A_k \subseteq [1, N_k]$ with $|A_k| = \delta_k N_k$ and $(A_k - A_k) \cap I(h_{d_k}) = \emptyset$ satisfying

$$N_k \ge (c\delta/Z^4)^k N, \quad \delta_k \ge \delta_{k-1}(1 + (\log N)^{-1+\epsilon}/8), \quad \text{and} \quad d_k \le Z^k \tag{10.8}$$

as long as $N_k \ge Z^4$ and either

$$\max_{q \le Z} \sum_{t \in \mathbf{M}_q(Z)} |\widehat{A_k}(t)|^2 \ge \delta_k^2 (\log N)^{-1+\epsilon} \tag{10.9}$$

or $|A_k \cap [1, N_k/2]| < \delta_k N_k/3$, as the latter condition implies A_k has density at least $3\delta_k/2$ on the interval $(N_k/2, N_k]$.

We see that by (10.1) and (10.8), the density δ_k will exceed 1 after

$$16\log(\delta^{-1})(\log N)^{1-\epsilon} \leq (\log N)^{1-\epsilon/2}$$

steps, hence $N_k < Z^4$ or (10.9) fails and $|A_k \cap [1, N_k/2]| \geq \delta_k N_k/3$ for some

$$k \leq (\log N)^{1-\epsilon/2}. \tag{10.10}$$

However, we see that (10.1), (10.8), and (10.10) imply

$$N_k \geq N(e^{-(\log N)^{\epsilon/4}})^{(\log N)^{1-\epsilon/2}} \geq Ne^{-(\log N)^{1-\epsilon/4}} \geq N^{.99},$$

so we set $B = A_k$, $L = N_k$, $\sigma = \delta_k$, and $d = d_k$, and we see further that

$$d \leq Z^{(\log N)^{1-\epsilon/2}} \leq e^{(\log N)^{1-\epsilon/4}} \leq N^{.01},$$

as required. □

10.4 The Inner Iteration I

In this section, we let $B \subseteq [1, L]$ and $h_d \in \mathbb{Z}[x]$ be as in the conclusion of Lemma 10.2, we let $B_1 = B \cap [1, L/2]$, and we assume $\sigma \geq Z^{-1/6}$. We set $M = \sqrt{L/10b_d}$, where b_d is the leading coefficient of h_d, and $H_d = \{n \in \mathbb{N} : 0 < h_d(n) < L/10\}$, noting by (6.1) that

$$|H_d \triangle [1, M]| \ll 1. \tag{10.11}$$

Proof of Lemma 10.3

Suppose we have a set P with parameters U, V, K as specified in the hypotheses of Lemma 10.3, and fix an element $s \in P$. Since $(B - B) \cap I(h_d) = \emptyset$, we see that there are no solutions to

$$a - b \equiv h_d(m) \mod L, \quad a \in B,\ b \in B_1,\ m \in H_d.$$

On the transform side as in Section 9.1, combined with (10.11), this implies

$$\sum_{t\in\mathbb{Z}_L} \widehat{B}(t)\overline{\widehat{B_1}(s+t)}\mathcal{S}(t) = \frac{1}{LM^2}\sum_{\substack{n\in\mathbb{Z}_L\\ m\in H_d}} mB(n+h_d(m))B_1(n)e^{2\pi ins/L} + O(M^{-1}) = O(M^{-1}),$$

where

$$\mathcal{S}(t) = \frac{1}{M^2}\sum_{m=1}^{M} me^{2\pi i h_d(m)t/L},$$

which immediately yields

$$\sum_{t\in\mathbb{Z}_L\setminus\{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{S}(t)| \geq |\widehat{B}(0)\widehat{B_1}(s)\mathcal{S}(0)| + O(M^{-1}) \geq \sigma^2/8U, \tag{10.12}$$

since $|\widehat{B_1}(s)| \geq \sigma/U$ and $\mathcal{S}(0) \geq 1/4$. Letting $\eta = c_0\sigma/U$ for a constant $c_0 > 0$, it follows from traditional Weyl sum estimates that

$$|\mathcal{S}(t)| \ll q^{-1/2}\min\{1, (L|t/L - a/q|)^{-1}\} \tag{10.13}$$

if $t \in \mathbf{M}_{a/q}(\eta^{-2})$, $(a,q) = 1$, and $q \leq \eta^{-2}$, and

$$|\mathcal{S}(t)| \leq C\eta \leq \sigma/16U \quad \text{for all } t \in \mathfrak{m}(\eta^{-2}), \tag{10.14}$$

provided $c_0 \leq 1/16C$. We discuss these estimates in more detail in Section 10.5. We have by (10.14), Cauchy-Schwarz, and Plancherel's Identity that

$$\sum_{t\in\mathfrak{M}(\eta^{-2})} |\widehat{B}(t)||\widehat{B_1}(t)||\mathcal{S}(t)| \geq \sigma^2/16U. \tag{10.15}$$

We now wish to assert that we can ignore those frequencies in the major arcs at which the transform of B or B_1 is particularly small. In order to make this precise, we first need to invoke a weighted version of a well-known estimate on the higher moments of Weyl sums.

Specifically, we have that

$$\sum_{t\in\mathbb{Z}_L} |\mathcal{S}(t)|^6 \le C, \tag{10.16}$$

of which we provide a proof in Section 10.5. Choosing a constant $0 < c_1 < (64C^{1/6})^{-3}$, where C comes from (10.16), we define

$$X = \Big\{ t \in \mathfrak{M}(\eta^{-2}) : \min\Big\{ |\widehat{B}(t)|, |\widehat{B_1}(s+t)| \Big\} \le c_1\sigma^{7/2}/U^3 \Big\} \quad \text{and} \quad Y = \mathfrak{M}(\eta^{-2}) \setminus X. \tag{10.17}$$

Using Hölder's Inequality to exploit the sixth moment estimate on $\mathcal{S}$, followed by Plancherel's Identity, we see that

$$\begin{aligned}
\sum_{t\in X} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{S}(t)| &\le \Big(\sum_{t\in X} |\widehat{B}(t)|^{6/5} |\widehat{B_1}(s+t)|^{6/5} \Big)^{5/6} \Big(\sum_{t\in\mathbb{Z}_L} |\mathcal{S}(t)|^6 \Big)^{1/6} \\
&\le \frac{c_1^{1/3}\sigma^{7/6}}{U} \Big(\sum_{t\in\mathbb{Z}_L} |\widehat{B}(t)|^2 + |\widehat{B_1}(s+t)|^2 \Big)^{5/6} \cdot C^{1/6} \\
&\le \sigma^2/32U,
\end{aligned}$$

and hence by (10.15) we have

$$\sum_{t\in Y} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{S}(t)| \ge \sigma^2/32U. \tag{10.18}$$

For $i, j, k \in \mathbb{N}$, we define

$$\mathcal{R}_{i,j,k} = \Big\{ a/q : (a,q) = 1,\ 2^{i-1} \le q \le 2^i, \frac{\sigma}{2^j} \le \max|\widehat{B}(t)| \le \frac{\sigma}{2^{j-1}}, \frac{\sigma}{2^k} \le \max|\widehat{B_1}(s+t)| \le \frac{\sigma}{2^{k-1}} \Big\},$$

where the maximums are taken over nonzero frequencies $t \in \mathbf{M}_{a/q}(\eta^{-2})$.

