Topics in Analytic Number Theory

Alastair James Irving
St John's College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy
Trinity 2014

Acknowledgements

I would like to thank the EPSRC who funded this DPhil, (grant EP/P505666/1). My thanks also go to my supervisor, Roger Heath-Brown, for all his help and advice over the last four years. This thesis would not have been possible without his valuable ideas and encouragement. His careful proof reading of all my work is also very much appreciated. I am grateful to my examiners, Ben Green and Tim Browning, for suggesting a number of minor corrections and improvements. My time as a member of the number theory group at Oxford has been very enjoyable. I have learnt a lot from the other members of the group and from the many interesting seminars which I have attended. Finally I would like to thank my family and friends, in particular my parents, for all their support over the years.

Abstract

In this thesis we prove several results in analytic number theory.

1. We show that there exist 3-digit palindromic primes in base b for a set of b having density 1 and that if b is sufficiently large then there is a 3-digit palindrome in base b having precisely two prime factors.

2. We prove various estimates for averages of sums of Kloosterman fractions over primes. The first of these improves previous results of Fouvry-Shparlinski and Baker.

3. By using the q-analogue of van der Corput's method to estimate short Kloosterman sums we study the divisor function in an arithmetic progression to modulus q. We show that the expected asymptotic formula holds for a larger range of q than was previously known, provided that q has a certain factorisation.

4. Let $\|x\|$ denote the distance from x to the nearest integer. We show that for any irrational α and any $\theta < \frac{8}{23}$ there are infinitely many n which are the product of two primes for which
$$\|n\alpha\| \leq n^{-\theta}.$$

5. By establishing an improved level of distribution we study almost-primes of the form $f(p, n)$ where f is an irreducible binary form over $\mathbb{Z}$.

6. We show that for an irreducible cubic $f \in \mathbb{Z}[x]$ and a full norm form $\mathbf{N}$ for a number field $K/\mathbb{Q}$, satisfying certain hypotheses, the variety
$$f(t) = \mathbf{N}(x_1, \ldots, x_k) \neq 0$$
satisfies the Hasse principle. Our proof uses sieve methods.

Contents

Chapter 1

Introduction

In this thesis we will study several problems in number theory using a variety of analytic methods. In particular we will make extensive use of estimates for exponential sums, sieves and the geometry of numbers. These can all be used to estimate the number of integers, or tuples of integers, which satisfy certain types of constraints. For example, exponential sums or the geometry of numbers can be used to count the number of solutions to congruences or Diophantine equations whereas sieves can be used to count primes or almost-primes.

Exponential sums in one variable are of the form

$$S = \sum_{M \leq n < M+N} e^{2\pi i f(n)}$$

for some $M < N$ and a function $f : [M, M+N) \to \mathbb{R}$. They arise frequently in analytic number theory as a result of the application of Fourier analysis. Since each term in the sum is bounded by 1 we have the trivial estimate $|S| \leq N$. This is best possible in general, for example if $f(n) = 0$ for all $n \in [M, M+n)$. However, many problems in number theory can be reduced to the estimation of sums in which we expect a significant amount of cancellation to occur. In the best possible case we might hope that the values $e^{2\pi i f(n)}$ behave like independent, uniformly distributed complex numbers with modulus 1. We could then conjecture that S is roughly of size $\sqrt{N}$.

Many different techniques for bounding S have been developed. The strength of the resulting bound depends both on the function f and the length N of the sum. If S can be considered as a sum over the points of an algebraic variety defined over a finite field then the Riemann Hypothesis for such varieties may be used. This was proved for curves by Weil [47] and in much more generality by Deligne [15, 16]. In many cases this leads to a bound for S which is essentially sharp. In this thesis we

will use several existing estimates for exponential sums as well as proving some new results. Our proofs typically combine elementary arguments with existing bounds for sums over algebraic varieties.

Given a finite set of integers $\mathcal{A}$ and a set of primes $\mathcal{P}$, a sieve is a combinatorial device for counting the number of elements in $\mathcal{A}$ not divisible by a prime from $\mathcal{P}$. In particular one could attempt to use a sieve to count the number of primes or almost-primes in $\mathcal{A}$. The development of the modern sieve began with Brun [9] who proved a nontrivial upper bound for the number of primes $p \leq x$ for which $p+2$ is also prime. A considerable amount of work, much of which is described in Friedlander and Iwaniec's book [25], has been done on sieve theory in the last century. Classical sieves are typically not capable of showing that $\mathcal{A}$ contains primes, this is an example of the "Parity Problem". However, they can often be used to prove an upper bound of the correct order for the number of primes in $\mathcal{A}$ as well as lower bounds for the number of almost-primes. There are some situations in which a sieve can be applied with a choice of $\mathcal{P}$ which only contains a positive proportion of the primes. For example, to count sums of two squares in $\mathcal{A}$ one might work with the set

$$\mathcal{P} = \{p : p \equiv 3 \,(\mathrm{mod}\, 4)\}.$$

The resulting sieve problem is then much easier. Some of the applications of sieves in this thesis will involve a set $\mathcal{P}$ containing all primes whereas in others $\mathcal{P}$ will only contain a small proportion of them.

In several chapters we will need to count the number of solutions in $\mathbb{Z}^2$ to a linear congruence. In such a situation it is convenient to use some basic results from the geometry of numbers which we will describe in Section 2.3. The key idea is that the set of solutions to our congruence will form a lattice so we can estimate their number in a given region using some standard results. This approach was employed very successfully by Daniel [13] who used it to prove an asymptotic formula for the sum of the divisor function over the values of a binary quartic form.

In Chapter 2 we will describe the notation which is used throughout this thesis as well as collecting some standard lemmas. Our first results will occur in Chapter 3, in which we discuss 3-digit palindromic primes. A palindrome in base b is a number whose base b expansion is the same when reversed. The main result of Chapter 3, Theorem 3.3, will show that there are 3-digit palindromic primes in almost all bases.

Chapters 4 and 5 are both primarily concerned with the estimation of exponential sums. In Chapter 4 we consider Kloosterman sums over primes, which have previously been studied by a number of authors. Our results, Theorems 4.1, 4.3 and 4.4 give

improved bounds for certain averages of these sums. One of the existing applications of such estimates is to show that there are infinitely many triples of primes p_1, p_2, p_3 such that $p_1p_2 + p_1p_3 + p_2p_3$ has a relatively large prime factor. In Theorem 4.2 we use our bounds to improve the exponent in this problem. Chapter 5 is also concerned with Kloosterman sums but we no longer restrict the variable of summation to the primes. In Theorem 5.3 we use the q-analogue of van der Corput's method to estimate short sums to a modulus q which has factors of a certain size. We apply our bound to prove Theorems 5.1 and 5.2, both of which are concerned with the sum of the divisor function in an in arithmetic progression.

In Chapter 6 we study a problem in Diophantine approximation. We are interested in the quality of approximations to irrational numbers by rationals with prime, or almost-prime, denominators. Theorem 6.2 gives a new result when the denominators are products of precisely two primes. This is an important step towards extending the existing results for prime denominators as it shows that the parity barrier can be broken in a wider range than was previously known. The proof of Theorem 6.2 involves harmonic analysis which eventually reduces the problem to that of estimating Kloosterman sums over primes. This is achieved using our results from Chapter 4, specifically Theorem 4.4. It transpires that there is a close connection between this Diophantine approximation problem and that of counting 3-digit palindromic primes. We can therefore show, Theorem 6.3, that for all sufficiently large b there are 3-digit palindromes in base b which are the product of precisely two primes.

In the final two chapters, 7 and 8, we use the geometry of numbers to study the values of a binary form f. The main result of Chapter 7, Theorem 7.1, shows that, under some natural hypotheses, there are infinitely many pairs (p, n), with p prime and n an integer, such that $f(p, n)$ has at most $\frac{3 \deg f}{4} + 1$ prime factors. This is proved by means of the weighted sieve and a level of distribution result for the values $f(p, n)$, Theorem 7.4. In Chapter 8 we assume that $\deg f = 3$ and use a sieve to find pairs (m, n) for which both n and $f(m, n)$ are norms from a given number field. The sieve is much more elaborate than that used in Chapter 7 and requires various level of distribution results for the values $nf(m, n)$. We use our result to show, in Theorem 8.1, that the Hasse principle holds for the problem of representing a value of a cubic polynomial by a norm from a certain type of number field.

Chapter 2

Notation and Preliminaries

2.1 Notation

Most of the following notation is standard in analytic number theory. Given functions $f(x)$ and $g(x)$ we write $f(x) = O(g(x))$, or equivalently $f(x) \ll g(x)$, if there is a constant $c > 0$ such that

$$|f(x)| \leq cg(x)$$

for all x. We call c the implied constant. The notation $f(x) \gg g(x)$ means that $g(x) \ll f(x)$. In many cases the implied constant will depend on some of the quantities appearing in our estimates. This dependence will be indicated by means of a subscript on the symbols $\ll$, $\gg$ or O. We will say that $f(x) = o(g(x))$ as $x \to x_0$ if

$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = 0.$$

We will use the notation $x \sim y$ to denote the inequality $y \leq x < 2y$ and $x \asymp y$ to denote that $Ay \leq x < By$ for some unspecified constants $A, B > 0$.

We will write $(a; b)$ for the greatest common divisor of the integers a and b. We have chosen not to use the more standard notation (a, b) for this so that (a, b) can always refer to an element in $\mathbb{Z}^2$. For an integer $n \geq 1$ we will denote Euler's totient function, the number of $m \leq n$ with $(m; n) = 1$, by $\varphi(n)$. For any $\epsilon > 0$ this satisfies the well known estimate

$$n^{1-\epsilon} \ll_\epsilon \varphi(n) \leq n.$$

The Möbius function will be written $\mu(n)$ and is given by $(-1)^r$ if n is the product of r distinct primes and 0 otherwise. The divisor function, $\tau(n)$, is the number of positive divisors of n. More generally, for any $k \in \mathbb{N}$ we define $\tau_k(n)$ to be the number

of $(n_1, \ldots, n_k) \in \mathbb{N}^k$ which satisfy

$$n = \prod_{i=1}^{k} n_i.$$

For any $\epsilon > 0$ we have the standard estimate

$$\tau_k(n) \ll_{k,\epsilon} n^{\epsilon}.$$

The number of primes not exceeding x will be written $\pi(x)$. The Prime Number Theorem asserts that as $x \to \infty$ we have

$$\pi(x) = \frac{(1 + o(1))x}{\log x},$$

or equivalently

$$\sum_{p \leq x} \log p = x + o(x).$$

If we define the von Mangoldt function by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^a, a \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

then the Prime Number Theorem is also equivalent to

$$\sum_{n \leq x} \Lambda(n) = x + o(x).$$

For an integer n the notation $\overline{n}$ will represent a multiplicative inverse of n modulo some other integer which will be clear from the context. For example if $\overline{n}$ occurs in a congruence to modulus q or in a fraction $\frac{\overline{n}}{q}$ then the inverse is taken with respect to q. Of course $\overline{n}$ is only determined modulo q and therefore we only use this notation when it does not matter which representative of the congruence class we choose.

The meaning of $\|x\|$ will depend on the context. If x is a real number then it represents the distance from x to the nearest integer, that is

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

This will be used in Chapters 5 and 6. However, in Chapters 7 and 8 we will write $\|x\|$ for the norm of a vector x.

Throughout this thesis we adopt the standard convention that $\epsilon > 0$ is a small quantity whose value may be different at each occurrence. For example, we may write $x^{\epsilon} \log x \ll x^{\epsilon}$ and $x^{2\epsilon} \ll x^{\epsilon}$.

2.2 Fourier Analysis

We will write

$$e(x) = e^{2\pi i x}.$$

We may then define the Fourier transform, $\hat{f}$, of a function $f \in L^1(\mathbb{R})$ by

$$\hat{f}(x) = \int_{-\infty}^{\infty} f(t)e(-tx)\,dt.$$

If both f and $\hat{f}$ are in $L^1(\mathbb{R})$ and have bounded variation then the Poisson Summation Formula states that

$$\sum_{m\in\mathbb{Z}} f(m) = \sum_{n\in\mathbb{Z}} \hat{f}(n),$$

both sums converging absolutely. A proof of this can be found in Iwaniec and Kowalski [38, Theorem 4.4]. If $v \in \mathbb{R}_{>0}$ and $u \in \mathbb{R}$ then, using basic properties of the Fourier transform, we can derive the following two forms of Poisson Summation:

$$\sum_{m\in\mathbb{Z}} f(vm+u) = \frac{1}{v}\sum_{n\in\mathbb{Z}} \hat{f}\left(\frac{n}{v}\right) e\left(\frac{un}{v}\right), \tag{2.1}$$

$$\sum_{n\in\mathbb{Z}} f\left(\frac{n}{v}\right) e\left(\frac{un}{v}\right) = v\sum_{m\in\mathbb{Z}} \hat{f}(vm-u). \tag{2.2}$$

We will usually apply these results to functions f which are smooth and compactly supported. In that case, for any $j \in \mathbb{N}$ and any $x \neq 0$, we may apply integration by parts j times to the definition of $\hat{f}$ to deduce that

$$\hat{f}(x) = (-2\pi i x)^{-j} \int_{-\infty}^{\infty} f^{(j)}(t)e(-tx)\,dt.$$

Therefore, for any $x \in \mathbb{R}$ and any $j \in \mathbb{N}$, we obtain the standard estimate

$$\hat{f}(x) \ll_{f,j} \min(1, |x|^{-j}).$$

The following lemma proves the existence of the types of function, f, which we require for our applications.

Lemma 2.1. *Suppose that $a < b < c < d \in \mathbb{R}$. There exists a smooth function $f : \mathbb{R} \to \mathbb{R}$, supported on $[a, d]$ with $f(x)$ monotone increasing for $x \in [a, b]$, $f(x) = 1$ for $x \in [b, c]$ and $f(x)$ monotone decreasing for $x \in [c, d]$.*

Proof. The function

$$g(x) = \begin{cases} 0 & x \leq 0 \\ e^{-1/x} & x > 0 \end{cases}$$

is smooth and therefore so is

$$h(x) = \frac{g(x)}{g(x) + g(1-x)}.$$

In addition $h(x) = 0$ if $x \leq 0$, it is monotone increasing for $x \in [0,1]$ and $h(x) = 1$ if $x \geq 1$. The result therefore follows by taking

$$f(x) = h\left(\frac{x-a}{b-a}\right) h\left(\frac{d-x}{d-c}\right).$$

□

2.3 Geometry of Numbers

We will require some standard definitions and results from the geometry of numbers.

Definition 2.2. If $\lambda \subseteq \mathbb{Z}^n$ then λ is a lattice if it is a subgroup of $\mathbb{Z}^n$ whose span over $\mathbb{R}$ is $\mathbb{R}^n$. The discriminant, or determinant, of λ is defined to be the index of λ in $\mathbb{Z}^n$, $\det \lambda = [\mathbb{Z}^n : \lambda]$.

We should point out that we are using the term "lattice" in a very restricted sense. In general a lattice will be a discrete additive subgroup of $\mathbb{R}^n$, and need not have dimension n.

The next lemma is well known, it gives an alternative definition of the determinant of a lattice.

Lemma 2.3. *If λ is a lattice in $\mathbb{Z}^n$ with $\mathbb{Z}$-basis $B_1, \ldots, B_n$ and B is the matrix with rows given by $B_1, \ldots, B_n$ then $\det \lambda = |\det B|$. In particular $\det \lambda$ is the volume of the parallelepiped spanned by the vectors $B_1, \ldots, B_n$.*

The norm $\|x\|$ of a vector will always refer to the Euclidean norm,

$$\|x\| = \left(\sum |x_i|^2\right)^{1/2}.$$

Lemma 2.4. *Let λ be a lattice in $\mathbb{Z}^2$. Let B_1 be a nonzero element in λ which satisfies $\|B_1\| \leq \|x\|$ for all nonzero $x \in \lambda$. Let B_2 be an element of λ which is not a multiple of B_1 and which satisfies $\|B_2\| \leq \|x\|$ for all $x \in \lambda$ for which x is not a*

scalar multiple of B_1. The vectors B_1, B_2 form a basis for λ and the angle θ between them is in $[\frac{\pi}{3}, \frac{2\pi}{3}]$. In particular

$$\|B_1\|\|B_2\| \asymp \det \lambda.$$

In addition $\|B_1\| \ll (\det \lambda)^{1/2}$.

Proof. By construction B_1, B_2 are not parallel so they are linearly independent. To show that they form a basis of λ it is therefore sufficient to show that every $x \in \lambda$ can be written as $\lambda_1 B_1 + \lambda_2 B_2$ for some $\lambda_1, \lambda_2 \in \mathbb{Z}$.

Let $x \in \lambda$. Since B_1, B_2 are linearly independent x can be expressed uniquely in the form $x = \lambda_1 B_1 + \lambda_2 B_2$ for some $\lambda_1, \lambda_2 \in \mathbb{R}$. Suppose that at least one of the λ_i is not in $\mathbb{Z}$. We may subtract integer multiples of B_1, B_2 from x and therefore without loss of generality we may assume that $\lambda_1, \lambda_2 \in [-1/2, 1/2)$ and at least one of the λ_i is not 0. If $\lambda_2 = 0$ then $\|x\| = \|\lambda_1 B_1\| < \|B_1\|$, which contradicts the minimality of $\|B_1\|$. If $\lambda_1 = 0$ then $\|x\| = \|\lambda_2 B_2\| < \|B_2\|$. This contradicts the definition of B_2 since $\lambda_2 B_2$ is not parallel to B_1. We may therefore assume that $\lambda_1 \lambda_2 \neq 0$. In this case

$$\|x\| = \|\lambda_1 B_1 + \lambda_2 B_2\| < |\lambda_1|\|B_1\| + |\lambda_2|\|B_2\| \leq \|B_2\|.$$

This also contradicts the definition of B_2 since x is not parallel to B_1. It follows that both of the original λ_1, λ_2 must be in $\mathbb{Z}$ and therefore B_1, B_2 is a basis for λ.

The vector $B_1 - B_2$ is not parallel to B_1 so, by the definition of B_2,

$$\|B_2\|^2 \leq \|B_1 - B_2\|^2 = \|B_1\|^2 + \|B_2\|^2 - 2\|B_1\|\|B_2\| \cos\theta.$$

Therefore, since $B_1 \neq 0$ we have $0 \leq \|B_1\| - 2\|B_2\| \cos\theta$ and so

$$\cos\theta \leq \frac{\|B_1\|}{2\|B_2\|} \leq \frac{1}{2}.$$

Similarly, $B_1 + B_2$ is not parallel to B_1 and thus

$$\|B_2\|^2 \leq \|B_1 + B_2\|^2.$$

Therefore $0 \leq \|B_1\| + 2\|B_2\| \cos\theta$ and so $\cos\theta \geq -1/2$.

In conclusion $\cos\theta \in [-1/2, 1/2]$ so $\theta \in [\frac{\pi}{3}, \frac{2\pi}{3}]$. In particular

$$\det \lambda = \|B_1\|\|B_2\| \sin\theta \asymp \|B_1\|\|B_2\|.$$

Finally, $\|B_1\| \leq \|B_2\|$ so $\|B_1\| \ll (\det \lambda)^{1/2}$, this is a special case of Minkowski's theorem. □

The next lemma can be used to count the number of points of $\mathbb{Z}^2$ in a parallelogram. It could, of course, be extended to much more general regions $\mathcal{R} \subset \mathbb{R}^2$.

Lemma 2.5. *Let $\mathcal{R} \subset \mathbb{R}^2$ be a parallelogram with area $A(\mathcal{R})$ and perimeter $P(\mathcal{R})$. If $C(\mathcal{R}) = \#(\mathbb{Z}^2 \cap \mathcal{R})$ then $C(\mathcal{R}) = A(\mathcal{R}) + O(P(\mathcal{R}) + 1)$.*

Proof. We may partition $\mathbb{R}^2$ into unit squares centred at integer points:

$$\mathbb{R}^2 = \bigcup_{(x,y)\in\mathbb{Z}^2} ([x - \frac{1}{2}, x + \frac{1}{2}) \times [y - \frac{1}{2}, y + \frac{1}{2})).$$

Let $C_1(\mathcal{R})$ be the number of these squares which are totally contained in $\mathcal{R}$ and $C_2(\mathcal{R})$ the number which intersect with the boundary of $\mathcal{R}$. It follows that

$$C_1(\mathcal{R}) \leq C(\mathcal{R}) \leq C_1(\mathcal{R}) + C_2(\mathcal{R})$$

and

$$C_1(\mathcal{R}) \leq A(\mathcal{R}) \leq C_1(\mathcal{R}) + C_2(\mathcal{R})$$

and thus

$$C(\mathcal{R}) = A(\mathcal{R}) + O(C_2(\mathcal{R})).$$

It is clear that $C_2(\mathcal{R}) \ll P(\mathcal{R}) + 1$ so the result follows. □

We can generalise the last lemma to count the number of points of any lattice in a parallelogram.

Lemma 2.6. *Let $\lambda \subseteq \mathbb{Z}^2$ be a lattice and let $\mathcal{R}$ be a parallelogram with area $A(\mathcal{R})$ and perimeter $P(\mathcal{R})$. Let B_1, B_2 be the basis of λ described in Lemma 2.4. We then have*

$$\#(\lambda \cap \mathcal{R}) = \frac{A(\mathcal{R})}{\det \lambda} + O\left(\frac{P(\mathcal{R})}{\|B_1\|} + 1\right).$$

Proof. Let B be the matrix with rows B_1 and B_2. We have

$$\lambda = \{(u, v)B : (u, v) \in \mathbb{Z}^2\}$$

so the quantity of interest is

$$\#\{(u, v) \in \mathbb{Z}^2 : (u, v)B \in \mathcal{R}\} = \#(\mathbb{Z}^2 \cap \mathcal{R}B^{-1}).$$

The region $\mathcal{R}B^{-1}$ is itself a parallelogram with area $\frac{A(\mathcal{R})}{\det \lambda}$. To bound its perimeter we estimate the norm of the linear operator $(u, v) \mapsto (u, v)B^{-1}$. We have

$$B^{-1} = \pm\frac{1}{\det \lambda}\begin{pmatrix} B_{22} & -B_{12} \\ -B_{21} & B_{11} \end{pmatrix}$$

so

$$\|(1,0)B^{-1}\| = \frac{1}{\det \lambda}\sqrt{B_{22}^2 + B_{12}^2} \ll \frac{\|B_2\|}{\det \lambda}$$

and

$$\|(0,1)B^{-1}\| = \frac{1}{\det \lambda}\sqrt{B_{21}^2 + B_{11}^2} \ll \frac{\|B_2\|}{\det \lambda}.$$

By Lemma 2.4 we know that $\frac{\|B_2\|}{\det \lambda} \ll \|B_1\|^{-1}$. It follows that the operator norm of B^{-1} is $O(\|B_1\|^{-1})$ so that the perimeter of $\mathcal{R}B^{-1}$ is $O(P(\mathcal{R})\|B_1\|^{-1})$. The result follows by applying the last lemma. $\square$

Chapter 3

Palindromic Primes

3.1 Introduction

A natural number is palindromic in base b if its expansion in that base is equal to its reverse.

Definition 3.1. Let $b \in \mathbb{N}$ with $b > 1$. Suppose $n \in \mathbb{N}$ has the base b expansion $n = \sum_{i=0}^{l-1} a_i b^i$ where $0 \leq a_i < b$ and $a_{l-1} \neq 0$. We say that n is a palindrome in base b if $a_i = a_{l-1-i}$ for all $0 \leq i \leq l-1$. We call l the number of digits, or length, of the palindrome.

Let $\mathcal{P}_l(b)$ denote the set of all l-digit palindromes in base b and let $\mathcal{P}(b) = \bigcup_{l=1}^{\infty} \mathcal{P}_l(b)$. In addition, let $\mathcal{P}_l(b,x) = \{n \in \mathcal{P}_l(b) : n \leq x\}$ and $\mathcal{P}(b,x) = \{n \in \mathcal{P}(b) : n \leq x\}$. It is natural to ask how many primes these sets contain. If b is fixed and l is allowed to vary then sieve methods were applied to this question by Banks, Hart and Sakata in [2] and by Col in [10]. Col proved an upper bound for the number of primes in $\mathcal{P}(b,x)$ which we expect is of the correct order of magnitude, specifically

$$\#\{n \in \mathcal{P}(b,x) : n \text{ prime}\} \ll_b \frac{\#\mathcal{P}(b,x)}{\log x}.$$

He also proved a lower bound of the same order for the number of almost-primes in $\mathcal{P}(b,x)$. Let $\Omega(n)$ be the number of prime divisors of n, counted with multiplicities. Col showed that there exists a constant k_b which depends only on b such that

$$\#\{n \in \mathcal{P}(b,x) : \Omega(n) \leq k_b\} \gg_b \frac{\#\mathcal{P}(b,x)}{\log x},$$

provided that x is sufficiently large in terms of b. In particular, we can take $k_2 = 60$, $k_{10} = 372$ and $k_b = (12\pi + o(1))b$ as $b \to \infty$.

It is conjectured that there are infinitely many palindromic primes in base b and more precisely that for all sufficiently large x we have

$$\#\{n \in \mathcal{P}(b,x) : n \text{ prime}\} \gg_b \frac{\#\mathcal{P}(b,x)}{\log x}.$$

We will not consider this question any further. Instead we will fix the number of digits l and allow the base b to vary. If $l = 1$ then

$$\mathcal{P}_1(b) = \{n \in \mathbb{N} : n < b\}.$$

Therefore the number of primes in $\mathcal{P}_1(b)$ is simply $\pi(b-1)$, for which the Prime Number Theorem gives us an asymptotic.

If l is even then the l-digit palindromic primes in base b are easy to describe.

Lemma 3.2. *If n is an l-digit palindrome in base b, with l even, then $b+1$ divides n. In particular the only possible palindromic prime in base b with an even number of digits is the 2-digit palindrome $b+1$.*

Proof. Let $l = 2k$ and express n in base b as

$$n = \sum_{i=0}^{2k-1} a_i b^i.$$

Since n is a palindrome the a_i satisfy $a_i = a_{2k-1-i}$ for all $0 \le i < 2k$. Therefore

$$n = \sum_{i=0}^{k-1} a_i (b^i + b^{2k-i-1})$$

and thus

$$n \equiv \sum_{i=0}^{k-1} a_i \left((-1)^i + (-1)^{2k-i-1}\right) \equiv \sum_{i=0}^{k-1} a_i \left((-1)^i + (-1)^{-i-1}\right) \equiv 0 \,(\mathrm{mod}\, b+1).$$

□

The above discussion shows that the first interesting case is that of the 3-digit palindromes. We therefore let

$$\pi_3(b) = \#\{n \in \mathcal{P}_3(b) : n \text{ prime}\}.$$

Observe that

$$\mathcal{P}_3(b) = \{j(b^2+1) + kb : 1 \le j < b, 0 \le k < b\}.$$

Therefore

$$\#\mathcal{P}_3(b) = b(b-1) = b^2 + O(b)$$

so it seems reasonable to conjecture that $\pi_3(b) \asymp b^2/\log b$.

One way to study the set $\mathcal{P}_3(b)$ is as a disjoint union of arithmetic progressions, specifically

$$\begin{aligned}\mathcal{P}_3(b) &= \bigcup_{j=1}^{b-1}\{jb^2 < n < (j+1)b^2 : n \equiv j \,(\mathrm{mod}\, b)\} \\ &= \bigcup_{k=0}^{b-1}\{b^2 < n < b^3 : n \equiv kb \,(\mathrm{mod}\, b^2+1)\}.\end{aligned}$$

If we were to assume a very strong conjecture concerning the number of primes in an arithmetic progression then we could prove an asymptotic formula for $\pi_3(b)$. However, the progressions in question are to very large moduli so it would be necessary to work with a result stronger than the Generalised Riemann Hypothesis. On the other hand, the Brun-Titchmarsh Theorem, (see for example Iwaniec and Kowalski [38, Theorem 6.6]), gives an upper bound of the correct order for the number of primes in each progression. It is therefore easy to show, unconditionally, that

$$\pi_3(b) \ll \frac{b^2}{\log b}.$$

The Bombieri-Vinogradov Theorem, Iwaniec and Kowalski [38, Theorem 17.1], handles primes in arithmetic progressions if we average over the modulus. It gives a result which is essentially as strong as the Generalised Riemann Hypothesis. This does not appear to be sufficient to say anything interesting about $\pi_3(b)$. However, by using a strengthening of the Bombieri-Vinogradov theorem, due to Bombieri, Friedlander and Iwaniec [6], we can prove the following result. It shows that the set of $b \in \mathbb{N}$ for which there are no primes in $\mathcal{P}_3(b)$ has density 0.

Theorem 3.3. *For any $B \geq 2$ we have*

$$\#\{2 \leq b \leq B : \pi_3(b) = 0\} \ll B(\log B)^{-2}(\log\log B)^2.$$

The problem of counting primes in $\mathcal{P}_3(b)$ will be considered again in Chapter 6. We will show that it is closely related to a question concerning Diophantine approximation with prime denominators. As a consequence of our work in that chapter we will show in Theorem 6.3 that for all sufficiently large b the set $\mathcal{P}_3(b)$ contains numbers which are the product of exactly two primes.

3.2 Proof of Theorem 3.3

Let $\pi(x; q, a)$ denote the number of primes $p \le x$ with $p \equiv a \pmod q$. We will use the following strengthening of the Bombieri-Vinogradov theorem.

Lemma 3.4. *Suppose $\alpha \in (0, 1)$. For any $x \ge 2$ we have*

$$\sum_{\alpha\sqrt{x} < q \le \sqrt{x}} |\pi(x; q, 1) - \frac{\pi(x)}{\varphi(q)}| \ll_\alpha x(\log x)^{-3}(\log\log x)^2.$$

Proof. This is a special case of Bombieri, Friedlander and Iwaniec's main theorem from [6]. We put $a = 1$, $Q = \sqrt{x}$ and $Q' = \alpha\sqrt{x}$ in that result so that

$$\theta = \frac{\log Q}{\log x} = \frac{1}{2}.$$

In addition, for $y \ge 1$ we have, (for example by Montgomery and Vaughan [42, Exercise 2.1.13]),

$$\sum_{n \le y} \frac{1}{\varphi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \log y + O(1).$$

We deduce that

$$\sum_{\alpha\sqrt{x} < q \le \sqrt{x}} \frac{1}{\varphi(q)} \ll_\alpha 1$$

so the result follows. □

Fix a number $\alpha \in (\frac{\sqrt{2}}{2}, 1)$. For any $B \ge 2$ we will give an upper bound for

$$\#\{b \in (\alpha B, B] : \pi_3(b) = 0\}.$$

Recall that

$$\{n \in [b^2, 2b^2] : n \equiv 1 \pmod b\} \subseteq \mathcal{P}_3(b).$$

For any integer $b \in (\alpha B, B]$ we have

$$(B^2, 2\alpha^2 B^2] \subseteq [b^2, 2b^2]$$

so

$$\{n \in (B^2, 2\alpha^2 B^2] : n \equiv 1 \pmod b\} \subseteq \mathcal{P}_3(b).$$

It is therefore enough to bound

$$f(B) = \#\{b \in (\alpha B, B] : \pi(2\alpha^2 B^2; b, 1) - \pi(B^2; b, 1) = 0\}.$$

By two applications of Lemma 3.4 we obtain

$$\sum_{\alpha B<b\le B}\left|\pi(2\alpha^2B^2;b,1)-\pi(B^2;b,1)-\frac{\pi(2\alpha^2B^2)-\pi(B^2)}{\varphi(b)}\right|\ll B^2(\log B)^{-3}(\log\log B)^2$$

which implies that

$$(\pi(2\alpha^2B^2)-\pi(B^2))\sum_{\substack{\alpha B<b\le B\\ \pi(2\alpha^2B^2;b,1)-\pi(B^2;b,1)=0}}\frac{1}{\varphi(b)}\ll B^2(\log B)^{-3}(\log\log B)^2.$$

For all sufficiently large B the prime number theorem gives

$$\pi(2\alpha^2B^2)-\pi(B^2)\gg\frac{B^2}{\log B}.$$

In addition, if $b\in(\alpha B,B]$ then

$$\frac{1}{\varphi(b)}\ge\frac{1}{b}\gg\frac{1}{B}$$

so we conclude that

$$f(B)\ll B(\log B)^{-2}(\log\log B)^2.$$

To estimate

$$\#\{2\le b\le B:\pi_3(b)=0\}$$

we trivially bound the contribution from $b\le\sqrt{B}$ by $\sqrt{B}$. We cover the remaining range, $(\sqrt{B},B]$, by intervals of the form $(\alpha B',B']$. For $B'\in(\sqrt{B},B]$ we have

$$\#\{b\in(\alpha B',B']:\pi_3(b)=0\}\ll B'(\log B')^{-2}(\log\log B')^2\ll B'(\log B)^{-2}(\log\log B)^2$$

so

$$\begin{aligned}\#\{b\in(\sqrt{B},B]:\pi_3(b)=0\}&\ll B(\log B)^{-2}(\log\log B)^2\sum_j 2^{-j}\\&\ll B(\log B)^{-2}(\log\log B)^2.\end{aligned}$$

Theorem 3.3 follows.

Chapter 4

Average Bounds for Kloosterman Sums Over Primes

4.1 Introduction

Short Kloosterman sums of the form

$$\sum_{\substack{n\sim x\\(n;q)=1}} e\left(\frac{a\overline{n}}{q}\right)$$

occur frequently in analytic number theory. They may be estimated by a result of Weil, given below as Lemma 4.5. One way in which these sums may arise is from the use of additive characters to count the number of integer solutions to a congruence, see Chapter 5 for an example. Given such a counting problem we might wish to estimate the number of solutions which satisfy the additional constraint that some of the variables are prime. This naturally leads us to consider the above sum where the variable of summation, n, is restricted to being prime. We will therefore investigate bounds for sums of the form

$$S_q(a;x) = \sum_{\substack{p\sim x\\(p;q)=1}} e\left(\frac{a\overline{p}}{q}\right)$$

where p runs over primes. These sums may be bounded trivially by x. If $(a;q) = 1$ then we conjecture that for any $\epsilon > 0$ a bound of

$$S_q(a;x) \ll_\epsilon x^{\frac{1}{2}+\epsilon}q^\epsilon$$

should hold. This conjecture, however, seems to be far out of reach of current methods.

A bound for $S_q(a;x)$ was given by Garaev [26] in the case that q is prime. He showed that for $x < q$ we have, for any $\epsilon > 0$,

$$\max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon \left(x^{\frac{15}{16}} + x^{\frac{2}{3}} q^{\frac{1}{4}}\right) q^\epsilon.$$

This gives us a nontrivial estimate for the sum provided that $x \geq q^{\frac{3}{4}+\delta}$ for some $\delta > 0$. For $q \geq x \geq q^{\frac{16}{17}+\delta}$ Garaev used this bound to prove an asymptotic for the number of prime solutions, p_1, p_2, p_3 with $p_i \in [0, x]$, to the congruence

$$p_1(p_2 + p_3) \equiv \lambda \,(\mathrm{mod}\, q).$$

Fouvry and Shparlinski [24] generalised Garaev's bound to arbitrary q in the larger range $q^{\frac{3}{4}} \leq x \leq q^{\frac{4}{3}}$. They also showed that if we average over q then a sharper estimate is possible. Specifically, their Theorem 5 states that if $Q^{\frac{3}{2}} \geq x \geq 2$ then for every $\epsilon > 0$ we have

$$\sum_{q \sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon \left(Q^{\frac{13}{10}} x^{\frac{3}{5}} + Q^{\frac{13}{12}} x^{\frac{5}{6}}\right) Q^\epsilon. \tag{4.1}$$

This bound is nontrivial when $x \geq Q^{\frac{3}{4}+\delta}$. Fouvry and Shparlinski used their estimates to study multiplicative properties of the set

$$\{p_1p_2 + p_1p_3 + p_2p_3 : p_i \sim x, p_i \text{ prime }\}.$$

They showed, for example, that for x sufficiently large this set contains numbers with a prime factor exceeding $x^{1.10028}$. Baker [1, Theorem 2] has recently improved the bound (4.1) in the range $Q^{\frac{1}{2}} \leq x \leq 2Q$. His result is

$$\sum_{q \sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon \left(Q^{\frac{11}{10}} x^{\frac{4}{5}} + Q x^{\frac{11}{12}}\right) Q^\epsilon. \tag{4.2}$$

This is nontrivial for $Q \geq x^{\frac{1}{2}+\delta}$ and sharper than (4.1) when $x \leq Q^{1-\delta}$. Baker applied this bound to the same ternary form problem as Fouvry and Shparlinski; combining it with a variant on the sieve argument he improved 1.10028 to 1.1673.

We are motivated by a new application of these sums to Diophantine approximation which will be given in Chapter 6. For this application we need only consider average bounds. We will show that by generalising the arguments from [24] it is possible to obtain a sharper estimate than that given in (4.1).

Theorem 4.1. *For any $\epsilon > 0$ we have*

$$\sum_{q \sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon \left(Q^{\frac{5}{4}} x^{\frac{5}{8}} + Q x^{\frac{9}{10}} + Q^{\frac{7}{6}} x^{\frac{13}{18}}\right) Q^\epsilon$$

for $Q^{\frac{3}{2}} \geq x \geq Q^{\frac{2}{3}}$.

This gives us a nontrivial result for $x \geq Q^{\frac{2}{3}+\delta}$. It is an improvement on (4.2) for $Q^{\frac{6}{7}+\delta} \leq x \leq 2Q$ and on (4.1) for $2Q \leq x \leq Q^{\frac{5}{4}-\delta}$. The proof uses similar methods to those of Fouvry and Shparlinski. However we introduce higher moments into one of their estimates. This results in a problem of counting solutions to a congruence with a larger number of variables; one which we can solve with a sharp bound when we average over q.

Using this theorem we give a further improvement of the exponent in the ternary form problem. Let $P^+(n)$ denote the largest prime factor of n.

Theorem 4.2. *Let $\theta_1 = 1.188\ldots$ be the unique root of the equation*

$$42\theta - 65 + 38\log\left(\frac{21\theta - 19}{4}\right) = 0.$$

Then, for any $\theta < \theta_1$ and any x which is sufficiently large in terms of θ,

$$\#\{p_1, p_2, p_3 : p_i \sim x, p_i \text{ prime}, P^+(p_1p_2 + p_1p_3 + p_2p_3) > x^\theta\} \gg_\theta \frac{x^3}{(\log x)^3}.$$

Extending our methods we can give a version of Theorem 4.1 which, like Baker's bound (4.2), is nontrivial for $x \geq Q^{\frac{1}{2}+\delta}$. We will only prove this result in the following qualitative form.

Theorem 4.3. *For any $\delta > 0$ there exists an $\eta > 0$ such that*

$$\sum_{q\sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\delta Qx^{1-\eta},$$

provided that $Q \geq x \geq Q^{\frac{1}{2}+\delta}$.

In some applications of Theorem 4.1 the maximum over a is not necessary. We therefore prove a bound when a is constant, which is stronger provided that a is not too large.

Theorem 4.4. *For any integer $a > 0$ and any $\epsilon > 0$ we have*

$$\sum_{q\sim Q} |S_q(a;x)| \ll_\epsilon \left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}} \left(Q^{\frac{1}{2}}x^{\frac{11}{8}} + Q^{\frac{7}{6}}x^{\frac{2}{3}}\right)(aQ)^\epsilon$$

for $Q^{\frac{4}{3}} \geq x \geq Q^{\frac{1}{2}}$.

This is nontrivial for $Q^{\frac{1}{2}+\delta} \leq x \leq Q^{\frac{4}{3}-\delta}$. The proof exploits the fact that, since there is no maximum over a, we can reorder summations to give an inner sum over $q \sim Q$. This is a longer range than those arising in the proof of Theorem 4.1. After inverting the Kloosterman fractions in such sums we reach a situation in which the Weil estimate for short Kloosterman sums can be used.

The sums in this last theorem are essentially bilinear forms with Kloosterman fractions, which were studied for arbitrary coefficients by Duke, Friedlander and Iwaniec in [19]. In the case that one of the coefficients is the indicator function of the primes then our theorem does better than the general result of [19], provided that x and Q are sufficiently close in size.

