The 3-Part of Class Numbers of Quadratic Fields

Lillian Beatrix Pierce
Master of Science
Oxford University

Trinity 2004

Acknowledgements

I am most grateful to D. R. Heath-Brown for the suggestion of this very interesting topic of research. During these two years at Oxford I have benefited immensely from his guidance, insight, and knowledge.

I would like to thank N. Katz for his generosity in answering several questions, and providing a key estimate. Also, I am grateful to both P. Sarnak and J. H. Silverman for their advice and encouragement. Finally, I would like to thank H. Helfgott and A. Venkatesh for providing me with a preprint of their independent work on this topic. I am also grateful to T. Browning for many interesting conversations.

During my time in Oxford I have been funded by the generous support of the Rhodes Trust; I owe many thanks both to the Trust, and to Magdalen College, which has been a wonderful place to live these two years.

Abstract

In 1801, Gauss published *Disquisitiones Arithmeticae*, which, among many other things, develops genus theory, describing the divisibility by 2 of class numbers of quadratic fields. In the centuries since this work, the divisibility properties of class numbers by integers $g \geq 3$ have largely remained mysterious. In particular, the problem of bounding the g-part $h_g(D)$ of class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$ for $g \geq 3$ has remained unsolved. This thesis provides three nontrivial bounds for $h_3(D)$, giving the first improvement on the previously known trivial bound $h_3(D) \ll |D|^{1/2+\epsilon}$.

This thesis approaches the problem via analytic number theory, phrasing the problem of bounding $h_3(D)$ in terms of counting the number of integer points in a bounded region on the cubic surface $4x^3 = y^2 + dz^2$, for a positive square-free integer d. We obtain our first two nontrivial bounds for $h_3(D)$ by regarding this as the congruence $4x^3 \equiv y^2$ modulo d. Using exponential sum techniques, we prove two nontrivial bounds for the number of solutions to a congruence of the more general form $x^a \equiv y^b \pmod{q}$, for a positive square-free integer q and nonzero integers a, b. As results of these bounds, we show that $h_3(D) \ll |D|^{5/12+\epsilon}$ if D has a divisor of size $|D|^{5/6}$, and $h_3(D) \ll |D|^{55/112+\epsilon}$ in general.

We obtain a third nontrivial bound of $h_3(D) \ll |D|^{27/56+\epsilon}$ by counting the number of integer points on the cubic surface directly. Specifically, we estimate the number of squares of the form $4x^3 - dz^2$, using the square sieve and the q-analogue of Van der Corput's method.

Each of our three bounds for $h_3(D)$ also gives a corresponding improvement on the previously known bound for the number of elliptic curves over $\mathbb{Q}$ with fixed conductor.

Contents

Chapter 1

Introduction

1.1 The class number

Let K be an algebraic number field and let J_K be the corresponding group of fractional ideals, with P_K the subgroup of fractional principal ideals. The class group is defined to be the quotient

$$CL_K = J_K/P_K.$$

The class group admits the exact sequence

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow J_K \longrightarrow CL_K \longrightarrow 1,$$

where $\mathcal{O}_K^*$ denotes the group of units in K. Thus the class group CL_K can be seen as measuring the expansion that takes place when passing from numbers to ideals. The class number h_K is the order of the class group,

$$h_K = \#CL_K.$$

It can be seen by Minkowski theory that h_K is always finite. In particular, if $h_K = 1$ then $\mathcal{O}_K$ is a principal ideal domain. In general, however, $h_K > 1$.

In this thesis we are concerned with class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$. Class numbers are remarkably unpredictable, both in terms of their size and their divisibility properties. In certain cases, computation of large sets of class numbers has led to heuristic predictions for the behaviour of class numbers, but it remains very difficult to prove properties of class numbers, even for as restricted a family as imaginary or real quadratic fields.

Moreover, the properties of class numbers associated with one type of field appear to be quite distinct from the properties of class numbers associated with another type of field. In the case of imaginary versus real quadratic fields, these differences are marked. For example, it is known that the only square-free

integers $D < 0$ for which the corresponding imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ has class number 1 are the nine values

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Yet in the case of real quadratic fields, class number 1 occurs much more frequently; for example, for square-free integers $2 \leq D < 100$, $\mathbb{Q}(\sqrt{D})$ has class number 1 for

$$\begin{aligned} D \quad = \quad & 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, \\ & 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97... \end{aligned}$$

It is conjectured that infinitely many real quadratic fields have class number 1. However, it remains unknown whether there are infinitely many fields of any degree with class number 1. And this is just one example of the variability of the properties of class numbers between different types of fields. (For the curious, tables of class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$ for square-free integers $-500 < D < 0$ and $2 \leq D < 100$ are included in Appendix A.)