We see that we have

$$\sum_{a/q\in\mathcal{R}_{i,j,k}}\sum_{t\in\mathbf{M}_{a/q}(\eta^{-2})\setminus\{0\}}|\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{S}(t)|\ll|\mathcal{R}_{i,j,k}|\frac{\sigma^2}{2^j2^k}\max_{a/q\in\mathcal{R}_{i,j,k}}\sum_{t\in\mathbf{M}_{a/q}(\eta^{-2})}|\mathcal{S}(t)|. \quad (10.19)$$

It follows from (10.13) and the bound $U,\sigma^{-1}\le Z^{1/6}$ that if $(a,q)=1$ and $q\le\eta^{-2}$, then

$$\sum_{t\in\mathbf{M}_{a/q}(\eta^{-2})}|\mathcal{S}(t)|\ll q^{-1/2}\log(Z),$$

hence by (10.19) we have

$$\sum_{a/q\in\mathcal{R}_{i,j,k}}\sum_{t\in\mathbf{M}_{a/q}(\eta^{-2})\setminus\{0\}}|\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{S}(t)|\ll|\mathcal{R}_{i,j,k}|\frac{\sigma^2}{2^j2^k}2^{-i/2}\log(Z). \quad (10.20)$$

By our definitions, the sets $\mathcal{R}_{i,j,k}$ exhaust Y by taking $1\le 2^i\le\eta^{-2}$ and $1\le 2^j,2^k\le U^3/c_1\sigma^{5/2}$, a total search space of size $\ll(\log Z)^3$. Therefore, by (10.18) and (10.20) there exist i,j,k in the above range such that

$$\frac{\sigma^2}{U(\log Z)^3}\ll|\mathcal{R}_{i,j,k}|\frac{\sigma^2}{2^j2^k}2^{-i/2}\log Z.$$

In other words, we can set $V_s=2^i$, $W_s=2^j$, and $U_s=2^k$ and take an appropriate nonzero frequency from each of the pairwise disjoint major arcs specified by $\mathcal{R}_{i,j,k}$ to form a set

$$P_s\subseteq\left\{t\in\bigcup_{q=V_s/2}^{V_s}\mathbf{M}_q(\eta^{-2}):\ |\widehat{B_1}(s+t)|\ge\frac{\sigma}{U_s}\right\}$$

which satisfies

$$|P_s|\gg\frac{U_sW_sV_s^{1/2}}{U(\log Z)^4},\quad |P_s\cap\mathbf{M}_{a,q}(\eta^{-2})|\le 1\ \text{ whenever }\ q\le V_s, \quad (10.21)$$

and

$$\max_{t\in\mathbf{M}_{a/q}(\eta^{-2})\setminus\{0\}}|\widehat{B}(t)|\ge\frac{\sigma}{W_s}\text{ whenever }q\le V_s\text{ and }\mathbf{M}_{a/q}(\eta^{-2})\cap P_s\ne\emptyset, \quad (10.22)$$

noting by disjointness of the major arcs that $a/q\in\mathcal{R}_{i,j,k}$ whenever $q\le V_s$ and $\mathbf{M}_{a/q}(\eta^{-2})\cap P_s\ne\emptyset$.

Remark. The exponent of $1/2$ on V_s in (10.21), which ultimately comes from the exponent on q in the estimate for the Gauss sum $G_{h_d}(a,q)$ given by Lemma 6.7, is absolutely essential to the argument. This is exactly the reason for our restriction to quadratic polynomials, as a polynomial of degree k would yield an exponent of $1/k$ on V_s. Balog et al. [1] used a sieve in defining their weighted exponential sum for k^{th}-powers, which resulted in the required "square root cancellation" in a modified Gauss sum, but this technigue intimately uses algebraic properties of the k^{th}-power map and does not generalize in any immediate way beyond monomials.

We now observe that there is a subset $\tilde{P} \subseteq P$ with

$$|\tilde{P}| \gg |P|/(\log Z)^3 \tag{10.23}$$

for which the triple U_s, W_s, V_s is the same. We call those common parameters $\tilde{U}, \tilde{W}$ and $\tilde{V}$, respectively, and we can now foreshadow by asserting that the claimed parameters in the conclusion of Lemma 10.3 will be $U' = \tilde{U}$, $V' = \tilde{V}V$, and $K' = K + \eta^{-2}$, which do satisfy the purported bound.

We let

$$\mathcal{R} = \left\{ \frac{a}{q} + \frac{b}{r} : s \in \mathbf{M}_{a/q}(K) \text{ for some } s \in \tilde{P} \text{ and } t \in \mathbf{M}_{b/r}(\eta^{-2}) \text{ for some } t \in P_s \right\}.$$

By taking one frequency $s+t$ associated to each element in $\mathcal{R}$, we form our set P', which immediately satisfies conditions (10.4) and (10.5) from the conclusion of Lemma 10.3. However, the crucial condition (10.6) on $|P'|$, which by construction is equal to $|\mathcal{R}|$, remains to be shown. To this end, we invoke the work on the combinatorics of rational numbers found in [18] and [1].

Specifically, it is a special case of Lemma CR of [1] that

$$|\mathcal{R}| \geq \frac{|\tilde{P}|(\min_{s\in\tilde{P}}|P_s|)^2}{\tilde{V}D\tau^8(1+\log V)}, \tag{10.24}$$

where

$$D = \max_{r\leq\tilde{V}}\Big|\Big\{b:\ (b,r)=1,\ \mathbf{M}_{b/r}(\eta^{-2})\cap\bigcup_{s\in\tilde{P}}P_s\neq\emptyset\Big\}\Big|,$$

$\tau(q)$ is the divisor function and $\tau = \max_{q\leq V\tilde{V}}\tau(q)$. It is a well-known fact of the divisor function that $\tau(n)\leq n^{1/\log\log n}$ for large n, and since $V\tilde{V}\leq Z$, we have that $\tau\leq(\log N)^{\epsilon}$. We also have from (10.2) that

$$\sigma^2(\log N)^{-1+\epsilon}\geq\max_{r\leq Z}\sum_{t\in\mathbf{M}_r(Z)}|\widehat{B}(t)|^2\geq\max_{r\leq\tilde{V}}\sum_{t\in\mathbf{M}_r(\eta^{-2})}|\widehat{B}(t)|^2\geq\frac{\sigma^2}{\tilde{W}^2}D,$$

where the last inequality follows from (10.22), and hence

$$D\leq\tilde{W}^2(\log N)^{-1+\epsilon}.$$

Combining the estimates on τ and D with (10.21), (10.23), and (10.24), we have

$$|P'|\gg\frac{|P|}{(\log Z)^3}\frac{\tilde{U}^2\tilde{W}^2\tilde{V}}{U^2(\log Z)^8}\frac{(\log N)^{1-\epsilon}}{\tilde{V}\tilde{W}^2(\log N)^{8\epsilon}(\log Z)}\geq\tilde{U}^2\frac{|P|}{U^2}(\log N)^{1-10\epsilon}.$$

Recalling that we set $U'=\tilde{U}$, the lemma follows. □

The following section is dedicated to establishing estimates (10.13), (10.14), and (10.16).

10.5 Weighted Exponential Sum Estimates for Quadratic Polynomials

The following is a weighted analog of Lemma 6.6 for quadratic polynomials.

Lemma 10.5. *Suppose $f(x) = a_0 + a_1x + a_2x^2 \in \mathbb{Z}[x]$ and let $J = |a_0| + |a_1| + |a_2|$. If $a, q \in \mathbb{N}$ and $\alpha = a/q + \beta$, then*

$$\sum_{m=1}^{M} me^{2\pi if(m)\alpha} = q^{-1}G_f(a,q)\int_0^M xe^{2\pi if(x)\beta}\mathrm{d}x + O(qM(1+JM^2\beta)),$$

where $G_f(a,q)$ is as in Lemma 6.6.