We are most interested in the situation when $x \asymp Q$ as this is the case in our application to Diophantine approximation. For this reason we have given estimates which, given our current ideas, are as sharp as possible in this case. For x sufficiently different in size to Q it is possible to improve the above theorems. In order to compare the various results we note that when $x \asymp Q$ we have the following bounds, valid for any $\epsilon > 0$.

1. Using Fouvry and Shparlinski's bound (4.1) or Baker's (4.2), we get
$$\sum_{q \sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon Q^{\frac{23}{12}+\epsilon}.$$

2. Theorem 4.1 improves this to
$$\sum_{q \sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon Q^{\frac{19}{10}+\epsilon}.$$

3. If $0 < a \ll Q^2$ then using Theorem 2 from Duke, Friedlander and Iwaniec, [19], we get a bound
$$\sum_{q \sim Q} |S_q(a;x)| \ll_\epsilon Q^{\frac{95}{48}+\epsilon}.$$

4. If $0 < a \ll Q^2$ then Theorem 4.4 gives a bound
$$\sum_{q \sim Q} |S_q(a;x)| \ll_\epsilon Q^{\frac{15}{8}+\epsilon}.$$

These results should be compared with the trivial bound of Q^2 and the conjectured best bound of $Q^{\frac{3}{2}+\epsilon}$.

4.2 Lemmas

We require the following estimate for short Kloosterman sums coming from the Weil bound.

Lemma 4.5. *For integers a and q with $q > 1$, and reals $Y < Z$ we have, for any $\epsilon > 0$, that*

$$\sum_{\substack{Y<n\leq Z\\(n;q)=1}} e\left(\frac{a\overline{n}}{q}\right) \ll_\epsilon \left((a;q)\left(\frac{Z-Y}{q}+1\right)+q^{\frac{1}{2}}\right)q^\epsilon.$$

Proof. This is a slight weakening of Lemma 1 from Fouvry and Shparlinski [24]. It follows immediately on inserting the estimate

$$n^{1-\epsilon} \ll \varphi(n) \ll n$$

as well as the standard bound for the divisor function, τ, into that lemma. □

We also require the following estimate for the number of solutions to a certain Diophantine equation.

Lemma 4.6. *Let $k \in \mathbb{N}$ and $\epsilon > 0$ be fixed. For any $N \geq 0$ we have*

$$\#\left\{(n_1,\dots,n_{2k}) \in \mathbb{Z}^{2k} : 0 < n_i \leq N, \sum_{i=1}^{k}\frac{1}{n_i} = \sum_{i=k+1}^{2k}\frac{1}{n_i}\right\} \ll_{\epsilon,k} N^{k+\epsilon}.$$

Proof. This is well known. For example, it follows from Karatsuba's first lemma in [39]. The key idea is that if $n_1,\dots,n_{2k}$ is a solution then the product $n_1\dots n_{2k}$ must be squarefull. □

The last lemma is essentially optimal for all k as there are $[N]^k$ solutions with $n_i = n_{k+i}$ for $1 \leq i \leq k$. We now let $J_M^{(k)}(q)$ denote the number of solutions to the congruence

$$\overline{m}_1 + \dots + \overline{m}_k \equiv \overline{m}_{k+1} + \dots + \overline{m}_{2k} \,(\mathrm{mod}\, q) \tag{4.3}$$

with $1 \leq m_i \leq M$ and $(m_i;q) = 1$. The following generalises Fouvry and Shparlinski's result [24, Lemma 3].

Lemma 4.7. *Fix some $k \in \mathbb{N}$. For any $\epsilon > 0$ and any $M \geq 1$ we have*

$$\sum_{q\sim Q} J_M^{(k)}(q) \ll_{k,\epsilon} \left(QM^k + M^{2k}\right)M^\epsilon.$$

Proof. For each $(m_1, \dots, m_{2k})$ with $1 \le m_i \le M$ we count the number of $q \sim Q$ with $(q; m_i) = 1$ for which the congruence (4.3) holds. If

$$\frac{1}{m_1} + \dots + \frac{1}{m_k} = \frac{1}{m_{k+1}} + \dots + \frac{1}{m_{2k}}$$

then the congruence is satisfied for every $q \sim Q$ for which q is coprime to $\prod m_i$. Using Lemma 4.6 it follows that the contribution from such $2k$-tuples $(m_1, \dots, m_{2k})$ is

$$O_{\epsilon,k}\left(QM^{k+\epsilon}\right).$$

In the alternative case we define

$$F = \prod_{i=1}^{2k} m_i \left(\sum_{i=1}^{k} m_i^{-1} - \sum_{i=k+1}^{2k} m_i^{-1} \right)$$

so that F is a nonzero integer with $F \ll_k M^{2k}$. Since $q|F$ there are $O_{\epsilon,k}(M^\epsilon)$ possible values for q. Thus the contribution from such $2k$-tuples $(m_1, \dots, m_{2k})$ is

$$O_{\epsilon,k}(M^{2k+\epsilon})$$

so the result follows. □

4.3 Estimates for Bilinear Sums

Throughout this section let α_l, β_m be arbitrary complex numbers bounded by 1. We will prove estimates for sums

$$W_{a,q} = \sum_{\substack{l \sim L, m \sim M \\ (ml;q)=1}} \alpha_l \beta_m e\left(\frac{a\overline{lm}}{q}\right),$$

either individually or on average over $q \sim Q$. If $\beta_m = 1$ then we call $W_{a,q}$ a Type I sum, if not then it is Type II.

Firstly we use Lemma 4.7 to estimate Type II sums on average. This is a generalisation of a bound of Fouvry and Shparlinski [24, Corollary 5].

Lemma 4.8. *Suppose that $1 \le L, M \le Q$. For any integer $k \ge 1$ and any $\epsilon > 0$ we have*

$$\sum_{q \sim Q} \max_{(a;q)=1} |W_{a,q}| \ll_{\epsilon,k} Q\left(Q^{\frac{1}{2k}} L^{\frac{2k-1}{2k}} M^{\frac{1}{2}} + L^{\frac{2k-1}{2k}} M\right) Q^\epsilon.$$

Proof. By Hölder's inequality we have

$$|W_{a,q}|^{2k} \leq L^{2k-1} \sum_{\substack{l\sim L\\(l;q)=1}} \left| \sum_{\substack{m\sim M\\(m;q)=1}} \beta_m e\left(\frac{a\overline{lm}}{q}\right)\right|^{2k}.$$

Since $L \leq Q$ we may bound this by extending the sum over l to a sum over all residues modulo q:

$$|W_{a,q}|^{2k} \leq L^{2k-1} \sum_{l=1}^{q} \left| \sum_{\substack{m\sim M\\(m;q)=1}} \beta_m e\left(\frac{a\overline{lm}}{q}\right)\right|^{2k}.$$

Expanding, reordering the summation and using the orthogonality of additive characters then results in

$$|W_{a,q}|^{2k} \ll L^{2k-1} Q J_M^{(k)}(q).$$

Using Hölder's inequality and Lemma 4.7 we then get

$$\begin{aligned}
\sum_{q\sim Q} \max_{(a;q)=1} |W_{a,q}| &\ll L^{\frac{2k-1}{2k}} Q^{\frac{1}{2k}} \sum_{q\sim Q} J_M^{(k)}(q)^{\frac{1}{2k}} \\
&\leq L^{\frac{2k-1}{2k}} Q \left(\sum_{q\sim Q} J_M^{(k)}(q)\right)^{\frac{1}{2k}} \\
&\ll_{\epsilon,k} L^{\frac{2k-1}{2k}} Q \left(QM^k + M^{2k}\right)^{\frac{1}{2k}} M^{\epsilon} \\
&\ll Q\left(Q^{\frac{1}{2k}} L^{\frac{2k-1}{2k}} M^{\frac{1}{2}} + L^{\frac{2k-1}{2k}} M\right) Q^{\epsilon}.
\end{aligned}$$

□

If we remove the maximum over a then we can obtain a sharper estimate by exploiting the sum over q.

Lemma 4.9. *For any integer $a > 0$, any $L, M, Q \geq 1$, and any $\epsilon > 0$, we have*

$$\sum_{q\sim Q} |W_{a,q}| \ll_{\epsilon} \left(1 + \frac{a}{LMQ}\right)^{\frac{1}{2}} \left(QLM^{\frac{1}{2}} + Q^{\frac{1}{2}} L^{\frac{5}{4}} M^{\frac{3}{2}}\right) (aQ)^{\epsilon}.$$

Proof. We first consider the case when α_l, β_m are supported on integers coprime to a. We trivially have

$$\sum_{q\sim Q} |W_{a,q}| \leq \sum_{\substack{l\sim L\\(l;a)=1}} W_1(l)$$

where

$$W_1(l) = \sum_{\substack{q\sim Q\\(q;l)=1}} \left| \sum_{\substack{m\sim M\\(m;aq)=1}} \beta_m e\left(\frac{a\overline{lm}}{q}\right)\right|.$$

By Cauchy's inequality we get

$$W_1(l)^2 \le Q \sum_{\substack{q\sim Q\\(q;l)=1}} \left| \sum_{\substack{m\sim M\\(m;aq)=1}} \beta_m e\left(\frac{a\overline{lm}}{q}\right)\right|^2.$$

Expanding and reordering the summation then gives us the bound

$$W_1(l)^2 \le Q \sum_{\substack{m_1,m_2\sim M\\(m_1m_2;a)=1}} \left| \sum_{\substack{q\sim Q\\(q;lm_1m_2)=1}} e\left(\frac{a(m_1-m_2)\overline{lm_1m_2}}{q}\right)\right|.$$

We can write

$$\overline{lm_1m_2} = \frac{1-q\overline{q}}{lm_1m_2}$$

where $\overline{q}$ is an inverse of q modulo lm_1m_2. Therefore

$$W_1(l)^2 \le Q \sum_{\substack{m_1,m_2\sim M\\(m_1m_2;a)=1}} \left| \sum_{\substack{q\sim Q\\(q;lm_1m_2)=1}} e\left(\frac{a(m_1-m_2)}{qlm_1m_2}\right) e\left(-\frac{a(m_1-m_2)\overline{q}}{lm_1m_2}\right)\right|.$$

If we let

$$f(t) = e\left(\frac{a(m_1-m_2)}{lm_1m_2t}\right)$$

then the factor $f(q)$ can be removed using summation by parts. For $t\sim Q$ we have

$$f'(t) \ll \frac{a}{LMQ^2}$$

and thus

$$W_1(l)^2 \ll Q\left(1+\frac{a}{LMQ}\right) \sum_{\substack{m_1,m_2\sim M\\(m_1m_2;a)=1}} \max_{Q'\sim Q} \left| \sum_{\substack{Q\le q<Q'\\(q;lm_1m_2)=1}} e\left(\frac{a(m_1-m_2)\overline{q}}{lm_1m_2}\right)\right|.$$

We get a contribution to this from pairs $m_1=m_2$ which is bounded by

$$Q\left(1+\frac{a}{LMQ}\right)MQ.$$

For the remaining terms let

$$b = a(m_1 - m_2)$$

and

$$c = lm_1m_2$$

so that the inner sum is

$$\sum_{\substack{Q \le q < Q' \\ (q;c)=1}} e\left(\frac{b\overline{q}}{c}\right).$$

We may bound this using Lemma 4.5 by

$$O_\epsilon\left(\left((b;c)\left(\frac{Q}{LM^2}+1\right)+(LM^2)^{\frac{1}{2}}\right)(LM^2)^\epsilon\right).$$

The result would be trivial if $LM^2 \ge Q^2$. We thus assume that $LM^2 \le Q^2$, which allows us to replace $(LM^2)^\epsilon$ by Q^ϵ in our bound.

The contribution to our estimate for $W_1(l)^2$ from the term $(LM^2)^{\frac{1}{2}}$ is then

$$O_\epsilon\left(Q\left(1+\frac{a}{LMQ}\right)L^{\frac{1}{2}}M^3Q^\epsilon\right)$$

and that from the remaining terms is

$$O_\epsilon\left(Q\left(1+\frac{a}{LMQ}\right)\left(\frac{Q}{LM^2}+1\right)Q^\epsilon\sum_{\substack{m_1,m_2\sim M \\ m_1\neq m_2}}(m_1-m_2;lm_1m_2)\right),$$

where we have used that $(m_1m_2l;a)=1$.

If we write $h = m_1 - m_2 \neq 0$ then

$$\begin{aligned}\sum_{\substack{m_1,m_2\sim M \\ m_1\neq m_2}}(m_1-m_2;lm_1m_2) &\ll \sum_{m_1\sim M}\sum_{0<h\ll M}(h;lm_1(m_1+h)) \\ &= \sum_{m_1\sim M}\sum_{0<h\ll M}(h;lm_1^2) \\ &\ll_\epsilon M^2Q^\epsilon,\end{aligned}$$

since one has in general that

$$\sum_{h=1}^{H}(h;n) = \sum_{d|n} d\#\{h \le H/d : (h;n)=1\} \le \sum_{d|n} H = H\tau(n) \ll_\epsilon Hn^\epsilon$$

for any $n \in \mathbb{N}$.

We conclude that

$$W_1(l)^2 \ll_\epsilon Q\left(1+\frac{a}{LMQ}\right)\left(QM+L^{\frac{1}{2}}M^3+\frac{Q}{L}+M^2\right)Q^\epsilon.$$

Since $L, M \geq 1$ this simplifies to

$$W_1(l)^2 \ll_\epsilon Q\left(1+\frac{a}{LMQ}\right)\left(QM+L^{\frac{1}{2}}M^3\right)Q^\epsilon$$

and therefore

$$\sum_{q\sim Q}|W_{a,q}| \ll_\epsilon \left(1+\frac{a}{LMQ}\right)^{\frac{1}{2}}\left(QLM^{\frac{1}{2}}+Q^{\frac{1}{2}}L^{\frac{5}{4}}M^{\frac{3}{2}}\right)Q^\epsilon.$$

This completes the proof under the assumption that the coefficients are supported on integers coprime to a. To remove this assumption we begin by writing $(l;a)=u$, $a=bu$ and $l=ku$ to get

$$\begin{aligned} W_{a,q} &= \sum_{\substack{l\sim L, m\sim M\\(ml;q)=1}} \alpha_l\beta_m e\left(\frac{a\overline{lm}}{q}\right) \\ &= \sum_{\substack{a=ub\\(u;q)=1}}\sum_{\substack{k\sim L/u, m\sim M\\(mk;q)=1,(k;b)=1}} \alpha_{uk}\beta_m e\left(\frac{b\overline{km}}{q}\right). \end{aligned}$$

Next we set $(m;b)=v$, $m=vj$ and $b=cv$ to rewrite this as

$$\sum_{\substack{a=uvc\\(uv;q)=1}}\sum_{\substack{k\sim L/u, j\sim M/v\\(jk;q)=1,(k;vc)=1,(j;c)=1}} \alpha_{uk}\beta_{vj} e\left(\frac{c\overline{kj}}{q}\right).$$

It follows that

$$\begin{aligned} \sum_{q\sim Q}|W_{a,q}| &\leq \sum_{a=uvc}\sum_{\substack{q\sim Q\\(uv;q)=1}}\left|\sum_{\substack{k\sim L/u, j\sim M/v\\(jk;q)=1,(k;vc)=1,(j;c)=1}} \alpha_{uk}\beta_{vj} e\left(\frac{c\overline{kj}}{q}\right)\right| \\ &\leq \sum_{a=uvc}\sum_{q\sim Q}\left|\sum_{\substack{k\sim L/u, j\sim M/v\\(jk;q)=1,(k;vc)=1,(j;c)=1}} \alpha_{uk}\beta_{vj} e\left(\frac{c\overline{kj}}{q}\right)\right|. \end{aligned}$$

For each factorisation $a=uvc$ the inner sum now has coefficients supported on integers coprime to c so the above bound applies. The number of factorisations is $O(a^\epsilon)$ so the bound for the general sum is the same as that for the sum with coprimality conditions except for an additional factor a^ϵ. □

Finally we use Lemma 4.5 directly to estimate Type I sums when L is small.

Lemma 4.10. *Suppose that $\beta_m = 1$. Then, for any $L, M \geq 1$ and any $\epsilon > 0$ we have*

$$W_{a,q} \ll_\epsilon \left((a;q)\left(\frac{LM}{Q} + L\right) + Q^{\frac{1}{2}}L\right)Q^\epsilon.$$

Proof. We have

$$|W_{a,q}| \leq \sum_{\substack{l\sim L\\(l;q)=1}} \left|\sum_{\substack{m\sim M\\(m;q)=1}} e\left(\frac{a\overline{lm}}{q}\right)\right|.$$

The result follows on applying Lemma 4.5 to the inner sum. □

Summing this result over $q \sim Q$ we immediately get the following.

Lemma 4.11. *Suppose that $L, M, Q \geq 1$ and that $\beta_m = 1$. For any $\epsilon > 0$ we have*

$$\sum_{q\sim Q} \max_{(a;q)=1} |W_{a,q}| \ll_\epsilon \left(LM + Q^{\frac{3}{2}}L\right)Q^\epsilon.$$

In addition if $a > 0$ then we have

$$\sum_{q\sim Q} |W_{a,q}| \ll_\epsilon \left(LM + Q^{\frac{3}{2}}L\right)(aQ)^\epsilon.$$

4.4 Proof of the Theorems

4.4.1 Approach

In the sums $S_q(a;x)$ we replace the indicator function of the primes with the von Mangoldt function $\Lambda(n)$. The contribution of prime powers p^α with $\alpha > 1$ is $O_\epsilon(x^{\frac{1}{2}+\epsilon})$. This is smaller than any of the bounds we will establish so it may be ignored. In addition the factor $\log p$ may be removed using partial summation with the cost of a factor $x^\epsilon \ll Q^\epsilon$. It is thus sufficient to establish the theorems for the sums containing Λ.

We decompose $\Lambda(n)$ using Vaughan's Identity, as described by Davenport in [14, Chapter 24]. We will use $U = V \leq x^{\frac{1}{3}}$; the precise choice of U for each theorem will be given later. The sum $S_q(a;x)$ is decomposed into Type I and II sums with $LM \asymp x$. The precise forms of the sums are given by Fouvry and Shparlinski in [24]. The coefficients are not all bounded by 1 but they are bounded by a divisor function. This divisor function may be absorbed into the Q^ϵ term. We must estimate Type I sums for $L \leq U^2$ and Type II sums for $U \leq L \leq x/U$. Since $U^2 \leq x/U$ any Type I

sum with $U \leq L \leq U^2$ may be regarded as a Type II sum. Hence it will be enough to consider Type I sums with $L \leq U$ and Type II sums with $U \leq L \leq x/U$. The variables of summation are restricted by the condition $lm \sim x$. In the Type II sums this may be removed by Fourier analysis, see for example the start of Garaev's proof [26, Lemma 2.4]. For the Type I sums, if we are simply treating them as Type II sums then the same argument applies, whereas if we are using Lemma 4.11 then it is clear that a condition $lm \sim x$ can be introduced by modifying the proof.

4.4.2 Proof of Theorem 4.1

The sums arising from Vaughan's identity are of the form

$$\sum_{q \sim Q} \max_{(a;q)=1} |W_{a,q}|.$$

We estimate the Type II sums using Lemma 4.8. We have

$$L, M \leq \frac{x}{U}$$

and thus the hypotheses are satisfied provided that our choice of U satisfies $\frac{x}{U} \leq Q$. Recalling that $M \ll x/L$ the bound from Lemma 4.8 is

$$Q\left(Q^{\frac{1}{2k}} x^{\frac{1}{2}} L^{\frac{k-1}{2k}} + xL^{\frac{-1}{2k}}\right) Q^{\epsilon}.$$

For $x^{\frac{2}{5}} \leq L \leq x^{\frac{1}{2}}$ we apply this with $k = 2$ to get a bound of

$$Q\left(Q^{\frac{1}{4}} x^{\frac{5}{8}} + x^{\frac{9}{10}}\right) Q^{\epsilon}.$$

For $x^{\frac{3}{5}} \leq L \leq x/U$ we use $k = 3$ to get

$$Q\left(Q^{\frac{1}{6}} x^{\frac{5}{6}} U^{-\frac{1}{3}} + x^{\frac{9}{10}}\right) Q^{\epsilon}.$$

Since $LM \asymp x$ and we can interchange l, m in our sums these two bounds in fact cover the whole range $U \leq L \leq x/U$. The contribution of all our Type II sums is therefore

$$O_{\epsilon}\left(Q\left(Q^{\frac{1}{4}} x^{\frac{5}{8}} + x^{\frac{9}{10}} + Q^{\frac{1}{6}} x^{\frac{5}{6}} U^{-\frac{1}{3}}\right) Q^{\epsilon}\right).$$

We need to estimate Type I sums for $L \leq U$. Lemma 4.11 gives a bound for these sums of

$$\left(x + Q^{\frac{3}{2}} U\right) Q^{\epsilon}.$$

Since $x \leq Q^{\frac{3}{2}}$ and $U \geq 1$ the second term is larger and thus

$$\sum_{q\sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon Q\left(Q^{\frac{1}{4}}x^{\frac{5}{8}} + x^{\frac{9}{10}} + Q^{\frac{1}{6}}x^{\frac{5}{6}}U^{-\frac{1}{3}} + Q^{\frac{1}{2}}U\right)Q^\epsilon.$$

We now choose

$$U = \min(x^{\frac{1}{3}}, Q^{-\frac{1}{4}}x^{\frac{5}{8}}).$$

Since $Q^{\frac{2}{3}} \leq x \leq Q^{\frac{3}{2}}$ we have

$$1 \leq U \leq x^{\frac{1}{3}}$$

and

$$\frac{x}{U} \leq Q.$$

This choice of U is therefore admissible so we can conclude that

$$\sum_{q\sim Q} \max_{(a;q)=1} |S_q(a;x)| \ll_\epsilon Q\left(Q^{\frac{1}{4}}x^{\frac{5}{8}} + x^{\frac{9}{10}} + Q^{\frac{1}{6}}x^{\frac{13}{18}}\right)Q^\epsilon,$$

thus proving Theorem 4.1.

4.4.3 Proof of Theorem 4.2

The following lemma generalises Baker's analysis from [1, Section 4].

Lemma 4.12. *Let $\beta > 0$ be fixed. Suppose $\alpha \in (1,2)$ is a constant such that for any $\epsilon > 0$ there exists a $\delta > 0$ for which*

$$\sum_{q\sim Q} \max_{(a;q)=1} \left| \sum_{\substack{x\leq p<(1+\beta)x \\ (p;q)=1}} e\left(\frac{a\overline{p}}{q}\right)\right| \ll_{\beta,\epsilon} x^{2-\delta} \tag{4.4}$$

holds for $x \leq Q \leq x^{\alpha-\epsilon}$. We may then deduce Theorem 4.2 with θ_1 the root of the equation

$$2\theta - \alpha - 2 + 2(2-\alpha)\log\left(\frac{\theta+\alpha-2}{2\alpha-2}\right) = 0.$$

Proof. As in [1] we write $\mathcal{L} = \log x$. Using our hypothesis (4.4) in the proof of [1, Theorem 4] we see that it holds with the exponent $\frac{13}{12}$ replaced by our constant α. We now use an almost identical proof to that of [1, Theorem 3]. We replace $Y := x^{13/12-\epsilon}$ by $Y := x^{\alpha-\epsilon}$. The asymptotic [1, (4.11)] becomes

$$\Sigma_1 = (\alpha - \epsilon + o(1))X\mathcal{L}.$$

Baker's quantity J is now given by

$$\begin{aligned} J &= \frac{\log(Z/Y)}{\mathcal{L}} + \frac{\log(x^2/Y)}{\mathcal{L}} \log\left[\frac{\log(YZx^{-2})}{\log(Y^2x^{-2})}\right] \\ &= \theta - \alpha + \epsilon + (2 - \alpha + \epsilon) \log\left[\frac{\theta + \alpha - \epsilon - 2}{2\alpha - 2\epsilon - 2}\right]. \end{aligned}$$

The bound [1, (4.21)] now becomes

$$\begin{aligned} \Sigma_3 \leq\ & (2 + 2\epsilon)\pi(x, \beta)^3(1 + \frac{2\log(1+\beta)}{\log 2}) \\ & \times \left[\theta - \alpha + \epsilon + (2 - \alpha + \epsilon) \log \frac{\theta + \alpha - \epsilon - 2}{2\alpha - 2\epsilon - 2}\right]. \end{aligned}$$

Since $\theta < \theta_1$ we may choose ϵ, β sufficiently small to get a bound of

$$\Sigma_3 < (2 - \alpha - \epsilon)\pi(x, \beta)^3\mathcal{L}.$$

The result follows. □

Theorem 4.1 shows that the hypotheses of this lemma are satisfied with $\alpha = \frac{23}{21}$. We only gave the proof for $\beta = 1$ but it is clear that it can be modified to handle any fixed β. The equation defining θ_1 is thus

$$42\theta - 65 + 38 \log\left(\frac{21\theta - 19}{4}\right) = 0.$$

The root of this is $\theta = 1.188\ldots$, as given in Theorem 4.2.

4.4.4 Proof of Theorem 4.3

For $\delta > \frac{1}{6}$ the result follows from Theorem 4.1 so we assume that $\delta \leq \frac{1}{6}$. Since we do not require the result to be optimal we take

$$U = Q^{\frac{\delta}{2}}.$$

It is then sufficient to estimate Type II sums for

$$x^{\frac{1}{2}} \leq L \leq xQ^{-\frac{\delta}{2}}.$$

Since $x \leq Q$ we know that $L, M \leq Q$ so the hypotheses for Lemma 4.8 are satisfied and we get a bound

$$Q\left(Q^{\frac{2-\delta(k-1)}{4k}} x^{\frac{2k-1}{2k}} + x^{1-\frac{1}{4k}}\right) Q^{\epsilon}.$$

We may choose $k = k_0$ sufficiently large in terms of δ so that

$$2 - \delta(k_0 - 1) < 0.$$

Our Type II sum is therefore bounded by

$$Q\left(x^{1-\frac{1}{2k_0}} + x^{1-\frac{1}{4k_0}}\right)Q^{\epsilon} \ll Q^{1+\epsilon}x^{1-\frac{1}{4k_0}}.$$

We also require an estimate for a Type I sum with $L \leq Q^{\frac{\delta}{2}}$. From Lemma 4.11 such sums may be bounded by

$$\left(x + Q^{\frac{3+\delta}{2}}\right)Q^{\epsilon}.$$

Since $x \leq Q$ the second term in this estimate is larger. Furthermore $x \geq Q^{\frac{1}{2}+\delta}$ so

$$Q^{\frac{1+\delta}{2}} \leq x^{\frac{1+\delta}{1+2\delta}}.$$

We conclude that

$$\sum_{q\sim Q}\max_{(a;q)=1}|S_q(a;x)| \ll_{\delta,\epsilon} Q\left(x^{1-\frac{1}{4k_0}} + x^{\frac{1+\delta}{1+2\delta}}\right)Q^{\epsilon}.$$

Since this holds for any $\epsilon > 0$ the result follows on taking

$$\eta < \min(\frac{1}{4k_0}, \frac{\delta}{1+2\delta}).$$

4.4.5 Proof of Theorem 4.4

The sums arising from Vaughan's identity are now of the form

$$\sum_{q\sim Q}|W_{a,q}|.$$

We estimate the Type II sums using Lemma 4.9. Since $LM \asymp x$ this gives a bound

$$\left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}}\left(Qx^{\frac{1}{2}}L^{\frac{1}{2}} + Q^{\frac{1}{2}}x^{\frac{3}{2}}L^{-\frac{1}{4}}\right)(aQ)^{\epsilon}.$$

It is sufficient to estimate the Type II sums for $x^{\frac{1}{2}} \leq L \leq x/U$. In this range we get a bound of

$$\left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}}\left(QxU^{-\frac{1}{2}} + Q^{\frac{1}{2}}x^{\frac{11}{8}}\right)(aQ)^{\epsilon}.$$

Lemma 4.11 gives us a bound for the Type I sums with $L \leq U$ of $Q^{\frac{3}{2}+\epsilon}Ua^{\epsilon}$. We now choose

$$U = \min(x^{\frac{1}{3}}, Q^{-\frac{1}{3}}x^{\frac{2}{3}}).$$

Since $x \geq Q^{\frac{1}{2}}$ we have

$$1 \leq U \leq x^{\frac{1}{3}}.$$

This choice of U is therefore admissible and we get

$$\sum_{q \sim Q} |S_q(a;x)| \ll_\epsilon \left(1 + \frac{a}{xQ}\right)^{\frac{1}{2}} \left(Qx^{\frac{5}{6}} + Q^{\frac{7}{6}}x^{\frac{2}{3}} + Q^{\frac{1}{2}}x^{\frac{11}{8}}\right)(aQ)^\epsilon.$$

If $x \leq Q$ then

$$Qx^{\frac{5}{6}} \leq Q^{\frac{7}{6}}x^{\frac{2}{3}}$$

and if $x \geq Q$ then

$$Qx^{\frac{5}{6}} \leq Q^{\frac{1}{2}}x^{\frac{11}{8}}.$$

The term $Qx^{\frac{5}{6}}$ is therefore not necessary in our bound so Theorem 4.4 follows.

Chapter 5

The Divisor Function in Arithmetic Progressions to Smooth Moduli

5.1 Introduction

Given an arithmetic function $f(n)$ it is natural to consider the sum

$$\sum_{\substack{n\leq x\\ n\equiv a \,(\mathrm{mod}\, q)}} f(n).$$

For many functions f we might hope to show that when $(a;q)=1$ this is asymptotic to

$$\frac{1}{\varphi(q)} \sum_{\substack{n\leq x\\ (n;q)=1}} f(n).$$

In applications it is often essential that we establish such a result uniformly in $q \leq x^{\theta}$ with θ as large as possible.

In this chapter we will consider the divisor function $\tau(n)$. We therefore let

$$D(x,q,a) = \sum_{\substack{n\leq x\\ n\equiv a \,(\mathrm{mod}\, q)}} \tau(n)$$

and

$$D(x,q) = \frac{1}{\varphi(q)} \sum_{\substack{n\leq x\\ (n;q)=1}} \tau(n).$$

We then wish to estimate $E(x,q,a) = D(x,q,a) - D(x,q)$. We hope to show that for some $\delta > 0$ we have the bound

$$E(x,q,a) \ll \frac{x^{1-\delta}}{q}. \tag{5.1}$$

If $q \leq x^{2/3-\eta}$ for some $\eta > 0$ then (5.1) holds with a δ depending on η. This was proved independently in unpublished work of Hooley, Linnik and Selberg, it is a consequence of the Weil bound for Kloosterman sums. For larger q, no nontrivial bound is known for individual $E(x, q, a)$ but there are various results on average. For example Fouvry [20, Corollaire 5] showed that for any $\eta, A > 0$ and any $a \in \mathbb{Z}$ we have

$$\sum_{\substack{x^{2/3+\eta} \leq q \leq x^{1-\eta} \\ (q;a)=1}} |E(x, q, a)| \ll_{A,a,\eta} x(\log x)^{-A}.$$

An average over moduli $x^{2/3-\eta} \leq q \leq x^{2/3+\eta}$ was considered by Fouvry and Iwaniec in [21]. Their approach requires them to work only with moduli q which have a squarefree factor r of a certain size. Specifically, they show that if r is squarefree with $r \leq x^{3/8}$ and $(r; a) = 1$ then for any $\eta > 0$ we have

$$\sum_{\substack{rs^2 \leq x^{1-6\eta} \\ (s;ar)=1}} |E(x, rs, a)| \ll_{\eta} r^{-1}x^{1-\eta}.$$

Observe that to handle moduli $q = rs$ of size $x^{2/3}$ with this result it is necessary that $r \geq x^{1/3+6\eta}$. Further results are possible if we exploit averaging over the residue class $a \pmod q$. See for example Banks, Heath-Brown and Shparlinski [3] and Blomer [5].

We will show that (5.1) holds for an individual $E(x, q, a)$ for q almost as large as $x^{\frac{55}{82}}$ provided that q factorises in a certain way. This will follow by optimising the sizes of the parameters in the following result.

Theorem 5.1. *Suppose that $q = q_0q_1q_2q_3$ is squarefree and $(a; q) = 1$. For any $x \geq q$, $\delta \in (0, \frac{1}{12})$ and any $\epsilon > 0$ we have*

$$E(x, q, a) \ll q^{-1}x^{1-\delta+\epsilon} + x^{2\delta+\epsilon}\left(\sum_{j=1}^{3} x^{2^{-j-1}}q^{1/2-2^{-j}}q_{4-j}^{2^{-j}} + x^{1/16}q^{3/8}q_0^{1/16} + q^{1/2}q_0^{-1/16}\right),$$

where the implied constant depends only on ϵ.

It is not immediately clear when the estimate in this theorem is nontrivial. We therefore prove the following, in which we exploit the fact that if q is sufficiently smooth then we can find a suitable factorisation for which our bound is close to optimal.

Theorem 5.2. *Suppose $\varpi, \eta > 0$ satisfy*

$$246\varpi + 18\eta < 1.$$

There exists a $\delta > 0$, depending on ϖ and η, such that for any x^η-smooth, squarefree $q \leq x^{2/3+\varpi}$ and any $(a;q) = 1$ we have

$$E(x,q,a) \ll_{\varpi,\eta} q^{-1}x^{1-\delta}.$$

Observe that for any $\varpi < \frac{1}{246}$ this theorem shows that there is an $\eta > 0$ for which the conclusion holds. This means that we get a bound for sufficiently smooth q which are almost as large as $x^{\frac{55}{82}}$. The smoothness assumption is not necessary, it is simply a convenient way of guaranteeing that suitably sized factors exist. For example, given a squarefree $q \sim x^{2/3}$, Theorem 5.1 gives a nontrivial estimate provided that, for some $\eta > 0$, we have $q = q_0q_1q_2q_3$ with

$$x^\eta \leq q_0 \leq x^{1/3-\eta}$$

and

$$q_j \leq x^{1/6-\eta} \text{ for } 1 \leq j \leq 3.$$

Writing

$$e_q(x) = e^{\frac{2\pi ix}{q}}, \tag{5.2}$$

the proof of Theorem 5.1 depends on estimates for short Kloosterman sums

$$\sum_{\substack{n\in I\\(n;q)=1}} e_q(b\overline{n}),$$

where b is an integer and I is an interval of length $O(\sqrt{x})$. If $(b;q) = 1$ then the Weil bound, Lemma 4.5, gives an estimate of $O_\epsilon(q^{1/2+\epsilon})$ for such a sum. For the sizes of x and q in which we are interested this is a significant saving over the trivial bound of $\sqrt{x}$. In particular it is enough to estimate $E(x,q,a)$ if $q \leq x^{2/3-\eta}$. For larger q we must improve upon the Weil estimate. This is achieved for special q by means of the following result.

Theorem 5.3. *Let $q = q_0q_1 \dots q_l$ be squarefree. Suppose that $(a;q) = 1$ and that I is an interval of length at most $N \leq q$. Let*

$$S = \sum_{\substack{n\in I\\(n;q)=1}} e_q(a\overline{n}). \tag{5.3}$$

For any $\epsilon > 0$ we have

$$S \ll_{\epsilon,l} q^\epsilon \left(\sum_{j=1}^{l} N^{2^{-j}} q^{1/2-2^{-j}} q_{l-j+1}^{2^{-j}} + N^{2^{-l}} q^{1/2-2^{-l}} q_0^{1/2^{l+1}} + q^{1/2} q_0^{-1/2^{l+1}} \right).$$

This theorem is very similar to that of Heath-Brown [33, Theorem 2]. His result can be applied to our sum S to obtain the bound

$$S \ll_{\epsilon,l} q^{\epsilon} \left(\sum_{j=1}^{l} N^{1-2^{-j}} q_{l-j+1}^{2^{-j}} + N^{1-2^{-l}} q_0^{1/2^{l+1}} + N q_0^{-1/2^{l+1}} \right).$$

When the sizes of the factors q_j are chosen optimally this result of Heath-Brown is nontrivial provided that N is approximately $q^{\frac{1}{l+1}}$. In contrast, our bound is most useful when $N \approx q^{1-\frac{1}{l+1}}$ in which case it can improve on the Weil bound.

As in Heath-Brown's work our proof of Theorem 5.3 uses the q-analogue of van der Corput's method. We begin by completing the sum S and then apply the differencing process l times, whereas Heath-Brown applied differencing directly to S. The result is a sum of products of 2^l Kloosterman sums which we estimate by another completion followed by the application of a bound for complete exponential sums due to Fouvry, Kowalski and Michel [23]. In other words, our result is a q-analogue of the BA^lB van der Corput estimate whereas Heath-Brown's is analogous to A^lB. A q-analogue of BA^2B was used by Heath-Brown in [35] but the exponential sums in that work are not Kloosterman sums.

The assumption that q is squarefree is important for two reasons. Firstly, it guarantees that the factors q_j are coprime in pairs, thereby avoiding many unpleasant technicalities. Secondly, it means that we need only consider complete exponential sums to prime moduli. To handle q which are not squarefree Lemma 5.7 would have to be generalised to prime-power moduli.

5.2 Proof of Theorem 5.1

In this section we will show that Theorem 5.1 follows from Theorem 5.3. Recall that we wish to estimate

$$E(x,q,a) = \sum_{\substack{uv \le x \\ uv \equiv a \,(\mathrm{mod}\, q)}} 1 - \frac{1}{\varphi(q)} \sum_{\substack{uv \le x \\ (uv;q)=1}} 1.$$

By a dyadic subdivision it is enough to consider each of the $O((\log x)^2)$ sums of the form

$$E_1(U,V,q,a) = \sum_{\substack{u\sim U, v\sim V \\ uv \le x, uv \equiv a \,(\mathrm{mod}\, q)}} 1 - \frac{1}{\varphi(q)} \sum_{\substack{u\sim U, v\sim V \\ uv \le x, (uv;q)=1}} 1 = D_1(U,V,q,a) - D_1(U,V,q),$$

say. We must bound $E_1(U, V, q, a)$ for all $U, V \geq 1$ for which $UV \leq x$. However, by symmetry we can assume that $U \leq \sqrt{x}$.