Yet class numbers are as useful as they are unpredictable. As a few examples, the class number of an algebraic number field is closely related to the Dedekind zeta function, as shown by Dirichlet's class number formula. The divisibility by p of the class number of $\mathbb{Q}(\xi)$, where ξ is a p-th root of unity, is closely related to Fermat's last theorem. The structures of class groups, and hence properties of class numbers, are related to properties of isogenies of elliptic curves. Finally, as we will study in more detail in Chapter 8, the 3-rank of class numbers of quadratic fields (or the 2-rank of class numbers of cubic fields), can be used to bound the number of elliptic curves over $\mathbb{Q}$ with fixed conductor.

Thus class numbers have fascinated mathematicians for hundreds of years, not only because of their mysterious behaviour, but also because of their tendency to appear unexpectedly in other areas of mathematics.

1.2 The 3-part of the class number

For a square-free integer D, consider the quadratic field $\mathbb{Q}(\sqrt{D})$ with class group $CL(D)$ and class number $h(D)$. The 3-part $h_3(D)$ is defined by

$$h_3(D) = \#\{[\mathfrak{a}] \in CL(D) : [\mathfrak{a}]^3 = 1\}.$$

This admits the trivial bound

$$h_3(D) \leq h(D) \ll |D|^{1/2+\epsilon}, \tag{1.1}$$

as we will see in Section 3.2. The following bound is conjectured:

Conjecture.

$$h_3(D) \ll |D|^{\epsilon}$$

for any $\epsilon > 0$.

In the case of real fields, it is conjectured that for most $D > 0$, $h(D)$ is itself very small. In the case of imaginary fields, when $D < 0$, this conjecture is more significant, as it indicates that although $h(D)$ itself tends to infinity at least as fast as $|D|^{1/2-\epsilon}$ for any $\epsilon > 0$, the 3-part is conjectured to be very small.

Before the work of this thesis, the only known unconditional bound in each case was the trivial bound (1.1). The goal of this thesis is to prove an unconditional nontrivial bound for both positive and negative square-free integers D,

$$h_3(D) \ll |D|^{\theta}, \text{with } \theta < 1/2.$$

1.3 The results of the Thesis

The main results of this thesis are three nontrivial upper bounds for the 3-part of class numbers of quadratic fields, the first improvements on the trivial bound.[1] We reduce the problem of bounding $h_3(D)$ to counting the number of integer points within a bounded region on the cubic surface

$$4x^3 = y^2 + dz^2, \tag{1.2}$$

where $d = |D|$, and we assume that D is square-free, $D < 0$. This is no handicap, as having proved a bound for the 3-part of class numbers of imaginary quadratic fields, we immediately obtain an equivalent bound for the 3-part of class numbers of real quadratic fields, since for any square-free positive integer d, the Scholz reflection principle [58] states that $\log_3(h_3(-d))$ and $\log_3(h_3(+3d))$ differ by at most one.

The first bounds we prove for $h_3(D)$ are derived by working modulo d and using exponential sum techniques to estimate the number of solutions in a bounded region to the congruence

$$4x^3 \equiv y^2 \pmod{d}. \tag{1.3}$$

In fact, we derive bounds for the number of solutions to a congruence of the more general form

$$x^a \equiv y^b \pmod{q}, \tag{1.4}$$

where q is a square-free positive integer and a and b are nonzero integers satisfying certain conditions. The bounds for $h_3(D)$ then follow as corollaries.

[1] Independently and simultaneously with the work of this thesis, Helfgott and Venkatesh [36] have also proved a nontrivial bound for the 3-part; we discuss their result briefly in Chapter 8.

Specifically, let $N_q(X,Y)$ denote the number of solutions to the congruence (1.4) with $(x,q)=1$, $(y,q)=1$ such that $x \le X$ and $y \le Y$. We prove in Theorem 5.1 that if a and b are nonzero integers with $(a,b)=1$ and $a \neq b$, and if $X \le q$ and $Y \le q/2$, then

$$N_q(X,Y) \ll q^{1/2} d(q)^\tau (\log q)^2 + q^{-1} XY d(q)^\tau + q^{-1/2} X d(q)^\tau,$$

where τ and the implied constant depend upon a, b. We further prove in Theorem 5.2 that if a and b are nonzero integers with $(b,q)=1$ and $a/b \notin \mathbb{Z}^+$, then for any integer $k \ge 1$,

$$N_q(X,Y) \ll X^{\frac{k}{k+1}} Y^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}},$$

as long as $X \le q^{\frac{k+1}{2k}}$ and $Y \le q/2$. Here τ_k and the implied constant depend upon a, b, k.