Proof. We begin by noting that for any $a, q \in \mathbb{N}$ and $x \geq 0$,

$$\sum_{m=1}^{x} me^{2\pi if(m)a/q} = \sum_{r=0}^{q-1} \sum_{\substack{m=1 \\ m\equiv r \bmod q}}^{x} me^{2\pi if(r)a/q} = q^{-1}G_f(a,q)x^2/2 + O(qx), \tag{10.25}$$

since

$$\sum_{\substack{m=1 \\ m\equiv r \bmod q}}^{x} m = \sum_{m=0}^{x/q} qm + r = x^2/2q + O(x).$$

Using (10.25) and successive applications of summation and integration by parts, we have that if $\alpha = a/q + \beta$, then

$$\begin{aligned}\sum_{m=1}^{M} me^{2\pi if(m)\alpha} &= q^{-1}G_f(a,q)\Big(\frac{M^2}{2}e^{2\pi if(M)\beta} - \int_0^M \frac{x^2}{2}(2\pi i\beta f'(x))e^{2\pi if(x)\beta}\mathrm{d}x\Big) \\ &\quad + O(qM(1+JM^2\beta)) \\ &= q^{-1}G_f(a,q)\int_0^M xe^{2\pi if(x)\beta}\mathrm{d}x + O(qM(1+JM^2\beta)),\end{aligned}$$

as required. □

Proof of (10.13)

If $t \in \mathbf{M}_{a/q}(\eta^{-2})$ with $(a,q)=1$ and $q \le \eta^{-2}$, then since

$$d, \delta^{-1} \le N^{.01} \le M^{.03}, \tag{10.26}$$

Lemmas 10.5, 6.7, and 6.8 yield

$$|\mathcal{S}(t)| \ll \frac{1}{\sqrt{q}M^2}\Big|\int_0^M xe^{2\pi i h_d(x)\beta}\mathrm{d}x\Big| + O(M^{-0.7}),$$

where $\beta = \alpha - a/q$. Further, if $h_d(x) = a_0 + a_1 x + b_d x^2$, then

$$\Big|\int_0^M x(e^{2\pi i b_d x^2\beta} - e^{2\pi i h_d(x)\beta})\mathrm{d}x\Big| \le a_1 M^3\beta \le M^{1.1} \tag{10.27}$$

and

$$\Big|\int_0^M xe^{2\pi i b_d x^2\beta}\mathrm{d}x\Big| = \frac{1}{2b_d}\Big|\int_0^{b_d M^2} e^{2\pi i x\beta}\mathrm{d}x\Big| \le \min\{M^2, |b_d\beta|^{-1}\}. \tag{10.28}$$

Recalling that $b_d M^2 = L/3$, the estimate follows. □

For the minor arcs, we use the following immediate consequence of Corollary 6.10 and summation by parts.

Corollary 10.6. *Suppose $f(x) = a_0 + a_1 x + a_2 x^2$ with $a_2 \in \mathbb{N}$. If $(a,q)=1$ and $|\alpha - a/q| \le q^{-2}$, then*

$$\Big|\sum_{m=1}^{M} me^{2\pi i f(m)\alpha}\Big| \ll M^{2+\epsilon}(a_2/q + a_2/M + q/M^2)^{1/2}$$

for any $\epsilon > 0$, where the implied constant depends only on ϵ.

Proof of (10.14)

For a fixed $t \in \mathfrak{m}(\eta^{-2})$ we have by the pigeonhole principle that there exist

$$1 \leq q \leq M^{1.9}$$

and $(a,q) = 1$ with

$$|t/L - a/q| < 1/qM^{1.9}.$$

If $\eta^{-2} \leq q \leq M^{0.1}$, then Lemmas 10.5, 6.7, and 6.8 yield

$$|\mathcal{S}(t)| \ll q^{-1/2} \leq \eta.$$

If $M^{0.1} \leq q \leq M^{1.9}$, then Corollary 10.6 and (10.26) imply

$$|\mathcal{S}(t)| \ll M^{-.03} \ll \eta.$$

If $1 \leq q \leq \eta^{-2}$, then, letting $\beta = \alpha - a/q$, it must be the case that

$$|\beta| > 1/\eta^2 L \gg 1/\eta^2 b_d M^2, \tag{10.29}$$

as otherwise we would have $t \in \mathfrak{M}(\eta^{-2})$. As in (10.27) and (10.28), we see that

$$\Big| \int_0^M x e^{2\pi i h_d(x)\beta} \mathrm{d}x \Big| \ll |b_d \beta|^{-1}. \tag{10.30}$$

Combining (10.29) and (10.30) with Lemma 10.5, we have

$$|\mathcal{S}(t)| \ll \eta^2,$$

and the minor arc estimate is established. □

We deduce (10.16) from the following sixth-moment estimate for unweighted Weyl sums over the circle.

Lemma 10.7. *If $f(x) = a_0x + a_1x + a_2x^2 \in \mathbb{Z}[x]$ and $J = |a_0| + |a_1| + |a_2|$, then*

$$\int_0^1 \Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big|^6 \mathrm{d}\alpha \ll \frac{M^4}{|a_2|} + O(J^2M^{3.9}),$$

where the implied constants depend only on $\mathrm{cont}(f)$.

Proof. For $a, q \in \mathbb{N}$, let

$$\mathbf{M}_{a/q} = \{\alpha \in \mathbb{T} : |\alpha - a/q| < M^{-15/8}\}, \quad \mathbf{M}_q = \bigcup_{(a,q)=1} \mathbf{M}_{a/q},$$

$$\mathfrak{M} = \bigcup_{q=1}^{M^{1/8}} \mathbf{M}_q, \quad \text{and} \quad \mathfrak{m} = \mathbb{T} \setminus \mathfrak{M}.$$

By the pigeonhole principle and Lemma 6.10, we have that

$$\Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big| \ll JM^{0.94}$$

if $\alpha \in \mathfrak{m}$, and hence

$$\int_{\mathfrak{m}} \Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big|^6 \ll J^2M^{1.88} \int_0^1 \Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big|^4 \mathrm{d}\alpha. \tag{10.31}$$

By Theorem 4 of [7], we have that

$$\int_0^1 \Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big|^4 \mathrm{d}\alpha \ll M^2(\log M)^C \tag{10.32}$$

for an absolute constant C, where the implied constant depends only on $\mathrm{cont}(f)$, so by (10.31) the integral over $\mathfrak{m}$ can be absorbed into the claimed error term.

Further, we have by Lemmas 6.6 and 6.7 that if $\alpha = a/q + \beta$ with $(a,q) = 1$, $q \le M^{1/8}$, and $|\beta| < M^{-15/8}$, then

$$\Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big| \ll q^{-1/2}\Big|\int_0^M e^{2\pi i f(x)\beta}\mathrm{d}x\Big| + O(JM^{1/4}). \tag{10.33}$$

As in (6.13) and (6.14), we see that

$$\Big|\int_0^M e^{2\pi i f(x)\beta}\mathrm{d}x\Big| \ll \min\{M, |a_2\beta|^{-1/2} + O(JM^2\beta)\} \ll M(1+|a_2M^2\beta|)^{-1/2} + O(JM^{1/8}). \tag{10.34}$$

Combining (10.33) and (10.34), we have

$$\int_{\mathfrak{M}} \Big|\sum_{x=1}^{M} e^{2\pi i f(x)\alpha}\Big|^6 \mathrm{d}\alpha \ll M^6 \sum_{q=1}^{M^{1/8}} \sum_{(a,q)=1} q^{-3} \int_{|\beta|<M^{-15/8}} (1+|a_2M^2\beta|)^{-3}\mathrm{d}\beta + O(JM^{21/4}|\mathfrak{M}|)$$

$$\le \frac{M^4}{|a_2|}\sum_{q=1}^{\infty} q^{-2}\int_{-\infty}^{\infty}(1+|\beta|)^{-3}\mathrm{d}\beta + O(JM^{29/8})$$

$$\ll \frac{M^4}{|a_2|} + O(JM^{29/8}),$$

and the result follows. □

Proof of (10.16)