We will use a short interval decomposition to remove the constraint $uv \leq x$ from $D_1(U, V, q, a)$ and $D_1(U, V, q)$. Specifically we divide the range $u \sim U$ into $O(x^\delta)$ intervals of length $Ux^{-\delta}$ and the range $v \sim V$ into $O(x^\delta)$ intervals of length $Vx^{-\delta}$. We will denote the resulting intervals by

$$I_1(U_1) = [U_1, U_1 + Ux^{-\delta})$$

and

$$I_2(V_1) = [V_1, V_1 + Vx^{-\delta}).$$

We only need consider the case that $U_1V_1 \leq x$. Dropping the constraint $uv \leq x$ has the effect of including in the above sums points $(u, v) \in I_1(U_1) \times I_2(V_1)$ with

$$x < uv \leq (U_1 + Ux^{-\delta})(V_1 + Vx^{-\delta}) \leq x + O(x^{1-\delta}).$$

It follows that the errors introduced by removing the constraint are bounded by

$$\sum_{\substack{x < n \leq x + O(x^{1-\delta}) \\ n \equiv a \,(\mathrm{mod}\, q)}} \tau(n) \ll_\epsilon q^{-1} x^{1-\delta+\epsilon}$$

and

$$\frac{1}{\varphi(q)} \sum_{\substack{x < n \leq x + O(x^{1-\delta}) \\ (n;q)=1}} \tau(n) \ll_\epsilon q^{-1} x^{1-\delta+\epsilon}.$$

We conclude that it is enough to bound $O(x^{2\delta}(\log x)^2)$ sums of the form

$$E_2(U_1, V_1, q, a) = D_2(U_1, V_1, q, a) - D_2(U_1, V_1, q)$$

where

$$D_2(U_1, V_1, q, a) = \#\{u \in I_1(U_1), v \in I_2(V_1) : uv \equiv a \,(\mathrm{mod}\, q)\}$$

and

$$D_2(U_1, V_1, q) = \frac{1}{\varphi(q)} \#\{u \in I_1(U_1), v \in I_2(V_1) : (uv; q) = 1\}.$$

Specifically we have

$$E(x, q, a) \ll_\epsilon q^{-1} x^{1-\delta+\epsilon} + x^{2\delta+\epsilon} \max_{U_1, V_1} |E_2(U_1, V_1, q, a)|.$$

We now write

$$\begin{aligned} D_2(U_1,V_1,q,a) &= \sum_{\substack{u\in I_1(U_1),v\in I_2(V_1)\\ uv\equiv a\,(\mathrm{mod}\,q)}} 1 \\ &= \sum_{\substack{u\in I_1(U_1)\\ (u;q)=1}} \sum_{\substack{v\in I_2(V_1)\\ v\equiv a\overline{u}\,(\mathrm{mod}\,q)}} 1 \\ &= \frac{1}{q}\sum_{\substack{u\in I_1(U_1)\\ (u;q)=1}} \sum_{v\in I_2(V_1)} \sum_{k=1}^{q} e_q(k(a\overline{u}-v)) \\ &= \frac{1}{q}\sum_{k=1}^{q}\left(\sum_{\substack{u\in I_1(U_1)\\ (u;q)=1}} e_q(ak\overline{u})\right)\left(\sum_{v\in I_2(V_1)} e_q(-kv)\right). \end{aligned}$$

The $k=q$ terms in this are

$$\frac{1}{q}\#\{u\in I_1(U_1):(u;q)=1\}\#I_2(V_1).$$

On the other hand

$$\begin{aligned} D_2(U_1,V_1,q) &= \frac{1}{\varphi(q)}\sum_{\substack{u\in I_1(U_1)\\ (u;q)=1}} \sum_{\substack{v\in I_2(V_1)\\ (v;q)=1}} 1 \\ &= \frac{1}{\varphi(q)}\sum_{\substack{u\in I_1(U_1)\\ (u;q)=1}} \left(\frac{\varphi(q)}{q}\#I_2(V_1)+O_\epsilon(q^\epsilon)\right) \\ &= \frac{1}{q}\#\{u\in I_1(U_1):(u;q)=1\}\#I_2(V_1)+O_\epsilon(q^{-1+\epsilon}x^{1/2}), \end{aligned}$$

where we have used our assumption that $U\le\sqrt{x}$. Since $\delta<\frac{1}{6}$ and $q\le x$ we have

$$x^{2\delta}\cdot q^{-1+\epsilon}x^{1/2} < q^{-1}x^{1-\delta+\epsilon}$$

so we conclude that the $k=q$ terms correspond to $D_2(U_1,V_1,q)$ with a sufficiently small error.

It remains to bound

$$\frac{1}{q}\sum_{k=1}^{q-1}\left|\sum_{\substack{u\in I_1(U_1)\\ (u;q)=1}} e_q(ak\overline{u})\right|\left|\sum_{v\in I_2(V_1)} e_q(-kv)\right|.$$

We write this as

$$\frac{1}{q}\sum_{d|q}\sum_{\substack{k=1\\(k;q)=d}}^{q-1}\left|\sum_{\substack{u\in I_1(U_1)\\(u;q)=1}}e_q(ak\overline{u})\right|\left|\sum_{v\in I_2(V_1)}e_q(-kv)\right|$$

$$=\frac{1}{q}\sum_{\substack{d|q\\d<q}}\sum_{k\,(\mathrm{mod}\,q/d)}^{\star}\left|\sum_{\substack{u\in I_1(U_1)\\(u;q)=1}}e_{q/d}(ak\overline{u})\right|\left|\sum_{v\in I_2(V_1)}e_{q/d}(-kv)\right|,$$

where $\sum^{\star}$ denotes that the summation is restricted to residue classes coprime to the modulus. However, since q is squarefree we have

$$\begin{aligned}\sum_{\substack{u\in I_1(U_1)\\(u;q)=1}}e_{q/d}(ak\overline{u}) &= \sum_{\substack{u\in I_1(U_1)\\(u;q/d)=1}}e_{q/d}(ak\overline{u})\sum_{e|(d;u)}\mu(e)\\ &= \sum_{e|d}\mu(e)\sum_{\substack{u\in I_1(U_1)/e\\(u;q/d)=1}}e_{q/d}(ak\overline{eu}).\end{aligned}$$

Our sum is therefore bounded by

$$\frac{1}{q}\sum_{\substack{d|q\\d<q}}\sum_{k\,(\mathrm{mod}\,q/d)}^{\star}\left|\sum_{v\in I_2(V_1)}e_{q/d}(-kv)\right|\sum_{e|d}\left|\sum_{\substack{u\in I_1(U)/e\\(u;q/d)=1}}e_{q/d}(ak\overline{eu})\right|.$$

We have the standard estimate

$$\sum_{v\in I_2(V_1)}e_{q/d}(-kv)\ll\min\left(Vx^{-\delta},\frac{1}{\|dk/q\|}\right)$$

so that this is at most

$$\frac{1}{q}\sum_{\substack{d|q\\d<q}}\sum_{e|d}\max_{(b;q/d)=1}\left|\sum_{\substack{u\in I_1(U)/e\\(u;q/d)=1}}e_{q/d}(b\overline{u})\right|\sum_{k\,(\mathrm{mod}\,q/d)}^{\star}\frac{1}{\|dk/q\|}$$

$$\ll_{\epsilon}q^{\epsilon}\sum_{\substack{d|q\\d<q}}\frac{1}{d}\sum_{e|d}\max_{(b;q/d)=1}\left|\sum_{\substack{u\in I_1(U)/e\\(u;q/d)=1}}e_{q/d}(b\overline{u})\right|.$$

To estimate the contribution to this from $d \geq qx^{-2/3+2\delta}$ we apply the Weil bound, Lemma 4.5, which gives

$$\max_{(b;q/d)=1} \left| \sum_{\substack{u \in I_1(U_1)/e \\ (u;q/d)=1}} e_{q/d}(b\overline{u}) \right| \ll_\epsilon (q/d)^\epsilon \left(\frac{Ux^{-\delta}d}{qe} + (q/d)^{1/2} \right).$$

The contribution to our sum from such d is therefore bounded by

$$q^\epsilon \sum_{\substack{d|q \\ qx^{-2/3+2\delta} \leq d < q}} (\frac{Ux^{-\delta}}{q} + q^{1/2}/d^{3/2}) \ll_\epsilon q^\epsilon (Ux^{-\delta}q^{-1} + q^{-1}x^{1-3\delta}).$$

The contribution of these d to $E(x,q,a)$ is therefore $O_\epsilon(q^{-1}x^{1-\delta+\epsilon})$. If $q < x^{2/3-2\delta}$ then this analysis covers all values of d and therefore completes the proof.

If $q \geq x^{2/3-2\delta}$ and $d < qx^{-2/3+2\delta}$ we apply Theorem 5.3 with $l = 3$ and the factorisation

$$\frac{q}{d} = \prod_{j=0}^{3} \frac{q_j}{(q_j; d)},$$

which holds since q is squarefree. We have

$$\frac{q}{d} \geq x^{2/3-2\delta} \geq \sqrt{x},$$

since $\delta < \frac{1}{12}$. We may therefore deduce that if $(b; q/d) = 1$ then

$$\frac{1}{d} \sum_{\substack{u \in I_1(U)/e \\ (u;q/d)=1}} e_{q/d}(b\overline{u}) \ll_\epsilon q^\epsilon \left(\sum_{j=1}^{3} x^{2^{-j-1}} q^{1/2-2^{-j}} q_{4-j}^{2^{-j}} + x^{1/16} q^{3/8} q_0^{1/16} + q^{1/2} q_0^{-1/16} \right).$$

It follows that we have

$$q^\epsilon \sum_{\substack{d|q \\ d < qx^{-2/3+2\delta}}} \frac{1}{d} \sum_{e|d} \max_{(b;q/d)=1} \left| \sum_{\substack{u \in I_1(U)/e \\ (u;q/d)=1}} e_{q/d}(b\overline{u}) \right|$$

$$\ll_\epsilon q^\epsilon \left(\sum_{j=1}^{3} x^{2^{-j-1}} q^{1/2-2^{-j}} q_{4-j}^{2^{-j}} + x^{1/16} q^{3/8} q_0^{1/16} + q^{1/2} q_0^{-1/16} \right).$$

We conclude that the contribution of this to $E(x,q,a)$ is majorised by

$$x^{2\delta+\epsilon} \left(\sum_{j=1}^{3} x^{2^{-j-1}} q^{1/2-2^{-j}} q_{4-j}^{2^{-j}} + x^{1/16} q^{3/8} q_0^{1/16} + q^{1/2} q_0^{-1/16} \right).$$

This completes the proof of Theorem 5.1.

5.3 Proof of Theorem 5.2

Suppose ϖ, η, q and a are as in Theorem 5.2. Let $\delta > 0$ be a parameter which we will eventually choose to be very small. We may suppose that $q \geq x^{2/3-2\delta}$ since the result is known for smaller q. Applying Theorem 5.1 we deduce that for any $\epsilon > 0$ we have

$$E(x,q,a) \ll q^{-1}x^{1-\delta+\epsilon} + x^{2\delta+\epsilon}\left(\sum_{j=1}^{3} x^{2^{-j-1}} q^{1/2-2^{-j}} q_{4-j}^{2^{-j}} + x^{1/16}q^{3/8}q_0^{1/16} + q^{1/2}q_0^{-1/16}\right),$$

with an implied constant which depends only on ϵ. The first term in this is sufficiently small. We optimise the remaining terms by working with a factorisation for which $q_j \approx Q_j$ with

$$Q_0 = q^{-2/15}x^{1/3},$$

$$Q_1 = q^{-1/15}x^{1/6},$$

$$Q_2 = q^{7/15}x^{-1/6}$$

and

$$Q_3 = q^{11/15}x^{-1/3}.$$

Observe that $Q_0Q_1Q_2Q_3 = q$ and that for all sufficiently small δ we have $Q_j > x^{1/18} > x^{\eta}$ for all j. Since q is x^{η}-smooth we may find a factorisation $q = q_0q_1q_2q_3$ with

$$q_1 \in [Q_1x^{-\eta/5}, Q_1x^{4\eta/5}],$$

$$q_2 \in [Q_2x^{-3\eta/5}, Q_2x^{2\eta/5}],$$

$$q_3 \in [Q_3x^{-4\eta/5}, Q_3x^{\eta/5}]$$

so that

$$q_0 \in [Q_0x^{-7\eta/5}, Q_0x^{8\eta/5}].$$

This gives

$$E(x,q,a) \ll_{\epsilon} q^{-1}x^{1-\delta+\epsilon} + x^{2\delta+\epsilon}\left(x^{1/12+\eta/10}q^{11/30} + x^{-1/48+7\eta/80}q^{61/120}\right).$$

Finally, recalling that $q \leq x^{2/3+\varpi}$, we get

$$\begin{aligned} E(x,q,a) &\ll_{\epsilon} q^{-1}x^{1-\delta+\epsilon} + q^{-1}x^{2\delta+\epsilon}\left(x^{1/12+\eta/10}q^{41/30} + x^{-1/48+7\eta/80}q^{181/120}\right) \\ &\ll_{\epsilon} q^{-1}x^{1-\delta+\epsilon} + q^{-1}x^{2\delta+\epsilon}\left(x^{\frac{179+18\eta+246\varpi}{180}} + x^{\frac{709+63\eta+1086\varpi}{720}}\right). \end{aligned}$$

We know that

$$246\varpi + 18\eta < 1.$$

In particular $\varpi < \frac{1}{246}$ and $\eta < \frac{1}{18}$ so

$$63\eta + 1086\varpi < \frac{649}{82} < 8.$$

Theorem 5.2 therefore follows on taking δ and ϵ sufficiently small in terms of ϖ and η.

5.4 Proof of Theorem 5.3

If we have $[q/N] < q_{l-j+1}$, for some $1 \leq j \leq l$, then

$$q^{\epsilon} N^{2^{-j}} q^{1/2-2^{-j}} q_{l-j+1}^{2^{-j}} \gg q^{1/2+\epsilon}.$$

Our result therefore follows from the Weil bound. We may therefore assume, for the remainder of the chapter, that $[q/N] \geq q_j$ for all $1 \leq j \leq l$.

5.4.1 Completion of S

Let $f(k)$ be the Fourier transform of the interval I:

$$f(k) = \sum_{n \in I} e_q(-nk),$$

where e_q was defined in (5.2).

Recall the definition, (5.3), of S. We have

$$S = \frac{1}{q} \sum_{k \,(\mathrm{mod}\, q)} f(k) S(a, k, q)$$

where $S(a, k, q)$ is the Kloosterman sum given by

$$S(a, k, q) = \sum_{n \,(\mathrm{mod}\, q)}^{\star} e_q(a\overline{n} + kn).$$

Since $f(0) \ll N$ and $S(a, 0, q) = \mu(q) \ll 1$ we get

$$S \ll \frac{N}{q} + \frac{1}{q} \left| \sum_{k \neq 0 \,(\mathrm{mod}\, q)} f(k) S(a, k, q) \right|.$$

The term N/q is clearly small enough.

We may assume that $I \subseteq [M, M+N)$ for some integer M. We then write

$$f(k) = e_q(-kM) \sum_{\substack{n<N \\ n+M\in I}} e_q(-kn) = e_q(-kM)g(k),$$

where

$$g(k) = \sum_{\substack{n<N \\ n+M\in I}} e_q(-kn)$$

is a function on $\mathbb{Z}/q\mathbb{Z}$ which extends to a differentiable function on $(-q/2, q/2)$. Thus

$$S \ll \frac{N}{q} + \frac{1}{q}\left|\sum_{k\neq 0 \,(\mathrm{mod}\, q)} g(k)e_q(-kM)S(a,k,q)\right|.$$

We will consider the contribution to this bound from $0 < k \leq q/2$. One can use a completely analogous treatment for the range $-q/2 < k < 0$.

We wish to remove the weight $g(k)$. We have the standard estimate

$$g(k) \ll \min\left(N, \frac{1}{\|k/q\|}\right) = \min\left(N, \frac{q}{k}\right).$$

In addition

$$g'(k) = -2\pi i \sum_{\substack{n<N \\ n+M\in I}} \frac{n}{q} e_q(-kn) \ll \frac{N}{q}\min\left(N, \frac{q}{k}\right).$$

We will split the sum over k into intervals on which we may remove $g(k)$ by partial summation. Specifically, let $K = [q/N]$ and

$$S(r) = \max_{0\leq L\leq K}\left|\sum_{(r-1)K<k\leq(r-1)K+L} e_q(-Mk)S(a,k,q)\right| \qquad (r = 1, 2, 3, \ldots).$$

Summing by parts we get, for any $K' \leq K$ that

$$\sum_{(r-1)K\leq k\leq(r-1)K+K'} g(k)e_q(-Mk)S(a,k,q) \ll S(r)\min\left(N, \frac{q}{(r-1)K}\right) \ll \frac{N}{r}S(r).$$

It is therefore sufficient to estimate

$$\frac{N}{q}\sum_{r\ll N}\frac{S(r)}{r}$$

which we accomplish by bounding each $S(r)$ individually. We will prove the following, which easily implies Theorem 5.3.

Lemma 5.4. *Under the hypotheses of Theorem 5.3 and with $K, S(r)$ as above we have*

$$S(r) \ll_{\epsilon,l} q^{1/2+\epsilon}\left(\sum_{j=1}^{l} K^{1-2^{-j}} q_{l-j+1}^{2^{-j}} + K^{1-2^{-l}} q_0^{1/2^{l+1}} + K q_0^{-1/2^{l+1}}\right).$$

5.4.2 Differencing the Sum $S(r)$

In what follows we will require the multiplicative property of Kloosterman sums. This states that for any integers a, b and any $q_0, q_1 \in \mathbb{N}$ with $(q_0; q_1) = 1$ we have

$$S(a, b, q_0 q_1) = S(a\overline{q_1}, b\overline{q_1}, q_0) S(a\overline{q_0}, b\overline{q_0}, q_1).$$

It can be proved using the Chinese Remainder Theorem. In addition, if $(c; q_0) = 1$ then we have the identity

$$S(a, b, q_0) = S(ac, b\overline{c}, q_0).$$

In the remainder of the chapter we will frequently use without comment the fact that, since q is squarefree, any pair of integers q', q'' with $q'q''|q$ must be coprime. We now apply a q-analogue of the van der Corput A-process. Let J be an interval whose length is bounded above by K. Suppose $(a; q) = 1$ and $s_1, \dots, s_j$ are integers, for some $j \geq 1$. We consider the more general sum

$$T = \sum_{k \in J} e_q(-Mk) \prod_{i=1}^{j} S(a, k + s_i, q)$$

in which the value of M may differ from that in $S(r)$. The sums $S(r)$ correspond to the case $j = 1$ and $s_1 = 0$ of this. The following lemma describes a single van der Corput differencing step applied to the sum T. Note that the quantities q, q_0, q_1 occurring need not correspond to those in Theorem 5.3.

Lemma 5.5. *Suppose $q = q_0 q_1$ with $q_1 \leq K$, $(q_0; q_1) = 1$ and $(a; q) = 1$. We have*

$$T^2 \ll_{\epsilon, j} q^{\epsilon} q_1^{j+1} \left(K q_0^j + \sum_{0 < |h| \leq K/q_1} \left| \sum_{k \in J(h)} \prod_{i=1}^{j} S(a', k + s_i, q_0) S(a', k + q_1 h + s_i, q_0) \right| \right)$$

where $J(h)$ is an interval of length at most K which depends on h, and where $a' = a(\overline{q}_1)^2$.

Proof. We let $H = [K/q_1] \geq 1$ and

$$a_k = \begin{cases} e_q(-Mk) \prod_{i=1}^{j} S(a, k + s_i, q) & k \in J \\ 0 & k \notin J. \end{cases}$$

Since $H \geq 1$ we have

$$\begin{aligned} T &= \sum_k a_k \\ &= \frac{1}{H} \sum_{h=1}^{H} \sum_k a_{k+q_1 h} \\ &= \frac{1}{H} \sum_k \sum_{h=1}^{H} a_{k+q_1 h}. \end{aligned}$$

If $k + q_1 h \in J$ then, since $(q_0; q_1) = 1$,

$$\begin{aligned} a_{k+q_1 h} &= e_q(-M(k+q_1 h)) \prod_{i=1}^{j} S(a, k+q_1 h + s_i, q) \\ &= e_q(-Mk) e_q(-Mq_1 h) \prod_{i=1}^{j} S(a\overline{q}_1, (k+q_1 h + s_i)\overline{q}_1, q_0) S(a\overline{q}_0, (k+s_i)\overline{q}_0, q_1). \end{aligned}$$

Since $q_1 H \leq K$ the sum over k is supported on an interval of length bounded by $O(K)$. By the Weil bound we get

$$S(a\overline{q}_0, (k+s_i)\overline{q}_0, q_1) \ll_\epsilon q_1^{1/2+\epsilon}.$$

Therefore, applying Cauchy's inequality, we obtain

$$H^2 T^2 \ll_{\epsilon, j} K q_1^{j+\epsilon} \sum_k \left| \sum_{\substack{h=1 \\ k+q_1 h \in J}}^{H} e_q(-Mq_1 h) \prod_{i=1}^{j} S(a\overline{q}_1, (k+q_1 h + s_i)\overline{q}_1, q_0) \right|^2.$$

Letting $a' = a(\overline{q}_1)^2$, as in the statement of the lemma, we have $(a'; q) = 1$ and

$$H^2 T^2 \ll_{\epsilon, j} K q_1^{j+\epsilon} \sum_k \left| \sum_{\substack{h=1 \\ k+q_1 h \in J}}^{H} e_q(-Mq_1 h) \prod_{i=1}^{j} S(a', k+q_1 h + s_i, q_0) \right|^2.$$

Expanding the square and reordering we deduce that

$$\begin{aligned} H^2T^2 & \\ \ll_{\epsilon,j} \quad & Kq_1^{j+\epsilon} \sum_{h_1,h_2=1}^{H} \left| \sum_{\substack{k \\ k+q_1h_1,k+q_1h_2 \in J}} \prod_{i=1}^{j} S(a',k+q_1h_1+s_i,q_0)S(a',k+q_1h_2+s_i,q_0) \right| \\ = \quad & Kq_1^{j+\epsilon} \sum_{h_1,h_2=1}^{H} \left| \sum_{\substack{k\in J \\ k+q_1(h_2-h_1)\in J}} \prod_{i=1}^{j} S(a',k+s_i,q_0)S(a',k+q_1(h_2-h_1)+s_i,q_0) \right| \\ \leq \quad & KHq_1^{j+\epsilon} \sum_{|h|\leq H} \left| \sum_{\substack{k\in J \\ k+q_1h\in J}} \prod_{i=1}^{j} S(a',k+s_i,q_0)S(a',k+q_1h+s_i,q_0) \right|. \end{aligned}$$

We estimate the $h = 0$ term using the Weil bound on the individual Kloosterman sums to get

$$HT^2 \ll_{\epsilon,j} q^{\epsilon}Kq_1^j \left(Kq_0^j + \sum_{0<|h|\leq H} \left| \sum_{\substack{k\in J \\ k+q_1h\in J}} \prod_{i=1}^{j} S(a',k+s_i,q_0)S(a',k+q_1h+s_i,q_0) \right| \right).$$

The result follows. □

The previous lemma bounds T in terms of sums with twice as many Kloosterman factors. The new shifts are $s_1,\dots,s_j,s_1+q_1h,\dots,s_j+q_1h$, and the exponential $e_q(-kM)$, if it exists, is removed. We will apply it l times, starting at the sum

$$T = \sum_{k\in J} e_q(-Mk)S(a,k,q).$$

For the remainder of the chapter T will refer to this particular $j = 1$ case of the above T whereas $T(\dots)$ will be one of the more general sums.

Lemma 5.6. *Let q be as in Theorem 5.3 and T as defined above. We have*

$$\begin{aligned} T^{2^l} \quad \ll_{\epsilon,l} \quad & q^{\epsilon} \Bigg(q^{2^{l-1}} \sum_{j=1}^{l} K^{2^l-2^{l-j}} q_{l-j+1}^{2^{l-j}} \\ & \qquad + K^{2^l-l-1} \left(q/q_0\right)^{2^{l-1}+1} \sum_{0<|h_1|\leq K/q_1} \cdots \sum_{0<|h_l|\leq K/q_l} |T(h_1,\dots,h_l)| \Bigg) \end{aligned}$$

where

$$T(h_1,\dots,h_l)=\sum_{k\in J(h_1,\dots,h_l)}\prod_{I\subseteq\{1,\dots,l\}}S\left(a',k+\sum_{i\in I}q_ih_i,q_0\right),$$

with $J(h_1,\dots,h_l)$ an interval of length at most K and $(a';q)=1$. The product over I includes $I=\emptyset$.

Proof. Observe that by our assumption that $[q/N]\geq q_i$ we know that $K\geq q_i$ for $1\leq i\leq l$. This means that the applications of Lemma 5.5 in the following proof are all justified.

We use induction in l. If $l=1$ then applying Lemma 5.5 gives

$$T^2\ll_\epsilon q^\epsilon\left(qKq_1+q_1^2\sum_{0<|h_1|\leq K/q_1}\left|\sum_{k\in J(h_1)}S(a',k,q_0)S(a',k+q_1h_1,q_0)\right|\right),$$

as required.

Now suppose $l>1$ and that the result holds for $l-1$. We assume that $q=q_0q_1\dots q_l$ and apply the inductive hypothesis with the factorisation

$$q=r_0r_1\dots r_{l-1}$$

where $r_0=q_0q_1$, and $r_i=q_{i+1}$ for $1\leq i\leq l-1$. This results in

$$\begin{aligned}T^{2^{l-1}}\quad\ll_{\epsilon,l}\quad & q^\epsilon\left(q^{2^{l-2}}\sum_{j=1}^{l-1}K^{2^{l-1}-2^{l-1-j}}q_{l-j+1}^{2^{l-1-j}}\right.\\&\left.+K^{2^{l-1}-l}\left(q/q_0q_1\right)^{2^{l-2}+1}\sum_{0<|h_2|\leq K/q_2}\dots\sum_{0<|h_l|\leq K/q_l}|T(h_2,\dots,h_l)|\right)\end{aligned}$$

with

$$T(h_2,\dots,h_l)=\sum_{k\in J(h_2,\dots,h_l)}\prod_{I\subseteq\{2,\dots,l\}}S\left(a',k+\sum_{i\in I}q_ih_i,q_0q_1\right).$$

Squaring our bound, using Cauchy's inequality on the final sum, we get

$$\begin{aligned}T^{2^l}\quad\ll_{\epsilon,l}\quad & q^\epsilon\left(q^{2^{l-1}}\sum_{j=1}^{l-1}K^{2^l-2^{l-j}}q_{l-j+1}^{2^{l-j}}\right.\\&\left.+K^{2^l-l-1}\left(q/q_0q_1\right)^{2^{l-1}+1}\sum_{0<|h_2|\leq K/q_2}\dots\sum_{0<|h_l|\leq K/q_l}|T(h_2,\dots,h_l)|^2\right).\end{aligned}$$

We now use Lemma 5.5 with $j = 2^{l-1}$ to obtain

$$T(h_2,\dots,h_l)^2 \ll_{\epsilon,l} q^{\epsilon} q_1^{2^{l-1}+1}\left(Kq_0^{2^{l-1}} + \sum_{0<|h_1|\le K/q_1} |T(h_1,\dots,h_l)|\right)$$

where

$$\begin{aligned} &T(h_1,\dots,h_l)\\ &= \sum_{k\in J(h_1,\dots,h_l)} \prod_{I\subseteq\{2,\dots,l\}} S\left(a'', k+\sum_{i\in I} q_i h_i, q_0\right) S\left(a'', k+\sum_{i\in I} q_i h_i + q_1 h_1, q_0\right)\\ &= \sum_{k\in J(h_1,\dots,h_l)} \prod_{I\subseteq\{1,\dots,l\}} S\left(a'', k+\sum_{i\in I} q_i h_i, q_0\right), \end{aligned}$$

for some $(a'';q) = 1$. Observe that this corresponds precisely to the $T(h_1,\dots,h_l)$ given in the claim.

We conclude that

$$\begin{aligned} T^{2^l} \ll_{\epsilon,l}\ & q^{\epsilon}\left(q^{2^{l-1}}\sum_{j=1}^{l-1} K^{2^l-2^{l-j}} q_{l-j+1}^{2^{l-j}} + K^{2^l-1}\left(q/q_0q_1\right)^{2^{l-1}} q_1^{2^{l-1}+1} q_0^{2^{l-1}}\right.\\ &\qquad \left. + K^{2^l-l-1}\left(q/q_0\right)^{2^{l-1}+1} \sum_{0<|h_1|\le K/q_1} \cdots \sum_{0<|h_l|\le K/q_l} |T(h_1,\dots,h_l)|\right)\\ =\ & q^{\epsilon}\left(q^{2^{l-1}}\sum_{j=1}^{l} K^{2^l-2^{l-j}} q_{l-j+1}^{2^{l-j}}\right.\\ &\qquad \left. + K^{2^l-l-1}\left(q/q_0\right)^{2^{l-1}+1} \sum_{0<|h_1|\le K/q_1} \cdots \sum_{0<|h_l|\le K/q_l} |T(h_1,\dots,h_l)|\right). \end{aligned}$$

□

5.4.3 Estimating $T(h_1,\dots,h_l)$

It remains to estimate

$$T(h_1,\dots,h_l) = \sum_{k\in J(h_1,\dots,h_l)} \prod_{I\subseteq\{1,\dots,l\}} S\left(a', k+\sum_{i\in I} q_i h_i, q_0\right),$$

where $(a';q_0) = 1$.

We begin with the following estimate for complete exponential sums to a prime modulus.

Lemma 5.7. *Let p be a prime, $(a;p)=1$ and let $s_1,\dots,s_j,b$ be integers. We have*

$$\sum_{k \,(\mathrm{mod}\, p)} e_p(-kb)\prod_{i=1}^{j} S(a,k+s_i,p) \ll_j \begin{cases} p^{\frac{j+2}{2}} & b=0 \text{ and } E(s_1,\dots,s_j) \\ p^{\frac{j+1}{2}} & \text{otherwise,} \end{cases}$$

where $E(s_1,\dots,s_j)$ denotes the property that all the s_i occur with even multiplicity modulo p.

Proof. The first part follows directly from the Weil bound

$$|S(a,k+s_i,p)| \le 2\sqrt{p}.$$

For the second part we use a result of Fouvry, Kowalski and Michel [23, Corollary 3.3]. Let

$$\mathrm{Kl}_2(a;p) = \frac{S(a,1,p)}{p^{1/2}}.$$

If $k \not\equiv 0 \,(\mathrm{mod}\, p)$ then

$$S(a,k,p) = p^{1/2}\,\mathrm{Kl}_2(ak;p).$$

We therefore have

$$\sum_{k \,(\mathrm{mod}\, p)} e_p(-kb)\prod_{i=1}^{j} S(a,k+s_i,p)$$

$$= p^{j/2} \sum_{\substack{k \,(\mathrm{mod}\, p) \\ k+s_i \not\equiv 0 \,(\mathrm{mod}\, p)}} e_p(-kb)\prod_{i=1}^{j} \mathrm{Kl}_2(a(k+s_i));p) + O(jp^{j/2}),$$

where the error comes from the terms with $k+s_i \equiv 0 \,(\mathrm{mod}\, p)$, for which we can use the Weil bound.

We identify $\mathbb{F}_p$ with the projective line minus the point at infinity. The group $\mathrm{PGL}_2(\mathbb{F}_p)$ has a natural action on the projective line so we can talk about its action on $\mathbb{F}_p$, provided that care is taken with points which map to ∞. The maps $k \mapsto a(k+s_i)$ then correspond to members of $\mathrm{PGL}_2(\mathbb{F}_p)$. If $s_i \not\equiv s_j \,(\mathrm{mod}\, p)$ then $k \mapsto a(k+s_i)$ and $k \mapsto a(k+s_j)$ correspond to different elements.

We now use [23, Corollary 3.3] which states that if $\beta_1,\dots,\beta_j \in \mathrm{PGL}_2(\mathbb{F}_p)$ then, provided the multiplicities of the β_i are not all even, we have

$$\sum_{\substack{k \,(\mathrm{mod}\, p) \\ \beta_i k \neq 0,\infty}} e_p(-kb)\prod_{i=1}^{j} \mathrm{Kl}_2(\beta_i k;p) \ll_j p^{1/2}.$$

□

We use this in conjunction with the following combinatorial result.

Lemma 5.8. *Let $p \geq 3$ be prime and let $h_1, \dots, h_l \in \mathbb{F}_p$. Suppose that the 2^l sums*

$$\sum_{i \in I} h_i \text{ for } I \subseteq \{1, \dots, l\}$$

form a list of elements all of whose entries have even multiplicities. At least one of the h_i must then be 0.

Proof. Let $\omega = e_p(1)$ and consider the algebraic integer $\alpha \in \mathbb{Z}[\omega]$ given by

$$\alpha = \prod_{i=1}^{l} \left(1 + \omega^{h_i}\right) = \sum_{I \subseteq \{1,\dots,l\}} \omega^{\sum_{i \in I} h_i}.$$

Our assumption that the $\sum_{i \in I} h_i$ all have even multiplicities therefore implies that α is a sum of even multiples of powers of ω. In particular $2 | N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\alpha)$.

If $h_i \not\equiv 0 \pmod p$ then since $p \geq 3$ it is well known that

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 + \omega^{h_i}) = 1.$$

We therefore have a contradiction unless at least one of the h_i is 0. □

Combining the last two lemmas we immediately deduce the following.

Lemma 5.9. *Let p be prime, $(a; p) = 1$ and let $h_1, \dots, h_l, b$ be integers. We have*

$$\sum_{k \pmod p} e_p(-kb) \prod_{I \subseteq \{1,\dots,l\}} S\left(a, k + \sum_{i \in I} h_i, p\right) \ll_l p^{\frac{2^l+1}{2}} (p; b; \prod h_i)^{1/2}.$$

Next we generalise this to squarefree moduli.

Lemma 5.10. *Let q be squarefree, $(a; q) = 1$ and let $h_1, \dots, h_l, b$ be integers. For any $\epsilon > 0$ we have*

$$\sum_{k \pmod q} e_q(-kb) \prod_{I \subseteq \{1,\dots,l\}} S\left(a, k + \sum_{i \in I} h_i, q\right) \ll_{\epsilon,l} q^{\frac{2^l+1}{2}+\epsilon} (q; b; \prod h_i)^{1/2}.$$

Proof. The sum has a multiplicative property. Specifically, if $(q_0; q_1) = 1$ then

$$\begin{aligned}
&\sum_{k \,(\mathrm{mod}\, q_0q_1)} e_{q_0q_1}(-kb) \prod_{I\subseteq\{1,\dots,l\}} S\left(a, k+\sum_{i\in I} h_i, q_0q_1\right) \\
&= \sum_{\substack{k_0 \,(\mathrm{mod}\, q_0)\\ k_1 \,(\mathrm{mod}\, q_1)}} e_{q_0}(-bk_0\overline{q_1}) e_{q_1}(-bk_1\overline{q_0}) \prod_{I\subseteq\{1,\dots,l\}} S(a, k_0q_1\overline{q_1}+k_1q_0\overline{q_0}+\sum_{i\in I} h_i, q_0q_1) \\
&= \sum_{k_0 \,(\mathrm{mod}\, q_0)} e_{q_0}(-bk_0\overline{q_1}) \prod_{I\subseteq\{1,\dots,l\}} S\left(a\overline{q_1}, (k_0q_1\overline{q_1}+\sum_{i\in I} h_i)\overline{q_1}, q_0\right) \\
&\qquad \times \sum_{k_1 \,(\mathrm{mod}\, q_1)} e_{q_1}(-bk_1\overline{q_0}) \prod_{I\subseteq\{1,\dots,l\}} S\left(a\overline{q_0}, (k_1q_0\overline{q_0}+\sum_{i\in I} h_i)\overline{q_0}, q_1\right).
\end{aligned}$$

It follows that if q is squarefree we may factorise the sum as a product over $p|q$ of sums to modulus p. Each sum may then be estimated using the last lemma. The integers b, h_i occurring in the factors are different to those in our sum to modulus q, however the changes are simply by multiplicative factors coprime to q. It follows that each factor may be bounded by

$$C_l p^{\frac{2^l+1}{2}} (p; b; \prod h_i)^{1/2}$$

for some constant C_l, whence our sum is bounded by

$$\prod_{p|q} \left(C_l p^{\frac{2^l+1}{2}} (p; b; \prod h_i)^{1/2}\right) \ll_{\epsilon,l} q^{\frac{2^l+1}{2}+\epsilon} (q; b; \prod h_i)^{1/2}.$$

□

We now return to our sum

$$\begin{aligned}
T(h_1, \dots, h_l) &= \sum_{k\in J(h_1,\dots,h_l)} \prod_{I\subseteq\{1,\dots,l\}} S\left(a', k+\sum_{i\in I} q_ih_i, q_0\right) \\
&= \sum_{j \,(\mathrm{mod}\, q_0)} \sum_{\substack{k\in J(h_1,\dots,h_l)\\ k\equiv j \,(\mathrm{mod}\, q_0)}} \prod_{I\subseteq\{1,\dots,l\}} S\left(a', j+\sum_{i\in I} q_ih_i, q_0\right) \\
&= \frac{1}{q_0} \sum_{b \,(\mathrm{mod}\, q_0)} h(b) \sum_{j \,(\mathrm{mod}\, q_0)} e_{q_0}(bj) \prod_{I\subseteq\{1,\dots,l\}} S\left(a', j+\sum_{i\in I} q_ih_i, q_0\right),
\end{aligned}$$

with

$$h(b) = \sum_{k\in J(h_1,\dots,h_l)} e_{q_0}(-bk).$$

We have the standard estimate

$$h(b) \ll \min\left(K, \frac{1}{\|b/q_0\|}\right).$$

Since $(q_i; q_0) = 1$ for $i \neq 0$ we can write

$$(q_0; b; \prod q_i h_i) = (q_0; b; \prod h_i).$$

We may therefore use the last lemma to obtain

$$T(h_1, \ldots, h_l) \ll_{\epsilon,l} q_0^{\frac{2^l+1}{2}+\epsilon} \cdot \frac{1}{q_0} \sum_{b \,(\mathrm{mod}\, q_0)} \min\left(K, \frac{1}{\|b/q_0\|}\right) (q_0; b; \prod h_i)^{1/2}.$$

Finally we estimate

$$\begin{aligned}
&\frac{1}{q_0} \sum_{b \,(\mathrm{mod}\, q_0)} \min\left(K, \frac{1}{\|b/q_0\|}\right) (q_0; b; \prod h_i)^{1/2} \\
&\ll \frac{K}{q_0}(q_0; \prod h_i)^{1/2} + \sum_{0<b\leq q_0/2} \frac{1}{b}(q_0; b; \prod h_i)^{1/2} \\
&= \frac{K}{q_0}(q_0; \prod h_i)^{1/2} + \sum_{d|(q_0; \prod h_i)} d^{1/2} \sum_{\substack{0<b\leq q_0/2 \\ (q_0; b; \prod h_i)=d}} \frac{1}{b} \\
&\ll_\epsilon \frac{K}{q_0}(q_0; \prod h_i)^{1/2} + q^\epsilon \\
&\ll_\epsilon q^\epsilon (q_0; \prod h_i)^{1/2} (\frac{K}{q_0} + 1)
\end{aligned}$$

so we conclude that

$$T(h_1, \ldots, h_l) \ll_{\epsilon,l} q^\epsilon (\frac{K}{q_0} + 1) q_0^{\frac{2^l+1}{2}} (q_0; \prod h_i)^{1/2}.$$

5.4.4 Conclusion

Inserting the above bound for $T(h_1, \ldots, h_l)$ into the result of Lemma 5.6 we obtain

$$\begin{aligned}
&T^{2^l} \\
&\ll_{\epsilon,l} q^\epsilon \left(q^{2^{l-1}} \sum_{j=1}^{l} K^{2^l - 2^{l-j}} q_{l-j+1}^{2^{l-j}} \right. \\
&\qquad \left. + (\frac{K}{q_0} + 1) K^{2^l - l - 1} (q/q_0)^{2^{l-1}+1} q_0^{\frac{2^l+1}{2}} \sum_{0<|h_1|\leq K/q_1} \cdots \sum_{0<|h_l|\leq K/q_l} (q_0; \prod h_i)^{1/2} \right).
\end{aligned}$$

We have

$$\begin{aligned}\sum_{0<|h_1|\leq K/q_1} \dots \sum_{0<|h_l|\leq K/q_l} (q_0; \prod h_i)^{1/2} &\leq \sum_{0<|h|\leq K^l/(q_1\dots q_l)} \tau_l(h)(q_0;h)^{1/2} \\ &\ll_{\epsilon,l} q^{\epsilon} \sum_{0<|h|\leq K^l/(q_1\dots q_l)} (q_0;h)^{1/2} \\ &\ll_{\epsilon} q^{\epsilon} K^l/(q_1\dots q_l) \\ &= q^{-1+\epsilon} K^l q_0.\end{aligned}$$

We conclude that

$$T^{2^l} \ll_{\epsilon,l} q^{2^{l-1}+\epsilon} \left(\sum_{j=1}^{l} K^{2^l-2^{l-j}} q_{l-j+1}^{2^{l-j}} + (\frac{K}{q_0}+1) K^{2^l-1} q_0^{1/2} \right).$$

Lemma 5.4 now follows, on recalling that the sums $S(r)$ were a special case of the sum T, and therefore Theorem 5.3 is proven.

Chapter 6

Diophantine Approximation with Products of Two Primes

6.1 Introduction

Diophantine approximation is the branch of number theory which studies approximations to real numbers by rationals. A fundamental result in the area is Dirichlet's Approximation Theorem which implies that given any irrational α there are infinitely many integer solutions, n, to the inequality

$$\|n\alpha\| \leq n^{-1}.$$

It can be shown that the exponent -1 in Dirichlet's theorem is best possible, for example when α is a quadratic irrational.