We first note that by the orthogonality relation (3.8), we have

$$\sum_{t\in\mathbb{Z}_L}|\mathcal{S}(t)|^6=\frac{1}{M^{12}}\sum_{1\le x_1,\dots,x_6\le M}x_1\cdots x_6\sum_{t\in\mathbb{Z}_L}e^{2\pi i(h_d(x_1)+h_d(x_2)+h_d(x_3)-h_d(x_4)-h_d(x_5)-h_d(x_6))t/L}$$

$$\le\frac{L}{M^6}\#\Big\{(x_1,\dots,x_6)\in[1,M]^6:h_d(x_1)+h_d(x_2)+h_d(x_3)\equiv h_d(x_4)+h_d(x_5)+h_d(x_6)\bmod L\Big\}.$$

Choosing our original parameter N sufficiently large with respect to h, we can assume that $-L/6<h_d(x)<L/6$ for all $x\in[1,M]$, hence the above congruences imply equality. Therefore, using the other orthogonality relation (2.1), we have

$$\sum_{t\in\mathbb{Z}_L}|\mathcal{S}(t)|^6\le\frac{L}{M^6}\int_0^1\Big|\sum_{m=1}^M e^{2\pi i h_d(m)\alpha}\Big|^6\mathrm{d}\alpha, \tag{10.35}$$

and since $d\le M^{.03}$, Lemma 10.7 yields

$$\int_0^1\Big|\sum_{m=1}^M e^{2\pi i h_d(m)\alpha}\Big|^6\mathrm{d}\alpha\ll\frac{M^4}{b_d}\ll\frac{M^6}{L},$$

and the estimate follows. □

10.6 Classification of Intersective Quadratic Polynomials

We conclude the chapter with an elementary proof of the classification of intersective quadratic polynomials, as promised in the introduction.

Proposition 10.8. *A quadratic polynomial $f \in \mathbb{Z}[x]$ is intersective if and only if f has rational roots with coprime denominators.*

Proof. First we recall that a polynomial is intersective if and only if it has a root in the p-adic integers for every prime p. Suppose $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ has no rational roots, and hence $b^2 - 4ac$ is not a perfect square. Let $p = 3$ if $b^2 - 4ac = -n^2$ for $n \in \mathbb{N}$, and otherwise let p be any prime such that $\mathrm{ord}_p(b^2 - 4ac)$, the exponent of p in the prime factorization of $b^2 - 4ac$, is odd. Letting $\mathbb{Q}_p$ denote the field of p-adic numbers, we have that $b^2 - 4ac$ is not a square in $\mathbb{Q}_p$. Therefore, by the quadratic formula, f has no roots in $\mathbb{Q}_p$, hence no p-adic integer roots, so f is not an intersective polynomial.

Now suppose that $f(x) = a(\alpha x + \beta)(\gamma x + \lambda)$ with $a, \alpha, \beta, \gamma, \lambda \in \mathbb{Z}$ and $(\alpha, \beta) = (\gamma, \lambda) = 1$. If p is a prime that divides both α and γ, then we see that f has no root modulo p^k whenever $p^k \nmid a$, hence f is not an intersective polynomial.

Conversely, if $(\alpha, \gamma) = 1$, we see that $-\beta/\alpha$ is a p-adic integer root of f whenever $p \nmid \alpha$, and $-\lambda/\gamma$ is a p-adic integer root of f whenever $p \nmid \gamma$. Since at least one of these divisibility conditions holds for every prime p, f is an intersective polynomial. □

11 Improved Bounds for $\mathcal{P}$-intersective Quadratic Polynomials

In this chapter we modify the method used to prove Theorem 10.1 and establish the analogous result for $\mathcal{P}$-intersective quadratic polynomials.

Theorem 11.1. *Suppose $h \in \mathbb{Z}[x]$ is a $\mathcal{P}$-intersective quadratic polynomial with positive leading term. If $A \subseteq [1, N]$ and $h(p) \notin A - A$ for all primes p with $h(p) > 0$, then*

$$\frac{|A|}{N} \ll (\log N)^{-\mu \log\log\log\log N}$$

for any $\mu < 1/2 \log 3$, where the implied constant depends only on h and μ.

11.1 Reduction of Theorem 11.1 to Two Lemmas

We fix a natural number N and a $\mathcal{P}$-intersective quadratic polynomial $h \in \mathbb{Z}[x]$ with positive leading term. We fix p-adic integer roots z_p of h for each prime p with $z_p \not\equiv 0 \bmod p$, which determine roots $r_d \in (-d, 0]$ of h modulo each $d \in \mathbb{N}$ satisfying $(r_d, d) = 1$, and we let the function λ and the auxiliary polynomials h_d be as in Definition 6.2. We let Λ_d and $\mathcal{V}_d(h)$ be as defined in Section 7.1, and we fix a set $A \subseteq [1, N]$ with $|A| = \delta N$ and $h(p) \notin A - A$ for all $p \in \mathcal{P}$ with $h(p) > 0$, that is to say $(A - A) \cap \mathcal{V}_1(h) = \emptyset$. We also fix an arbitrary $\epsilon > 0$, set $Z = (\log N)^{\epsilon \log\log\log N}$ and $\gamma = 2 + \epsilon$, and we prove Theorem 11.1 with $\mu = (1 - 22\epsilon)/2 \log(\gamma + 1)$.

Further, we set $K = 2^{20}$ and $Q = e^{c\sqrt{\log N}}$ as in Section 7.1, as well as the same $q_0 \leq Q^{10K}$, $\rho \in [1/2, 1)$, and Dirichlet character χ guaranteed by Lemma 5.2. In particular, we again have that if c is sufficiently small and $X \geq N^{1/10}$, then

$$\psi(x,a,q) = \frac{x}{\phi(q)} - \frac{\chi(a)x^{\rho}}{\phi(q)\rho} + O(XQ^{-1000K^2}) \tag{11.1}$$

for all $x \le X$, provided $q_0 \mid q$, $(a,q) = 1$, and $q \le (q_0 Q)^{10K}$. We deduce Theorem 11.1 from the following two lemmas, analogous to Lemmas 10.2 and 10.3, respectively.

Lemma 11.2. *If*

$$\delta \ge e^{-(\log N)^{\epsilon/8}}, \tag{11.2}$$

then there exists $B \subseteq [1,L]$ satisfying $L \ge N/Q^C$, $|B|/L = \sigma \ge \delta$, and $(B-B) \cap \mathcal{V}_d(h) = \emptyset$ with $q_0 \mid d$ and $d/q_0 \le Q$. Further, B satisfies $|B \cap [1, L/2]| \ge \sigma L/3$ and

$$\max_{q \le Z} \sum_{t \in \mathbf{M}_q(Z)} |\widehat{B}(t)|^2 \le \sigma^2 (\log N)^{-1/2+\epsilon}. \tag{11.3}$$

Lemma 11.3. *Suppose $B \subseteq [1,L]$ is as in the conclusion of Lemma 11.2, let $B_1 = B \cap [1, L/2]$, and suppose $\sigma \ge Z^{-1/6}$. Given $U, V, K \in \mathbb{N}$ with $\max\{U,V,K\} \le Z^{1/6}$ and a set*

$$P \subseteq \left\{ t \in \bigcup_{q=1}^{V} \mathbf{M}_q(K) \cup \{0\} : |\widehat{B_1}(t)| \ge \frac{\sigma}{U} \right\}$$

satisfying

$$|P \cap \mathbf{M}_{a,q}(K)| \le 1 \quad \textit{whenever} \quad q \le V, \tag{11.4}$$

there exist $U', V', K' \in \mathbb{N}$ with $\max\{U', V', K'\} \ll (\max\{U,V,K\})^{\gamma+1} \sigma^{-5/2}$ and a set

$$P' \subseteq \left\{ t \in \bigcup_{q=1}^{V'} \mathbf{M}_q(K') \cup \{0\} : |\widehat{B_1}(t)| \ge \frac{\sigma}{U'} \right\} \tag{11.5}$$

satisfying

$$|P' \cap \mathbf{M}_{a,q}(K')| \le 1 \quad \textit{whenever} \quad q \le V' \tag{11.6}$$

and

$$\frac{|P'|}{(U')^2} \ge \frac{|P|}{U^2} (\log N)^{1/2-10\epsilon}. \tag{11.7}$$