It is natural to ask whether, for all irrational α, the above inequality has infinitely many prime solutions n. This was shown to be false, for uncountably many α, by Harman [31]. However, since the density of the primes near N is about $\frac{1}{\log N}$, it seems sensible to conjecture that

$$\|p\alpha\| \leq p^{-\theta} \tag{6.1}$$

has infinitely many prime solutions, p, for any irrational α and any $\theta < 1$. It is an easy consequence of the Generalised Riemann Hypothesis that this conjecture holds for any $\theta < \frac{1}{3}$. This was proved unconditionally by Matomäki [40] and is currently the strongest result known.

Progress on this problem began with Vinogradov [46] who proved that we can take any $\theta < \frac{1}{5}$. His proof was simplified by Vaughan [45] who improved the exponent to $\theta < \frac{1}{4}$. Harman [30] introduced a sieve method to the problem. He increased the size of θ to $\theta < \frac{3}{10}$, improving this in [32] to $\theta < \frac{7}{22}$. These results of Harman used identical arithmetic information to the results of Vaughan; the improvements were

in the sieve method. Heath-Brown and Jia [36] found new arithmetic information which they were able to use to get $\theta < \frac{16}{49}$. Finally, by using results on averages of Kloosterman sums, Matomäki was able to extend this to handle any $\theta < \frac{1}{3}$.

If we only require the solutions of (6.1) to have at most two prime factors then the problem is considerably easier as classical sieve methods may be used. In particular Harman [30, Theorem 2] states that any $\theta < 0.46$ is sufficient. One reason for a stronger result is that the parity problem of sieve theory is no longer an issue. In order to circumvent the parity problem and detect primes it is necessary to prove estimates for bilinear forms, known as "Type II" sums. Matomäki [40] describes all the estimates known for $\theta < \frac{1}{3}$ but none of her proofs are valid for $\theta \geq \frac{1}{3}$. We will prove a Type II bound in which one may take θ slightly larger than $\frac{1}{3}$. This estimate is too weak to show the existence of prime solutions to (6.1). It does, however, show that there are solutions which have precisely two prime factors. Hence we can break the parity barrier for some $\theta > \frac{1}{3}$.

We are also interested in the set $\mathcal{P}_3(b)$ of 3-digit palindromes in base b. Recall, from Definition 3.1, that

$$\mathcal{P}_3(b) = \{j(b^2+1) + kb : j \in (0,b) \cap \mathbb{Z}, k \in [0,b) \cap \mathbb{Z}\}.$$

As we shall see in Section 6.5, elements in this set correspond closely to solutions of (6.1) when $\theta = \frac{1}{3}$. We may therefore also conclude that $\mathcal{P}_3(b)$ contains numbers with precisely two prime factors provided that b is sufficiently large.

To handle both of these problems simultaneously we work with the following set. For a natural number q, positive reals x, z and an integer a with $(a;q) = 1$ we let

$$\mathcal{A} = \mathcal{A}(x,q,z,a) = \{n \in (\frac{x}{4}, x] : n \equiv ak \,(\mathrm{mod}\, q) \text{ for some } k \in [0,z) \cap \mathbb{Z}\}.$$

For a fixed constant $\theta \in (0,1)$ we shall only consider the case when

$$z \in \left[\frac{1}{2}q^{\frac{1-\theta}{1+\theta}}, 2q^{\frac{1-\theta}{1+\theta}}\right]$$

and

$$x \in \left[\frac{1}{2}q^{\frac{2}{1+\theta}}, 2q^{\frac{2}{1+\theta}}\right].$$

All implied constants in our results may depend on θ. Observe that $zq \asymp x$ and therefore

$$\#\mathcal{A} \asymp \frac{xz}{q} \asymp z^2.$$

Our aim is to estimate Type I and Type II sums for the set $\mathcal{A}$ and use them to prove the following.

Theorem 6.1. *Suppose $\theta < \frac{8}{23}$ is fixed. Let $\mathcal{E}_2$ be the set of natural numbers having precisely 2 prime factors. With the above definitions and hypotheses we have*

$$\#(\mathcal{A} \cap \mathcal{E}_2) \gg \frac{z^2}{\log z},$$

provided that q is sufficiently large in terms of θ.

A result of this form for $\theta < \frac{1}{3}$ would follow immediately from Vaughan's work in [45]. The key new idea to handle larger θ is our Type II estimate, Theorem 6.13.

This theorem enables us to prove the following results regarding the problems discussed above.

Theorem 6.2. *Let α be irrational. For any $\theta < \frac{8}{23}$ there exist infinitely many $n \in \mathcal{E}_2$ such that*

$$\|n\alpha\| \leq n^{-\theta}.$$

Theorem 6.3. *For all sufficiently large b we have*

$$\#(\mathcal{P}_3(b) \cap \mathcal{E}_2) \gg \frac{b^2}{\log b}.$$

In this chapter we will write

$$\mathbf{1}_{\mathcal{A}}(n) = \begin{cases} 1 & n \in \mathcal{A} \\ 0 & n \notin \mathcal{A}. \end{cases}$$

It is slightly more convenient to work with a weighted version of the primes so we let

$$\Lambda'(n) = \begin{cases} \log n & n \text{ is prime} \\ 0 & \text{otherwise.} \end{cases}$$

The remaining notation is as described in Chapter 2.

6.2 Reduction of the Problem

As we only require a lower bound we may smooth the function $\mathbf{1}_{\mathcal{A}}$. We therefore let W be the function constructed by Lemma 2.1 with $a = \frac{1}{4}$, $b = \frac{1}{3}$, $c = \frac{2}{3}$ and $d = \frac{3}{4}$. Recall that for any $B \in \mathbb{N}$ we have the estimate

$$|\hat{W}(x)| \ll_B \min(1, |x|^{-B}). \tag{6.2}$$

We let

$$\Phi(n) = \sum_{\substack{k \\ n \equiv ka \,(\mathrm{mod}\, q)}} W\left(\frac{k}{z}\right).$$

It is easy to show that this is a lower bound for $\mathbf{1}_{\mathcal{A}}$.

Lemma 6.4. *If* $\frac{x}{4} < n < x$ *then*

$$0 \leq \Phi(n) \leq \mathbf{1}_{\mathcal{A}}(n) \leq 1.$$

Therefore, to prove Theorem 6.1 it is sufficient to give a lower bound for

$$\sum_{\substack{\frac{x}{4}<n<x \\ n\in\mathcal{E}_2}} \Phi(n).$$

Proof. This follows immediately from the definitions of $\mathcal{A}$ and Φ. □

6.3 Type I Sums

The Type I estimate we prove, Theorem 6.8, has been known in essence since the work of Vaughan [45]. However, it is useful to prove it again to get a result which is valid in our precise situation. In addition, Vaughan's proof uses estimates for exponential sums whereas we use results from the geometry of numbers. The exponential sum approach is possibly simpler for standard Type I sums but we also need to estimate a variant of such sums, Theorem 6.12, which is easier with the geometry of numbers.

Throughout this section we make repeated use of the following assumptions:

(A1) $M, N \geq 1$, $\frac{x}{4} \leq MN \leq 4x$ and $M \leq z^{2-\delta}$ for some $\delta > 0$.

Observe that this implies

$$N \gg \frac{x}{M} \gg \frac{q}{z^{1-\delta}}.$$

All our implied constants may depend on δ.

For an integer m let

$$\Psi(m) = \Psi(m; N) = \sum_{n\sim N} \Phi(mn).$$

We will consider $\Psi(m)$ as a counting function of points of a certain lattice, $\lambda(m)$, recall Definition 2.2.

Lemma 6.5. *Let*

$$\lambda(m) = \{(j,k) \in \mathbb{Z}^2 : jq + ka \equiv 0 \,(\mathrm{mod}\, m)\}.$$

The set $\lambda(m)$ *is a lattice in* $\mathbb{Z}^2$ *with determinant* m.

Proof. It is clear that $\lambda(m)$ is a lattice. Since $(a;q)=1$ we know that $jq+ka$ takes on all integer values as j,k vary over $\mathbb{Z}^2$. Thus $jq+ka$ represents all congruence classes mod m so the determinant of $\lambda(m)$ is m. □

Define $b_1(m)$ to be the shortest nonzero vector in $\lambda(m)$ and let $R_1(m)$ be the Euclidean length of $b_1(m)$. We know, by Lemma 2.4, that $R_1(m) \ll \sqrt{m}$.

Lemma 6.6. *Under the assumptions (A1) we have*

$$\Psi(m) = \frac{N\hat{W}(0)z}{q} + O\left(\frac{z}{R_1(m)}\right),$$

for any $m \sim M$.

Proof. From the definitions of Ψ and Φ we get

$$\begin{aligned}
\Psi(m) &= \sum_{n\sim N} \Phi(mn) \\
&= \sum_{n\sim N} \sum_{\substack{k \\ mn\equiv ka \,(\mathrm{mod}\, q)}} W\left(\frac{k}{z}\right) \\
&= \sum_{n\sim N} \sum_{\substack{j,k \\ mn=jq+ka}} W\left(\frac{k}{z}\right) \\
&= \sum_{\substack{(j,k)\in\lambda(m) \\ (jq+ka)/m\sim N}} W\left(\frac{k}{z}\right).
\end{aligned}$$

Since W is supported on $(0,1)$ the sum only contains points with $k \in (0,z)$. Let

$$f(t) = \#\{(j,k) \in \lambda(m) : \frac{jq+ka}{m} \sim N, k \in (0,t]\}.$$

Summing by parts we get

$$\Psi(m) = -\frac{1}{z}\int_0^z f(t) W'\left(\frac{t}{z}\right)\, dt.$$

Let

$$A(t) = \{(x,y) \in \mathbb{R}^2 : \frac{xq+ya}{m} \sim N, y \in (0,t]\}.$$

By Lemma 2.6 we have

$$f(t) = \frac{\mathrm{area}(A(t))}{m} + O\left(\frac{\mathrm{perimeter}(A(t))}{R_1(m)} + 1\right).$$

The vertices of $A(t)$ are

$$(Nm/q, 0), (2Nm/q, 0), ((Nm - ta)/q, t), ((2Nm - ta)/q, t).$$

Therefore

$$\text{area}(A(T)) = \frac{Nmt}{q}$$

and

$$\text{perimeter}(A(T)) \ll \frac{NM}{q} + t + \frac{ta}{q} \ll z.$$

It follows that

$$\begin{aligned}
\Psi(m) &= -\frac{1}{z}\int_0^z \left(\frac{Nt}{q} + O\left(\frac{z}{R_1(m)} + 1\right)\right) W'\left(\frac{t}{z}\right)\, dt \\
&= -\frac{N}{qz}\int_0^z tW'\left(\frac{t}{z}\right)\, dt + O\left(\frac{z}{R_1(m)} + 1\right) \\
&= \frac{N\hat{W}(0)z}{q} + O\left(\frac{z}{R_1(m)} + 1\right).
\end{aligned}$$

Since $R_1(m) \ll \sqrt{m} \ll \sqrt{M} \ll z$ the result follows. □

We need a bound for the number of m for which $R_1(m)$ is unusually small.

Lemma 6.7. *For any $\epsilon > 0$, any $M \leq z^{2-\delta}$ and any integer l we have*

$$\#\{m \leq M : R_1(m)^2 = l\} \ll_\epsilon z^\epsilon.$$

Proof. We know that $R_1(m)^2 \ll m \ll M$. Thus the only case to consider is $0 < l \ll M$.

If $R_1(m)^2 = l$ then there exist integers j, k with $j^2 + k^2 = l$ and $m|jq + ka$. It follows that the quantity of interest is bounded by

$$\sum_{\substack{(j,k)\in\mathbb{Z}^2 \\ j^2+k^2=l}} \#\{m : m|jq + ka\} \leq \sum_{\substack{(j,k)\in\mathbb{Z}^2 \\ j^2+k^2=l}} \tau(jq + ka).$$

For the remainder of the proof let $h = jq + ka$, where $j^2 + k^2 = l$. We now use an argument by contradiction to show that $h \neq 0$. If $h = 0$ then $k \neq 0$ since $(j, k) \neq (0, 0)$. Moreover $q|k$, whence $|k| \geq q$. However

$$k \leq \sqrt{l} \ll \sqrt{M} = o(z) = o(q),$$

giving a contradiction if q is large enough. We therefore conclude that $h \neq 0$. In addition we have

$$h \ll q\sqrt{l} \ll qz \ll x,$$

so that $\tau(h) \ll x^{\epsilon}$. Letting $r(l)$ denote the number of ways in which l may be written as the sum of two squares, the cardinality of the set in the lemma is then

$$\ll r(l)x^{\epsilon} \ll z^{\epsilon}.$$

□

We may now prove an estimate for Type I sums.

Theorem 6.8. *If α_m are complex numbers with $|\alpha_m| \leq 1$ then, with the assumptions (A1) we have, for any $A > 0$*

$$\sum_{m\sim M, n\sim N} \alpha_m \Phi(mn) = \frac{\hat{W}(0)Nz}{q} \sum_{m\sim M} \alpha_m + O_A(z^2(\log z)^{-A}).$$

Proof. Let

$$S = \sum_{m\sim M, n\sim N} \alpha_m \Phi(mn) = \sum_{m\sim M} \alpha_m \Psi(m).$$

Applying Lemma 6.6 we get

$$S = \frac{N\hat{W}(0)z}{q} \sum_{m\sim M} \alpha_m + O\left(z \sum_{m\sim M} \frac{1}{R_1(m)}\right).$$

Using Lemma 6.7 we deduce that

$$\begin{aligned} \sum_{m\sim M} \frac{1}{R_1(m)} &= \sum_{l\ll M} \frac{1}{\sqrt{l}} \#\{m \sim M, R_1(m)^2 = l\} \\ &\ll_{\epsilon} z^{\epsilon} \sum_{l\ll M} l^{-\frac{1}{2}} \\ &\ll_{\epsilon} z^{\epsilon} M^{\frac{1}{2}}. \end{aligned}$$

We conclude that

$$S = \frac{N\hat{W}(0)z}{q} \sum_{m\sim M} \alpha_m + O(z^{1+\epsilon} M^{\frac{1}{2}}).$$

Since $M \ll z^{2-\delta}$ the error term is

$$O(z^{2+\epsilon-\delta/2}).$$

The result follows on taking $\epsilon < \frac{\delta}{2}$. □

Observe that if

$$\sum_{m\sim M} \alpha_m \asymp M$$

then the leading term in this estimate has size $\frac{xz}{q} \asymp z^2$. This is larger than the error term.

It is also necessary to bound a Type I sum where $\sum_{n\sim N}$ is replaced by a smooth weight.

Theorem 6.9. *Suppose the conditions (A1) hold. If α_m are complex numbers with $|\alpha_m| \leq 1$ then, for any $A > 0$, we have*

$$\sum_{\substack{n \\ m\sim M}} \alpha_m W\left(\frac{n}{3N}\right) \Phi(mn) = \frac{3\hat{W}(0)^2 Nz}{q} \sum_{m\sim M} \alpha_m + O_A(z^2(\log z)^{-A}).$$

Proof. After using partial summation to remove the smooth weight $W(\frac{n}{3N})$, the result follows by an almost identical proof to that of Theorem 6.8. □

Define $\Psi_1(m)$ by

$$\Psi(m) = \frac{\hat{W}(0)Nz}{q} + \Psi_1(m).$$

We will require the following two lemmas.

Lemma 6.10. *For any $\epsilon > 0$ and any M, N, x, q and z satisfying the assumptions (A1) we have*

$$\sum_{m\asymp M} \Psi_1(m)^2 \ll_\epsilon z^{2+\epsilon}.$$

Proof. From Lemma 6.6 we have

$$\Psi_1(m)^2 \ll_\epsilon \frac{z^2}{R_1(m)^2}.$$

By Lemma 6.7 we get

$$\begin{aligned} \sum_{m\asymp M} \frac{1}{R_1(m)^2} &\ll \sum_{l\ll M} \frac{1}{l} \#\{m \asymp M, R_1(m)^2 = l\} \\ &\ll_\epsilon z^\epsilon \sum_{l\ll M} l^{-1} \\ &\ll_\epsilon z^\epsilon. \end{aligned}$$

The result follows. □

Lemma 6.11. *Under the assumptions (A1) we have*

$$\sum_{m \asymp M} \Psi(m)^2 \ll \frac{Nz^3}{q}.$$

Proof. We have

$$\begin{aligned}
\sum_{m \asymp M} \Psi(m)^2 &= \sum_{m \asymp M} \left(\frac{N\hat{W}(0)z}{q} + \Psi_1(m) \right)^2 \\
&\ll \sum_{m \asymp M} \frac{N^2 z^2}{q^2} + \sum_{m \asymp M} \psi_1(m)^2 \\
&\ll_\epsilon \frac{MN^2 z^2}{q^2} + z^{2+\epsilon} \\
&\ll_\epsilon \frac{Nz^3}{q} + z^{2+\epsilon}.
\end{aligned}$$

Since $N \gg \frac{q}{z^{1-\delta}}$ the first term is larger if we take a small enough ϵ. □

We may now estimate a variant of a Type I sum which will be useful later.

Theorem 6.12. *Suppose that the assumptions (A1) on M, N, x, z and q hold. In addition, assume that $N \leq z^{2-\delta}$. Then, for any complex numbers β_n bounded by 1 and any $A > 0$,*

$$\sum_{\substack{m \\ n_1, n_2 \sim N}} \beta_{n_1} W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2) = \frac{3NM\hat{W}(0)^3 z^2}{q^2} \sum_{n \sim N} \beta_n + O_A\left(\frac{z^4 (\log z)^{-A}}{M} \right).$$

Proof. Let

$$S = \sum_{\substack{m \\ n_1, n_2 \sim N}} \beta_{n_1} W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2) = \sum_{\substack{m \\ n \sim N}} \beta_n W\left(\frac{m}{3M}\right) \Phi(mn)\Psi(m).$$

Writing

$$\Psi(m) = \frac{\hat{W}(0)Nz}{q} + \Psi_1(m)$$

we get a contribution from $\frac{\hat{W}(0)Nz}{q}$ of

$$\frac{\hat{W}(0)Nz}{q} \sum_{\substack{m \\ n \sim N}} \beta_n W\left(\frac{m}{3M}\right) \Phi(mn).$$

This sum is in a form which can be estimated by Theorem 6.9, with m, n interchanged. All the conditions needed for that theorem are satisfied since $N \leq z^{2-\delta}$. The main term is thus

$$\frac{3\hat{W}(0)^3 NMz^2}{q^2} \sum_{n \sim N} \beta_n + O_A\left(\frac{z^3(\log z)^{-A}N}{q}\right).$$

On writing $N \ll \frac{zq}{M}$ the error here is

$$O_A\left(\frac{z^4(\log z)^{-A}}{M}\right).$$

The contribution from $\Psi_1(m)$ is

$$\sum_{\substack{m \\ n \sim N}} \beta_n W\left(\frac{m}{3M}\right) \Phi(mn)\Psi_1(m).$$

Trivially estimating the β_n by 1 this is majorised by

$$\sum_{m} W\left(\frac{m}{3M}\right) \Psi(m)|\Psi_1(m)|.$$

Since $W(x) \leq 1$ for all x we may remove the factor $W(\frac{m}{3M})$ and apply Cauchy's inequality to get a bound of

$$\left(\sum_{m \asymp M} \Psi(m)^2\right)^{1/2} \left(\sum_{m \asymp M} \Psi_1(m)^2\right)^{1/2}.$$

Applying the previous two lemmas this is

$$\ll_\epsilon N^{1/2} z^{5/2+\epsilon} q^{-1/2} \ll \frac{z^{3+\epsilon}}{\sqrt{M}}.$$

Since $M \leq z^{2-\delta}$ the error here is

$$\frac{z^{3+\epsilon}\sqrt{M}}{M} \leq \frac{z^{4+\epsilon-\delta/2}}{M}.$$

The result follows on taking $\epsilon < \frac{\delta}{2}$. □

Observe that if

$$\sum_{n \sim N} \beta_n \asymp N$$

then the main term in this last theorem has size

$$\frac{N^2 M z^2}{q^2} \asymp \frac{z^4}{M}.$$

6.4 Type II Sums

In this section we make repeated use of the following assumptions:

(A2) $\frac{x}{4} \le MN \le 4x$ and

$$\max\left(z, \frac{q}{z^{1-\delta}}\right) \le N \le z^{\frac{16}{15}-\delta}$$

for some $\delta > 0$.

We will prove the following Type II result.

Theorem 6.13. *Let α_m be complex numbers bounded by 1. Suppose that (A2) holds. Then, for every $A > 0$, we have*

$$\sum_{m\sim M, n\sim N} \alpha_m(\Lambda'(n) - 1)\Phi(mn) \ll z^2(\log z)^{-A},$$

where the implied constant depends on both A and the value of δ in (A2).

Observe that (A2) implies that

$$M \ll z^{2-\delta}.$$

The hypothesis that $N \ge z$ is only used in the proof of Lemma 6.20. When $\theta > \frac{1}{3}$ this assumption is weaker than

$$N \ge \frac{q}{z^{1-\delta}}.$$

Let

$$S = \sum_{m\sim M, n\sim N} \alpha_m\beta_n\Phi(mn),$$

where

$$\beta_n = \Lambda'(n) - 1.$$

We wish to show that $S = O(z^2(\log z)^{-A})$. Our arguments can be modified to handle arbitrary β_n, although the range of N is then much smaller. However, this introduces some additional technicalities. Since our Type II estimate does not cover a sufficiently large range of N to detect primes we have chosen to give the details only for the specific choice $\beta_n = \Lambda'(n) - 1$.

Vaughan [45] used exponential sum methods to establish Type II estimates which are only valid when $x^\theta < N < x^{1-2\theta}$. This range is empty when $\theta \ge \frac{1}{3}$. Heath-Brown and Jia [36] introduced a new method which reduces the problem to the estimation of certain Kloosterman sums. Matomäki [40] used the same reduction but then used stronger bounds on the resulting averages of Kloosterman sums and was thus able

to get enough Type II information to detect primes for any $\theta < \frac{1}{3}$. The range of N in the Type II bounds found by Heath-Brown, Jia and Matomäki remains nonempty as $\theta \to \frac{1}{3}$. However, it is not valid for $\theta \geq \frac{1}{3}$ as the reduction to Kloosterman sums gives an error which is too large in this case. Our method is essentially an extension of that of Heath-Brown and Jia which avoids this problem.

The proof of Theorem 6.13 begins by applying Cauchy's inequality to the sum S. After applying our Type I results we reach a sum S_2 to which the Poisson Summation Formula and various rearrangements are applied. After estimating some special subsums we eventually reach a sum S_{10} which can be estimated using results on Kloosterman sums over primes, for example those given in Chapter 4. The strength of the estimate for S_{10} determines the range of N in Theorem 6.13 which then determines the admissible values of θ in Theorem 6.1.

Lemma 6.14. *We have* $S = O(\sqrt{MS_1})$ *where*

$$S_1 = \sum_{n_1,n_2\sim N} \beta_{n_1}\beta_{n_2} \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2).$$

It follows that a bound of

$$S_1 = O\left(\frac{z^4(\log z)^{-A}}{M}\right)$$

will be sufficient.

Proof. Applying Cauchy's inequality gives

$$S^2 \leq \sum_{m\sim M} |\alpha_m|^2 \sum_{m\sim M} \left(\sum_{n\sim N} \beta_n \Phi(mn)\right)^2.$$

By definition of the function W we know that $W\left(\frac{m}{3M}\right) = 1$ when $m \sim M$. Therefore

$$\begin{aligned} S^2 &\ll M \sum_m W\left(\frac{m}{3M}\right) \left(\sum_{n\sim N} \beta_n \Phi(mn)\right)^2 \\ &= M \sum_{n_1,n_2\sim N} \beta_{n_1}\beta_{n_2} \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2) \\ &= MS_1. \end{aligned}$$

□

On putting $\beta_n = \Lambda'(n) - 1$ into S_1 we will get three sums all of which must be evaluated asymptotically. However, on combining the sums, all the main terms will cancel and we will get the required result. Specifically, let

$$S_1 = S_{1,1} - 2S_{1,2} + S_{1,3}$$

where

$$S_{1,1} = \sum_{n_1,n_2\sim N} \Lambda'(n_1)\Lambda'(n_2) \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2),$$

$$S_{1,2} = \sum_{n_1,n_2\sim N} \Lambda'(n_1) \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2)$$

and

$$S_{1,3} = \sum_{n_1,n_2\sim N} \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2).$$

We begin by dealing with the sums $S_{1,2}$ and $S_{1,3}$.

Lemma 6.15. *Under the assumptions (A2) we have, for $i = 2, 3$ that*

$$S_{1,i} = \frac{3N^2M\hat{W}(0)^3z^2}{q^2} + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right).$$

Proof. We have

$$N \leq z^{\frac{16}{15}-\delta} \leq z^{2-\delta}.$$

We may therefore use Theorem 6.12 with $\beta_n = \Lambda'(n)$ or $\beta_n = 1$. These coefficients are only bounded by $\log n$ but this can be absorbed into the error term. In either case we have

$$\sum_{n\sim N} \beta_n = N + O(N(\log N)^{-A})$$

so the result follows. □

Next we deal with the contribution to $S_{1,1}$ from pairs with $n_1 = n_2$. This is

$$\sum_{n\sim N} \Lambda'(n)^2 \sum_m W\left(\frac{m}{3M}\right) \Phi(mn)^2.$$

All the terms are positive and Φ takes values in $[0, 1]$ so this is at most

$$\sum_{n\sim N} \Lambda'(n)^2 \sum_m W\left(\frac{m}{3M}\right) \Phi(mn).$$

Using Theorem 6.9 we may bound this Type I sum by $O(z^2 \log N)$. Since $M \ll z^{2-\delta}$ this is $O(\frac{z^4(\log z)^{-A}}{M})$.

The remaining terms in $S_{1,1}$ have $n_1 \neq n_2$. Since the coefficients $\Lambda'(n)$ are supported on primes all such pairs actually satisfy $(n_1; n_2) = 1$. We therefore consider

$$S_2 = \sum_{\substack{n_1,n_2 \sim N \\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2) \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2).$$

6.4.1 Harmonic Analysis of the Sum S_2

Let

$$T = \sum_m W\left(\frac{m}{3M}\right) \Phi(mn_1)\Phi(mn_2).$$

Since $(a; q) = 1$ there exists an $\overline{a}$ satisfying

$$a\overline{a} \equiv 1 \,(\mathrm{mod}\, q).$$

Lemma 6.16. *We have*

$$T = \frac{3Mz^2}{q^2} \sum_{k_1,k_2} \hat{W}\left(\frac{k_1 z}{q}\right) \hat{W}\left(\frac{k_2 z}{q}\right) \sum_m \hat{W}\left(3M\left(m - \frac{\overline{a}(k_1 n_1 + k_2 n_2)}{q}\right)\right).$$

Proof. The definition of Φ gives

$$\begin{aligned} \Phi(n) &= \sum_{\substack{k \\ k \equiv n\overline{a} \,(\mathrm{mod}\, q)}} W\left(\frac{k}{z}\right) \\ &= \sum_m W\left(\frac{qm + n\overline{a}}{z}\right). \end{aligned}$$

Applying the Poisson Summation Formula in the form (2.1) we therefore get

$$\Phi(n) = \frac{z}{q} \sum_k \hat{W}\left(\frac{kz}{q}\right) e\left(\frac{n\overline{a}k}{q}\right),$$

so that

$$T = \frac{z^2}{q^2} \sum_{k_1,k_2} \hat{W}\left(\frac{k_1 z}{q}\right) \hat{W}\left(\frac{k_2 z}{q}\right) \sum_m W\left(\frac{m}{3M}\right) e\left(\frac{m\overline{a}(k_1 n_1 + k_2 n_2)}{q}\right).$$

We can now use the Poisson Summation Formula (2.2) to obtain

$$\sum_m W\left(\frac{m}{3M}\right) e\left(\frac{m\overline{a}(k_1 n_1 + k_2 n_2)}{q}\right) = 3M \sum_m \hat{W}\left(3Mm - \frac{3M\overline{a}(k_1 n_1 + k_2 n_2)}{q}\right).$$

The result follows on substituting this into the above expression for T. □

Let S_3 be the subsum of S_2 coming from terms with $k_1n_1 + k_2n_2 = 0$. Since $(n_1; n_2) = 1$ any solution of this may be written uniquely as $k_1 = n_2h$ and $k_2 = -n_1h$ for some $h \in \mathbb{Z}$. Therefore

$$S_3 = \frac{3Mz^2}{q^2} \sum_{\substack{n_1,n_2\sim N\\(n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2) \sum_{h,m} \hat{W}\left(\frac{n_2hz}{q}\right) \hat{W}\left(\frac{-n_1hz}{q}\right) \hat{W}(3Mm).$$

Lemma 6.17. *For any $A > 0$ we have, under the assumptions (A2), that*

$$S_3 = \frac{3MN^2z^2\hat{W}(0)^3}{q^2} + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right).$$

Proof. Our assumptions imply that for $n_i \sim N$ we have

$$\frac{n_iz}{q} \gg \frac{Nz}{q} \gg z^\delta$$

and that

$$M \gg z^\delta.$$

It follows, using the bound (6.2), that the contribution to S_3 from terms with $h \neq 0$ or $m \neq 0$ is negligible. Specifically, for any $B \in \mathbb{N}$ we have

$$S_3 = \frac{3Mz^2\hat{W}(0)^3}{q^2} \sum_{\substack{n_1,n_2\sim N\\(n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2) + O_B(z^{-B}).$$

Observe that

$$\frac{Mz^2}{q^2} \sum_{n\sim N} \Lambda'(n)^2 \ll \frac{MNz^2 \log N}{q^2} \ll \frac{z^3 \log N}{q} \ll_A \frac{z^4(\log z)^{-A}}{M},$$

where the last inequality uses that $M \ll z^{2-\delta} \leq qz^{1-\delta}$. We deduce that

$$S_3 = \frac{3Mz^2\hat{W}(0)^3}{q^2} \sum_{n_1,n_2\sim N} \Lambda'(n_1)\Lambda'(n_2) + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right).$$

The result follows on applying the Prime Number Theorem to the sum

$$\sum_{n\sim N} \Lambda'(n).$$

□

Let S_4 be the sum of the remaining terms from S_2, those with $k_1n_1 + k_2n_2 \neq 0$. Thus

$$S_4 = \sum_{\substack{n_1,n_2\sim N\\(n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)T_1,$$

where

$$T_1 = \frac{3Mz^2}{q^2} \sum_{\substack{k_1,k_2\\k_1n_1+k_2n_2\neq 0}} \hat{W}\left(\frac{k_1z}{q}\right)\hat{W}\left(\frac{k_2z}{q}\right)\sum_m \hat{W}\left(3M\left(m - \frac{\overline{a}(k_1n_1+k_2n_2)}{q}\right)\right).$$

For any integers m, k_1, k_2 there exists a unique integer k such that

$$m - \frac{\overline{a}(k_1n_1+k_2n_2)}{q} = \frac{k}{q}.$$

There is then a unique integer j such that

$$k_1n_1 + k_2n_2 = jq - ka.$$

Writing $c = jq - ka$ it follows that

$$T_1 = \frac{3Mz^2}{q^2} \sum_{\substack{j,k,k_1,k_2\\k_1n_1+k_2n_2=c\neq 0}} \hat{W}\left(\frac{k_1z}{q}\right)\hat{W}\left(\frac{k_2z}{q}\right)\hat{W}\left(\frac{3Mk}{q}\right).$$

If we let

$$F(n_1,n_2;c) = \sum_{\substack{k_1,k_2\\k_1n_1+k_2n_2=c}} \hat{W}\left(\frac{k_1z}{q}\right)\hat{W}\left(\frac{k_2z}{q}\right)$$

then

$$S_4 = \frac{3Mz^2}{q^2}\sum_{\substack{j,k\\c\neq 0}} \hat{W}\left(\frac{3Mk}{q}\right) \sum_{\substack{n_1,n_2\sim N\\(n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)F(n_1,n_2;c).$$

6.4.2 Transforming the Function F

To deal with the sum S_4 we begin by applying Poisson Summation to the function F.

Lemma 6.18. *Let $\overline{n}_1$ be an inverse of n_1 modulo n_2, which exists since $(n_1;n_2) = 1$. We have*

$$F(n_1,n_2;c) = \frac{1}{n_2}\sum_l \hat{g}\left(\frac{l}{n_2};n_1,n_2,c\right)e\left(\frac{c\overline{n}_1l}{n_2}\right),$$

where

$$g(t;n_1,n_2,c) = \hat{W}\left(\frac{tz}{q}\right)\hat{W}\left(\frac{(c-tn_1)z}{n_2q}\right)$$

and $\hat{g}$ is the Fourier transform of g with respect to the single variable t.

Proof. We are interested in pairs k_1, k_2 satisfying the equation

$$k_1 n_1 + k_2 n_2 = c.$$

For a given k_1 this has at most 1 solution which exists if and only if

$$k_1 n_1 \equiv c \,(\mathrm{mod}\, n_2).$$

Since $(n_1; n_2) = 1$ this condition is equivalent to

$$k_1 \equiv c\overline{n_1} \,(\mathrm{mod}\, n_2).$$

If this congruence holds then the corresponding k_2 is given by

$$k_2 = \frac{c - k_1 n_1}{n_2}.$$

We therefore have

$$F(n_1, n_2; c) = \sum_{\substack{k \\ k \equiv c\overline{n_1} \,(\mathrm{mod}\, n_2)}} \hat{W}\left(\frac{kz}{q}\right) \hat{W}\left(\frac{(c - kn_1)z}{n_2 q}\right).$$

Now, if we let

$$g(t; n_1, n_2, c) = \hat{W}\left(\frac{tz}{q}\right) \hat{W}\left(\frac{(c - tn_1)z}{n_2 q}\right),$$

then by the Poisson Summation Formula, (2.1), we get

$$F(n_1, n_2; c) = \frac{1}{n_2} \sum_{l} \hat{g}\left(\frac{l}{n_2}\right) e\left(\frac{c\overline{n}_1 l}{n_2}\right).$$

□

Applying this lemma to the sum S_4 we deduce that

$$S_4 = \frac{3Mz^2}{q^2} \sum_{\substack{j,k,l \\ c \neq 0}} \hat{W}\left(\frac{3Mk}{q}\right) \sum_{\substack{n_1, n_2 \sim N \\ (n_1; n_2) = 1}} \Lambda'(n_1)\Lambda'(n_2) \frac{1}{n_2} \hat{g}\left(\frac{l}{n_2}; n_1, n_2, c\right) e\left(\frac{c\overline{n}_1 l}{n_2}\right).$$

The sums considered by Heath-Brown and Jia, as well as by Matomäki, are essentially just the $k = 0$ terms of S_4.

6.4.3 Terms with $l = 0$

We will need the following result concerning the function $\hat{g}$.

Lemma 6.19. *For all t and all $n_1, n_2 \sim N$ we have $\hat{g}(t) \ll \frac{q}{z}$. Furthermore, if $|t| \geq \frac{4z}{q}$ then $\hat{g}(t) = 0$.*

Proof. Recall that

$$g(t) = \hat{W}\left(\frac{tz}{q}\right)\hat{W}\left(\frac{(c-tn_1)z}{n_2 q}\right) = g_1(t)g_2(t),$$

say. It follows that

$$\hat{g}(t) = (\hat{g}_1 \star \hat{g}_2)(t) = \int_{-\infty}^{\infty} \hat{g}_1(x)\hat{g}_2(t-x)\,dx.$$

We have

$$g_1(t) = \hat{W}\left(\frac{tz}{q}\right)$$

so

$$\hat{g}_1(t) = \frac{q}{z}W\left(\frac{-tq}{z}\right).$$

We also have

$$g_2(t) = \hat{W}\left(\frac{(c-tn_1)z}{n_2 q}\right)$$

so

$$\hat{g}_2(t) = \frac{n_2 q}{n_1 z}W\left(\frac{n_2 qt}{n_1 z}\right)e\left(\frac{-ctq}{n_2 z}\right).$$

Therefore, for all t we deduce that

$$\hat{g}_i(t) \ll \frac{q}{z}.$$

Furthermore, if $|t| \geq \frac{2z}{q}$, then

$$\hat{g}_i(t) = 0.$$

It follows that for all t we have

$$\hat{g}(t) = \int_{-\infty}^{\infty} \hat{g}_1(x)\hat{g}_2(t-x)\,dx \ll \int_{|x|\leq\frac{2z}{q}} (q/z)^2\,dx \ll \frac{q}{z}.$$

In addition, if $|t| \geq \frac{4z}{q}$ then for any x either

$$|x| \geq \frac{2z}{q}$$

or

$$|t-x| \geq \frac{2z}{q}.$$

It follows that $\hat{g}(t) = 0$. □

Let S_5 be the subsum of S_4 containing the terms with $l = 0$, that is

$$S_5 = \frac{3Mz^2}{q^2} \sum_{\substack{j,k \\ c\neq 0}} \hat{W}\left(\frac{3Mk}{q}\right) \sum_{\substack{n_1,n_2\sim N \\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)\frac{1}{n_2}\hat{g}(0;n_1,n_2,c).$$

It is convenient to reinstate the terms with $c = 0$. These correspond to pairs (j,k) with $k = hq, j = ha$ so their contribution is

$$\frac{3Mz^2}{q^2} \sum_{h} \hat{W}(3Mh) \sum_{\substack{n_1,n_2\sim N \\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)\frac{1}{n_2}\hat{g}(0;n_1,n_2,0).$$

From the estimate (6.2) we may deduce that for any $B \in \mathbb{N}$ the contribution to this from terms with $h \neq 0$ is $O_B(z^{-B})$. Using the estimate for $\hat{g}$ given in Lemma 6.19 we may bound the $h = 0$ terms by

$$\frac{MNz}{q} \ll z^2 \ll_A \frac{z^4(\log z)^{-A}}{M},$$

since $M \ll z^{2-\delta}$. It is therefore enough to bound

$$S_6 = \frac{3Mz^2}{q^2} \sum_{j,k} \hat{W}\left(\frac{3Mk}{q}\right) \sum_{\substack{n_1,n_2\sim N \\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)\frac{1}{n_2}\hat{g}(0;n_1,n_2,c).$$

We may move the sum over j inside the other summations to transform this to

$$S_6 = \frac{3Mz^2}{q^2} \sum_{k} \hat{W}\left(\frac{3Mk}{q}\right) \sum_{\substack{n_1,n_2\sim N \\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)\frac{1}{n_2} \sum_{j} \hat{g}(0;n_1,n_2,c).$$

Inserting the definition of $\hat{g}$ and reordering we see that

$$S_6 = \frac{3Mz^2}{q^2} \sum_{k} \hat{W}\left(\frac{3Mk}{q}\right) \sum_{\substack{n_1,n_2\sim N \\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)\frac{1}{n_2} \int_{-\infty}^{\infty} \hat{W}\left(\frac{tz}{q}\right) T_2\, dt$$

with

$$T_2 = \sum_{j} \hat{W}\left(\frac{(c-tn_1)z}{n_2 q}\right).$$

Lemma 6.20. *For all $t \in \mathbb{R}$, $N \geq z$ and $n_1, n_2 \sim N$ we have $T_2 = 0$.*

Proof. The sum is

$$\sum_{j} \hat{W}\left(\frac{(jq-ka-tn_1)z}{n_2 q}\right).$$

We may apply the Poisson Summation Formula, (2.1), to obtain

$$\frac{n_2}{z}\sum_j W\left(\frac{n_2 j}{z}\right)e(\gamma j),$$

for a γ which depends on all the outer variables.

Since $N \geq z$ we have

$$\frac{n_2}{z} \geq \frac{N}{z} \geq 1.$$

However, W is supported on $[\frac{1}{4}, \frac{3}{4}]$ and thus for all $j \in \mathbb{N}$ we have

$$W\left(\frac{n_2 j}{z}\right) = 0.$$

□

It follows from this that $S_6 = 0$ and therefore that

$$S_5 \ll_A \frac{z^A(\log z)^{-A}}{M}.$$

6.4.4 The Remaining Terms

Let S_7 be the subsum of S_4 containing all the remaining terms, that is to say, all those with $l \neq 0$. Thus

$$S_7 = \frac{3Mz^2}{q^2}\sum_{\substack{j,k,l\\ c\neq 0, l\neq 0}} \hat{W}\left(\frac{3Mk}{q}\right)\sum_{\substack{n_1,n_2\sim N\\ (n_1;n_2)=1}} \Lambda'(n_1)\Lambda'(n_2)\frac{1}{n_2}\hat{g}\left(\frac{l}{n_2}; n_1, n_2, c\right)e\left(\frac{c\overline{n}_1 l}{n_2}\right).$$

We now truncate the sums over j, k, l to finite ranges.