Proof of Theorem 11.1

In order to prove Theorem 11.1, we can assume that

$$\delta \geq (\log N)^{-\log\log\log\log N}.$$

Therefore, Lemma 10.2 produces a set B of density $\sigma \geq \delta$ with the stipulated properties, and we set $P_0 = \{0\}$, $U_0 = 3$, and $V_0 = K_0 = 1$. Lemma 11.3 then yields, for each n, a set P_n with parameters U_n, V_n, K_n such that

$$\max\{U_n, V_n, K_n\} \leq (\log N)^{(\gamma+1)^{n+1}\log\log\log\log N}$$

and

$$\frac{1}{\sigma} \geq \frac{1}{\sigma^2}\sum_{t\in P_n}|\widehat{B_1}(t)|^2 \geq \frac{|P_n|}{U_n^2} \gg (\log N)^{n(1/2-10\epsilon)},$$

where the left-hand inequality comes from Plancherel's Identity, as long as $\max\{U_n, V_n, K_n\} \leq Z^{1/6}$. This holds with $n = (1-\epsilon)(\log\log\log\log N)/\log(\gamma+1)$, as $(\gamma+1)^{n+1} \leq (\log\log\log N)^{1-\epsilon/2}$, and Theorem 10.1 follows. □

11.2 The Outer Iteration II

Just like Lemma 10.2, we deduce Lemma 11.2 from a density increment lemma which follows immediately from Lemma 9.2 and Proposition 7.2.

Lemma 11.4. *Suppose $B \subseteq [1, L]$ with $|B| = \sigma L$ and $(B - B) \cap \mathcal{V}_d(h) = \emptyset$. If $L \geq Z^4$ and*

$$\sum_{t\in\mathbf{M}_q(Z)}|\widehat{B}(t)|^2 \geq \sigma^2(\log N)^{-1/2+\epsilon}, \tag{11.8}$$

for some $q \leq Z$, then there exists $B' \subseteq [1, L']$ satisfying $L' \gg \sigma L/Z^4$, $(B' - B') \cap \mathcal{V}_{qd}(h) = \emptyset$, and

$$|B'|/L' \geq \sigma(1 + (\log N)^{-1/2+\epsilon}/8).$$

Proof of Lemma 11.2

Partitioning $[1, N]$, the pigeonhole principle guarantees the existence of an arithmetic progression

$$P = \{x + \ell\lambda(q_0) : 1 \le \ell \le N_0\} \subseteq [1, N]$$

with $N_0 \ge N/2\lambda(q_0)$ and $|A \cap P| \ge \delta N_0$. Defining $A_0 \subseteq [1, N_0]$ by

$$A' = \{\ell \in [1, N_0] : x + \ell\lambda(q_0) \in A\},$$

we see that $|A_0| \ge \delta N_0$ and $(A - A) \cap \mathcal{V}_{q_0}(h) = \emptyset$. Lemma 11.4 then yields, for each k, a set $A_k \subseteq [1, N_k]$ with $|A_k| = \delta_k N_k$ and $(A_k - A_k) \cap \mathcal{V}_{d_k}(h) = \emptyset$ satisfying

$$N_k \ge (c\delta/Z^4)^k N/q_0^2, \quad \delta_k \ge \delta_{k-1}(1 + (\log N)^{-1/2+\epsilon}/8), \quad q_0 \mid d_k, \quad \text{and} \quad d_k/q_0 \le Z^k \tag{11.9}$$

as long as $N_k \ge Z^4$ and either

$$\max_{q \le Z} \sum_{t \in \mathbf{M}_q(Z)} |\widehat{A_k}(t)|^2 \ge \delta_k^2 (\log N)^{-1/2+\epsilon} \tag{11.10}$$

or $|A_k \cap [1, N_k/2]| < \delta_k N_k/3$, as the latter condition implies A_k has density at least $3\delta_k/2$ on the interval $(N_k/2, N_k]$. We see that by (11.2) and (11.9), the density δ_k will exceed 1 after

$$16 \log(\delta^{-1})(\log N)^{1/2-\epsilon} \le (\log N)^{1/2-\epsilon/2}$$

steps, hence $N_k < Z^4$ or (10.9) fails and $|A_k \cap [1, N_k/2]| \ge \delta_k N_k/3$ for some

$$k \le (\log N)^{1/2-\epsilon/2}. \tag{11.11}$$

However, we see that (11.2), (11.9), and (11.11) imply

$$N_k \ge N(e^{-(\log N)^{\epsilon/4}})^{(\log N)^{1/2-\epsilon/2}} q_0^{-2} \ge N/Q^C,$$

so we set $B = A_k$, $L = N_k$, $\sigma = \delta_k$, and $d = d_k$, and we see further that

$$d/q_0 \le Z^{(\log N)^{1/2-\epsilon/2}} \le e^{(\log N)^{1/2-\epsilon/4}} \le Q,$$

as required. □

11.3 The Inner Iteration II

In this section, we let $B \subseteq [1, L]$ and $h_d \in \mathbb{Z}[x]$ be as in the conclusion of Lemma 10.2, we let $B_1 = B \cap [1, L/2]$, and we assume $\sigma \ge Z^{-1/6}$. We set $M = \sqrt{L/10b_d}$, where b_d is the leading coefficient of h_d, and $H_d = \{n \in \mathbb{N} : 0 < h_d(n) < L/10\}$, noting by (6.1) that

$$|H_d \triangle [1, M]| \ll 1. \tag{11.12}$$

We also let ν_d be as in the proof of Lemma 4.4, and we let $\Psi = \phi(d)\psi(dM + r_d, r_d, d)/d$.

Proof of Lemma 11.3

Suppose we have a set P with parameters U, V, K as specified in the hypotheses of Lemma 11.3, and fix an element $s \in P$. Since $(B - B) \cap \mathcal{V}_d(h) = \emptyset$, we see that there are no solutions to

$$a - b \equiv h_d(m) \mod L, \quad a \in B,\ b \in B_1,\ m \in H_d.$$

On the transform side as in Section 9.1, combined with (11.12), this implies

$$\sum_{t \in \mathbb{Z}_L} \widehat{B}(t)\overline{\widehat{B_1}(s+t)}\mathcal{W}(t) = \frac{1}{LM\Psi} \sum_{\substack{n \in \mathbb{Z}_L \\ m \in H_d}} m\nu_d(m)B(n + h_d(m))B_1(n)e^{2\pi ins/L} + O\Big(\frac{\log L}{\Psi}\Big)$$

$$= O\Big(\frac{\log L}{\Psi}\Big),$$

where

$$\mathcal{W}(t) = \frac{1}{M\Psi}\sum_{m=1}^{M} m\nu_d(m)e^{2\pi i h_d(m)t/L},$$

which immediately yields

$$\sum_{t\in\mathbb{Z}_L\setminus\{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{W}(t)| \geq \widehat{W}(0)\widehat{B_1}(s)\mathcal{S}(0) + O\Big(\frac{\log L}{\Psi}\Big) \geq \sigma^2/8U, \tag{11.13}$$

since $|\widehat{B_1}(s)| \geq \sigma/U$ and $\mathcal{W}(0) \geq 1/4$, the latter of which follows from (11.1) and summation by parts, and the error term is negligible by (11.1) and (5.2) . Letting $\eta = c_0\sigma/U$ for a constant $c_0 > 0$, we have analogous to the estimates in Section 7.3 that

$$|\mathcal{W}(t)| \ll \frac{\sqrt{q}}{\phi(q)}\min\{1, (L|t/L - a/q|)^{-1}\} \ll q^{-1/2}\log\log q \min\{1, (L|t/L - a/q|)^{-1}\} \tag{11.14}$$

if $t \in \mathbf{M}_{a/q}(\eta^{-\gamma})$, $(a,q) = 1$, and $q \leq \eta^{-\gamma}$, where the last inequality follows from the standard estimate $\phi(q) \gg q/\log\log q$, and

$$|\mathcal{W}(t)| \leq C\eta \leq \sigma/16U \quad \text{for all } t \in \mathfrak{m}(\eta^{-\gamma}), \tag{11.15}$$

provided $c_0 \leq 1/16C$. We discuss these estimates in more detail in Section 11.4. We have by (11.15), Cauchy-Schwarz, and Plancherel's Identity that

$$\sum_{t\in\mathfrak{M}(\eta^{-\gamma})} |\widehat{B}(t)||\widehat{B_1}(t)||\mathcal{W}(t)| \geq \sigma^2/16U. \tag{11.16}$$

We now wish to assert that we can ignore those frequencies in the major arcs at which the transform of B or B_1 is particularly small. In order to make this precise, we need a higher moment esimate on $\mathcal{W}$ analogous to (10.16). Specifically, we have that

$$\sum_{t\in\mathbb{Z}_L} |\mathcal{W}(t)|^6 \leq C, \tag{11.17}$$

of which we provide a proof in Section 11.4.

Choosing a constant $0 < c_1 < (64C^{1/6})^{-3}$, where C comes from (10.16), we define

$$X = \Big\{ t \in \mathfrak{M}(\eta^{-\gamma}) : \min\Big\{ |\widehat{B}(t)|, |\widehat{B_1}(s+t)| \Big\} \leq c_1 \sigma^{7/2}/U^3 \Big\} \quad \text{and} \quad Y = \mathfrak{M}(\eta^{-\gamma}) \setminus X. \tag{11.18}$$

Using Hölder's Inequality to exploit the sixth moment estimate on $\mathcal{W}$, followed by Plancherel's Identity, we see that

$$\begin{aligned}
\sum_{t \in X} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{W}(t)| &\leq \Big(\sum_{t \in X} |\widehat{B}(t)|^{6/5} |\widehat{B_1}(s+t)|^{6/5} \Big)^{5/6} \Big(\sum_{t \in \mathbb{Z}_L} |\mathcal{W}(t)|^6 \Big)^{1/6} \\
&\leq \frac{c_1^{1/3} \sigma^{7/6}}{U} \Big(\sum_{t \in \mathbb{Z}_L} |\widehat{B}(t)|^2 + |\widehat{B_1}(s+t)|^2 \Big)^{5/6} \cdot C^{1/6} \\
&\leq \sigma^2/32U,
\end{aligned}$$

and hence by (11.16) we have

$$\sum_{t \in Y} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{W}(t)| \geq \sigma^2/32U. \tag{11.19}$$

For $i, j, k \in \mathbb{N}$, we define

$$\mathcal{R}_{i,j,k} = \Big\{ a/q : (a,q) = 1,\ 2^{i-1} \leq q \leq 2^i, \frac{\sigma}{2^j} \leq \max |\widehat{B}(t)| \leq \frac{\sigma}{2^{j-1}}, \frac{\sigma}{2^k} \leq \max |\widehat{B_1}(s+t)| \leq \frac{\sigma}{2^{k-1}} \Big\},$$

where the maximums are taken over nonzero frequencies $t \in \mathbf{M}_{a/q}(\eta^{-\gamma})$. We see that we have

$$\sum_{a/q \in \mathcal{R}_{i,j,k}} \sum_{t \in \mathbf{M}_{a/q}(\eta^{-\gamma}) \setminus \{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{S}(t)| \ll |\mathcal{R}_{i,j,k}| \frac{\sigma^2}{2^j 2^k} \max_{a/q \in \mathcal{R}_{i,j,k}} \sum_{t \in \mathbf{M}_{a/q}(\eta^{-\gamma})} |\mathcal{W}(t)|. \tag{11.20}$$

It follows from (11.14) and the bound $U, \sigma^{-1} \le Z^{1/6}$ that if $(a,q) = 1$ and $q \le \eta^{-\gamma}$, then

$$\sum_{t \in \mathbf{M}_{a/q}(\eta^{-\gamma})} |\mathcal{W}(t)| \ll q^{-1/2} (\log(Z))^2,$$

hence by (10.19) we have

$$\sum_{a/q \in \mathcal{R}_{i,j,k}} \sum_{t \in \mathbf{M}_{a/q}(\eta^{-\gamma}) \setminus \{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||\mathcal{W}(t)| \ll |\mathcal{R}_{i,j,k}| \frac{\sigma^2}{2^j 2^k} 2^{-i/2} (\log(Z))^2. \tag{11.21}$$

By our definitions, the sets $\mathcal{R}_{i,j,k}$ exhaust Y by taking $1 \le 2^i \le \eta^{-\gamma}$ and $1 \le 2^j, 2^k \le U^3/c_1\sigma^{5/2}$, a total search space of size $\ll (\log Z)^3$. Therefore, by (11.19) and (11.21) there exist i, j, k in the above range such that

$$\frac{\sigma^2}{U(\log Z)^3} \ll |\mathcal{R}_{i,j,k}| \frac{\sigma^2}{2^j 2^k} 2^{-i/2} (\log Z)^2.$$

In other words, we can set $V_s = 2^i$, $W_s = 2^j$, and $U_s = 2^k$ and take an appropriate nonzero frequency from each of the pairwise disjoint major arcs specified by $\mathcal{R}_{i,j,k}$ to form a set

$$P_s \subseteq \left\{ t \in \bigcup_{q=V_s/2}^{V_s} \mathbf{M}_q(\eta^{-\gamma}) : \ |\widehat{B_1}(s+t)| \ge \frac{\sigma}{U_s} \right\}$$

which satisfies

$$|P_s| \gg \frac{U_s W_s V_s^{1/2}}{U(\log Z)^5}, \quad |P_s \cap \mathbf{M}_{a,q}(\eta^{-\gamma})| \le 1 \ \text{ whenever } \ q \le V_s, \tag{11.22}$$

and

$$\max_{t \in \mathbf{M}_{a/q}(\eta^{-2}) \setminus \{0\}} |\widehat{B}(t)| \ge \frac{\sigma}{W_s} \text{ whenever } q \le V_s \text{ and } \mathbf{M}_{a/q}(\eta^{-\gamma}) \cap P_s \ne \emptyset, \tag{11.23}$$

We now observe that there is a subset $\tilde{P} \subseteq P$ with

$$|\tilde{P}| \gg |P|/(\log Z)^3 \tag{11.24}$$

for which the triple U_s, W_s, V_s is the same.