Lemma 6.21. *Suppose $\eta > 0$. The contribution to S_7 from (j, k, l) for which any of*

$$|l| \geq \frac{8Nz}{q},$$

$$|k| \geq \frac{qz^\eta}{M}$$

or

$$|j| \geq Nz^{-1+2\eta}$$

hold is $O_{B,\eta}(z^{-B})$ for any $B \in \mathbb{N}$.

Proof. From Lemma 6.19 we know that if $|t| \geq \frac{4z}{q}$ then $\hat{g}(t) = 0$. It follows that terms with

$$|l| \geq \frac{8Nz}{q}$$

make no contribution to the sum.

Let R be the set of (j, k) for which

$$|k| \geq \frac{qz^{\eta}}{M}$$

or

$$|j| \geq Nz^{-1+2\eta}.$$

To complete the proof it is sufficient to give a bound of $O_B(z^{-B})$ for

$$\sum_{(j,k)\in R} \left| \hat{W}\left(\frac{3Mk}{q}\right) \hat{g}\left(\frac{l}{n_2}; n_1, n_2, c\right) \right|.$$

By the definition of $\hat{g}$ this is at most

$$\int_{-\infty}^{\infty} \sum_{(j,k)\in R} \left| \hat{W}\left(\frac{3Mk}{q}\right) \hat{W}\left(\frac{tz}{q}\right) \hat{W}\left(\frac{(jq - ka - tn_1)z}{n_2 q}\right) \right| dt.$$

We make repeated use of the estimate (6.2). This shows that any part of the above where $\hat{W}$ is evaluated at a point x with $|x| \geq z^{\eta}$ may be bounded by $O_B(z^{-B})$. From the factor $\hat{W}(\frac{tz}{q})$ we see that such a bound holds when

$$|t| \geq \frac{q}{z^{1-\eta}}$$

and from the factor $\hat{W}(\frac{3Mk}{q})$ it holds when

$$|k| \geq \frac{qz^{\eta}}{M}.$$

Finally we assume that

$$|t| < \frac{q}{z^{1-\eta}}$$

and

$$|k| < \frac{qz^{\eta}}{M}.$$

In this case we have

$$|j| \geq Nz^{-1+2\eta}.$$

For sufficiently large q these assumptions imply that

$$\frac{(jq - ka - tn_1)z}{n_2 q} \gg z^{\eta}.$$

A bound of $O_B(z^{-B})$ therefore holds for all parts of the sum. □

Let S_8 be the sum S_7 with the following ranges of summation:

$$0 < |l| < \frac{8Nz}{q},$$

$$|k| < \frac{qz^\eta}{M}$$

and

$$|j| < Nz^{-1+2\eta}.$$

The last lemma shows that, for a fixed $\eta > 0$, we only need to bound S_8. We ignore any potential cancellation in the outer sums so we write

$$S_8 \ll \frac{Mz^2 \log N}{q^2 N} \sum_{\substack{|j|<Nz^{-1+2\eta},\, |k|<\frac{qz^\eta}{M},\, 0<|l|<\frac{8Nz}{q} \\ c\neq 0}} S_9$$

where

$$S_9 = \sum_{n_2 \sim N} \left| \sum_{\substack{n_1 \sim N \\ (n_1;n_2)=1}} \Lambda'(n_1) \hat{g}\left(\frac{l}{n_2}; n_1, n_2, c\right) e\left(\frac{c\overline{n}_1 l}{n_2}\right) \right|.$$

Let $h(n_1, n_2)$ be the weight in this sum:

$$h(n_1, n_2) = \hat{g}\left(\frac{l}{n_2}\right) = \int_{-\infty}^{\infty} \hat{W}\left(\frac{tz}{q}\right) \hat{W}\left(\frac{(c - tn_1)z}{n_2 q}\right) e(-\frac{tl}{n_2})\, dt.$$

Lemma 6.22. *The function h depends smoothly on n_1 and n_2. For $n_1, n_2 \sim N$ and the same η as above, we have*

$$h(n_1, n_2) \ll \frac{q}{z}$$

and

$$h_{n_1}(n_1, n_2) \ll_\eta \frac{q}{Nz^{1-\eta}},$$

where h_{n_1} denotes the partial derivative of h with respect to n_1.

Proof. Since W is smooth, it follows that g depends smoothly on n_1, n_2 and therefore so does $\hat{g}$ and hence so does h. The bound for h follows from that for $\hat{g}$ given in Lemma 6.19.

Differentiating we get

$$h_{n_1}(n_1, n_2) = \int_{-\infty}^{\infty} \hat{W}\left(\frac{tz}{q}\right) \frac{-tz}{n_2 q} \hat{W}'\left(\frac{(c - tn_1)z}{n_2 q}\right) e(-\frac{tl}{n_2})\, dt.$$

The contribution to the integral from $|t| \geq \frac{q}{z^{1-\eta/2}}$ can be shown to be sufficiently small. The remainder of the integral is then bounded by

$$\int_{|t|\leq \frac{q}{z^{1-\eta/2}}} \frac{tz}{Nq}\, dt \leq \int_{|t|\leq \frac{q}{z^{1-\eta/2}}} \frac{z^{\eta/2}}{N}\, dt \ll \frac{q}{Nz^{1-\eta}}.$$

□

We may now use partial summation to remove the weight $h(n_1, n_2)$ from S_9. We deduce that

$$S_9 \ll_\eta \frac{q}{z^{1-\eta}} S_{10}$$

where

$$S_{10} = \max_{N'\sim N} \sum_{n_2\sim N} \left| \sum_{\substack{N\leq n_1<N' \\ (n_1;n_2)=1}} \Lambda'(n_1) e\left(\frac{c\overline{n}_1 l}{n_2}\right)\right|.$$

We will estimate S_{10} using Theorem 4.4. To apply the theorem as stated we must use partial summation to replace the weight Λ' with the indicator function of the primes. However, this is not necessary since the proof of Theorem 4.4 actually estimates a sum weighted by Λ and the contribution of proper prime powers is sufficiently small (see the discussion at the start of Section 4.4.1). We conclude that for any $\epsilon > 0$ this gives

$$S_{10} \ll_\epsilon \left(1 + \frac{|cl|}{N^2}\right)^{\frac{1}{2}} N^{2-\alpha-\epsilon},$$

with the specific value $\alpha = \frac{1}{8}$. Since

$$0 < |cl| \ll N^2 z^{2\eta}$$

we deduce that

$$S_{10} \ll_\epsilon z^\eta N^{2-\alpha+\epsilon}.$$

We will eventually choose η in such a way that the factor z^η in this bound has no effect on the quality of our final result. It is the value of α which determines the size of the admissible range for N and hence the limitation on θ.

Lemma 6.23. *Under the assumptions (A2) we have*

$$S_7 \ll_A \frac{z^4 (\log z)^{-A}}{M},$$

for any fixed $A > 0$.

Proof. We deduce from our bound for S_{10} that

$$S_9 \ll_\epsilon \frac{q}{z^{1-2\eta}} N^{2-\alpha+\epsilon}$$

and therefore that

$$S_8 \ll_\epsilon \frac{N^{3-\alpha} z^{1+5\eta+\epsilon}}{q}.$$

By assumption we have

$$N \leq z^{\frac{16}{15}-\delta} = z^{\frac{2}{2-\alpha}-\delta}.$$

It follows that

$$\begin{aligned} MS_8 &\ll_\epsilon \frac{MN^{3-\alpha} z^{1+5\eta+\epsilon}}{q} \\ &\ll N^{2-\alpha} z^{2+5\eta+\epsilon} \\ &\leq z^{4-\delta(2-\alpha)+5\eta+\epsilon}. \end{aligned}$$

We can choose ϵ, η sufficiently small so that

$$5\eta + \epsilon < \delta(2-\alpha),$$

whence

$$S_8 \ll_\delta \frac{z^4 (\log z)^{-A}}{M}.$$

The bound for S_7 follows. □

Recall that we are assuming $N \gg \frac{q}{z^{1-\delta}}$. Observe that

$$\frac{q}{z} < z^{\frac{2}{2-\alpha}}$$

if and only if

$$q < z^{\frac{4-\alpha}{2-\alpha}}.$$

We note that

$$\frac{4-\alpha}{2-\alpha} \frac{1-\theta}{1+\theta} > 1$$

if and only if $\theta < \frac{1}{3-\alpha} = \frac{8}{23}$. We therefore impose the condition $\theta < \frac{8}{23}$ in order to ensure that our range for N is nonempty.

It should be noted that in this section, specifically in our application of Theorem 4.4, we have made nontrivial use of the fact that our coefficients are the indicator function of the primes. If we want to estimate a general Type II sum with coefficients β_n then different bounds must be used. Specifically, if we use Duke, Friedlander and Iwaniec's result [19, Theorem 2] then we can take $\alpha = \frac{1}{48}$. This is much worse than the value $\frac{1}{8}$ which we have for our special coefficients; although even that is considerably weaker than $\alpha = \frac{1}{2}$, which we conjecture should be best possible.

6.4.5 Completing the Proof of Theorem 6.13

The result follows on combining all the above estimates. We have

$$\begin{aligned} S_1 &= S_{1,1} - 2S_{1,2} + S_{1,3} \\ &= S_{1,1} - \frac{3N^2M\hat{W}(0)^3z^2}{q^2} + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right) \\ &= S_2 - \frac{3N^2M\hat{W}(0)^3z^2}{q^2} + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right) \\ &= S_3 + S_4 - \frac{3N^2M\hat{W}(0)^3z^2}{q^2} + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right) \\ &= S_4 + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right) \\ &= S_5 + S_7 + O_A\left(\frac{z^4(\log z)^{-A}}{M}\right) \\ &= O_A\left(\frac{z^4(\log z)^{-A}}{M}\right). \end{aligned}$$

It follows that

$$S = O_A(z^2(\log z)^{-A}),$$

as required.

6.5 Proof of the Theorems

6.5.1 Proof of Theorem 6.1

Suppose $MN = \frac{x}{4}$ and $M \leq z^{2-\delta}$, for some $\delta > 0$. For any $A > 0$ we have

$$\sum_{m\sim M} \Lambda'(m) = M + O_A(M(\log M)^{-A}).$$

It follows by Theorem 6.8 that

$$\sum_{m\sim M, n\sim N} \Lambda'(m)\Phi(mn) = \frac{\hat{W}(0)}{4}z^2 + O_{\delta,A}(z^2(\log z)^{-A});$$

the fact that $\Lambda'(n)$ is only bounded by $\log n$ does not matter as this factor can be absorbed into the error term.

Suppose, in addition, that

$$\max(z, \frac{q}{z^{1-\delta}}) \leq N \leq z^{\frac{16}{15}-\delta}.$$

It follows from Theorem 6.13 that for any $A > 0$ we have

$$\sum_{m\sim M, n\sim N} \Lambda'(m)(\Lambda'(n)-1)\Phi(mn) \ll_{A,\delta} z^2(\log z)^{-A}.$$

Combining these two estimates we immediately deduce that

$$\sum_{m\sim M, n\sim N} \Lambda'(m)\Lambda'(n)\Phi(mn) = \frac{\hat{W}(0)}{4}z^2 + O_{A,\delta}(z^2(\log z)^{-A}).$$

If m and n are prime then $\Lambda'(m)\Lambda'(n) \asymp (\log z)^2$. It follows that for sufficiently large q we have

$$\sum_{\substack{m\sim M, n\sim N \\ mn\in\mathcal{E}_2}} \Phi(mn) \gg \frac{z^2}{(\log z)^2}.$$

For $\theta < \frac{8}{23}$ there are exponents $a(\theta) < b(\theta)$ such that the above bound holds for any range $[M, 2M) \subseteq (z^{a(\theta)}, z^{b(\theta)}]$. There are therefore $\gg_\theta \log z$ dyadic ranges available so Theorem 6.1 follows.

6.5.2 Proof of Theorem 6.2

Suppose α is irrational and $\theta < \frac{8}{23}$. By replacing θ by $\theta + \epsilon$ for a sufficiently small $\epsilon > 0$ it is enough to show that there are infinitely many $n \in \mathcal{E}_2$ with

$$\|n\alpha\| \ll n^{-\theta}.$$

Let $\frac{c}{q}$ be a convergent in the continued fraction expansion of α with a sufficiently large denominator. We therefore have

$$|\alpha - \frac{c}{q}| \leq \frac{1}{q^2}.$$

If we let $x = q^{\frac{2}{1+\theta}}$, $z = \frac{x}{q}$, $a = \overline{c}$ and $\mathcal{A}$ as in Theorem 6.1 then any $n \in \mathcal{A}$ satisfies

$$an \equiv k \,(\mathrm{mod}\, q) \text{ for some } k \in [0, z].$$

We therefore have

$$\|\frac{an}{q}\| \leq \frac{z}{q}.$$

It follows that

$$\|n\alpha\| \leq \|(\alpha - \frac{c}{q})n\| + \|\frac{an}{q}\| \ll n^{-\theta}.$$

Since there are infinitely many convergents to α it is thus sufficient to show that $\mathcal{A}$ contains members of $\mathcal{E}_2$. This follows from Theorem 6.1.

6.5.3 Proof of Theorem 6.3

Recall that

$$\mathcal{P}_3(b) = \{j(b^2+1) + kb : j \in (0,b) \cap \mathbb{Z}, k \in [0,b) \cap \mathbb{Z}\}.$$

We take $\theta = \frac{1}{3}, q = b^2+1$, $z = b$, $x = b^3$ and $a = b$. The set $\mathcal{A}$ is then contained in $\mathcal{P}_3(b)$ so the result follows from Theorem 6.1.

Chapter 7

Almost-Prime Values of Binary Forms with One Prime Variable

7.1 Introduction

A well known problem in number theory is to show that if $f \in \mathbb{Z}[x]$ is an irreducible polynomial with $\deg f \geq 2$ then, provided the values of f have no fixed prime divisor, there are infinitely many $n \in \mathbb{Z}$ for which $f(n)$ is prime. This seems to be out of reach of current methods. However, using sieves one can show that there are infinitely many $n \in \mathbb{Z}$ for which $f(n)$ has a small number of prime factors. Let P_r denote numbers with at most r prime factors, counted with multiplicities, and let $k = \deg f$. Richert [44] showed that there are infinitely many n for which $f(n)$ is a P_{k+1}. An even harder question is to ask whether there are infinitely many primes p for which $f(p)$ is itself prime. This was also considered by Richert who showed that there are infinitely many p for which $f(p)$ is a P_{2k+1} (provided we impose conditions on f to avoid the obvious counterexamples).

Both problems are made easier if we consider irreducible binary forms $f \in \mathbb{Z}[x, y]$ instead of single variable polynomials. A theorem of Fermat states that any prime $p \equiv 1 \pmod 4$ is the sum of two squares and therefore the binary quadratic form $m^2 + n^2$ represents infinitely many primes. The case of a general binary quadratic form was handled by Dirichlet. Much more recently, Heath-Brown [34] showed that the cubic $m^3 + 2n^3$ represents infinitely many primes. If f is a binary form with $k \geq 4$ then the best result known is due to Greaves [28] who showed that if f is irreducible then the values $f(m, n)$ are infinitely often $P_{[k/2]+1}$, provided of course that they have no fixed prime divisor. In this chapter we will consider the values $f(p, n)$ of a binary form where n is an integer and p a prime. A result of Fouvry and Iwaniec [22] shows that there are infinitely many primes of the form $p^2 + n^2$; we are unaware of any

existing results dealing with higher degree forms. It is clear that by fixing the prime variable p and applying the above result of Richert to the resulting polynomial values we can obtain infinitely many P_{k+1}. We will improve this result for all $k \geq 3$ as follows.

Theorem 7.1. *Let $f \in \mathbb{Z}[x, y]$ be an irreducible binary form of degree $k \geq 3$. Suppose that for every prime p we have*

$$\#\{n \,(\mathrm{mod}\, p) : f(1, n) \equiv 0 \,(\mathrm{mod}\, p)\} < p.$$

There are then infinitely many pairs (p, n) with $n \in \mathbb{Z}$ and p prime for which $f(p, n)$ is a $P_{[3k/4]+1}$.

The proof of this depends on an improved "level of distribution" result for the values $f(p, n)$. Roughly speaking, we count the number of these which are divisible by an integer d when p and n have size N. If we were to consider each prime p separately then we could only handle $d \leq N^{1-\delta}$ for any $\delta > 0$. We will show that we can obtain a result on average over d provided that $d \leq N^{4/3-\delta}$. Theorem 7.1 then follows easily by using the weighted sieve. The details of our level of distribution are somewhat technical so we will leave a precise statement until Section 7.3.

Our level of distribution should be compared with Fouvry and Iwaniec's for the values $p^2 + n^2$ [22, Lemma 4]. In our notation their result essentially states that one can take d as large as $N^{2-\delta}$ for that form. Their proof depends crucially on the fact that the roots of the congruence $n^2 + 1 \equiv 0 \,(\mathrm{mod}\, d)$ satisfy very strong distribution properties. This enables them to prove a large sieve inequality for the fractions n/d which is essentially optimal. Our result also depends on a large sieve type inequality. However we do not have comparable distribution estimates for the roots of higher degree polynomial congruences and therefore our level of distribution is weaker. In the next section we will give details of the variant of the large sieve we use. It concerns the sum of a sequence of coefficients α_m, for example the indicator function of the primes, over the points (m, n) in a sublattice of $\mathbb{Z}^2$. We will show that if we average over a suitable family of lattices then we can control such a sum. To reduce the binary form question to one concerning lattices we use methods similar to those of Daniel [13].

In the proof of Theorem 7.1 we will give a lower bound for the number of almost-primes represented which is sufficient to show that the set of pairs (p, n), for which $f(p, n)$ is a $P_{[3k/4]+1}$, is Zariski dense. This would not be true if we fixed the prime variable and applied the result of Richert to the resulting polynomial. In the language

of Nevo and Sarnak [43] we have shown that the "saturation number" for this problem is at most $[3k/4] + 1$.

In this chapter the notation $\|x\|$ denotes the Euclidean length of a vector $x \in \mathbb{R}^2$. We will denote the indicator function of the primes by $\mathbf{1}_P(n)$. We use Lemma 2.1 to construct a smooth function W which has compact support in $[0, 1]$ and which takes nonnegative values. All our implied constants may depend on W and the binary form f.

7.2 A Large Sieve for Lattices

7.2.1 Introduction

Let α_m be a sequence of complex numbers with $|\alpha_m| \leq 1$ and let $\lambda \subseteq \mathbb{Z}^2$ be a lattice, as in Definition 2.2. For $N \geq 0$ we are interested in the quantity

$$\psi(\lambda, N, \alpha) = \sum_{(m,n)\in\lambda\cap(0,N]\times\mathbb{Z}} \alpha_m W\left(\frac{n}{N}\right).$$

We expect that for a typical λ we have

$$\psi(\lambda, N, \alpha) \approx \frac{N\hat{W}(0)}{\det\lambda} \sum_{m\leq N} \alpha_m.$$

We will show that this holds if we average over a suitable set of lattices λ. We will only consider the case that the set of m-coordinates of points in λ:

$$\{m : (m, n) \in \lambda\}$$

has greatest common factor 1, since if this does not hold then only a homogeneous arithmetic progression of m occur so the result cannot be true.

We will write $\det\lambda = d$ and restrict our consideration to lattices with $d \sim D$ for some parameter D. For a given lattice λ we let B_1, B_2 be the basis constructed in Lemma 2.4. Recall that we have

$$\|B_1\|\|B_2\| \asymp \det\lambda.$$

Let B be the matrix with rows B_1, B_2. Since we are free to choose the signs of both B_1 and B_2 we may assume that $B_{11} \geq 0$ and $\det B = \det\lambda$. We know that $\|B_1\| \ll (\det\lambda)^{1/2}$ and thus we have the same bound for B_{11} and B_{12}. We will consider an average over lattices where each possible value for B_{11} occurs at most once but we make no assumption on the distribution of the remaining entries in B.

Our result is then as follows. It should be noted that the shortest nonzero vector in λ may not be unique. In that case we are free to choose it in such a way that the conditions of the theorem are satisfied.

Theorem 7.2. *Let α_m be a sequence of complex numbers with $|\alpha_m| \leq 1$ and let $D, M_1 \geq 1$. Let Λ be a set of lattices in $\mathbb{Z}^2$ such that if $\lambda \in \Lambda$ then $\det \lambda \sim D$ and, letting B be as above, we have $B_{11} \sim M_1$. Assume that for each $\lambda \in \Lambda$ the m-coordinates of points are coprime, as described above. In addition, suppose that for each $m \sim M_1$ we have*

$$\#\{\lambda \in \Lambda : B_{11}(\lambda) = m\} \leq 1.$$

Suppose that $\delta > 0$.

1. *If $D \leq N^{1-\delta}$ then for any $A > 0$ we have*

$$\sum_{\lambda \in \Lambda} \left| \psi(\lambda, N, \alpha) - \frac{N\hat{W}(0)}{\det \lambda} \sum_{m \leq N} \alpha_m \right| \ll_{\delta, A} N^{-A}.$$

2. *If*

$$N^{1-\delta} \leq D < M_1 N^{1-\delta}$$

then

$$\sum_{\lambda \in \Lambda} \left| \psi(\lambda, N, \alpha) - \frac{N\hat{W}(0)}{\det \lambda} \sum_{m \leq N} \alpha_m \right| \ll_{\epsilon, \delta} N^{1+2\delta+\epsilon} M_1^{-1/2} D^{1/2}$$

for any $\epsilon > 0$.

It is useful to know when this result is nontrivial. We note that, since $\#\Lambda \ll M_1$, we have

$$\sum_{\lambda \in \Lambda} \frac{N\hat{W}(0)}{\det \lambda} \sum_{m \leq N} \alpha_m \ll \frac{N^2 M_1}{D}$$

and that

$$N^{1+2\delta+\epsilon} M_1^{-1/2} D^{1/2} < \frac{N^2 M_1}{D}$$

if and only if

$$D < N^{2/3 - 4\delta/3 - 2\epsilon/3} M_1.$$

Our bound can therefore only be nontrivial if $D \leq N^{2/3-\eta} M_1$ for some $\eta > 0$. In particular, since $M_1 \ll D^{1/2}$ the largest D we can handle is $D \ll N^{4/3-\eta}$. However, if M_1 is smaller then the range of D must be decreased.

7.2.2 Transforming the Sum

We can write

$$\lambda = \{(u,v)B : (u,v) \in \mathbb{Z}^2\}.$$

Our assumption that the m-coordinates of points in λ have greatest common factor 1 implies that we must have $(B_{11}; B_{21}) = 1$. In addition, since $B_{11} \sim M_1 \geq 1$ we have $B_{11} > 0$.

For a fixed $m \in (0, N]$ we consider the quantity

$$S(m) = \sum_{\substack{n\in\mathbb{Z}\\(m,n)\in\lambda}} W\left(\frac{n}{N}\right) = \sum_{\substack{(u,v)\in\mathbb{Z}^2\\B_{11}u+B_{21}v=m}} W\left(\frac{B_{12}u+B_{22}v}{N}\right).$$

The condition

$$m = B_{11}u + B_{21}v$$

is equivalent to

$$m \equiv B_{21}v \,(\mathrm{mod}\, B_{11})$$

in which case

$$u = \frac{m - B_{21}v}{B_{11}}.$$

We therefore have

$$\begin{aligned} S(m) &= \sum_{v\equiv m\overline{B_{21}}\,(\mathrm{mod}\,B_{11})} W\left(\frac{B_{12}(m-B_{21}v)+B_{11}B_{22}v}{B_{11}N}\right)\\ &= \sum_{v\equiv m\overline{B_{21}}\,(\mathrm{mod}\,B_{11})} W\left(\frac{B_{12}m+dv}{B_{11}N}\right)\\ &= \sum_{u\in\mathbb{Z}} W\left(\frac{B_{12}m+d(m\overline{B_{21}}+uB_{11})}{B_{11}N}\right)\\ &= \sum_{u\in\mathbb{Z}} W\left(\frac{m(B_{12}+d\overline{B_{21}})}{B_{11}N}+\frac{du}{N}\right). \end{aligned}$$

We may now apply the Poisson Summation Formula, (2.1), to deduce that

$$S(m) = \frac{N}{d}\sum_{v\in\mathbb{Z}} \hat{W}\left(\frac{vN}{d}\right) e\left(\frac{mv(B_{12}+d\overline{B_{21}})}{dB_{11}}\right).$$

We therefore conclude that

$$\psi(\lambda, N, \alpha) = \frac{N}{d}\sum_{v\in\mathbb{Z}} \hat{W}\left(\frac{vN}{d}\right)\sum_{m\leq N}\alpha_m e\left(\frac{mv(B_{12}+d\overline{B_{21}})}{dB_{11}}\right).$$

The $v = 0$ term in this is

$$\frac{N\hat{W}(0)}{d}\sum_{m\leq N}\alpha_m$$

which is precisely the main term we require.

For any $A \in \mathbb{N}$ we have the estimate

$$\hat{W}(x) \ll_A \min(1, |x|^{-A}).$$

Recall that we have $d \sim D$. We will truncate the sum over v to $|v| \leq DN^{-1+\delta}$. Specifically, for any $\delta > 0$ and $A \in \mathbb{N}$ we have

$$\frac{N}{d}\sum_{|v|>DN^{-1+\delta}}\hat{W}\left(\frac{vN}{d}\right)\sum_{m\leq N}\alpha_m e\left(\frac{mv(B_{12}+d\overline{B_{21}})}{dB_{11}}\right) \ll_{\delta,A} N^{-A}.$$

Combining all of the above we see that

$$\psi(\lambda, N, \alpha) = \frac{N\hat{W}(0)}{d}\sum_{m\leq N}\alpha_m + \psi_1(\lambda, N, \alpha, \delta) + O_{\delta,A}(N^{-A})$$

where

$$\psi_1(\lambda, N, \alpha, \delta) = \frac{N}{d}\sum_{0<|v|\leq DN^{-1+\delta}}\hat{W}\left(\frac{vN}{d}\right)\sum_{m\leq N}\alpha_m e\left(\frac{mv(B_{12}+d\overline{B_{21}})}{dB_{11}}\right).$$

It remains to bound ψ_1, at least on average over λ. This is trivial if $DN^{-1+\delta} < 1$ that is $D < N^{1-\delta}$ as then $\psi_1 = 0$. This is thus enough to prove the first assertion in Theorem 7.2. We may therefore assume that $D \geq N^{1-\delta}$.

We have

$$\psi_1(\lambda, N, \alpha, \delta) \ll \frac{N}{D}\sum_{0<|v|\leq DN^{-1+\delta}}\left|\sum_{m\leq N}\alpha_m e\left(\frac{mv(B_{12}+d\overline{B_{21}})}{dB_{11}}\right)\right|.$$

We will remove the factor $e\left(\frac{mvB_{12}}{dB_{11}}\right)$ using partial summation. This results in

$$\psi_1(\lambda, N, \alpha, \delta) \ll \frac{N}{D}\left(1 + N^{\delta}\frac{|B_{12}|}{B_{11}}\right)\sum_{0<|v|\leq DN^{-1+\delta}}\max_{N'\leq N}\left|\sum_{m\leq N'}\alpha_m e\left(\frac{mv\overline{B_{21}}}{B_{11}}\right)\right|.$$

Recalling that $B_{12} \ll D^{1/2}$, $B_{11} \sim M_1 \ll D^{1/2}$ and using our assumption that each B_{11} occurs at most once we thus see that

$$\begin{aligned}&\sum_{\lambda\in\Lambda}|\psi_1(\lambda, N, \alpha, \delta)|\\ &\ll N^{1+\delta}D^{-1/2}M_1^{-1}\sum_{B_{11}\sim M_1}\max_{(B_{21};B_{11})=1}\sum_{0<|v|\leq DN^{-1+\delta}}\max_{N'\leq N}\left|\sum_{m\leq N'}\alpha_m e\left(\frac{mv\overline{B_{21}}}{B_{11}}\right)\right|.\end{aligned}$$

By Cauchy's inequality we may bound this by

$$N^{1/2+3\delta/2}M_1^{-1/2}\psi_2(\Lambda,N,\alpha,\delta)^{1/2}$$

where

$$\psi_2(\Lambda,N,\alpha,\delta)=\sum_{B_{11}\sim M_1}\max_{(b;B_{11})=1}\sum_{0<|v|\leq DN^{-1+\delta}}\max_{N'\leq N}\left|\sum_{m\leq N'}\alpha_m e\left(\frac{mvb}{B_{11}}\right)\right|^2.$$

7.2.3 Applying the Large Sieve

Each $\frac{vb}{B_{11}}$ occurring in ψ_2 is congruent mod $\mathbb{Z}$ to a unique $\frac{a}{q}$ with $(a;q)=1$, $0\leq a<q$ and $q\ll M_1$. We will group together terms with the same a/q and bound the resulting sums over dyadic intervals $q\sim Q$. We must therefore give an upper bound for the number of times each $\frac{a}{q}$ occurs in our sum.

Lemma 7.3. *Assume that $D,M_1\geq 1$ and $\delta>0$ satisfy*

$$N^{1-\delta}\leq D<M_1N^{1-\delta}.$$

Suppose that for each integer $B_{11}\sim M_1$ we are given an integer b with $(b;B_{11})=1$. Then, if $(a;q)=1$ and $0\leq a<q\ll M_1$, we have

$$\#\{B_{11}\sim M_1,0<|v|\leq DN^{-1+\delta}:\frac{vb}{B_{11}}\equiv\frac{a}{q}\,(\mathrm{mod}\,\mathbb{Z})\}$$

$$=\begin{cases}0 & \text{if } q<N^{1-\delta}M_1D^{-1}\\ O(M_1q^{-1}) & \text{otherwise.}\end{cases}$$

Proof. If

$$\frac{vb}{B_{11}}\equiv\frac{a}{q}\,(\mathrm{mod}\,\mathbb{Z})$$

with $(a;q)=1$ then since $(b;B_{11})=1$ we must have

$$q=\frac{B_{11}}{(B_{11};v)}\geq\frac{B_{11}}{|v|}\geq M_1N^{1-\delta}D^{-1}.$$

This proves that there are no solutions if $q<N^{1-\delta}M_1D^{-1}$ so the first part of the lemma follows.

For the remainder of the proof we suppose that $q\geq N^{1-\delta}M_1D^{-1}$. If $(a;q)=1$ and

$$\frac{vb}{B_{11}}\equiv\frac{a}{q}\,(\mathrm{mod}\,\mathbb{Z})$$

then $q|B_{11}$. It follows that

$$vb \equiv aB_{11}/q \,(\mathrm{mod}\, B_{11}).$$

We therefore see that for given q and B_{11} there are $O(DN^{-1+\delta}M_1^{-1}+1)$ possible v. Moreover, since $q \mid B_{11}$ there are $O(M_1q^{-1})$ possible B_{11}. By assumption we know that

$$DN^{-1+\delta}M_1^{-1} < 1$$

so we may conclude that the quantity of interest is $O(M_1q^{-1})$ as required. □

Using the last lemma we deduce that the part of ψ_2 with $q \sim Q$, for $Q \geq N^{1-\delta}M_1D^{-1}$, is bounded by

$$M_1Q^{-1}\sum_{q\sim Q}\sum_{(a;q)=1}\max_{N'\leq N}\left|\sum_{m\leq N'}\alpha_m e\left(\frac{am}{q}\right)\right|^2.$$

Applying a maximal form of the large sieve, as given by Montgomery [41], we can majorise this by

$$M_1Q^{-1}N(N+Q^2) = M_1N(Q^{-1}N+Q).$$

Recall that

$$N^{1-\delta}M_1D^{-1} \ll Q \ll M_1$$

so our bound is at most

$$M_1N(N^{\delta}M_1^{-1}D + M_1).$$

We have $M_1 \ll D^{1/2}$ so the first term is always larger and the bound is simply $N^{1+\delta}D$. This holds for all the dyadic intervals $q \sim Q$ under consideration so we conclude that for any $\epsilon > 0$ we have

$$\psi_2(\Lambda, N, \alpha, \delta) \ll_\epsilon N^{1+\delta+\epsilon}D$$

and therefore that

$$\sum_{\lambda\in\Lambda}|\psi_1(\lambda, N, \alpha, \delta)| \ll_\epsilon N^{1+2\delta+\epsilon}M_1^{-1/2}D^{1/2}.$$

This completes the proof of Theorem 7.2.

7.3 Level of Distribution

Rather than only considering the values $f(p,n)$ we will consider values $\alpha_m f(m,n)$ for sequences of complex numbers α_m with $|\alpha_m| \leq 1$. Letting α_m be the indicator function of the primes will then recover the case in which we are most interested. Our approach is able to handle any sequence α_m but there are a number of unpleasant technicalities to deal with. To avoid this we will only consider α_m supported on primes m. We will study the quantity

$$A_d(N,\alpha) = \sum_{\substack{(m,n)\in(0,N]\times\mathbb{Z}\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, d)}} \alpha_m W\left(\frac{n}{N}\right).$$

We expect that for α_m supported on primes we have, at least on average over a suitable range of d,

$$A_d(N,\alpha) \approx M_d(N,\alpha)$$

where

$$M_d(N,\alpha) = \frac{N\nu(d)\hat{W}(0)}{d} \sum_{m\leq N} \alpha_m$$

and $\nu(d)$ is the number of solutions, n, of the congruence

$$f(1,n) \equiv 0 \,(\mathrm{mod}\, d).$$

We therefore wish to estimate the sum

$$\sum_{d\sim D} |A_d(N,\alpha) - M_d(N,\alpha)|.$$

Theorem 7.4. *Let α_m be a sequence of complex numbers with $|\alpha_m| \leq 1$ supported on prime values of m. Suppose $\delta_1 > 0$ and $1 \leq D \leq N^{4/3-\delta_1}$. There exists a $\delta_2 > 0$ depending only on δ_1 such that*

$$\sum_{d\sim D} |A_d(N,\alpha) - M_d(N,\alpha)| \ll_{\delta_1} N^{2-\delta_2}.$$

The advantage of working with α_m supported on primes is that the contribution to our sum from points (m,n) with $(m;d) > 1$ is small.

Lemma 7.5. *Under the hypotheses of Theorem 7.4 we have, for any $\epsilon > 0$, that*

$$\sum_{d\sim D} \sum_{\substack{(m,n)\in(0,N]\times\mathbb{Z}\\ (m;d)>1, f(m,n)\equiv 0 \,(\mathrm{mod}\, d)}} |\alpha_m| W\left(\frac{n}{N}\right) \ll_\epsilon N^{1+\epsilon}.$$

Proof. Since α_m is supported on primes the condition $(m;d) > 1$ implies $m|d$. We therefore have

$$\begin{aligned}
&\sum_{d\sim D} \sum_{\substack{(m,n)\in(0,N]\times\mathbb{Z}\\(m;d)>1, f(m,n)\equiv 0 \,(\mathrm{mod}\, d)}} |\alpha_m| W\left(\frac{n}{N}\right) \\
&\ll \sum_{d\sim D} \sum_{\substack{m\leq N\\ m|d}} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, d)}} 1 \\
&= \sum_{m\leq N} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, m)}} \#\{d | f(m,n) : d\sim D, m|d\} \\
&\leq \sum_{m\leq N} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, m)}} \tau(f(m,n)) \\
&\ll_\epsilon \sum_{m\leq N} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, m)}} N^\epsilon,
\end{aligned}$$

where we have used the fact that f is irreducible so $f(m,n) \neq 0$.

Let f_0 be the coefficient of $n^{\deg f}$ in f. We have

$$\sum_{\substack{m\leq N\\ m|f_0}} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, m)}} N^\epsilon \ll_f N^{1+\epsilon}.$$

If a prime m does not divide f_0 but $m|f(m,n)$ then we must have $m|n$. Therefore

$$\sum_{\substack{m\leq N\\ m\nmid f_0}} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ f(m,n)\equiv 0 \,(\mathrm{mod}\, m)}} N^\epsilon = \sum_{\substack{m\leq N\\ m\nmid f_0}} \mathbf{1}_P(m) \sum_{\substack{n\leq N\\ m|n}} N^\epsilon \ll_\epsilon N^{1+\epsilon}.$$

The result follows. □

Our proof of Theorem 7.4 begins by applying methods from the geometry of numbers, similar to those employed by Daniel in [13]. We call a point (m,n) primitive modulo d if $(m;n;d) = 1$. We say that the primitive points (m_1,n_1) and (m_2,n_2) are equivalent modulo d if

$$(m_2,n_2) \equiv \lambda(m_1,n_1) \,(\mathrm{mod}\, d)$$

for some $\lambda \in \mathbb{Z}$ which must necessarily satisfy $(\lambda;d) = 1$. We observe that the property $f(m,n) \equiv 0 \,(\mathrm{mod}\, d)$ is preserved by equivalence so we may let $\mathcal{U}(d)$ be the set of equivalence classes mod d for which it holds.

For each $x \in \mathcal{U}(d)$ we let $\lambda(x)$ be the lattice in $\mathbb{Z}^2$ generated by the points of x. Thus if we fix an $(m,n) \in x$ then $\lambda(x)$ consists of all the points congruent mod d to

some multiple of (m,n). It follows that $\det \lambda(x) = d$ and that the set of primitive points in $\lambda(x)$ is precisely x. Each primitive solution of $f(m,n) \equiv 0 \pmod d$ occurs in precisely one lattice $\lambda(x)$ but a nonprimitive solution may occur in more than one. Since any nonprimitive point has $(m;d) > 1$ and $\#\mathcal{U}(d) \ll_{\epsilon,f} d^{\epsilon}$, (see for example Daniel [13, (3.5)]), we can handle this multiplicity issue with the last lemma.

We let $\mathcal{U}'(d)$ be the subset of $\mathcal{U}(d)$ containing those x generated by a point (m,n) with $(m;d) = 1$. If $x \notin \mathcal{U}'(d)$ then all $(m,n) \in \lambda(x)$ have $(m;d) > 1$. It is clear that $\#\mathcal{U}'(d) = \nu(d)$. We can therefore deduce using the last lemma that

$$\sum_{d\sim D} |A_d(N,\alpha) - M_d(N,\alpha)|$$

$$\ll_{\epsilon} N^{1+\epsilon} + \sum_{d\sim D} \sum_{x\in\mathcal{U}'(d)} \left| \sum_{(m,n)\in\lambda(x)\cap(0,N]\times\mathbb{Z}} \alpha_m W\left(\frac{n}{N}\right) - \frac{N\hat{W}(0)}{d} \sum_{m\leq N} \alpha_m \right|.$$

We must therefore bound

$$S = \sum_{d\sim D} \sum_{x\in\mathcal{U}'(d)} \left| \psi(\lambda(x),N,\alpha) - \frac{N\hat{W}(0)}{d} \sum_{m\leq N} \alpha_m \right|$$

where ψ is the quantity studied in the last section.

We let $B_1(x), B_2(x)$ denote the minimal basis of $\lambda(x)$ and write $B(x)$ for the matrix with rows the B_i. If $D \geq N^{\delta_1}$ it is necessary to remove from S any lattices for which B_{11} is unusually small, say $B_{11}(x) \leq D^{1/2-\eta}$ for some $\eta > 0$. For these lattices we bound the sums

$$\sum_{d\sim D} \sum_{\substack{x\in\mathcal{U}'(d) \\ B_{11}(x)\leq D^{1/2-\eta}}} |\psi(\lambda(x),N,\alpha)|$$

and

$$\sum_{d\sim D} \sum_{\substack{x\in\mathcal{U}'(d) \\ B_{11}(x)\leq D^{1/2-\eta}}} \left| \frac{N\hat{W}(0)}{d} \sum_{m\leq N} \alpha_m \right|.$$

The first sum is bounded by

$$S_1 = \sum_{d\sim D} \sum_{\substack{x\in\mathcal{U}'(d) \\ B_{11}(x)\leq D^{1/2-\eta}}} \#(\lambda(x)\cap[0,N]^2)$$

whilst the second is at most of order

$$S_2 = \frac{N^2}{D} \sum_{d\sim D} \sum_{\substack{x\in\mathcal{U}'(d) \\ B_{11}(x)\leq D^{1/2-\eta}}} 1.$$

We estimate these using the following lemma.