We call those common parameters $\tilde{U}, \tilde{W}$ and $\tilde{V}$, respectively, and we can now foreshadow by asserting that the claimed parameters in the conclusion of Lemma 11.3 will be $U' = \tilde{U}$, $V' = \tilde{V}V$, and $K' = K + \eta^{-2}$, which do satisfy the purported bound. We let

$$\mathcal{R} = \left\{ \frac{a}{q} + \frac{b}{r} : s \in \mathbf{M}_{a/q}(K) \text{ for some } s \in \tilde{P} \text{ and } t \in \mathbf{M}_{b/r}(\eta^{-\gamma}) \text{ for some } t \in P_s \right\}.$$

By taking one frequency $s+t$ associated to each element in $\mathcal{R}$, we form our set P', which immediately satisfies conditions (11.5) and (11.6) from the conclusion of Lemma 11.3. However, the crucial condition (10.6) on $|P'|$, which by construction is equal to $|\mathcal{R}|$, remains to be shown. From Lemma CR of [1], we have

$$|\mathcal{R}| \geq \frac{|\tilde{P}|(\min_{s\in\tilde{P}} |P_s|)^2}{\tilde{V} D \tau^8 (1 + \log V)}, \tag{11.25}$$

where

$$D = \max_{r \leq \tilde{V}} \Big| \Big\{ b : \ (b,r) = 1, \ \mathbf{M}_{b/r}(\eta^{-\gamma}) \cap \bigcup_{s\in\tilde{P}} P_s \neq \emptyset \Big\} \Big|,$$

$\tau(q)$ is the divisor function and $\tau = \max_{q \leq V\tilde{V}} \tau(q)$. We also have from (10.2) that

$$\sigma^2 (\log N)^{-1/2+\epsilon} \geq \max_{r \leq Z} \sum_{t \in \mathbf{M}_r(Z)} |\widehat{B}(t)|^2 \geq \max_{r \leq \tilde{V}} \sum_{t \in \mathbf{M}_r(\eta^{-\gamma})} |\widehat{B}(t)|^2 \geq \frac{\sigma^2}{\tilde{W}^2} D,$$

where the last inequality follows from (10.22), and hence

$$D \leq \tilde{W}^2 (\log N)^{-1/2+\epsilon}.$$

Combining the estimates on τ and D with (11.22), (11.24), and (11.25), we have

$$|P'| \gg \frac{|P|}{(\log Z)^3} \frac{\tilde{U}^2 \tilde{W}^2 \tilde{V}}{U^2 (\log Z)^{10}} \frac{(\log N)^{1/2-\epsilon}}{\tilde{V}\tilde{W}^2 (\log N)^{8\epsilon} (\log Z)} \geq \tilde{U}^2 \frac{|P|}{U^2} (\log N)^{1/2-10\epsilon}.$$

Recalling that we set $U' = \tilde{U}$, the lemma follows. □

The remainder of the chapter is dedicated to establishing the estimates (11.14), (11.15), and (11.17).

11.4 Weighted Exponential Sum Estimates for Quadratic Polynomials in Shifted Primes

The following is the analog of Lemma 10.5 for polynomials in shifted primes.

Lemma 11.5. *Suppose $f(x) = a_0 + a_1x + a_2x^2 \in \mathbb{Z}[x]$ and let $J = |a_0| + |a_1| + |a_2|$. If $q_0 \mid d$, $d/q_0 \leq Q$, $a, q \in \mathbb{N}$, $q \leq (q_0Q)^{8K}$, and $\alpha = a/q + \beta$, then*

$$\sum_{m=1}^{M} m\nu_d(m)e^{2\pi if(m)\alpha} = \frac{\phi(d)}{\phi(qd)}\mathcal{G}_f(a,q)\int_0^M x(1-\chi(r_d)(dx)^{\rho-1})e^{2\pi if(x)\beta}\mathrm{d}x$$

$$+ O(qM^2(1+JM^2\beta)Q^{-900K^2}),$$

where $\mathcal{G}_f(a,q)$ is as defined in Lemma 7.5.

Proof. First we see that for any $a, q \in \mathbb{N}$ and $x \geq 0$,

$$\sum_{1\leq m\leq x} m\nu_d(m)e^{2\pi if(m)a/q} = \sum_{\ell=0}^{q-1} e^{2\pi if(\ell)a/q} \sum_{\substack{1\leq m\leq x \\ m\equiv \ell \bmod q}} m\nu_d(m). \tag{11.26}$$

By summation by parts and (11.1), we have that if $(d\ell + r_d, q) = 1$, then

$$\sum_{\substack{1\leq m\leq x \\ m\equiv \ell \bmod q}} m\nu_d(m) = \frac{\phi(d)}{d}\Big(x\psi(dx + r_d, d\ell + r_d, qd) - \int_0^x \psi(dt + r_d, d\ell + r_d, qd)\mathrm{d}t\Big)$$

$$= \frac{\phi(d)}{\phi(qd)}\Big(x(x - \chi(r_d)\frac{(dx)^\rho}{d\rho}) - (\frac{x^2}{2} - \chi(r_d)\frac{d^\rho x^{1+\rho}}{d\rho(1+\rho)})\Big) + O(xMQ^{-900K^2})$$

$$= \frac{\phi(d)}{\phi(qd)}\Big(\frac{x^2}{2} - \chi(r_d)\frac{d^\rho x^{1+\rho}}{d(1+\rho)}\Big) + O(xMQ^{-900K^2}),$$

so by (11.26) and successive applications of summation and integration by parts, we have

$$\sum_{m=1}^{M} m\nu_d(m)e^{2\pi i f(m)\alpha} = \frac{\phi(d)}{\phi(qd)}\mathcal{G}_f(a,q)\Big((\frac{M^2}{2} - \chi(r_d)\frac{d^\rho M^{1+\rho}}{d(1+\rho)})e^{2\pi i f(M)\beta}$$

$$- \int_0^M (\frac{x^2}{2} - \chi(r_d)\frac{d^\rho x^{1+\rho}}{d(1+\rho)})(2\pi i f'(x)\beta)e^{2\pi i f(x)\beta}\mathrm{d}x\Big)$$

$$+ O(qM^2(1+JM^2\beta)Q^{-900K^2})$$

$$= \frac{\phi(d)}{\phi(qd)}\mathcal{G}_f(a,q)\int_0^M x(1-\chi(r_d)(dx)^{\rho-1})e^{2\pi i f(x)\beta}\mathrm{d}x$$

$$+ O(qM^2(1+JM^2\beta)Q^{-900K^2}),$$

as required. □

Proof of (11.14)

If $t \in \mathbf{M}_{a/q}(\eta^{-2})$ with $(a,q) = 1$ and $q \leq \eta^{-2}$, then by Lemmas 11.5 and 7.7 we have

$$|\mathcal{W}(t)| \ll \frac{\sqrt{q}}{M\Psi\phi(q)}\Big|\int_0^M x(1-\chi(r_d)(dx)^{\rho-1})e^{2\pi i f(x)\beta}\mathrm{d}x\Big| + O(MQ^{-800K^2}/\Psi).$$

As seen previously, we have by (11.1) and (5.2) that

$$\Psi \gg (1-\rho)M \gg M/q_0 \geq M/Q^{10K}, \tag{11.27}$$

and since $\sigma^{-1}, U \geq Z^{1/6}$, the error term is certainly negligible. By (10.27) and (10.28), we have that

$$\Big|\int_0^M xe^{2\pi i f(x)\beta}\mathrm{d}x\Big| \ll \min\{M^2, |b_d\beta|^{-1}\}, \tag{11.28}$$

which by (11.27) and integration by parts yields

$$\Big| \int_0^M x(1-\chi(r_d)(dx)^{\rho-1})e^{2\pi i f(x)\beta}\mathrm{d}x \Big| \ll \min\{M\Psi, |b_d\beta|^{-1}\Psi/M\}. \tag{11.29}$$

Recalling that $b_d M^2 = L/10$, the estimate follows. □

For the minor arcs we need the following estimate, which follows immediately from Lemma 7.8 and summation by parts.

Corollary 11.6. *Suppose $f(x) = a_0 + a_1 x + a_2 x^2 \in \mathbb{Z}[x]$ with $a_2 > 0$, $D, W \in \mathbb{N}$, and $b \in \mathbb{Z}$. If $U \geq \log D$, $a_2 \gg |a_0| + |a_1|$, and $W, |b|, a_k \leq U^2$, then*

$$\sum_{\substack{x=1 \\ Wx+b\in\mathcal{P}}}^{D} x\log(Wx+b)e^{2\pi i f(x)\alpha} \ll \frac{D^2}{U} + U^C D^{2-c}$$

for absolute constants $C, c > 0$, provided

$$|\alpha - a/q| \leq q^{-2} \quad \textit{for some} \quad U^K \leq q \leq f(D)/U^K \quad \textit{and} \quad (a,q) = 1.$$

Proof of (11.15)

For a fixed $\alpha \in \mathfrak{m}(\eta^{-\gamma})$ we have by the pigeonhole principle that there exist

$$1 \leq q \leq L/(q_0 Q)^K$$

and $(a,q) = 1$ with

$$|\alpha - a/q| < (q_0 Q)^K/qL.$$

If $\eta^{-\gamma} \leq q \leq (q_0 Q)^K$, then by Lemma 11.5 we have

$$|\mathcal{W}(t)| \ll q^{-1/\gamma} \ll \eta,$$

where the first inequality uses the fact that $\phi(q) \gg q/\log\log q$.

If $(q_0Q)^K \leq q \leq L/(q_0Q)^K$, then by Corollary 11.6, (11.27), and the bounds $\sigma^{-1}, U \leq Z^{1/6}$, we have

$$|\mathcal{W}(t)| \ll M/\Psi q_0 Q \leq \eta.$$

If $1 \leq q \leq \eta^{-\gamma}$, then letting $\beta = \alpha - a/q$, we must have

$$|\beta| > 1/\eta^\gamma L \gg 1/\eta^\gamma b_d M^2. \tag{11.30}$$

Combining (11.30) with Lemma 11.5 and (11.29) yields

$$|\mathcal{W}(t)| \ll \eta^\gamma,$$

and the minor arc estimate is established. □

Proof of (11.17)

Analogous to the proof of (10.16), we have

$$\sum_{t \in \mathbb{Z}_L} |\mathcal{W}(t)|^6 \leq \frac{L}{\Psi^6} \int_0^1 \Big| \sum_{m=1}^M \nu_d(m) e^{2\pi i h_d(m)\alpha} \Big|^6 \mathrm{d}\alpha. \tag{11.31}$$

Reverting to the definitions of major and minor arcs on the circle from Chapter 2.3, we have by the pigeonhole principle and Lemma 7.8 that

$$\Big| \sum_{m=1}^M \nu_d(m) e^{2\pi i h_d(m)\alpha} \Big| \ll M/(q_0Q)^8 \tag{11.32}$$

for all $\alpha \in \mathfrak{m}((q_0Q)^{8K})$.

Combined with (10.32), (11.27), and the bound $b_d \ll d \le q_0 Q$, (11.32) yields

$$\int_{\mathfrak{m}((q_0Q)^{8K})} \Big| \sum_{m=1}^{M} \nu_d(m) e^{2\pi i h_d(m)\alpha} \Big|^6 \mathrm{d}\alpha \le \frac{M^2(\log M)^6}{(q_0Q)^8} \int_0^1 \Big| \sum_{m=1}^{M} e^{2\pi i h_d(m)\alpha} \Big|^4 \mathrm{d}\alpha$$

$$\ll \frac{M^4(\log M)^C}{(q_0Q)^8} \ll \frac{\Psi^6}{(q_0Q)^3\Psi^2} \ll \frac{\Psi^6}{L}.$$

Further, we have by Lemma 7.5, Corollary 7.7, and integration by parts that if $\alpha = a/q + \beta$, $(a,q) = 1$, $q \le (q_0Q)^{8K}$, and $|\beta| < L/(q_0Q)^{8K}$, then

$$\Big| \sum_{m=1}^{M} \nu_d(m) e^{2\pi i h_d(m)\alpha} \Big| \ll q^{-1/\gamma} \Big| \int_0^M (1 - \chi(r_d)(dx)^{\rho-1}) e^{2\pi i h_d(x)\beta} \mathrm{d}x \Big| + O(MQ^{-500K^2})$$

$$\ll q^{-1/\gamma} \min\{\Psi, |b_d\beta|^{-1/2}\Psi/M\}$$

$$\ll q^{-1/\gamma} \Psi (1 + |b_d M^2 \beta|)^{-1/2}$$

Finally, we have

$$\int_{\mathfrak{M}((q_oQ)^{8K})} \Big| \sum_{m=1}^{M} \nu_d(m) e^{2\pi i h_d(m)\alpha} \Big|^6 \ll \Psi^6 \sum_{q=1}^{(q_0Q)^{8K}} \sum_{(a,q)=1} q^{-5/2} \int_{|\beta|<(q_0Q)^{8K}/L} (1 + |b_d M^2 \beta|)^{-3} \mathrm{d}\beta$$

$$\ll \frac{\Psi^6}{b_d M^2} \sum_{q=1}^{\infty} q^{-3/2} \int_{-\infty}^{\infty} (1 + |\beta|)^{-3} \mathrm{d}\beta$$

$$\ll \frac{\Psi^6}{L},$$

and by (11.31) the estimate follows. □

Bibliography

[1] A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference Sets Without k-th Powers*, Acta. Math. Hungar. 65 (2) (1994), pp. 165-187.

[2] D. Berend, Y. Bilu, *Polynomials with roots modulo every integer*, Proc. Amer. Math. Soc. 124 (1996), pp. 1663-1671.

[3] J. R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1997), pp. 711-719.

[4] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math, 71 (1977), 204-256.

[5] B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour. 114 (2002), (2), pp. 215-238

[6] M. Hamel, N. Lyall, A. Rice, *Improved bounds on Sárközy's theorem for quadratic polynomials*, to appear in Int. Math. Res. Not., arXiv:1111.5786v4.

[7] L. K. Hua, *Additive theory of prime numbers* , American Mathematical Society, Providence, RI 1965.

[8] T. Kamae, M. Mendès France, van der Corput's difference theorem, Israel J. Math. 31, no. 3-4, (1978), pp. 335-342.

[9] H.-Z. Li, H. Pan, *Difference sets and polynomials of prime variables*, Acta. Arith. 138, no. 1 (2009), pp. 25-52.

[10] J. Lucier, *Difference sets and shifted primes*, Acta. Math. Hungar. 120 (2008), pp.79-102.

[11] J. Lucier, *Intersective Sets Given by a Polynomial*, Acta Arith. 123 (2006), pp. 57-95.

[12] N. Lyall, *A new proof of Sárközy's Theorem*, to appear in Proc. Amer. Math. Soc., arXiv:1107.0243v3.

[13] N. Lyall, À. Magyar, *Polynomial configurations in difference sets*, J. Number Theory 129 (2009), pp. 439-450.

[14] N. Lyall, Á. Magyar, *Simultaneous polynomial recurrence*, Bull. Lond. Math. Soc. 43 (2011), no. 4, pp. 765-785.

[15] H. L. Montgomery *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, 84.

[16] H. L. Montgomery, R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge Studies in Advanced Mathematics 97, 2007.

[17] V. I. Nechaev, *An estimate of the complete rational trigonmetric sum*, Mat. Zametki 17 (1975), pp. 839-849 (in Russian); English translation: Math. Notes 17 (1975), pp. 504-511.

[18] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. 37 (1988), pp. 219-231.

[19] A. Rice, *Sárközy's theorem for $\mathcal{P}$-intersective polynomials*, to appear in Acta Arithmetica, arXiv:1111.6559v3.

[20] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. 28 (1953), pp. 104-109.

[21] I. Ruzsa, T. Sanders, *Difference sets and the primes*, Acta. Arith. 131, no. 3 (2008), pp. 281-201.

[22] A. Sárközy, *On difference sets of sequences of integers I*, Acta. Math. Hungar. 31(1-2) (1978), pp. 125-149.

[23] A. Sárközy, *On difference sets of sequences of integers III*, Acta. Math. Hungar. 31(3-4) (1978), pp. 355-386.

[24] S. Slijepčević, *A polynomial Sárközy-Furstenberg theorem with upper bounds*, Acta Math. Hungar. 98 (2003), pp. 275-280

[25] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, Second Edition, 1997.

[26] M. Wierdl, Ph. D. Thesis, Ohio State University, 1989.