Lemma 7.6. *Suppose $0 \neq (u,v) \in \mathbb{Z}^2$. Then for any $\epsilon > 0$ we have*

$$\#\{(d,x) : d \sim D, x \in \mathcal{U}'(d), (u,v) \in \lambda(x)\} \ll_\epsilon \|(u,v)\|^\epsilon.$$

Proof. Since f is irreducible and $(u,v) \neq 0$ we know that $f(u,v) \neq 0$. The number of possible d is then bounded by

$$\tau(f(u,v)) \ll_\epsilon \|(u,v)\|^\epsilon.$$

For each such d the number of possible x cannot exceed $\nu(d) = O_\epsilon(d^\epsilon)$. The result follows. □

Recall that $\det \lambda(x) \sim D$. Therefore, if $B_{11}(x) \leq D^{1/2-\eta}$ we must have $B_{11}(x) = (u,v)$ for some $0 \neq (u,v) \in \mathbb{Z}^2$ with $u \leq D^{1/2-\eta}$ and $v \ll D^{1/2}$. It follows that the number of terms in our sums S_1, S_2 is at most $O_\epsilon(D^{1-\eta}N^\epsilon)$. We immediately deduce that

$$S_2 \ll_\epsilon N^{2+\epsilon}D^{-\eta}.$$

To bound S_1 we use Lemma 2.6 to get

$$S_1 \ll \sum_{d \sim D} \sum_{\substack{x \in \mathcal{U}'(d) \\ B_{11}(x) \leq D^{1/2-\eta}}} \left(\frac{N^2}{d} + \frac{N}{\|B_1(x)\|} + 1 \right).$$

From the above discussion we obtain the bounds

$$\sum_{d \sim D} \sum_{\substack{x \in \mathcal{U}'(d) \\ B_{11}(x) \leq D^{1/2-\eta}}} \frac{N^2}{d} \ll_\epsilon N^{2+\epsilon}D^{-\eta}$$

and

$$\sum_{d \sim D} \sum_{\substack{x \in \mathcal{U}'(d) \\ B_{11}(x) \leq D^{1/2-\eta}}} 1 \ll_\epsilon D^{1-\eta}N^\epsilon.$$

Finally we use Lemma 7.6 to get

$$\begin{aligned} &\sum_{d \sim D} \sum_{\substack{x \in \mathcal{U}'(d) \\ B_{11}(x) \leq D^{1/2-\eta}}} \frac{N}{\|B_1(x)\|} \\ &\ll_\epsilon N^{1+\epsilon} \sum_{0 < \|(u,v)\| \ll D^{1/2}} \frac{1}{\sqrt{u^2+v^2}} \\ &\ll_\epsilon N^{1+\epsilon}D^{1/2}. \end{aligned}$$

We conclude that

$$S_1 + S_2 \ll_\epsilon N^{1+\epsilon} D^{1/2} + D^{1-\eta} N^\epsilon + N^{2+\epsilon} D^{-\eta}$$

so this bound also holds for the contribution to S from lattices with $B_{11} \leq D^{1/2-\eta}$. Recalling that $N^{\delta_1} \leq D \leq N^{4/3-\delta_1}$ we see that if we take a small enough ϵ then this bound is $O(N^{2-\delta_2})$ for $\delta_2 > 0$ sufficiently small in terms of δ_1 and η. It should be noted that the exponent $\frac{4}{3}$ is not critical for this part of the argument.

It remains to consider

$$S_3 = \sum_{d \sim D} \sum_{\substack{x \in \mathcal{U}'(d) \\ B_{11}(x) > D^{1/2-\eta}}} \left| \psi(\lambda(x), N, \alpha) - \frac{N\hat{W}(0)}{d} \sum_{m \leq N} \alpha_m \right|,$$

to which we will apply Theorem 7.2. If $D \geq N^{\delta_1}$ then η is a quantity that we can take arbitrarily small, whereas if $D \leq N^{\delta_1}$ then we shall take $\eta > 1/2$ so that all lattices are included.

If $x \in \mathcal{U}'(d)$ then $\lambda(x)$ consists of all points congruent modulo d to a multiple of some (m, n) with $(m; d) = 1$. It follows that the m-coordinates of points in $\lambda(x)$ are coprime. The sum is over lattices $\lambda(x)$ which have

$$\det \lambda(x) \sim D \quad \text{and} \quad D^{1/2-\eta} < B_{11}(x) \ll D^{1/2}.$$

For each possible value of $B_{11}(x)$ in this range there are $O(D^{1/2})$ permissible values for $B_{12}(x)$. It follows by Lemma 7.6 that the number of lattices in the sum with any given value of B_{11} is at most $O_\epsilon(D^{1/2} N^\epsilon)$. We therefore subdivide S_3 into $O_\epsilon(N^\epsilon)$ dyadic intervals depending on the size of B_{11} and then subdivide each dyadic sum into $O_\epsilon(D^{1/2} N^\epsilon)$ subsums in which each possible value of B_{11} occurs at most once. The resulting subsums may be estimated using Theorem 7.2. Suppose $\delta > 0$. If $D \leq N^{1-\delta}$ we get

$$S_3 \ll_{\epsilon, A} D^{1/2} N^{\epsilon - A},$$

for any $A \in \mathbb{N}$, which is certainly small enough. If $D \geq N^{1-\delta}$ we must check the condition

$$D \leq M_1 N^{1-\delta}.$$

However $M_1 \geq D^{1/2-\eta}$ so it is sufficient that

$$D \leq N^{\frac{1-\delta}{1/2+\eta}}.$$

Since $D \leq N^{4/3-\delta_1}$ this is certainly satisfied if we take δ, η small enough. (Since $D \geq N^{1-\delta}$ we are in the case in which any $\eta > 0$ is admissible). We may therefore deduce from Theorem 7.2 that

$$S_3 \ll_\epsilon N^\epsilon D^{1/2} \cdot N^{1+2\delta+\epsilon} D^{1/4+\eta/2} \ll_\epsilon N^{1+2\delta+\epsilon} D^{3/4+\eta/2}.$$

Since $D \leq N^{4/3-\delta_1}$ we see that if we take δ, ϵ and η sufficiently small in terms of δ_1 then

$$S_3 \ll_{\delta_1} N^{2-\delta_2}$$

for some $\delta_2 > 0$. This is where the value $4/3$ is critical as for larger D we do not get a nontrivial bound from Theorem 7.2.

We conclude that

$$\sum_{d \sim D} |A_d(N, \alpha) - M_d(N, \alpha)| \ll_{\delta_1} N^{2-\delta_2}$$

for some $\delta_2 > 0$, thus completing the proof of Theorem 7.4.

When we apply the weighted sieve in the next section we will use the following upper bound to show that not too many values of f are divisible by the square of a prime.

Lemma 7.7. *Let α_m be a sequence of complex numbers with $|\alpha_m| \leq 1$. For any $\delta_1 > 0$ there exists a $\delta_2 > 0$, depending only on δ_1, such that*

$$\sum_{N^{\delta_1} \leq p \leq N^{2-\delta_1}} |A_{p^2}(N, \alpha)| \ll_{\delta_1} N^{2-\delta_2},$$

the sum being over primes p.

Proof. We have

$$\begin{aligned} A_{p^2}(N, \alpha) &= \sum_{\substack{(m,n) \in (0,N] \times \mathbb{Z} \\ f(m,n) \equiv 0 \,(\mathrm{mod}\, p^2)}} \alpha_m W\left(\frac{n}{N}\right) \\ &\ll \#\{(m, n) \in [0, N]^2 : f(m, n) \equiv 0 \,(\mathrm{mod}\, p^2)\}. \end{aligned}$$

If $f(m, n) \equiv 0 \,(\mathrm{mod}\, p^2)$ then $(m, n) \in \lambda(x)$ for at least one $x \in \mathcal{U}(p^2)$. It follows that

$$A_{p^2}(N, \alpha) \ll \sum_{x \in \mathcal{U}(p^2)} \#(\lambda(x) \cap [0, N]^2).$$

Applying Lemma 2.6 we may bound this by

$$\sum_{x\in\mathcal{U}(p^2)}(\frac{N^2}{p^2}+\frac{N}{\|B_1(x)\|}+1).$$

Using that $\#\mathcal{U}(p^2)\ll_\epsilon N^\epsilon$ we have

$$\sum_{N^{\delta_1}\leq p\leq N^{2-\delta_1}}\sum_{x\in\mathcal{U}(p^2)}\left(\frac{N^2}{p^2}+1\right)\ll_\epsilon N^{2-\delta_1+\epsilon}.$$

It therefore remains to estimate

$$N\sum_{N^{\delta_1}\leq p\leq N^{2-\delta_1}}\sum_{x\in\mathcal{U}(p^2)}\frac{1}{\|B_1(x)\|}.$$

If points are equivalent modulo p^2 then they must also be equivalent modulo p. It follows that if $x\in\mathcal{U}(p^2)$ then there is some $x'\in\mathcal{U}(p)$ with $\lambda(x)\subseteq\lambda(x')$. Different equivalence classes in $\mathcal{U}(p^2)$ may give rise to the same class in $\mathcal{U}(p)$ but the total number of times a class may occur cannot exceed $\#\mathcal{U}(p^2)\ll_\epsilon N^\epsilon$. Our sum is therefore majorised by

$$N^{1+\epsilon}\sum_{N^{\delta_1}\leq p\leq N^{2-\delta_1}}\sum_{x\in\mathcal{U}(p)}\frac{1}{\|B_1(x)\|}.$$

To estimate this final sum we use part of Daniel's proof of [13, Lemma 3.2], which is very similar to our above derivation of a bound on S_1. Specifically, if we set $Q=N^{2-\delta_1}$, our sum is bounded by the quantity $T_1^*(Q)$ defined in that proof so it is $O_\epsilon(N^{1-\delta_1/2+\epsilon})$. We therefore conclude that

$$N^{1+\epsilon}\sum_{N^{\delta_1}\leq p\leq N^{2-\delta_1}}\sum_{x\in\mathcal{U}(p)}\frac{1}{\|B_1(x)\|}\ll_\epsilon N^{2-\delta_1/2+\epsilon}.$$

The result follows on combining the above estimates and taking $\delta_2<\delta_1/2$. □

7.4 Proof of Theorem 7.1

We will sieve the sequence $\mathcal{A}=(a_l)$ given by

$$a_l=\sum_{\substack{(m,n)\in(0,N]\times\mathbb{Z}\\ |f(m,n)|=l}}\mathbf{1}_P(m)W\left(\frac{n}{N}\right).$$

This is supported on $l\ll_f N^k$ and by Theorem 7.4 we know that it has level of distribution N^θ for any $\theta<\frac{4}{3}$. Recall that $\nu(d)$ counts solutions of the congruence

$$f(1,n)\equiv 0\,(\mathrm{mod}\,d).$$

Since f is irreducible it can be shown using ideas from algebraic number theory, see for example Diamond and Halberstam [18, Proposition 10.1], that

$$\sum_{p \leq x} \frac{\nu(p) \log p}{p} = \log x + O(1).$$

We therefore use a 1-dimensional weighted sieve. By assumption we know that $\nu(p) < p$ for all primes p. It can therefore be shown that

$$\prod_{p<z} (1 - \frac{\nu(p)}{p}) = \frac{c_f + o(1)}{\log z}$$

for some $c_f > 0$.

We use the weighted sieve as described by Greaves in [29, Chapter 5]. If $r \geq 2$ we deduce that if

$$\frac{3}{4}k < r - \delta_r$$

then for all sufficiently large N we have

$$\sum_{l}^{\star} a_l \gg \frac{N^2}{(\log N)^2},$$

where $\sum^{\star}$ denotes a sum over certain l which are the product of at most r distinct primes. Specifically, [29, Section 5.2] shows that we can take $\delta_r = 0.144001\ldots$. The above estimate therefore follows if

$$r > \frac{3}{4}k + 0.15$$

which is equivalent to $r \geq [3k/4] + 1$. Observe that it is essential that we had $\delta_r < \frac{1}{4}$. The simplest form of the weighted sieve [29, Section 5.1] would therefore have been insufficient.

It remains to show that we can produce numbers with at most r prime factors when counted with multiplicity. Examining the construction of the sieve it can be seen that there are constants $0 < \alpha < \beta < 2$, depending on r, such that $\sum^{\star}$ is actually a sum over l all of whose prime factors exceed N^{α} and for which

$$\sum_{\substack{p|l \\ p \leq N^{\beta}}} 1 + \sum_{p \geq N^{\beta}} \sum_{a:\, p^a | l} 1 \leq r.$$

This means that only prime factors smaller than N^{β} are counted without multiplicities. We can deduce from Lemma 7.7 that the contribution of l which are divisible

by p^2 for $p \in [N^\alpha, N^\beta]$ is $O(N^{2-\delta})$ for some $\delta > 0$ depending on α and β. We may therefore conclude that for all sufficiently large N we have

$$\sum_{l \in P_r} a_l \gg \frac{N^2}{(\log N)^2}$$

thereby completing the proof of Theorem 7.1.

Chapter 8

Cubic Polynomials Represented by Norm Forms

8.1 Introduction

A fundamental question in arithmetic geometry is to determine whether a given algebraic variety, defined over $\mathbb{Q}$, has a point over $\mathbb{Q}$. It is clear that a necessary condition for this is that the variety has points over all completions of $\mathbb{Q}$, that is over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p. If this condition holds and the variety has a point over $\mathbb{Q}$ then we say that it satisfies the Hasse principle, whereas if there are points over all completions of $\mathbb{Q}$ but not over $\mathbb{Q}$ itself then we say it violates the Hasse principle. The well known Hasse–Minkowski theorem states that any quadratic form defined over $\mathbb{Q}$ satisfies the Hasse principle. However, varieties defined by higher degree polynomials may violate it. A famous example, due to Selmer, is the projective curve given by

$$3x^3 + 4y^3 + 5z^3 = 0.$$

In this chapter we will consider the variety defined by the Diophantine equation

$$f(t) = \mathbf{N}(x_1, \ldots, x_k) \neq 0, \tag{8.1}$$

where $f \in \mathbb{Z}[x]$ is a polynomial and $\mathbf{N}(x_1, \ldots, x_k)$ is a full norm form for some number field $K/\mathbb{Q}$. Thus, for some basis $\omega_1, \ldots, \omega_k$ for the degree k extension $K/\mathbb{Q}$, we have

$$\mathbf{N}(x_1, \ldots, x_k) = N_{K/\mathbb{Q}}(x_1\omega_1 + \ldots + x_k\omega_k).$$

We are interested in describing families of fields $K/\mathbb{Q}$ and polynomials f for which (8.1) satisfies the Hasse principle.

Browning and Heath-Brown, in [7], describe many of the existing results on this problem. They establish that the Hasse principle holds when f is an irreducible polynomial of degree 2 and $K/\mathbb{Q}$ is a quartic extension containing a root of f. Their results were extended by Derenthal, Smeets and Wei [17] who establish that for any quadratic f and any extension $K/\mathbb{Q}$ the Brauer–Manin obstruction is the only obstruction to the Hasse principle.

We are interested in the case that f is an irreducible cubic. Previous work establishes that the Hasse principle holds when $K/\mathbb{Q}$ has degree 2 or 3. Specifically, if $[K:\mathbb{Q}] = 2$ then (8.1) defines a Châtelet surface so the result follows by the work of Colliot-Thélène, Sansuc and Swinnerton-Dyer [12], whereas if $[K:\mathbb{Q}] = 3$ it follows from Colliot-Thélène and Salberger [11]. As far as we know, no case of the Hasse principle has been established when f is an irreducible cubic and $[K:\mathbb{Q}] > 3$.

If, instead of being irreducible, f splits completely into linear factors over $\mathbb{Q}$ then the problem is considerably different. A recent result of Browning and Matthiesen [8] establishes that for any such f and any number field $K/\mathbb{Q}$ the Hasse principle holds provided that the Brauer–Manin obstruction is empty.

We will say that the number field $K/\mathbb{Q}$ satisfies the Hasse norm principle if, for any $a \in \mathbb{Q}^*$, a sufficient condition for the equation

$$N_{K/\mathbb{Q}}(\alpha) = a$$

to have a solution $\alpha \in K$ is that a is a norm from the group of ideles, I_K, of K. In other words the Hasse norm principle asserts that

$$\mathbb{Q}^* \cap N_{K/\mathbb{Q}}(I_K) = N_{K/\mathbb{Q}}(K^*).$$

Our main result is the following, which establishes the Hasse principle for a certain class of fields $K/\mathbb{Q}$, whose degree may be arbitrarily large.

Theorem 8.1. *Let $f \in \mathbb{Z}[x]$ be an irreducible cubic and let $K/\mathbb{Q}$ be a number field satisfying the Hasse norm principle. Suppose that there exists a prime $q \geq 7$ such that for all but finitely many unramified primes p with $p \not\equiv 1 \pmod{q}$ the prime ideal factorisation of p,*

$$(p) = \prod_{i=1}^{r} P_i,$$

consists of prime ideals P_i of norms p^{f_i} with $f_1, \dots, f_r$ coprime. In addition, assume that the number field generated by f is not contained in the cyclotomic field $\mathbb{Q}(\zeta_q)$. We can then conclude that (8.1) satisfies the Hasse principle.

An example of a field $K/\mathbb{Q}$ satisfying all the conditions of this theorem can be found by adjoining to $\mathbb{Q}$ a root of

$$x^q - 2,$$

for any prime $q \geq 7$. Since $[K : \mathbb{Q}] = q$ is prime, the extension $K/\mathbb{Q}$ satisfies the Hasse norm principle by the work of Bartels [4]. In addition, for any prime $p \not\equiv 1 \pmod{q}$ the equation

$$x^q - 2 \equiv 0 \pmod{p}$$

has a root. If we exclude finitely many values of p it then follows that K has an integral ideal of norm p. This clearly implies that the degrees f_i are coprime. In conclusion, for this choice of K and any f which does not generate a subfield of $\mathbb{Q}(\zeta_q)$, (8.1) satisfies the Hasse principle.

After various algebraic reductions we will prove Theorem 8.1 using sieve methods. We will show that for an integer to be a norm from $K/\mathbb{Q}$ it is sufficient that it satisfies certain congruences and that it has no prime factors $p \equiv 1 \pmod{q}$. We may therefore estimate the number of norms in a set of integers by sieving out these primes. Our sieve problem will have dimension $\frac{2}{q-1}$. For large q this is close to 0 and therefore both the upper and lower bounds coming from the sieve are close to the truth. We will show that for $q \geq 7$ the losses in the sieve are sufficiently small to give us a positive lower bound for the number of rational points on (8.1). There are many well known applications of sieves whose dimension is an integer or $\frac{1}{2}$. However we are not aware of any existing work which uses a sieve whose dimension is between 0 and $\frac{1}{2}$.

It seems very likely that the method of this chapter can be adapted to prove weak approximation, meaning that the set of rational points is dense in the set of idelic points, for the variety (8.1) provided that it can be shown that weak approximation holds for the equation

$$N_{K/\mathbb{Q}}(u) = 1.$$

As part of our proof we will show that p-adic conditions, for finitely many primes p, can be imposed on the variable t. To handle the infinite place our sieve would have to be modified: sieving a more general region instead of $(0, N]^2$. This modification would enable us to find a rational solution, $(t, x_1, \ldots, x_k)$, to (8.1) with the variable t sufficiently close to any idelic point. If we define $x \in K$ by

$$x = x_1\omega_1 + \ldots + x_k\omega_k.$$

then, for any $u \in K$ with $N_{K/\mathbb{Q}}(u) = 1$, we can write

$$ux = y_1\omega_1 + \ldots + y_k\omega_k$$

and we have

$$f(t) = \mathbf{N}(y_1, \ldots, y_k).$$

It could be shown, using our assumption that weak approximation holds for

$$N_{K/\mathbb{Q}}(u) = 1,$$

that we can choose a u to make $(y_1, \ldots, y_k)$ sufficiently close to any idelic point.

We decided to restrict to the case that q is prime to simplify some of the technical details in the sieve. It seems probable that the argument could work for composite q, however the condition $q \geq 7$ would have to be changed as our bounds would involve the value of $\varphi(q)$. We use the assumption that f does not generate a subfield of $\mathbb{Q}(\zeta_q)$ to avoid any correlation between the splitting of primes in the number field $K/\mathbb{Q}$ and in the field generated by f. This will be made precise in Lemma 8.13. Observe that if $q \equiv 2 \pmod 3$ then this condition is satisfied for all cubics f as $\mathbb{Q}(\zeta_q)$ cannot contain a subfield of degree 3.

8.2 Algebraic Reduction of the Problem

It does not matter which norm form $\mathbf{N}$ we choose as they are all equivalent under a linear change of variables defined over $\mathbb{Q}$. In particular we may assume that $\mathbf{N} \in \mathbb{Z}[x_1, \ldots, x_k]$. As we eventually wish to apply sieve methods we reduce from a problem over $\mathbb{Q}$ to one over $\mathbb{Z}$. We therefore let $f(a, b)$ denote the homogeneous form of f, that is

$$f(a, b) = b^3 f\left(\frac{a}{b}\right).$$

Lemma 8.2. *Suppose there exist integers a and b for which*

$$b, f(a, b) \in N_{K/\mathbb{Q}}(K^*).$$

There is then a solution to (8.1) over $\mathbb{Q}$.

Proof. Clearly $b \neq 0$. We have

$$f\left(\frac{a}{b}\right) = b^{-3} f(a, b).$$

This is a norm from K since both b and $f(a, b)$ are, and the norm map is multiplicative. In addition $f(\frac{a}{b}) \neq 0$ since f is irreducible. □

We know that the Hasse norm principle holds for $K/\mathbb{Q}$. This means that a nonzero $a \in \mathbb{Q}$ is a norm from K if and only if it is a norm from the group of ideles I_K:

$$\mathbb{Q}^* \cap N_{K/\mathbb{Q}}(I_K) = N_{K/\mathbb{Q}}(K^*).$$

Let V denote the set of all places of K. To show that $a \in \mathbb{Q}^*$ is a norm from K it is thus sufficient to construct a sequence $(x_v)_{v \in V}$, where x_v is a nonzero element of K_v, with the following two properties:

1. For all non-Archimedean places v, with finitely many exceptions, we have $x_v \in R_v^*$, where R_v is the valuation ring of K_v. This condition ensures that $(x_v) \in I_K$.

2. For all places w of $\mathbb{Q}$ we have

$$\prod_{v|w} N_{K_v/\mathbb{Q}_w}(x_v) = a.$$

We will derive arithmetic conditions which are sufficient to show that a nonzero integer a is in $N_{K/\mathbb{Q}}(K^*)$.

Lemma 8.3. *Suppose $a \neq 0$ is an integer. Let p be a prime which does not divide a and which is unramified in $K/\mathbb{Q}$. Then there exist elements $x_v \in R_v^*$, for each place v above p, such that*

$$\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = a.$$

Proof. Let v_1 be one of the places above p. Since p is unramified in $K/\mathbb{Q}$ we know that the extension $K_{v_1}/\mathbb{Q}_p$ is unramified. Furthermore, $p \nmid a$ so $a \in \mathbb{Z}_p^*$. It follows by local class field theory, (for example Gras [27, Corollary 1.4.3, part (ii), page 75]), that there exists $x_{v_1} \in K_{v_1}$ with

$$N_{K_{v_1}/\mathbb{Q}_p}(x_{v_1}) = a.$$

We must have $x_{v_1} \in R_{v_1}^*$ since

$$|x_{v_1}|_{K_{v_1}} = |N_{K_{v_1}/\mathbb{Q}_p}(x_{v_1})|_{\mathbb{Q}_p}^{1/[K_{v_1}:\mathbb{Q}_p]} = |a|_{\mathbb{Q}_p}^{1/[K_{v_1}:\mathbb{Q}_p]} = 1.$$

For all $v|p$ with $v \neq v_1$ we define $x_v = 1$ so

$$N_{K_v/\mathbb{Q}_p}(x_v) = 1.$$

The result follows. □

For any fixed a this lemma has dealt with all but a finite number of places. It follows that for the remaining places we need not consider the condition $x_v \in R_v^*$.

Lemma 8.4. *Suppose $a \neq 0$ is an integer. Let p be a prime dividing a which is unramified in $K/\mathbb{Q}$. In addition suppose that in the prime ideal factorisation*

$$(p) = \prod P_i,$$

with $N(P_i) = p^{f_i}$, the various f_i are coprime. It follows that there exist $x_v \in K_v^*$, for each $v|p$, with

$$\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = a.$$

Proof. Let v_i be the place corresponding to the prime ideal P_i in the factorisation of (p). We have $[K_{v_i} : \mathbb{Q}_p] = f_i$ so

$$N_{K_{v_i}/\mathbb{Q}_p}(a) = a^{f_i}.$$

Since the f_i are coprime there exist integers k_i such that

$$\sum k_i f_i = 1.$$

The result follows on taking $x_{v_i} = a^{k_i}$. □

It remains to deal with the primes p which ramify in $K/\mathbb{Q}$. For such primes it is easier to interpret the idelic condition in terms of the solubility of the norm equation over $\mathbb{Q}_p$.

Lemma 8.5. *Let $a \neq 0$ be an integer and suppose there exist $x_1, \ldots, x_k \in \mathbb{Q}_p$ such that*

$$a = \mathbf{N}(x_1, \ldots, x_k).$$

Then there exist $x_v \in K_v^*$, for $v|p$, such that

$$\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = a.$$

Proof. Since $a \neq 0$ we know that

$$(x_1, \ldots, x_k) \neq 0.$$

Let $x^{(n)}$ be a sequence in $\mathbb{Q}^k$ which converges p-adically to $(x_1, \ldots, x_k)$. Let $\omega_1, \ldots, \omega_k$ be the basis of $K/\mathbb{Q}$ used to construct the norm form $\mathbf{N}$ and define $y^{(n)} \in K$ by

$$y^{(n)} = x_1^{(n)}\omega_1 + \ldots + x_k^{(n)}\omega_k.$$

For each $v|p$ write $y_v^{(n)}$ for the image of $y^{(n)}$ under the embedding of K into K_v. The sequence $y_v^{(n)}$ converges to some $x_v \in K_v^*$.

We now have

$$\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = \lim_{n\to\infty} \prod_{v|p} N_{K_v/\mathbb{Q}_p}(y_v^{(n)}).$$

However, since $y^{(n)} \in K$ it follows, (for example by Gras [27, Proposition 2.2, page 93]), that

$$\prod_{v|p} N_{K_v/\mathbb{Q}_p}(y_v^{(n)}) = N_{K/\mathbb{Q}}(y^{(n)}) = \mathbf{N}(x_1^{(n)}, \ldots, x_k^{(n)}).$$

We conclude, by continuity of $\mathbf{N}$, that

$$\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = \mathbf{N}(x_1, \ldots, x_k) = a.$$

□

Lemma 8.6. *Let p be a prime for which (8.1) has a solution in $\mathbb{Q}_p$. There exist $a_0, b_0 \in \mathbb{Z}$ and $l \in \mathbb{N}$, all depending on p, satisfying*

$$b_0, f(a_0, b_0) \neq 0 \,(\mathrm{mod}\, p^l),$$

such that for any $a, b \in \mathbb{Z}$ with

$$a \equiv a_0 \,(\mathrm{mod}\, p^l) \text{ and } b \equiv b_0 \,(\mathrm{mod}\, p^l)$$

we have

$$b, f(a, b) \in \mathbf{N}(\mathbb{Q}_p^k) \setminus \{0\}.$$

Proof. For the duration of this proof let

$$N = \mathbf{N}(\mathbb{Q}_p^k) \setminus \{0\}.$$

By assumption there exist $a_1, b_1 \in \mathbb{Z}_p$ with $b_1 \neq 0$ such that

$$f\left(\frac{a_1}{b_1}\right) \in N.$$

By replacing (a_1, b_1) by $(b_1^{k-1}a_1, b_1^k)$ we may assume that $b_1 \in N$ and therefore $f(a_1, b_1) \in N$. The set N is open and f is continuous with respect to the p-adic topology. It follows that there exists $\delta > 0$ such that for any $a, b \in \mathbb{Z}_p$ with

$$|a - a_1|, |b - b_1| < \delta \tag{8.2}$$

we have

$$b, f(a,b) \in N.$$

For an $l \in \mathbb{N}$ which is sufficiently large in terms of δ the hypotheses (8.2) are equivalent to

$$a \equiv a_1 \,(\mathrm{mod}\, p^l), \quad b \equiv b_1 \,(\mathrm{mod}\, p^l).$$

The result follows on taking $a_0, b_0 \in \mathbb{Z}$ which are congruent modulo p^l to a_1, b_1. Since

$$b_1, f(a_1, b_1) \neq 0$$

we can guarantee that

$$b_0, f(a_0, b_0) \neq 0 \,(\mathrm{mod}\, p^l)$$

provided l is large enough. □

We may now use all the previous lemmas to reduce our original problem to one involving prime divisors of b and $f(a,b)$.

Lemma 8.7. *Suppose that (8.1) has solutions in every $\mathbb{Q}_p$ and in $\mathbb{R}$. Let $\mathcal{P}_1$ be a finite set of primes which contains the ramified primes in $K/\mathbb{Q}$ as well as the finitely many $p \not\equiv 1 \,(\mathrm{mod}\, q)$ for which the degrees f_i are not coprime. Then there exists a $\Delta \in \mathbb{N}$, divisible only by primes in $\mathcal{P}_1$, and integers a_0, b_0 such that if $p \in \mathcal{P}_1$ and p^l is the maximal power of p dividing Δ then*

$$b_0, f(a_0, b_0) \not\equiv 0 \,(\mathrm{mod}\, p^l)$$

and the following implication is true.

Suppose that a, b are integers for which the following hold:

1. *We have*
$$a \equiv a_0 \,(\mathrm{mod}\, \Delta) \text{ and } b \equiv b_0 \,(\mathrm{mod}\, \Delta). \tag{8.3}$$
2. *Each prime p with $p | bf(a,b)$ and $p \notin \mathcal{P}_1$ satisfies*
$$p \not\equiv 1 \,(\mathrm{mod}\, q).$$
3. *We have $b > 0$ and $f(a,b) \geq 0$.*

Then (8.1) has a solution over $\mathbb{Q}$.

Proof. By Lemma 8.2 it is sufficient to show that

$$b, f(a,b) \in N_{K/\mathbb{Q}}(K^*).$$

By the Hasse norm principle this is equivalent to showing that

$$b, f(a,b) \in N_{K/\mathbb{Q}}(I_K).$$

We must therefore show, for all places of $\mathbb{Q}$, that b and $f(a,b)$ are products of local norms.

1. For each prime $p \in \mathcal{P}_1$ we may use Lemma 8.6 to construct $l_p, a_{0,p}, a_{1,p}$. These will satisfy

   $$b_{0,p}, f(a_{0,p}, b_{0,p}) \not\equiv 0 \,(\mathrm{mod}\, p^{l_p}).$$

   We now let

   $$\Delta = \prod_{p \in \mathcal{P}_1} p^{l_p}$$

   and use the Chinese Remainder Theorem to construct a_0, b_0 satisfying

   $$a_0 \equiv a_{0,p} \,(\mathrm{mod}\, p^{l_p}), \quad b_0 \equiv b_{0,p} \,(\mathrm{mod}\, p^{l_p})$$

   for all $p \in \mathcal{P}_1$. It follows by our assumption (8.3) and Lemma 8.6 that

   $$b, f(a,b) \in \mathbf{N}(\mathbb{Q}_p^k) \setminus \{0\}.$$

   We conclude, using Lemma 8.5, that b and $f(a,b)$ are suitable products of local norms for all primes in $\mathcal{P}_1$.

2. For primes not in $\mathcal{P}_1$ we know that either $p \nmid b$, in which case we use Lemma 8.3 to write b as a suitable product of local norms, or $p|b$. In the latter situation $p \not\equiv 1 \,(\mathrm{mod}\, q)$ and therefore the degrees of the prime ideals above p are coprime. The required local condition for b now follows by Lemma 8.4. We may use an identical argument for $f(a,b)$.

3. Finally we consider the infinite place. Since $b, f(a,b) \geq 0$ they are both local norms at infinity.

The above cases cover all the places of $\mathbb{Q}$ so the result follows. □

For the remainder of this chapter we let $\mathcal{P}_1$ be a finite set of primes including those which are ramified in $K/\mathbb{Q}$ or which divide the coefficients of a^3 or b^3 in the polynomial $f(a,b)$ or which divide the discriminant of f. In addition $\mathcal{P}_1$ will contain those primes $p \not\equiv 1 \pmod q$ for which the degrees f_i are not coprime. We also include in $\mathcal{P}_1$ the prime q and all primes up to some absolute constant P_1, (which will be determined in Lemma 8.18 below). We let a_0, b_0, Δ be the quantities constructed in the last lemma and use the notation $C(a,b)$ to denote that a, b satisfy (8.3).

Since f is a cubic, we can, without loss of generality, apply a linear change of variable over $\mathbb{Q}$ to guarantee that its leading coefficient is positive and all its real roots are negative. We may thus assume that if $x > 0$ then $f(x) > 0$. In particular, if $a, b > 0$ then $f(a,b) > 0$. For a large N we will apply a sieve to count pairs $(a,b) \in (0,N]^2$ satisfying $C(a,b)$ for which $bf(a,b)$ has no prime factor $p \notin \mathcal{P}_1$ with $p \equiv 1 \pmod q$. If we can prove a positive lower bound for this quantity then it follows by the last lemma that (8.1) has a solution over $\mathbb{Q}$.

8.3 Levels of Distribution

We need various level of distribution results for the values $bf(a,b)$. All implied constants in this section may depend on the polynomial f and on Δ.

The main result of this section, Lemma 8.11, is proved using very similar methods to those of Daniel, [13, Lemmas 3.2 and 3.3]. We extend his results to handle the form $bf(a,b)$, rather than $f(a,b)$, with a, b in a fixed arithmetic progression. Let $\mathcal{R}$ be a parallelogram in $\mathbb{R}^2$. We begin by considering the quantity

$$R^*(\mathcal{R}, d_1, d_2) = \#\{(a,b) \in \mathcal{R} : C(a,b), (a;b;d) = 1, d_1 | f(a,b), d_2 | bf(a,b)\}.$$

We need only consider $R^*(\mathcal{R}, d_1, d_2)$ for $d_1, d_2 \in \mathbb{N}$ satisfying

$$(d_1; d_2) = (d_1 d_2; \Delta) = 1.$$

We will write $d = d_1 d_2$.

As in our proof of Theorem 7.4 we say that points $(a_1, b_1), (a_2, b_2)$ with

$$(a_1; b_1; d) = (a_2; b_2; d) = 1$$

are equivalent modulo d if

$$(a_1, b_1) \equiv \lambda(a_2, b_2) \pmod d$$

for some $\lambda \in \mathbb{Z}$ which must necessarily satisfy $(\lambda; d) = 1$. We will call points with $(a; b; d) = 1$ primitive modulo d. The number of primitive points in each equivalence class which are distinct modulo d is $\varphi(d)$.

Observe that the properties $f(a, b) \equiv 0 \pmod{d_1}$ and $bf(a, b) \equiv 0 \pmod{d_2}$ are preserved by equivalence. We may therefore define $\mathcal{U}(d_1, d_2)$ to be the set of equivalence classes of primitive points modulo $d = d_1 d_2$ for which $f(a, b) \equiv 0 \pmod{d_1}$ and $bf(a, b) \equiv 0 \pmod{d_2}$.

For an equivalence class $x \pmod{d}$ we let $\lambda(x)$ be the lattice in $\mathbb{Z}^2$ generated by the points of x. Thus $y \in \lambda(x)$ if and only if there exists some $(a, b) \in x$ and $\lambda \in \mathbb{Z}$ with

$$y \equiv \lambda(a, b) \pmod{d}.$$

In particular the primitive points in $\lambda(x)$ are precisely those in x. It follows that

$$\begin{aligned}
R^*(\mathcal{R}, d_1, d_2) &= \sum_{x \in \mathcal{U}(d_1, d_2)} \#\{(a, b) \in \mathcal{R} \cap x : C(a, b)\} \\
&= \sum_{x \in \mathcal{U}(d_1, d_2)} \#\{(a, b) \in \mathcal{R} \cap \lambda(x) : C(a, b), (a; b; d) = 1\} \\
&= \sum_{x \in \mathcal{U}(d_1, d_2)} \sum_{\substack{(a,b) \in \mathcal{R} \cap \lambda(x) \\ C(a,b)}} \sum_{e | (a;b;d)} \mu(e) \\
&= \sum_{x \in \mathcal{U}(d_1, d_2)} \sum_{e | d} \mu(e) \#\{(a, b) \in \mathcal{R} \cap \lambda(x) : C(a, b), e | (a, b)\} \\
&= \sum_{x \in \mathcal{U}(d_1, d_2)} \sum_{e | d} \mu(e) \#\{(a, b) \in \mathcal{R} \cap \lambda(x, e) : C(a, b)\}
\end{aligned}$$

where $\lambda(x, e)$ is the sublattice of $\lambda(x)$ consisting of points divisible by e.

We have $(d; \Delta) = 1$ so $(e; \Delta) = 1$. It follows that the sublattice of $\lambda(x, e)$ consisting of those points which are divisible by Δ is precisely $\lambda(x, e\Delta)$. It is then clear that the set

$$\{(a, b) \in \lambda(x, e) : C(a, b)\}$$

is a coset of the lattice $\lambda(x, e\Delta)$.

Lemma 8.8. *We have*

$$\det \lambda(x, e\Delta) = de\Delta^2.$$

Proof. In general, if a lattice in $\mathbb{Z}^2$ is formed from all points whose reduction mod n is in a set of c equivalence classes then its determinant is $\frac{n^2}{c}$.

For our specific problem we take $n = d\Delta$. Let (a, b) be a fixed point of x. Since $(a; b; d) = 1$ we know that the number of points modulo d which are multiples of (a, b) and divisible by e is $\frac{d}{e}$. Since $(d; \Delta) = 1$ it follows by the Chinese Remainder Theorem that $c = \frac{d}{e}$ and therefore

$$\det \lambda(x, e\Delta) = \frac{d^2\Delta^2}{d/e} = de\Delta^2.$$

□

Let $R_1(x, e\Delta)$ denote the length of the shortest nonzero vector in $\lambda(x, e\Delta)$. It is clear that this is bounded below by $R_1(x)$, the length of the shortest nonzero vector in $\lambda(x)$. Let $A(\mathcal{R})$ and $P(\mathcal{R})$ denote the area and perimeter of $\mathcal{R}$, respectively. By Lemma 2.6 we get

$$R^*(\mathcal{R}, d_1, d_2) = \sum_{x \in \mathcal{U}(d_1,d_2)} \sum_{e|d} \mu(e) \left(\frac{A(\mathcal{R})}{de\Delta^2} + O\left(1 + \frac{P(\mathcal{R})}{R_1(x)}\right)\right).$$

Let $\rho^*(d_1, d_2)$ denote the number of primitive solutions modulo d to

$$f(a, b) \equiv 0 \,(\mathrm{mod}\, d_1) \text{ and } bf(a, b) \equiv 0 \,(\mathrm{mod}\, d_2).$$

Since the number of distinct points modulo d in each equivalence class is $\varphi(d)$ we have

$$\sum_{x \in \mathcal{U}(d_1,d_2)} \sum_{e|d} \frac{\mu(e)}{e} = \sum_{x \in \mathcal{U}(d_1,d_2)} \frac{\varphi(d)}{d} = \frac{\rho^*(d_1, d_2)}{d}.$$

We conclude that for any $\epsilon > 0$ we have

$$R^*(\mathcal{R}, d_1, d_2) = \frac{\rho^*(d_1, d_2)A(\mathcal{R})}{d^2\Delta^2} + O_\epsilon \left(d^\epsilon \left(1 + P(\mathcal{R}) \sum_{x \in \mathcal{U}(d_1,d_2)} R_1(x)^{-1} \right)\right).$$

Averaging this over d_1 and d_2 we get

$$\sum_{\substack{d_1 \le D_1, d_2 \le D_2 \\ (d_1;d_2)=(d_1d_2;\Delta)=1}} \max_{P(\mathcal{R}) \le M} \left| R^*(\mathcal{R}, d_1, d_2) - \frac{\rho^*(d_1, d_2)A(\mathcal{R})}{d_1^2 d_2^2 \Delta^2} \right|$$

$$\ll_\epsilon \quad (D_1D_2)^\epsilon \left(D_1D_2 + M \sum_{\substack{d_1 \le D_1, d_2 \le D_2 \\ (d_1;d_2)=(d_1d_2;\Delta)=1}} \sum_{x \in \mathcal{U}(d_1,d_2)} R_1(x)^{-1} \right).$$

Let $v_1(x)$ denote the shortest nonzero vector in $\lambda(x)$. We know, by Lemma 2.4, that

$$\|v_1(x)\|^2 \ll \det \lambda(x) \ll D_1D_2.$$

We may thus write the final sum as

$$\sum_{0<a^2+b^2\ll D_1D_2} \frac{1}{\sqrt{a^2+b^2}} \#\{d_1,d_2,x : (d_1;d_2)=(d_1d_2;\Delta)=1, v_1(x)=(a,b)\}.$$

If $v_1(x)=(a,b)$ then

$$d_1d_2 | bf(a,b).$$

We first consider the contribution to the above sum from pairs (a,b) with $b\neq 0$. Since f is irreducible we have $bf(a,b)\neq 0$. It follows that the number of d_1,d_2 for a given (a,b) is bounded by

$$\tau_3(bf(a,b)) \ll_\epsilon (D_1D_2)^\epsilon.$$

For each such d_1,d_2 the number of $x\in\mathcal{U}(d_1,d_2)$ for which $v_1(x)=(a,b)$ is at most

$$\#\mathcal{U}(d_1,d_2)=\frac{\rho^*(d_1,d_2)}{\varphi(d_1d_2)} \ll_\epsilon (D_1D_2)^\epsilon.$$

We conclude that

$$\begin{aligned}
&\sum_{\substack{0<a^2+b^2\ll D_1D_2\\ b\neq 0}} \frac{1}{\sqrt{a^2+b^2}} \#\{d_1,d_2,x : (d_1;d_2)=(d_1d_2;\Delta)=1, v_1(x)=(a,b)\}\\
&\ll_\epsilon (D_1D_2)^\epsilon \sum_{0<a^2+b^2\ll D_1D_2} \frac{1}{\sqrt{a^2+b^2}}\\
&\ll_\epsilon (D_1D_2)^{\frac{1}{2}+\epsilon}.
\end{aligned}$$

It remains to estimate the contribution from pairs $(a,0)$:

$$\sum_{0<a\ll\sqrt{D_1D_2}} \frac{1}{a} \#\{d_1,d_2,x : (d_1;d_2)=(d_1d_2;\Delta)=1, v_1(x)=(a,0)\}.$$

Suppose that $v_1(x)=(a,0)$. We then have

$$f(a,0)\equiv 0 \,(\mathrm{mod}\, d_1).$$

Since $f(a,0)\neq 0$ it follows that the number of possible d_1 is bounded by

$$\tau(f(a,0)) \ll_\epsilon D_1^\epsilon.$$

For each such d_1 the number of d_2 is clearly bounded by D_2. As above, the number of x is then $O_\epsilon((D_1D_2)^\epsilon)$. We conclude that

$$\begin{aligned}
&\sum_{0<a\ll\sqrt{D_1D_2}} \frac{1}{a} \#\{d_1,d_2,x : (d_1;d_2)=(d_1d_2;\Delta)=1, v_1(x)=(a,0)\}\\
&\ll_\epsilon D_1^\epsilon D_2^{1+\epsilon} \sum_{0<a\ll\sqrt{D_1D_2}} \frac{1}{a} \ll_\epsilon D_1^\epsilon D_2^{1+\epsilon}.
\end{aligned}$$

Combining these two cases we get

$$\sum_{0<a^2+b^2\ll D_1D_2} \frac{1}{\sqrt{a^2+b^2}} \#\{d_1,d_2,x : (d_1;d_2)=(d_1d_2;\Delta)=1, v_1(x)=(a,b)\}$$

$$\ll_\epsilon (D_1D_2)^\epsilon((D_1D_2)^{\frac{1}{2}}+D_2).$$

We have therefore proved the following.

Lemma 8.9. *For any $D_1, D_2 > 0$ and any $\epsilon > 0$ we have*

$$\sum_{\substack{d_1\le D_1, d_2\le D_2\\ (d_1;d_2)=(d_1d_2;\Delta)=1}} \max_{P(\mathcal{R})\le M} \left| R^*(\mathcal{R},d_1,d_2) - \frac{\rho^*(d_1,d_2)A(\mathcal{R})}{d_1^2d_2^2\Delta^2}\right|$$

$$\ll_\epsilon (D_1D_2)^\epsilon(D_1D_2 + M((D_1D_2)^{\frac{1}{2}}+D_2)).$$

We next remove the restriction to primitive points. As in Daniel's work, [13, Lemma 3.3], we need the multiplicative functions ψ_k which map the prime power $p^{\alpha k+\beta}$, for $1\le\beta\le k$, to $p^{\alpha+1}$.

Let

$$\begin{aligned} R(\mathcal{R},d_1,d_2) &= \#\{(a,b)\in\mathcal{R} : C(a,b), d_1|f(a,b), d_2|bf(a,b)\}\\ &= \sum_{\substack{e_1|\psi_3(d_1)\\ e_2|\psi_4(d_2)}} N(d_1,d_2,e_1,e_2)\end{aligned}$$

where

$$\begin{aligned} &N(d_1,d_2,e_1,e_2)\\ &= \#\{(a,b)\in\mathcal{R} : C(a,b), (a;b;\psi_3(d_1)\psi_4(d_2))=e_1e_2, d_1|f(a,b), d_2|bf(a,b)\}\\ &= \#\{(a,b)\in\mathcal{R}/e_1e_2 : C(e_1e_2(a,b)), (a;b;\frac{\psi_3(d_1)\psi_4(d_2)}{e_1e_2})=1,\\ &\qquad \frac{d_1}{(d_1;e_1^3)}|f(a,b), \frac{d_2}{(d_2;e_2^4)}|bf(a,b)\}\\ &= \#\{(a,b)\in\mathcal{R}/e_1e_2 : C(e_1e_2(a,b)), (a;b;\frac{d_1d_2}{(d_1;e_1^3)(d_2;e_2^4)})=1,\\ &\qquad \frac{d_1}{(d_1;e_1^3)}|f(a,b), \frac{d_2}{(d_2;e_2^4)}|bf(a,b)\}\\ &= R^*(\mathcal{R}/e_1e_2, \frac{d_1}{(d_1;e_1^3)}, \frac{d_2}{(d_2;e_2^4)}; e_1,e_2).\end{aligned}$$

Thus

$$R(\mathcal{R},d_1,d_2) = \sum_{\substack{e_1|\psi_3(d_1)\\ e_2|\psi_4(d_2)}} R^*(\mathcal{R}/e_1e_2, \frac{d_1}{(d_1;e_1^3)}, \frac{d_2}{(d_2;e_2^4)}; e_1,e_2).$$

Here the addition of $(;e_1,e_2)$ to R^* denotes that the congruences $C(a,b)$ are replaced by $C(e_1e_2(a,b))$. Since $(e_1e_2;\Delta)=1$ these congruences are

$$a \equiv \overline{e_1e_2}a_0 \,(\mathrm{mod}\,\Delta)$$

and

$$b \equiv \overline{e_1e_2}b_0 \,(\mathrm{mod}\,\Delta).$$

The precise choice of coset has no effect on the above analysis of R^* so Lemma 8.9 still holds when different congruence classes are taken for each pair d_1, d_2 in the sum.

Let $\rho(d_1,d_2)$ be the number of solutions modulo d_1d_2 to

$$f(a,b) \equiv 0 \,(\mathrm{mod}\,d_1), \quad bf(a,b) \equiv 0 \,(\mathrm{mod}\,d_2).$$

Applying the above analysis to the region $(0,d_1d_2]^2$ with no congruence C gives the decomposition

$$\rho(d_1,d_2) = \sum_{\substack{e_1|\psi_3(d_1)\\ e_2|\psi_4(d_2)}} (\frac{(d_1;e_1^3)}{e_1}\frac{(d_2;e_2^4)}{e_2})^2\rho^*(\frac{d_1}{(d_1;e_1^3)},\frac{d_2}{(d_2;e_2^4)}).$$

It follows that

$$\begin{aligned} &R(\mathcal{R},d_1,d_2) - \frac{\rho(d_1,d_2)A(\mathcal{R})}{d_1^2d_2^2\Delta^2} \\ &= \sum_{\substack{e_1|\psi_3(d_1)\\ e_2|\psi_4(d_2)}} \Bigg(R^*(\mathcal{R}/e_1e_2,\frac{d_1}{(d_1;e_1^3)},\frac{d_2}{(d_2;e_2^4)}) \\ &\qquad - \frac{V(\mathcal{R}/e_1e_2)(d_1;e_1^3)^2(d_2;e_2^4)^2\rho^*(\frac{d_1}{(d_1;e_1^3)},\frac{d_2}{(d_2;e_2^4)})}{d_1^2d_2^2\Delta^2}\Bigg). \end{aligned}$$

We are interested in the average of this over $d_1 \le D_1, d_2 \le D_2$ so we consider

$$\sum_{\substack{e_1f_1\le D_1, e_2f_2\le D_2\\ (e_1f_1;e_2f_2)=(e_1f_1e_2f_2;\Delta)=1}} \delta(e_1,e_2,f_1,f_2) \max_{P(\mathcal{R})\le M} |R^*(\mathcal{R}/e_1e_2,f_1,f_2) - \frac{\rho^*(f_1,f_2)V(\mathcal{R}/e_1e_2)}{f_1^2f_2^2}|$$

where $\delta(e_1,e_2,f_1,f_2)$ is the number of pairs $d_1 \le D_1, d_2 \le D_2$ with

$$e_1|\psi(d_1),\ e_2|\psi(d_2),\ f_1 = \frac{d_1}{(d_1;e_1^3)},\ f_2 = \frac{d_2}{(d_2;e_2^4)}.$$

It is clear that δ is the product of the number of suitable d_1 by the number of d_2. These latter quantities were estimated by Daniel: they are bounded by divisor functions. It follows that for any $\epsilon > 0$ we have

$$\delta(e_1,e_2,f_1,f_2) \ll_\epsilon (D_1D_2)^\epsilon.$$

Our sum is thus majorised by

$$(D_1D_2)^\epsilon \sum_{\substack{e_1f_1\leq D_1, e_2f_2\leq D_2\\ (e_1f_1;e_2f_2)=(e_1f_1e_2f_2;\Delta)=1}} \max_{P(\mathcal{R})\leq M}\left|R^*(\mathcal{R}/e_1e_2,f_1,f_2)-\frac{\rho^*(f_1,f_2)V(\mathcal{R}/e_1e_2)}{f_1^2f_2^2}\right|.$$

For each pair (e_1,e_2) in this sum we apply Lemma 8.9 to the sum over f_1,f_2. This results in a bound

$$(D_1D_2)^\epsilon \sum_{e_1\leq D_1, e_2\leq D_2}\left(\frac{D_1D_2}{e_1e_2}+\frac{M}{e_1e_2}((\frac{D_1D_2}{e_1e_2})^{\frac{1}{2}}+\frac{D_2}{e_2})\right).$$

We may therefore conclude with the following level of distribution result.

Lemma 8.10. *For any $D_1,D_2>0$ and any $\epsilon>0$ we have*

$$\sum_{\substack{d_1\leq D_1, d_2\leq D_2\\ (d_1;d_2)=(d_1d_2;\Delta)=1}} \max_{P(\mathcal{R})\leq M}\left|R(\mathcal{R},d_1,d_2)-\frac{\rho(d_1,d_2)A(\mathcal{R})}{d_1^2d_2^2\Delta^2}\right|$$
$$\ll_\epsilon (D_1D_2)^\epsilon(D_1D_2+M((D_1D_2)^{\frac{1}{2}}+D_2)).$$

We are interested in this result when $\mathcal{R}=(0,N]^2$ for large N.

Lemma 8.11. *Let*

$$R(d_1,d_2)=R((0,N]^2,d_1,d_2).$$

Suppose $\eta>0$ is fixed. Then there exists $\delta>0$, depending on η, such that if

$$0<D_1D_2\leq N^{2-\eta}$$

and

$$0<D_2\leq N^{1-\eta}$$

we have

$$\sum_{\substack{d_1\leq D_1, d_2\leq D_2\\ (d_1;d_2)=(d_1d_2;\Delta)=1}}\left|R(d_1,d_2)-\frac{\rho(d_1,d_2)N^2}{d_1^2d_2^2\Delta^2}\right|\ll_\eta N^{2-\delta}.$$

Proof. This follows on putting $A(\mathcal{R})=N^2$, $P(\mathcal{R})\ll N$ into the previous lemma and taking ϵ sufficiently small in terms of η. □

If we let $\rho_1(d)$ be the number of solutions modulo d to $f(a,b)\equiv 0\,(\mathrm{mod}\,d)$ and $\rho_2(d)$ the number of solutions to $bf(a,b)\equiv 0\,(\mathrm{mod}\,d)$ then if $(d_1;d_2)=1$ we have

$$\rho(d_1,d_2)=\rho_1(d_1)\rho_2(d_2).$$

We also need to understand the quantity

$$R_1(d_1, d_2) = \#\{(a, b) \in (0, N]^2 : C(a, b),\, bf(a, b) \equiv 0 \pmod{d_1},\, b \equiv 0 \pmod{d_2}\}.$$

This is only required for small d_1, d_2 so the following is sufficient.

Lemma 8.12. *For any $d_1, d_2 \in \mathbb{N}$ with $(d_1; d_2) = (d_1 d_2; \Delta) = 1$ and $d_1 d_2 \leq N$ we have, for any $\epsilon > 0$ that*

$$R_1(d_1, d_2) = \frac{N^2 \rho_2(d_1)}{d_1^2 d_2 \Delta^2} + O_\epsilon(N d_1^\epsilon).$$

Proof. The number of points counted by R_1 congruent to a given solution modulo $d_1 d_2 \Delta$ is

$$\frac{N^2}{d_1^2 d_2^2 \Delta^2} + O\left(1 + \frac{N}{d_1 d_2 \Delta}\right) = \frac{N^2}{d_1^2 d_2^2 \Delta^2} + O\left(\frac{N}{d_1 d_2}\right).$$

However, by the Chinese Remainder Theorem the number of solutions modulo $d_1 d_2 \Delta$ is $d_2 \rho_2(d_1)$. It follows that

$$R(d_1, d_2) = \frac{N^2 \rho_2(d_1)}{d_1^2 d_2 \Delta^2} + O\left(\frac{N \rho_2(d_1)}{d_1}\right) = \frac{N^2 \rho_2(d_1)}{d_1^2 d_2 \Delta^2} + O_\epsilon(N d_1^\epsilon).$$

□

8.4 The Functions ρ_1 and ρ_2

We need various estimates for sums and products involving the functions ρ_1 and ρ_2. Let $\nu(d)$ be the number of solutions to the congruence

$$f(x) \equiv 0 \,(\mathrm{mod}\, d).$$

For all primes $p \notin \mathcal{P}_1$ we may write $\rho_1(p)$ and $\rho_2(p)$ in terms of $\nu(p)$:

$$\rho_1(p) = (p - 1)\nu(p) + 1$$

and

$$\rho_2(p) = (p - 1)\nu(p) + p.$$

In the following equations let c denote a real constant which may depend on q and f and which may differ from line to line. It is well known that

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + c + o(1),$$

$$\sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} \frac{1}{p} = \frac{1}{q-1}\log\log x + c + o(1),$$

if $(a;q) = 1$, and

$$\sum_{p\le x} \frac{1}{p^2} = c + o(1).$$

Let L be the cubic field generated by the polynomial f and let ζ_L be its Dedekind zeta function. For all primes $p \notin \mathcal{P}_1$ we know that $\nu(p)$ is equal to the coefficient of p^{-s} in $\zeta_L(s)$. It follows from the Prime Ideal Theorem that

$$\sum_{p\le x} \frac{\nu(p)}{p} = \log\log x + c + o(1).$$

Finally we would like to show that, for $(a;q) = 1$, we have

$$\sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} \frac{\nu(p)}{p} \sim \frac{1}{q-1}\log\log x. \tag{8.4}$$

Unfortunately this is not always true. For example, suppose we have

$$f(t) = t^3 - 7t^2 + 14t - 7.$$

The field L is then abelian of degree 3 and contained in the cyclotomic field $\mathbb{Q}(\zeta_7)$. It is easy to deduce from this that

$$\nu(p) = \begin{cases} 3 & p \equiv \pm 1 \,(\mathrm{mod}\, 7) \\ 0 & p \equiv \pm 2, \pm 3 \,(\mathrm{mod}\, 7). \end{cases}$$

The formula (8.4) is therefore not true for this f when $q = 7$. It follows that many of the details of the sieve would be different in this case. In order to avoid these difficulties we restrict our attention to those polynomials f and primes q for which (8.4) holds. We will show that (8.4) follows from our hypothesis that the number field L is not contained in $\mathbb{Q}(\zeta_q)$.

Expanding using characters we are interested in

$$\frac{1}{q-1} \sum_{\chi \,(\mathrm{mod}\, q)} \overline{\chi(a)} \sum_{p\le x} \frac{\chi(p)\nu(p)}{p}.$$

For $p \notin \mathcal{P}_1$ the quantity $\chi(p)\nu(p)$ is the coefficient of p^{-s} in the function $\zeta_L(s,\chi)$. This is the Hecke L-function coming from the character which maps an ideal I to $\chi(N(I))$.

Lemma 8.13. *If $\chi \neq \chi_0$ is a character modulo q then, under our assumption that $L \not\subseteq \mathbb{Q}(\zeta_q)$, $\zeta_L(s,\chi)$ is regular at $s = 1$.*

Proof. We say that a property holds for almost all primes if it holds for all primes with finitely many exceptions. The only primitive Hecke character whose L-function has a singularity at $s = 1$ is the trivial one. It is therefore enough to show that $I \mapsto \chi(N(I))$ is not induced from the trivial character. In other words we need to show that there are infinitely many prime ideals P for which $\chi(N(P)) \neq 1$. We suppose that this is false so that, in particular, almost all primes p, for which there is an ideal of norm p, are in a proper subgroup H of $(\mathbb{Z}/q\mathbb{Z})^*$.

We first consider the case that $L/\mathbb{Q}$ is not Galois, so its discriminant, δ, is not a square. It can be shown that if a prime p satisfies $(\frac{\delta}{p}) = -1$ then it factorises in L into prime ideals of norms p and p^2. It follows that the reduction modulo q of almost all such primes must be in H. However, we can show using Dirichlet's theorem on primes in arithmetic progressions that for any prime q and any nonsquare integer δ the reductions modulo q of almost all the primes p for which $(\frac{\delta}{p}) = -1$ generate the whole of $(\mathbb{Z}/q\mathbb{Z})^*$. This is a contradiction so χ cannot be induced from the trivial character and $\zeta_L(s,\chi)$ is regular at 1.

Next we consider the case that $L/\mathbb{Q}$ is Galois. We know, by assumption, that the primes which split completely in L are contained in H.

Suppose in general that we have Galois number fields L_1, L_2 and almost all the primes which split completely in L_1 also split completely in L_2. It follows that almost all the primes which split in L_1 also split in the composite extension L_1L_2. By Chebotarev's Density Theorem the density of primes which split in L_1 is $\frac{1}{[L_1:\mathbb{Q}]}$ whereas the density of those splitting in L_1L_2 is $\frac{1}{[L_1L_2:\mathbb{Q}]}$. We conclude that

$$\frac{1}{[L_1:\mathbb{Q}]} \leq \frac{1}{[L_1L_2:\mathbb{Q}]}$$

so that $L_1L_2 = L_1$ and therefore L_2 is a subfield of L_1.

By class field theory, for example Gras [27, Sections 5.5 and 5.6, part (ii)], we can construct a number field L_H whose only ramified prime is q and for which the primes which split completely are those in H, (L_H is the class field coming from the modulus (q) and the subgroup H). It follows by the previous paragraph that L_H is contained in L. However, $[L:\mathbb{Q}] = 3$ so we must have $L = L_h$. On the other hand we know that $L_H \subseteq \mathbb{Q}(\zeta_q)$, which contradicts our assumption on L. We deduce that the Hecke character is not induced from the trivial one and thus its L-function has no singularities. □

It now follows by general theory, for example as given by Heilbronn [37], that for $\chi \neq \chi_0$ we have, as $x \to \infty$,

$$\sum_{p \leq x} \frac{\chi(p)\nu(p)}{p} = c + o(1),$$

for some constant c depending on f, q and χ. We can therefore conclude that

$$\sum_{\substack{p \leq x \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{\nu(p)}{p} = \frac{1}{q-1} \log\log x + c + o(1),$$

with c depending on f, q and a.

Let

$$\mathcal{P} = \{p : p \notin \mathcal{P}_1, p \equiv 1 \,(\mathrm{mod}\, q)\}$$

and

$$\mathcal{P}' = \{p : p \notin \mathcal{P}_1, p \not\equiv 1 \,(\mathrm{mod}\, q)\}.$$

Lemma 8.14. *As $x \to \infty$ we have*

$$\prod_{\substack{p \leq x \\ p \in \mathcal{P}}} \left(1 - \frac{\rho_2(p)}{p^2}\right) = \frac{(c_2(f,q) + o(1))}{(\log x)^{\frac{2}{q-1}}}$$

and

$$\prod_{\substack{p \leq x \\ p \in \mathcal{P}'}} \left(1 - \frac{\rho_1(p)}{p^2}\right) = \frac{(c_1(f,q) + o(1))}{(\log x)^{\frac{q-2}{q-1}}}$$

where $c_1(f,q), c_2(f,q) > 0$.

Proof. Let

$$P = \prod_{\substack{p \leq x \\ p \in \mathcal{P}}} \left(1 - \frac{\rho_2(p)}{p^2}\right).$$

Since all the primes dividing f are in $\mathcal{P}_1$ and hence not in $\mathcal{P}$ we know that $\rho_2(p) < p^2$

for all $p \in \mathcal{P}$. It follows that the terms in P are all positive so we may take logs:

$$\begin{aligned}
\log P &= \sum_{\substack{p \le x \\ p \in \mathcal{P}}} \log\left(1 - \frac{\rho_2(p)}{p^2}\right) \\
&= \sum_{\substack{p \le x \\ p \in \mathcal{P}}} \left(-\frac{\rho_2(p)}{p^2} + O\left(\frac{1}{p^2}\right)\right) \\
&= \sum_{\substack{p \le x \\ p \in \mathcal{P}}} \left(-\frac{\nu(p)+1}{p} + O\left(\frac{1}{p^2}\right)\right) \\
&= -\frac{2}{q-1}\log\log x + c + o(1).
\end{aligned}$$

The first result follows on taking $c_2(f,q) = e^c$, with the c from the last line, and the second can be proved analogously. □

It is clear that if $p \notin \mathcal{P}_1$ then $\nu(p) \le 3$ so that $\rho_1(p) \le 3p$. We also need a bound for ρ_1 at prime powers.

Lemma 8.15. *For any prime $p \notin \mathcal{P}_1$ and any $\alpha \in \mathbb{N}$ we have*

$$\rho_1(p^\alpha) \ll p^{\frac{4\alpha}{3}},$$

the implied constant being absolute.

Proof. We substitute Daniel's bound [13, (3.2)], which holds for all $p \notin \mathcal{P}_1$, into his identity [13, (7.4)]. This results in

$$\begin{aligned}
\rho_1(p^\alpha) &\le 3 \sum_{0 \le \beta < \lceil \alpha/3 \rceil} p^{\alpha+\beta} + p^{2(\alpha - \lceil \alpha/3 \rceil)} \\
&\le 3\frac{p^{\alpha + \lceil \alpha/3 \rceil}}{p-1} + p^{2(\alpha - \lceil \alpha/3 \rceil)} \ll p^{\frac{4\alpha}{3}}.
\end{aligned}$$

□

As a consequence of this we see that for any r with no prime factors in $\mathcal{P}_1$ we have

$$\rho_1(r) \ll r^{\frac{4}{3}}.$$

8.5 The Sum of a Multiplicative Function in an Arithmetic Progression

Let g be a nonnegative multiplicative function supported on squarefree numbers which satisfies

$$\sum_{p\le x} g(p)\log p = k\log x + O(1), \tag{8.5}$$

for some $k>0$. If $2\le w<z$ we assume that

$$\prod_{w\le p<z}(1+g(p)) \ll \left(\frac{\log z}{\log w}\right)^k. \tag{8.6}$$

We also suppose that

$$\sum_{p} g(p)^2\log p < \infty. \tag{8.7}$$

Under these assumptions Friedlander and Iwaniec [25, Theorem A.5] show that

$$\sum_{m\le x} g(m) = c_g(\log x)^k + O((\log x)^{k-1}), \tag{8.8}$$

where

$$c_g = \frac{1}{\Gamma(k+1)}\prod_p (1-\frac{1}{p})^k(1+g(p)).$$

We require the following modified version of this result.

Lemma 8.16. *Let g be a nonnegative multiplicative function supported on squarefree numbers which satisfies (8.5), (8.6) and (8.7) for some $k>0$. Let $q>2$ be prime. Suppose that $g(q)=0$ and that for all primes $p\equiv 1 \pmod q$ we have $g(p)=0$. Finally suppose that if $a\not\equiv 0,1 \pmod q$ then*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod q}} g(p)\log p = \frac{1}{q-2}\,k\log x + O(1). \tag{8.9}$$

Then, for any a with $(a;q)=1$ we have

$$\sum_{\substack{m\le x\\ m\equiv a \pmod q}} g(m) = \left(\frac{c_g}{q-1}+o(1)\right)(\log x)^k.$$

The implied constant in the assumption (8.9) and the rate of convergence of $o(1)$ in the conclusion may both depend on q.

Proof. Let

$$M_g(x) = \sum_{\substack{m\le x\\ m\equiv a \,(\mathrm{mod}\, q)}} g(m).$$

We begin by considering

$$\sum_{\substack{m\le x\\ m\equiv a \,(\mathrm{mod}\, q)}} g(m)\log m = \sum_{\substack{np\le x\\ np\equiv a \,(\mathrm{mod}\, q)}} g(np)\log p.$$

Using that g is multiplicative and supported on squarefree numbers coprime to q this can be written as

$$\sum_{n\le x} g(n) \sum_{\substack{p\le x/n\\ p\equiv a\overline{n} \,(\mathrm{mod}\, q)}} g(p)\log p - \sum_{\substack{np^2\le x\\ np^2\equiv a \,(\mathrm{mod}\, q)}} g(np)g(p)\log p.$$

From (8.6) we get

$$\sum_{n\le x} g(n) \le \prod_{p\le x}(1+g(p)) \ll (\log x)^k$$

and from (8.7) we deduce

$$\sum_{np^2\le x} g(np)g(p)\log p \ll \sum_{n\le x} g(n)\sum_{p} g(p)^2\log p \ll (\log x)^k.$$

Using these bounds as well as (8.9) the above sum becomes

$$\frac{k}{q-2} \sum_{\substack{n\le x\\ n\not\equiv a \,(\mathrm{mod}\, q)}} g(n)(\log x - \log n) + O((\log x)^k).$$

We can write this as

$$\frac{k}{q-2}\left(\sum_{n\le x} g(n)(\log x - \log n) - \sum_{\substack{n\le x\\ n\equiv a \,(\mathrm{mod}\, q)}} g(n)(\log x - \log n)\right) + O((\log x)^k).$$

From the bound (8.8) we have

$$\sum_{n\le x} g(n) = c_g(\log x)^k + O((\log x)^{k-1})$$

and, summing by parts,

$$\sum_{n\le x} g(n)\log n = \frac{kc_g}{k+1}(\log x)^{k+1} + O((\log x)^k).$$

Our sum is thus

$$\frac{k}{q-2}\left(\frac{c_g}{k+1}(\log x)^{k+1}-\sum_{\substack{n\le x\\ n\equiv a \pmod q}} g(n)(\log x-\log n)\right)+O((\log x)^k).$$

We therefore get

$$(q-2-k)\sum_{\substack{m\le x\\ m\equiv a \pmod q}} g(m)\log m+k\log x M_g(x)-\frac{kc_g}{k+1}(\log x)^{k+1}\ll (\log x)^k.$$

Since

$$\log x M_g(x)-\sum_{\substack{m\le x\\ m\equiv a \pmod q}} g(m)\log m=\sum_{\substack{m\le x\\ m\equiv a \pmod q}} g(m)\log\frac{x}{m}=\int_1^x M_g(t)t^{-1}\,dt$$

we have

$$M_g(x)\log x-\left(1-\frac{k}{q-2}\right)\int_1^x M_g(t)t^{-1}\,dt-\frac{kc_g}{(k+1)(q-2)}(\log x)^{k+1}\ll(\log x)^k.$$

We therefore conclude that for $x\ge 2$

$$M_g(x)\log x-\left(1-\frac{k}{q-2}\right)\int_2^x M_g(t)t^{-1}\,dt-\frac{kc_g}{(k+1)(q-2)}(\log x)^{k+1}\ll(\log x)^k.$$

Let

$$l=1-\frac{k}{q-2}$$

so that this is

$$M_g(x)\log x-l\int_2^x M_g(t)t^{-1}\,dt-\frac{kc_g}{(k+1)(q-2)}(\log x)^{k+1}\ll(\log x)^k.$$

Dividing by $x(\log x)^{l+1}$ we then get

$$x^{-1}(\log x)^{-l}\left(M_g(x)-l(\log x)^{-1}\int_2^x M_g(t)t^{-1}\,dt-\frac{kc_g}{(k+1)(q-2)}(\log x)^k\right)$$
$$\ll x^{-1}(\log x)^{k-l-1}.$$

We integrate this from 2 to x, replacing x by t and t by u. For any $\epsilon>0$ the RHS will be

$$\int_2^x t^{-1}(\log t)^{k-l-1}\,dt\ll_\epsilon 1+(\log x)^{k-l+\epsilon},$$

and the LHS will be

$$\int_2^x t^{-1}(\log t)^{-l}\left(M_g(t)-l(\log t)^{-1}\int_2^t M_g(u)u^{-1}\,du-\frac{kc_g}{(k+1)(q-2)}(\log t)^k\right)dt.$$

Reordering the double integral we see that

$$(\log x)^{-l}\int_2^x M_g(t)t^{-1}\,dt - \frac{kc_g}{(k+1)(q-2)}\int_2^x t^{-1}(\log t)^{k-l}\,dt \ll 1+(\log x)^{k-l+\epsilon}.$$

However

$$M_g(x)\log x - \frac{kc_g}{(k+1)(q-2)}(\log x)^{k+1} + O((\log x)^k) = l\int_2^x M_g(t)t^{-1}\,dt$$

so this simplifies to

$$\begin{aligned} M_g(x) &= \frac{kc_g}{(k+1)(q-2)}\left((\log x)^k + l(\log x)^{l-1}\int_2^x t^{-1}(\log t)^{k-l}\,dt\right) \\ &\qquad + O((\log x)^{l-1} + (\log x)^{k-1+\epsilon}). \end{aligned}$$

We know that

$$k-l = k-1+\frac{k}{q-2} > -1$$

so

$$\begin{aligned} M_g(x) &= kc_g\frac{1+l(k-l+1)^{-1}}{(k+1)(q-2)}(\log x)^k + o((\log x)^k) \\ &= kc_g\frac{(kq-2k+q-2)/(kq-k)}{(k+1)(q-2)}(\log x)^k + o((\log x)^k) \\ &= \frac{c_g}{q-1}(\log x)^k + o((\log x)^k). \end{aligned}$$

□

8.6 The Sieve

8.6.1 The Sieve Decomposition

Let $\mathcal{A} = (a_n)$ be the sequence given by

$$a_n = \sum_{\substack{(a,b)\in(0,N]^2 \\ C(a,b),bf(a,b)=n}} 1.$$

We will sieve $\mathcal{A}$ by the set of primes

$$\mathcal{P} = \{p : p \notin \mathcal{P}_1, p \equiv 1 \,(\mathrm{mod}\, q)\}.$$

Let

$$x = \max\{f(a,b) : (a,b) \in (0,N]^2\} = (c+o(1))N^3,$$

for some constant c which depends on f. We wish to prove a positive lower bound for the sifting function

$$S(\mathcal{A},\mathcal{P},x) = \sum_{(n;P(x))=1} a_n$$

where

$$P(z) = \prod_{\substack{p<z\\ p\in\mathcal{P}}} p.$$

Applying the Buchstab identity we get, for some $\alpha \in (\frac{1}{2},1)$, that

$$S(\mathcal{A},\mathcal{P},x) = S(\mathcal{A},\mathcal{P},N^\alpha) - \sum_{\substack{N^\alpha\le p<x\\ p\in\mathcal{P}}} S(\mathcal{A}_p,\mathcal{P},p).$$

If a prime p divides $bf(a,b)$ then either $p|b$ or $p|f(a,b)$. We may therefore write

$$S(\mathcal{A},\mathcal{P},x) \ge S(\mathcal{A},\mathcal{P},N^\alpha) - \sum_{\substack{N^\alpha\le p<x\\ p\in\mathcal{P}}} (S(\mathcal{A}_p^{(1)},\mathcal{P},p) + S(\mathcal{A}_p^{(2)},\mathcal{P},p))$$

where $\mathcal{A}_p^{(1)}$ is the subsequence of $\mathcal{A}_p$ coming from pairs (a,b) with $p|b$ whereas $\mathcal{A}_p^{(2)}$ is the subsequence coming from $p|f(a,b)$.

If $p|b$ we must have $p \le N$ so we can truncate the sum over $\mathcal{A}_p^{(1)}$ to $p \le N$. As our level of distribution, Lemma 8.11, is only nontrivial for $D_1D_2 \le N^2$ we split the sum over $\mathcal{A}_p^{(2)}$ at N^β for some $\beta \in (\frac{3}{2},2)$. We conclude that

$$S(\mathcal{A},\mathcal{P},x) \ge S_1 - S_2 - S_3 - S_4$$

where

$$S_1 = S(\mathcal{A},\mathcal{P},N^\alpha),$$

$$S_2 = \sum_{\substack{N^\alpha\le p\le N\\ p\in\mathcal{P}}} S(\mathcal{A}_p^{(1)},\mathcal{P},p),$$

$$S_3 = \sum_{\substack{N^\alpha\le p<N^\beta\\ p\in\mathcal{P}}} S(\mathcal{A}_p^{(2)},\mathcal{P},p)$$

and

$$S_4 = \sum_{\substack{N^\beta\le p<x\\ p\in\mathcal{P}}} S(\mathcal{A}_p^{(2)},\mathcal{P},p).$$

We then need a lower bound for S_1 and upper bounds for S_2, S_3 and S_4. All our bounds will eventually depend on the β-sieve as given by Friedlander and Iwaniec in [25, Theorem 11.13]. We let A_1, B_1 denote the constants A, B in the sieve of dimension $\frac{2}{q-1}$ and A_2, B_2 those for the sieve of dimension $\frac{q-2}{q-1}$. These are the only sieves we will use.

Throughout this section q, f and Δ are fixed. All use of the notation o is as $N \to \infty$.

8.6.2 The Sum S_1

We have

$$S_1 = S(\mathcal{A}, \mathcal{P}, N^\alpha).$$

Since $\alpha < 1$ we can take $D_1 = 1$ and $D_2 = N^\alpha$ in Lemma 8.11. This shows that we can apply a lower bound sieve of level N^α as the remainder term is $O(N^{2-\delta})$ for some $\delta > 0$. Using the notation of [25] we have

$$X = \frac{N^2}{\Delta^2}$$

and $g(p)$ is the multiplicative function given by

$$g(p) = \begin{cases} \frac{\rho_2(p)}{p^2} & p \in \mathcal{P} \\ 0 & \text{otherwise.} \end{cases}$$

It follows from Lemma 8.14 that the sieve dimension is $\frac{2}{q-1}$. If $q > 5$ then

$$\frac{2}{q-1} < \frac{1}{2},$$

and so the sifting limit is 1. We may therefore use the lower bound sieve to deduce that

$$S_1 \geq \frac{(B_1 + o(1))N^2}{\Delta^2} \prod_{\substack{p < N^\alpha \\ p \in \mathcal{P}}} \left(1 - \frac{\rho_2(p)}{p^2}\right) + O(N^{2-\delta}).$$

Applying Lemma 8.14 we conclude that

$$S_1 \geq \frac{(c_2(f,q)B_1 + o(1))N^2}{\Delta^2(\alpha \log N)^{\frac{2}{q-1}}}.$$

Finally, for any $\epsilon > 0$ we can choose α sufficiently close to 1 in terms of ϵ to get the bound

$$S_1 \geq \frac{(c_2(f,q)B_1 - \epsilon + o(1)N^2}{\Delta^2(\log N)^{\frac{2}{q-1}}}.$$

8.6.3 The Sum S_2

In our bound for S_2 we will exploit the fact that α may be taken as close to 1 as we require. We therefore do not need to give a bound which is as sharp as possible. It is enough to show that for any $\epsilon > 0$ we can choose $\alpha < 1$ depending on ϵ such that

$$S_2 \leq \frac{(\epsilon + o(1))N^2}{(\log N)^{\frac{2}{q-1}}}.$$

We have

$$S_2 \leq \sum_{\substack{N^\alpha \leq p \leq N \\ p \in \mathcal{P}}} S(\mathcal{A}_p^{(1)}, \mathcal{P}, N^\alpha).$$

For each pair (a, b) counted by S_2 we may write $b = pr$ where

$$p \in \mathcal{P} \cap [N^\alpha, N],$$

$$r \leq N^{1-\alpha} = R$$

and

$$(r; P(R)) = 1.$$

In addition we have $b \equiv b_0 \,(\mathrm{mod}\, \Delta)$. By our construction of b_0 we know that for each $p'|\Delta$ there exists an l for which $p'^l|\Delta$ and

$$b_0 \not\equiv 0 \,(\mathrm{mod}\, p'^l).$$

It follows that for each such prime its power dividing b is the same as that dividing b_0. For $p \in \mathcal{P}$ we have $(\Delta; p) = 1$. It follows that for each $p'|\Delta$ the power of p' dividing r is precisely that dividing b_0. In other words we may write

$$r = (b_0; \Delta)r' \text{ with } (r'; \Delta) = 1.$$

Given such an r and a pair (a, b) satisfying $C(a, b)$ the condition $r|b$ is equivalent to $r'|b$.

We may therefore write

$$S_2 \leq \sum_{\substack{r \leq R/(b_0;\Delta) \\ (r;P(R)\Delta)=1}} S_2(r)$$

where

$$S_2(r) = \#\{(a, b) \in (0, N]^2 : C(a, b), r|b, b/r(b_0; \Delta) \in \mathcal{P}, (bf(a, b); P(N^\alpha)) = 1\}.$$

Note that the variable of summation, r, is r' in the above notation.

Recall that

$$\mathcal{P}' = \{p : p \notin \mathcal{P}_1, p \not\equiv 1 \,(\mathrm{mod}\, q)\}$$

and let

$$P'(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}'}} p.$$

If we let $z = N^\delta$ for some $\delta > 0$ then provided $\delta < \alpha$ we have

$$S_2(r) \le \#\{(a,b) \in (0,N]^2 : C(a,b), r|b, (bf(a,b); P(z)) = (b/r; P'(z)) = 1\}.$$

Suppose that μ_1^+, μ_2^+ are upper bound sieves of level z. We have

$$S_2(r) \le \sum_{\substack{(a,b)\in(0,N]^2 \\ r|b, C(a,b)}} \left(\sum_{d|\,(P(z);bf(a,b))} \mu_1^+(d) \right) \left(\sum_{e|\,(b/r;P'(z))} \mu_2^+(e) \right).$$

Reordering the summations we get

$$\begin{aligned} S_2(r) &\le \sum_{d|P(z)} \sum_{e|P'(z)} \mu_1^+(d)\mu_2^+(e) \#\{(a,b) \in (0,N]^2 : C(a,b), re|b, d|bf(a,b)\} \\ &= \sum_{d|P(z)} \sum_{e|P'(z)} \mu_1^+(d)\mu_2^+(e) R_1(d, re). \end{aligned}$$

If δ is sufficiently small so that

$$1 - \alpha + 2\delta < 1$$

then

$$rde \le N.$$

Furthermore $(re; d) = (dre; \Delta) = 1$ so Lemma 8.12 applies and we get

$$S_2(r) \le \sum_{d|P(z)} \sum_{e|P'(z)} \mu_1^+(d)\mu_2^+(e) \left(\frac{N^2 \rho_2(d)}{d^2 re \Delta^2} + O_\epsilon(Nd^\epsilon) \right).$$

The contribution of the error term to S_2 is bounded by

$$\sum_{r\le R} N^{1+2\delta+\epsilon} \ll N^{2-\alpha+2\delta+\epsilon} = o(\frac{N^2}{(\log N)^{\frac{2}{q-1}}}),$$

in view of our assumption on the size of δ.

The main term in the above estimate for $S_2(r)$ is

$$\frac{N^2}{r\Delta^2}\left(\sum_{d|P(z)}\mu_1^+(d)\frac{\rho_2(d)}{d^2}\right)\left(\sum_{e|P'(z)}\frac{\mu_2^+(e)}{e}\right).$$

The two sums may now be estimated using the sieve. We let (μ_1^+) be a sieve of dimension $\frac{2}{q-1}$. It follows using Lemma 8.14 that

$$\begin{aligned}\sum_{d|P(z)}\mu_1^+(d)\frac{\rho_2(d)}{d^2} &\leq (A_1+o(1))\prod_{\substack{p<z\\ p\in\mathcal{P}}}\left(1-\frac{\rho_2(p)}{p^2}\right)\\ &= (A_1+o(1))\frac{c_2(f,q)}{(\delta\log N)^{\frac{2}{q-1}}}.\end{aligned}$$

We let (μ_2^+) be a sieve of dimension $\frac{q-2}{q-1}$ and thus we get

$$\sum_{e|P'(z)}\frac{\mu_2^+(e)}{e}\leq(A_2+o(1))\prod_{\substack{p<z\\ p\in\mathcal{P}'}}\left(1-\frac{1}{p}\right).$$

Finally we have the bound

$$\sum_{\substack{r\leq R/(b_0;\Delta)\\ (r;P(R)\Delta=1}}\frac{1}{r}\leq\prod_{\substack{p<R\\ p\in\mathcal{P}'}}\left(1-\frac{1}{p}\right)^{-1}.$$

By taking α sufficiently close to 1 we can assume that $R<z$. It follows that

$$\prod_{\substack{p<z\\ p\in\mathcal{P}'}}\left(1-\frac{1}{p}\right)\prod_{\substack{p<R\\ p\in\mathcal{P}'}}\left(1-\frac{1}{p}\right)^{-1}=\prod_{\substack{R<p<z\\ p\in\mathcal{P}'}}\left(1-\frac{1}{p}\right)\sim\left(\frac{1-\alpha}{\delta}\right)^{\frac{q-2}{q-1}}.$$

We finally conclude that

$$S_2\leq\left(\frac{1-\alpha}{\delta}\right)^{\frac{q-2}{q-1}}\frac{(A_1A_2c_2(f,q)+o(1))N^2}{\Delta^2(\delta\log N)^{\frac{2}{q-1}}}.$$

It follows that for any $\epsilon>0$ there exists an $\alpha<1$ depending on ϵ such that

$$S_2\leq\frac{(\epsilon+o(1))N^2}{(\log N)^{\frac{2}{q-1}}}.$$

8.6.4 The Sum S_3

Let $S_3(P_1, P_2)$ denote the part of S_3 with $P_1 \le p < P_2$. We have

$$S_3(P_1, P_2) \le \sum_{\substack{P_1 \le p < P_2 \\ p \in \mathcal{P}}} S(\mathcal{A}_p^{(2)}, \mathcal{P}, P_1).$$

We will apply an upper bound sieve to each summand separately. For every prime p and all $d \in \mathbb{N}$ we have

$$\sum_{n \equiv 0 \,(\mathrm{mod}\, d)} (a_p^{(2)})_n = R(p, d).$$

If $d < p$ then clearly $(d; p) = 1$. We will apply Lemma 8.11 with $D_1 = P_2$ and

$$D_2 = D_2(P_1, P_2) = \min(N^{1-\gamma}, P_1, \frac{N^{2-\gamma}}{P_2})$$

for some $\gamma > 0$ which we will choose arbitrarily small. We then have

$$\sum_{\substack{p \le P_2, d \le D_2 \\ (d;\Delta)=1, \mu(d)^2=1}} \left| R(p, d) - \frac{\rho_1(p)\rho_2(d)N^2}{p^2 d^2 \Delta^2} \right| \ll N^{2-\delta},$$

for some $\delta > 0$ which depends on γ.

Applying the upper bound sieve of dimension $\frac{2}{q-1}$ results in

$$S_3(P_1, P_2) \le \frac{(A_1 + o(1))N^2}{\Delta^2} \left(\prod_{\substack{p < D_2 \\ p \in \mathcal{P}}} \left(1 - \frac{\rho_2(p)}{p^2}\right) \right) \sum_{\substack{P_1 \le p < P_2 \\ p \in \mathcal{P}}} \frac{\rho_1(p)}{p^2} + O(N^{2-\delta}).$$

We can evaluate the product using Lemma 8.14 to get

$$S_3(P_1, P_2) \le \frac{(c_2(f, q)A_1 + o(1))N^2}{\Delta^2 (\log D_2)^{\frac{2}{q-1}}} \sum_{\substack{P_1 \le p < P_2 \\ p \in \mathcal{P}}} \frac{\rho_1(p)}{p^2} + O(N^{2-\delta}).$$

In addition, using our previous convention that the value c may vary from line to line, we have

$$\begin{aligned} \sum_{\substack{p \le x \\ p \in \mathcal{P}}} \frac{\rho_1(p)}{p^2} &= \sum_{\substack{p \le x \\ p \in \mathcal{P}}} \frac{(p-1)\nu(p) + 1}{p^2} \\ &= \sum_{\substack{p \le x \\ p \in \mathcal{P}}} \frac{\nu(p)}{p} + c + o(1) \\ &= \frac{1}{q-1} \log\log x + c + o(1). \end{aligned}$$

We first consider $S_3(N^\alpha, N^{2-\alpha})$. As in the previous section we will take α close to 1 which is enough to make this part of the sum small. We take $D_2 = N^\alpha$, getting

$$S_3(N^\alpha, N^{2-\alpha}) \leq \frac{1}{q-1}(\log(2-\alpha) - \log\alpha)\frac{(c_2(f,q)A_1 + o(1))N^2}{\Delta^2(\alpha\log N)^{\frac{2}{q-1}}}.$$

It follows that for any $\epsilon > 0$ we can choose α sufficiently close to 1 to deduce that

$$S_3(N^\alpha, N^{2-\alpha}) \leq \frac{(\epsilon + o(1))N^2}{(\log N)^{\frac{2}{q-1}}}.$$

It remains to estimate $S_3(N^{2-\alpha}, N^\beta)$. We divide this range into dyadic intervals $[P_1, 2P_1)$. For each such interval we have

$$D_2 = \frac{N^{2-\gamma}}{P_1}.$$

By taking $\gamma < 2-\beta$ we have $D_2 \geq 1$ for all the dyadic intervals. In addition if $p \sim P_1$ then

$$(\log D_2)^{-\frac{2}{q-1}} = \left(\log\frac{N^{2-\gamma}}{P_1}\right)^{-\frac{2}{q-1}} \leq \left(\log\frac{N^{2-\gamma}}{p}\right)^{-\frac{2}{q-1}}.$$

We therefore have

$$S_3(P_1, 2P_1) \leq \frac{(c_2(f,q)A_1 + o(1))N^2}{\Delta^2} \sum_{\substack{P_1 \leq p < 2P_1 \\ p\in\mathcal{P}}} \frac{\rho_1(p)}{p^2\left(\log\frac{N^{2-\gamma}}{p}\right)^{\frac{2}{q-1}}} + O(N^{2-\delta})$$

and thus

$$S_3(N^{2-\alpha}, N^\beta) \leq \frac{(c_2(f,q)A_1 + o(1))N^2}{\Delta^2(\log N)^{\frac{2}{q-1}}} \sum_{\substack{N^{2-\alpha} \leq p < N^\beta \\ p\in\mathcal{P}}} \frac{\rho_1(p)}{p^2(2-\gamma-\log p/\log N)^{\frac{2}{q-1}}}.$$

We have

$$\sum_{\substack{N \leq p < t \\ p\in\mathcal{P}}} \frac{\rho_1(p)}{p^2} = \frac{1}{q-1}(\log\log t - \log\log N) + o(1),$$

so we can sum by parts to get

$$\begin{aligned}
&\sum_{\substack{N^{2-\alpha}\le p<N^\beta\\ p\in\mathcal{P}}} \frac{\rho_1(p)}{p^2(2-\gamma-\log p/\log N)^{\frac{2}{q-1}}}\\
&\le \sum_{\substack{N\le p<N^\beta\\ p\in\mathcal{P}}} \frac{\rho_1(p)}{p^2(2-\gamma-\log p/\log N)^{\frac{2}{q-1}}}\\
&= \frac{1}{q-1}\frac{\log\beta}{(2-\gamma-\beta)^{\frac{2}{q-1}}} - \frac{2}{(q-1)^2}\int_N^{N^\beta} \frac{\log\log t-\log\log N}{t\log N(2-\gamma-\log t/\log N))^{\frac{q+1}{q-1}}}\,dt+o(1)\\
&= \frac{1}{q-1}\frac{\log\beta}{(2-\gamma-\beta)^{\frac{2}{q-1}}} - \frac{2}{(q-1)^2}\int_1^{\beta} \log s(2-\gamma-s)^{-\frac{q+1}{q-1}}\,ds+o(1)\\
&= \frac{1}{q-1}\int_1^{\beta}(2-\gamma-s)^{-\frac{2}{q-1}}\,\frac{ds}{s}+o(1).
\end{aligned}$$

We conclude that

$$S_3(N^{2-\alpha},N^\beta)\le \frac{(c_2(f,q)A_1+o(1))N^2}{\Delta^2(q-1)(\log N)^{\frac{2}{q-1}}}\int_1^{\beta}(2-\gamma-s)^{-\frac{2}{q-1}}\,\frac{ds}{s}.$$

Combining the above bounds we see that for any $\epsilon>0$ we can choose α sufficiently close to 1 and γ sufficiently small to get the bound

$$S_3\le \frac{(c_2(f,q)A_1+\epsilon+o(1))N^2}{\Delta^2(q-1)(\log N)^{\frac{2}{q-1}}}\int_1^{\beta}(2-s)^{-\frac{2}{q-1}}\,\frac{ds}{s}.$$

8.6.5 The Sum S_4

We have

$$S_4\le \sum_{\substack{N^\beta\le p<x\\ p\in\mathcal{P}}} S(\mathcal{A}_p^{(2)},\mathcal{P},N^\beta).$$

For each pair (a,b) counted by S_4 we can write $f(a,b)=pr$ where

$$p\in[N^\beta,x]\cap\mathcal{P},$$

$$r\le\frac{x}{N^\beta}=R$$

and

$$(r;P(R))=1.$$

Let $f_0=f(a_0,b_0)$. For each prime $p'|\Delta$ we know that there exists an l for which $p'^l|\Delta$ and

$$f_0\not\equiv 0\,(\mathrm{mod}\,p'^l).$$

It follows that the power of p' dividing $f(a,b)$ is the same as that dividing f_0. Since $(p;\Delta)=1$ this power is the same as that dividing r. In other words we can write

$$r=(f_0;\Delta)r', \quad (r';\Delta)=1.$$

Given a pair (a,b) with $C(a,b)$ the condition $r|f(a,b)$ is equivalent to $r'|f(a,b)$.

The prime q divides Δ. In addition since $p\in\mathcal{P}$ we have $p\equiv 1\,(\mathrm{mod}\,q)$. It follows that there exists r_0 depending only on a_0,b_0,Δ with $(r_0;q)=1$ such that

$$r'\equiv r_0\,(\mathrm{mod}\,q).$$

We may now write

$$S_4\leq \sum_{\substack{r\leq R/(f_0;\Delta)\\(r;P(R)\Delta)=1, r\equiv r_0\,(\mathrm{mod}\,q)}} S_4(r)$$

where

$$\begin{aligned} S_4(r) &= \#\{(a,b)\in(0,N]^2 : C(a,b), r|f(a,b),\\ &\qquad (f(a,b)/r; P'(z'))=(bf(a,b);P(z))=1\},\end{aligned}$$

for some z,z' satisfying $0\leq z,z'\leq N^\beta$. Note that the variable of summation, r, is r' in the above notation. We will split the sum over r into dyadic segments $r\sim R_1$.

Let μ_1^+,μ_2^+ be upper bound sieves of levels D' and D, respectively, where D,D' depend on R_1. It follows that

$$\begin{aligned} S_4(r) &\leq \sum_{\substack{d|P'(z')\\(d;r)=1}}\sum_{e|P(z)}\mu_1^+(d)\mu_2^+(e)\#\{(a,b)\in(0,N]^2 : C(a,b), dr|f(a,b), e|bf(a,b)\}\\ &= \sum_{\substack{d|P'(z')\\(d;r)=1}}\sum_{e|P(z)}\mu_1^+(d)\mu_2^+(e)R(dr,e).\end{aligned}$$

Since $(dr;e)=(dre;\Delta)=1$ we may apply Lemma 8.11. If we write $D=N^\eta, D'=N^{\eta'}$ this requires that

$$\eta\leq 1-\delta$$

and

$$\eta+\eta'+\frac{\log R_1}{\log N}\leq 2-\delta,$$

for some $\delta>0$ which we will eventually take arbitrarily small. Given these assumptions on η and η' the contribution of the error term to S_4 is $o(\frac{N^2}{\log N^{\frac{2}{q-1}}})$.

It remains to deal with the main term coming from Lemma 8.11. This is

$$\frac{N^2\rho_1(r)}{r^2\Delta^2}\left(\sum_{\substack{d|\,P'(z')\\(d;r)=1}}\mu_1^+(d)\frac{\rho_1(d)}{d^2}\right)\left(\sum_{e|\,P(z)}\mu_2^+(e)\frac{\rho_2(e)}{e^2}\right).$$

The two terms can now be estimated using the sieve. Considering the results of Lemma 8.14 we let μ_1^+ be a sieve of dimension $\frac{q-2}{q-1}$ and we let μ_2^+ be a sieve of dimension $\frac{2}{q-1}$. We may assume that $z = D$ and either $z' = D'$ or $z' = N^\beta \le D' \le N^2$. It follows that the values of z, z' do not affect the sieve upper bounds and therefore

$$\begin{aligned}\sum_{\substack{d|P'(z')\\(d;r)=1}}\mu_1^+(d)\frac{\rho_1(d)}{d^2} &\le (A_2+o(1))\prod_{\substack{p<D'\\p\in\mathcal{P}'}}\left(1-\frac{\rho_1(p)}{p^2}\right)\prod_{p|r}\left(1-\frac{\rho_1(p)}{p^2}\right)^{-1}\\ &= \frac{(c_1(f,q)A_2+o(1))}{(\eta'\log N)^{\frac{q-2}{q-1}}}\prod_{p|r}\left(1-\frac{\rho_1(p)}{p^2}\right)^{-1}\end{aligned}$$

and

$$\sum_{e|P(z)}\mu_2^+(e)\frac{\rho_2(e)}{e^2} \le (A_1+o(1))\prod_{\substack{p<z\\p\in\mathcal{P}}}\left(1-\frac{\rho_2(p)}{p^2}\right) = \frac{(c_2(f,q)A_1+o(1))}{(\eta\log N)^{\frac{2}{q-1}}}.$$

The contribution to our upper bound from the η, η' is then

$$\frac{1}{\eta'^{\frac{q-2}{q-1}}\eta^{\frac{2}{q-1}}}.$$

Therefore, to give an optimal result, we want to maximise

$$\eta'^{q-2}\eta^2$$

subject to the constraints

$$\eta \le 1-\delta$$

and

$$\eta+\eta' \le 2-\frac{\log R_1}{\log N}-\delta.$$

By monotonicity it is clear that the maximum occurs when we have equality in the last constraint so

$$\eta' = 2-\delta-\eta-\frac{\log R_1}{\log N}.$$

We therefore wish to maximise

$$(2-\delta-\eta-\frac{\log R_1}{\log N})^{q-2}\eta^2$$

for $\eta \in (0, 1-\delta]$. Taking logs we maximise

$$(q-2)\log\left(2-\delta-\eta-\frac{\log R_1}{\log N}\right)+2\log\eta$$

so we solve

$$-(q-2)\left(2-\delta-\eta-\frac{\log R_1}{\log N}\right)^{-1}+2\eta^{-1}=0.$$

This gives

$$\eta = 2q^{-1}\left(2-\delta-\frac{\log R_1}{\log N}\right).$$

Observe that this is in $(0, 1-\delta]$ if $q \geq 5$ and δ is sufficiently small. We then get

$$\eta' = 2-\delta-\eta-\frac{\log R_1}{\log N} = (1-2q^{-1})\left(2-\delta-\frac{\log R_1}{\log N}\right).$$

If $q \geq 5$ and δ is sufficiently small then $\eta' > 0$. The factor coming from η, η' is thus

$$\left((1-2q^{-1})\left(2-\delta-\frac{\log R_1}{\log N}\right)\right)^{-\frac{q-2}{q-1}}\left(2q^{-1}\left(2-\delta-\frac{\log R_1}{\log N}\right)\right)^{-\frac{2}{q-1}}.$$

This increases as we increase R_1 so we can replace R_1 by r getting the smooth weight

$$w(r,\delta) = (1-2q^{-1})^{-\frac{q-2}{q-1}}(2q^{-1})^{-\frac{2}{q-1}}\left(2-\delta-\frac{\log R_1}{\log N}\right)^{-\frac{q}{q-1}}.$$

Combining all of the above we see that the main term in our estimate for S_4 is

$$\frac{A_1A_2c_1(f,q)c_2(f,q)N^2}{\Delta^2(\log N)^{\frac{q}{q-1}}}\sum_{\substack{r\leq R/(f_0;\Delta)\\ r\equiv r_0 \,(\mathrm{mod}\, q)}} w(r,\delta)g(r),$$

where $g(r)$ is the multiplicative function which is 0 unless all the prime factors of r are in $\mathcal{P}'$, in which case it is given by

$$g(r) = \frac{\rho_1(r)}{r^2}\prod_{p|r}\left(1-\frac{\rho_1(p)}{p^2}\right)^{-1}.$$

To estimate the sum over r we begin by dealing with the r which are squarefree.

Lemma 8.17. *The multiplicative function g, when restricted to squarefree numbers, satisfies all the hypotheses of Lemma 8.16.*

Proof. Since $q|\Delta$ we know that $g(q) = 0$. In addition if $g(p) \neq 0$ then $p \in \mathcal{P}'$ so $p \not\equiv 1 \,(\mathrm{mod}\, q)$.

If $a \not\equiv 0, 1 \pmod q$ then

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} g(p)\log p &= \sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} \left(1-\frac{\rho_1(p)}{p^2}\right)^{-1}\frac{\rho_1(p)}{p^2}\log p + O(1)\\ &= \sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} \frac{\rho_1(p)}{p^2}\log p + O(1)\\ &= \sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} \frac{(p-1)\nu(p)+1}{p^2}\log p + O(1)\\ &= \frac{1}{q-1}\log x + O(1).\end{aligned}$$

This establishes (8.5) and (8.9) with

$$k = \frac{q-2}{q-1}.$$

If $2 \le w < z$ then, by Lemma 8.14, we have

$$\prod_{w\le p<z}(1+g(p)) = \prod_{\substack{w\le p<z\\ p\in\mathcal{P}'}}\left(1-\frac{\rho_1(p)}{p^2}\right)^{-1} \ll \left(\frac{\log z}{\log w}\right)^{\frac{q-2}{q-1}},$$

so (8.6) holds. Finally

$$\sum_p g(p)^2\log p = \sum_{p\in\mathcal{P}'}\left(1-\frac{\rho_1(p)}{p^2}\right)^{-2}\frac{\rho_1(p)^2}{p^4}\log p \ll \sum_p \frac{1}{p^2}\log p < \infty$$

and therefore (8.7) also holds. □

Summing by parts and applying Lemma 8.16 we have

$$\begin{aligned}
&\sum_{\substack{r\le R/(f_0;\Delta)\\ \mu(r)\neq 0,\, r\equiv r_0 (\mathrm{mod}\, q)}} w(r,\delta)g(r)\\
&\le \sum_{\substack{r\le R\\ \mu(r)\neq 0,\, r\equiv r_0 (\mathrm{mod}\, q)}} w(r,\delta)g(r)\\
&= w(R,\delta) \sum_{\substack{r\le R\\ \mu(r)\neq 0,\, r\equiv r_0 (\mathrm{mod}\, q)}} g(r) - \int_1^R \left(\sum_{\substack{r\le t\\ \mu(r)\neq 0,\, r\equiv r_0 (\mathrm{mod}\, q)}} g(r) \right) w'(t)\, dt\\
&= (c_g+o(1))\frac{1}{q-1}\left(w(R,\delta)(\log R)^{\frac{q-2}{q-1}} - \int_1^R w'(t)(\log t)^{\frac{q-2}{q-1}}\, dt \right)\\
&= (c_g+o(1))\frac{q-2}{(q-1)^2}\int_1^R w(t,\delta)(\log t)^{\frac{-1}{q-1}} t^{-1}\, dt\\
&= (c_g+o(1))\frac{q-2}{(q-1)^2}(\log N)^{\frac{q-2}{q-1}}\int_0^{\log R/\log N} w(N^s,\delta)s^{\frac{-1}{q-1}}\, ds,
\end{aligned}$$

where

$$c_g = \frac{1}{\Gamma(2-\frac{1}{q-1})}\prod_p \left(1-\frac{1}{p}\right)^{\frac{q-2}{q-1}}(1+g(p)).$$

Observe that

$$w(N^s,\delta) = (1-2q^{-1})^{-\frac{q-2}{q-1}}(2q^{-1})^{-\frac{2}{q-1}}(2-\delta-s)^{-\frac{q}{q-1}}$$

does not depend on N. In addition

$$\frac{\log R}{\log N} = \frac{\log x}{\log N} - \beta = 3-\beta+o(1)$$

as $N\to\infty$. We may therefore replace the upper limit of integration by $3-\beta$ at the cost of an error which is $o(1)$. We conclude that

$$\sum_{\substack{r\le R/(f_0;\Delta)\\ \mu(r)\neq 0,\, r\equiv r_0 (\mathrm{mod}\, q)}} w(r,\delta)g(r) \le (c_g+o(1))\frac{q-2}{(q-1)^2}(\log N)^{\frac{q-2}{q-1}}\int_0^{3-\beta} w(N^s,\delta)s^{\frac{-1}{q-1}}\, ds.$$

Let

$$W(s) = w(N^s,0)s^{\frac{-1}{q-1}}.$$

For any $\epsilon>0$ we can choose a sufficiently small δ to get

$$\int_0^{3-\beta} w(N^s,\delta)s^{\frac{-1}{q-1}}\, ds \le \int_0^{3-\beta} W(s)\, ds + \epsilon + o(1)$$

and thus

$$\sum_{\substack{r\le R/(f_0;\Delta)\\ \mu(r)\neq 0,\, r\equiv r_0 \pmod q}} w(r,\delta)g(r) \le (c_g+\epsilon+o(1))\frac{q-2}{(q-1)^2}(\log N)^{\frac{q-2}{q-1}}\int_0^{3-\beta} W(s)\,ds.$$

It remains to deal with the sum over those r which are not squarefree.

Lemma 8.18. *For any $\epsilon>0$ there exists a P_1, depending on ϵ, q and f but not on N, such that if we include all primes $p\le P_1$ in $\mathcal{P}_1$ then*

$$\sum_{\substack{r\le R/(f_0;\Delta)\\ \mu(r)=0,\, r\equiv r_0 \pmod q}} w(r,\delta)g(r) \le (\epsilon+o(1))(\log N)^{\frac{q-2}{q-1}}.$$

Proof. Any $r\in\mathbb{N}$ can be written uniquely as $r=r_1r_2$ for some squarefree r_1 and some squarefull r_2 satisfying $(r_1;r_2)=1$. In addition if $\mu(r)=0$ then $r_2>1$. Since $w(r,\delta)\ll 1$ and $g(r)\ge 0$ our sum may be bounded by

$$\sum_{\substack{r_1r_2\le R/(f_0;\Delta)\\ r_2>1}} g(r_1)g(r_2),$$

where the sum is restricted to squarefree r_1 and squarefull r_2 with $(r_1;r_2)=1$.

Since $g(r)$ is supported on numbers having no prime factor in $\mathcal{P}_1$ we can use Lemma 8.15 to deduce that for all r

$$g(r) \ll_\epsilon r^{-\frac{2}{3}+\epsilon}.$$

It follows that

$$\sum_{r \text{ squarefull}} g(r) < \infty.$$

Furthermore, if we include all primes up to P_1 in $\mathcal{P}_1$ then all terms in this sum with $r\le P_1$ are 0. It follows that for any $\epsilon>0$ we can choose P_1 sufficiently large so that

$$\sum_{\substack{r>1\\ r \text{ squarefull}}} g(r) < \epsilon.$$

Our original sum may therefore be bounded by

$$\left(\sum_{\substack{r_1\le R/(f_0;\Delta)\\ \mu(r_1)\neq 0}} g(r_1)\right)\left(\sum_{r_2 \text{ squarefull}} g(r_2)\right).$$

Using Lemma 8.16 the first sum is $O((\log R)^{\frac{q-2}{q-1}})$ so the result follows. □

It follows from the last lemma that, with a suitable choice of P_1, the non-squarefree r give a contribution to S_4 bounded by

$$\frac{(\epsilon + o(1))N^2}{(\log N)^{\frac{2}{q-1}}}.$$

Combining all of the results of this subsection we see that for any $\epsilon > 0$, by taking sufficiently many small primes in $\mathcal{P}_1$ and δ sufficiently small, we get the bound

$$S_4 \leq \int_0^{3-\beta} W(s)\, ds \frac{(A_1 A_2 c_g c_1(f,q) c_2(f,q) + \epsilon + o(1))(q-2)N^2}{\Delta^2 (q-1)^2 (\log N)^{\frac{2}{q-1}}}.$$

Finally we must remove the constants $c_g, c_1(f,q)$ from this bound. Recall that these are defined by

$$\begin{aligned} c_g &= \frac{1}{\Gamma(2-\frac{1}{q-1})} \prod_p \left(1-\frac{1}{p}\right)^{\frac{q-2}{q-1}} (1+g(p)) \\ &= \frac{1}{\Gamma(2-\frac{1}{q-1})} \lim_{x\to\infty} \prod_{p\leq x} \left(1-\frac{1}{p}\right)^{\frac{q-2}{q-1}} (1+g(p)) \\ &= \frac{1}{\Gamma(2-\frac{1}{q-1})} \lim_{x\to\infty} \left(\frac{e^{-\gamma}}{\log x}\right)^{\frac{q-2}{q-1}} \prod_{\substack{p\leq x \\ p\in\mathcal{P}'}} \left(1-\frac{\rho_1(p)}{p^2}\right)^{-1} \end{aligned}$$

and

$$c_1(f,q) = \lim_{x\to\infty} (\log x)^{\frac{q-2}{q-1}} \prod_{\substack{p<x \\ p\in\mathcal{P}'}} \left(1-\frac{\rho_1(p)}{p^2}\right).$$

It follows that

$$c_g c_1(f,q) = \frac{e^{-\gamma\frac{q-2}{q-1}}}{\Gamma(2-\frac{1}{q-1})}.$$

We therefore conclude that

$$S_4 \leq \int_0^{3-\beta} W(s)\, ds \frac{\left(A_1 A_2 e^{-\gamma\frac{q-2}{q-1}} c_2(f,q)(q-2) + \epsilon + o(1)\right) N^2}{\Delta^2 \Gamma(2-\frac{1}{q-1})(q-1)^2 (\log N)^{\frac{2}{q-1}}}.$$

It is possible to give a somewhat simpler treatment of the sum S_4 to obtain a bound which is worse than the above by a constant factor. This would be enough to prove Theorem 8.1 for sufficiently large q. For example the quantities η and η' could be chosen independently of R_1, thereby avoiding the above optimisation and the weight W. We could then work with an upper bound for the sum of the multiplicative function $g(r)$, rather than an asymptotic, which would remove the need for Lemma 8.16.

8.6.6 Conclusion

Combining the bounds for S_1, S_2, S_3 and S_4 we conclude that for any $\epsilon > 0$ we can take sufficiently many small primes in $\mathcal{P}_1$ so that we have, as $N \to \infty$, that

$$S(\mathcal{A}, \mathcal{P}, x) \geq \frac{c_2(f,q)N^2}{\Delta^2 (\log N)^{\frac{2}{q-1}}}(F(q) - \epsilon + o(1))$$

where

$$F(q) = B_1 - \frac{A_1}{q-1}\int_1^\beta (2-s)^{-\frac{2}{q-1}}\,\frac{ds}{s} - \frac{A_1 A_2 e^{-\gamma\frac{q-2}{q-1}}(q-2)}{\Gamma(2-\frac{1}{q-1})(q-1)^2}\int_0^{3-\beta} W(s)\,ds$$

and

$$W(s) = (1-2q^{-1})^{-\frac{q-2}{q-1}}(2q^{-1})^{-\frac{2}{q-1}}(2-s)^{-\frac{q}{q-1}}s^{\frac{-1}{q-1}}.$$

Recall that the values A_1, B_1 and A_2 all depend on q. As the sieve dimension $\kappa \to 0$ we have $A(\kappa), B(\kappa) \to 1$. It follows that

$$\lim_{q\to\infty} F(q) = 1.$$

Therefore $F(q)$ is positive for $q \geq q_0$ for some absolute q_0. For any such q we can then choose N sufficiently large to get $S(\mathcal{A}, \mathcal{P}, x) > 0$ and thus (8.1) has a rational solution.

To give the best possible bound we must choose β to minimise

$$\int_1^\beta (2-s)^{-\frac{2}{q-1}}\,\frac{ds}{s} + \frac{A_2 e^{-\gamma\frac{q-2}{q-1}}(q-2)}{\Gamma(2-\frac{1}{q-1})(q-1)}\int_0^{3-\beta} W(s)\,ds.$$

Thus we must solve

$$(2-\beta)^{-\frac{2}{q-1}}\beta^{-1} - \frac{A_2 e^{-\gamma\frac{q-2}{q-1}}(q-2)}{\Gamma(2-\frac{1}{q-1})(q-1)}W(3-\beta) = 0,$$

that is

$$(2-\beta)^{-\frac{2}{q-1}}\beta^{-1} - \frac{A_2 e^{-\gamma\frac{q-2}{q-1}}(q-2)}{\Gamma(2-\frac{1}{q-1})(q-1)}(1-2q^{-1})^{-\frac{q-2}{q-1}}(2q^{-1})^{-\frac{2}{q-1}}(\beta-1)^{-\frac{q}{q-1}}(3-\beta)^{\frac{-1}{q-1}} = 0.$$

To complete the proof of Theorem 8.1 we must show that for all primes $q \geq 7$ there exists a choice of $\beta \in (\frac{3}{2}, 2)$ for which $F(q) > 0$. The case $q = 7$ is the most delicate numerically so we deal with it first.

From Friedlander and Iwaniec's table in [25, Section 11.19] we obtain the value

$$A_2 = A(5/6) = 2.56140\ldots.$$

The constants A_1, B_1 are given by [25, (11.62)]. We find by numerical integration that

$$A_1 = A(1/3) = 1.27713\ldots$$

and

$$B_1 = B(1/3) = 0.71213\ldots.$$

By solving the above equation numerically we discover that the optimal choice for β is approximately 1.994. We conclude, evaluating all integrals numerically, that

$$F(7) \approx 0.0504 > 0.$$

Due to the use of numerical integration we cannot be completely sure that $F(7) > 0$. However we are confident that the computations were sufficiently accurate to make this extremely likely. The two integrals occurring in the above formula for $F(q)$ can be computed to a sufficiently high degree of precision. However the constants A_1 and B_1 are defined in a rather complex way, involving double integrals over an infinite region, so that we expect that the above values might be comparatively less accurate.

For $q \geq 11$ we do not need to be quite so careful. Since $A_2 \leq A(1)$ we have

$$F(q) \geq B_1 - \frac{A_1}{q-1}\int_1^\beta (2-s)^{-\frac{2}{q-1}}\,\frac{ds}{s} - \frac{A_1 A(1) e^{-\gamma\frac{q-2}{q-1}}(q-2)}{\Gamma(2-\frac{1}{q-1})(q-1)^2}\int_0^{3-\beta} W(s)\,ds.$$

As q increases $B_1 = B(\frac{2}{q-1})$ is increasing whereas $A_1 = A(\frac{2}{q-1})$ is decreasing. In addition, for any $s \in (1,\beta)$ the quantity

$$(2-s)^{-\frac{2}{q-1}}$$

is decreasing, as are

$$e^{-\gamma\frac{q-2}{q-1}},$$

$$\frac{q-2}{(q-1)^2}$$

and

$$\frac{1}{\Gamma(2-\frac{1}{q-1})}.$$

Recall that

$$W(s) = (1-2q^{-1})^{-\frac{q-2}{q-1}}(2q^{-1})^{-\frac{2}{q-1}}(2-s)^{-\frac{q}{q-1}}s^{\frac{-1}{q-1}}.$$

It can be shown that for any $s \in (0, 3-\beta)$ this decreases as we increase q.

We can conclude that, for a fixed $\beta \in (\frac{3}{2}, 2)$, the above bound for $F(q)$ is an increasing function of q. It follows that it is sufficient that the bound is positive when $q = 11$. Using that

$$A(1) = 2e^{\gamma} = 3.562144\ldots,$$

$$A(1/5) = 1.15147\ldots$$

and

$$B(1/5) = 0.92055\ldots$$

we can deduce, by taking $\beta = 1.9$, that for any prime $q \geq 11$ we have

$$F(q) \geq 0.514.$$

In conclusion, $F(q) > 0$ for all primes $q \geq 7$ so Theorem 8.1 holds for all primes $q \geq 7$.

Bibliography

[1] R. C. Baker. Kloosterman sums with prime variable. *Acta Arith.*, 156(4):351–372, 2012.

[2] W. D. Banks, D. N. Hart, and M. Sakata. Almost all palindromes are composite. *Math. Res. Lett.*, 11(5-6):853–868, 2004.

[3] W. D. Banks, D. R. Heath-Brown, and I. E. Shparlinski. On the average value of divisor sums in arithmetic progressions. *Int. Math. Res. Not.*, (1):1–25, 2005.

[4] H.-J. Bartels. Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen. *J. Algebra*, 70(1):179–199, 1981.

[5] V. Blomer. The average value of divisor sums in arithmetic progressions. *Q. J. Math.*, 59(3):275–286, 2008.

[6] E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. III. *J. Amer. Math. Soc.*, 2(2):215–224, 1989.

[7] T. D. Browning and D. R. Heath-Brown. Quadratic polynomials represented by norm forms. *Geom. Funct. Anal.*, 22(5):1124–1190, 2012.

[8] T. D. Browning and L. Matthiesen. Norm forms for arbitrary number fields as products of linear polynomials. arXiv:1307.7641.

[9] V. Brun. Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare. *Arch. Math. Naturvid.*, 34(8):3–19, 1915.

[10] S. Col. Palindromes dans les progressions arithmétiques. *Acta Arith.*, 137(1):1–41, 2009.

[11] J.-L. Colliot-Thélène and P. Salberger. Arithmetic on some singular cubic hypersurfaces. *Proc. London Math. Soc. (3)*, 58(3):519–549, 1989.

[12] J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces. I. *J. Reine Angew. Math.*, 373:37–107, 1987.

[13] S. Daniel. On the divisor-sum problem for binary forms. *J. Reine Angew. Math.*, 507:107–129, 1999.

[14] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. Revised by Hugh L. Montgomery.

[15] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[16] P. Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[17] U. Derenthal, A. Smeets, and D. Wei. Universal torsors and values of quadratic polynomials represented by norms. arXiv:1202.3567.

[18] H. G. Diamond and H. Halberstam. *A higher-dimensional sieve method*, volume 177 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2008. With an appendix ("Procedures for computing sieve functions") by William F. Galway.

[19] W. Duke, J. Friedlander, and H. Iwaniec. Bilinear forms with Kloosterman fractions. *Invent. Math.*, 128(1):23–43, 1997.

[20] É. Fouvry. Sur le problème des diviseurs de Titchmarsh. *J. Reine Angew. Math.*, 357:51–76, 1985.

[21] É. Fouvry and H. Iwaniec. The divisor function over arithmetic progressions. *Acta Arith.*, 61(3):271–287, 1992. With an appendix by Nicholas Katz.

[22] E. Fouvry and H. Iwaniec. Gaussian primes. *Acta Arith.*, 79(3):249–287, 1997.

[23] É. Fouvry, E. Kowalski, and P. Michel. A study in sums of products. arXiv:1405.2293.

[24] É. Fouvry and I. E. Shparlinski. On a ternary quadratic form over primes. *Acta Arith.*, 150(3):285–314, 2011.

[25] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[26] M. Z. Garaev. An estimate for Kloosterman sums with primes and its application. *Mat. Zametki*, 88(3):365–373, 2010.

[27] G. Gras. *Class field theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.

[28] G. Greaves. Large prime factors of binary forms. *J. Number Theory*, 3:35–59, 1971.

[29] G. Greaves. *Sieves in number theory*, volume 43 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 2001.

[30] G. Harman. On the distribution of αp modulo one. *J. London Math. Soc. (2)*, 27(1):9–18, 1983.

[31] G. Harman. Numbers badly approximable by fractions with prime denominator. *Math. Proc. Cambridge Philos. Soc.*, 118(1):1–5, 1995.

[32] G. Harman. On the distribution of αp modulo one. II. *Proc. London Math. Soc. (3)*, 72(2):241–260, 1996.

[33] D. R. Heath-Brown. The largest prime factor of $X^3 + 2$. *Proc. London Math. Soc. (3)*, 82(3):554–596, 2001.

[34] D. R. Heath-Brown. Primes represented by $x^3 + 2y^3$. *Acta Math.*, 186(1):1–84, 2001.

[35] D. R. Heath-Brown. Bounds for the cubic Weyl sum. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 377(Issledovaniya po Teorii Chisel. 10):199–216, 244–245, 2010.

[36] D. R. Heath-Brown and C. Jia. The distribution of αp modulo one. *Proc. London Math. Soc. (3)*, 84(1):79–104, 2002.

[37] H. Heilbronn. Zeta-functions and L-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 204–230. Thompson, Washington, D.C., 1967.

[38] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[39] A. A. Karatsuba. Analogues of Kloosterman sums. *Izv. Ross. Akad. Nauk Ser. Mat.*, 59(5):93–102, 1995.

[40] K. Matomäki. The distribution of αp modulo one. *Math. Proc. Cambridge Philos. Soc.*, 147(2):267–283, 2009.

[41] H. L. Montgomery. Maximal variants of the large sieve. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):805–812 (1982), 1981.

[42] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[43] A. Nevo and P. Sarnak. Prime and almost prime integral points on principal homogeneous spaces. *Acta Math.*, 205(2):361–402, 2010.

[44] H.-E. Richert. Selberg's sieve with weights. *Mathematika*, 16:1–22, 1969.

[45] R. C. Vaughan. On the distribution of αp modulo 1. *Mathematika*, 24(2):135–141, 1977.

[46] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers*. Dover Publications Inc., Mineola, NY, 2004. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.

[47] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.