If both $a, b > 0$, we may define $N'_q(X,Y)$ to be the number of solutions to (1.4) with $x \le X$ and $y \le Y$, without assuming the relative primality conditions $(x,q)=1$, $(y,q)=1$. Then equivalent results hold for $N'_q(X,Y)$ as for $N_q(X,Y)$, which we present in Theorems 5.3 and 5.4.

Applying these results to the congruence (1.3), we obtain Theorem 6.1, which states that if D has a divisor of size $|D|^{5/6}$, then

$$h_3(D) \ll |D|^{5/12+\epsilon},$$

and Theorem 6.2, which states that

$$h_3(D) \ll |D|^{55/112+\epsilon},$$

for all square-free integers D.

We prove a third nontrivial bound for $h_3(D)$ by counting the number of integer points on the cubic surface (1.2) directly. Specifically, we use the square sieve and the q-analogue of van der Corput's method to estimate the number of squares of the form

$$4x^3 - dz^2,$$

within a bounded region. The result is Theorem 7.1:

$$h_3(D) \ll |D|^{27/56+\epsilon}.$$

1.4 Immediate consequences of a nontrivial bound for the 3-part

A nontrivial bound for the 3-part $h_3(D)$ is important in its own right, but such a bound also has immediate results for several closely related problems.

1.4.1 Cubic extensions of discriminant D

By Hasse's result [26], the class number of $\mathbb{Q}(\sqrt{D})$ is divisible by 3 if and only if there is a cubic extension of $\mathbb{Q}$ of discriminant D. Thus our results for $h_3(D)$ show that there are at most $O(|D|^{27/56+\epsilon})$ cubic extensions of $\mathbb{Q}$ with discriminant D. In the case that D has a divisor of size $|D|^{5/6}$, there are at most $O(|D|^{5/12+\epsilon})$ cubic extensions of $\mathbb{Q}$ with discriminant D.

1.4.2 Elliptic curves with fixed conductor

As we will study in more detail in Chapter 8, $h_3(D)$ plays a critical role in bounding the number of elliptic curves over $\mathbb{Q}$ with conductor N. A result of Brumer and Silverman [5] shows that there are at most $O(N^{1/2+\epsilon})$ such curves. Furthermore, any nontrivial bound $h_3(D) \ll |D|^{\theta}$ immediately refines this bound to $O(N^{\theta+\epsilon})$. Thus the conjectured bound $h_3(D) \ll |D|^{\epsilon}$ would imply that there are $O(N^{\epsilon})$ such curves, for any $\epsilon > 0$.

Our results for $h_3(D)$ show that the number of elliptic curves over $\mathbb{Q}$ with conductor N is at most $O(N^{27/56+\epsilon})$ in general, and at most $O(N^{5/12+\epsilon})$ if N has a divisor of size $N^{5/6}$. The work of Helfgott and Venkatesh [36] refines these bounds further and allows us to show that if the conductor N has a divisor of size $N^{5/6}$, then the number of elliptic curves over $\mathbb{Q}$ with conductor N is $O(N^{\lambda+\epsilon})$, where $\lambda = 0.21105....$ These results are stated as Theorems 8.1 and 8.2.

1.4.3 Bounds for $\mathcal{N}_3^{\pm}(X)$

A nontrivial bound for the 3-part also gives an estimate for the number of square-free integers D of bounded size such that $3|h(D)$. Let $\mathcal{N}_g^-(X)$ denote the number of square-free integers $-X \leq D < 0$ such that the class group $CL(D)$ contains an element of order g, and let $\mathcal{N}_g^+(X)$ denote the corresponding quantity for $0 < D \leq X$. It is conjectured (as we will see in more detail in Section 2.3.2) that for each integer $g \geq 2$,

$$\mathcal{N}_g^-(X) \sim C_g^- X \quad \text{and} \quad \mathcal{N}_g^+(X) \sim C_g^+ X,$$

for constants C_g^- in the imaginary case and C_g^+ in the real case. This is known to be true for $g = 2$, but remains unproven for $g \geq 3$. In fact, it remains to be proven in both the imaginary and real cases even that

$$\mathcal{N}_3^{\pm}(X) \gg X^{1-\epsilon}. \tag{1.5}$$

A bound of $h_3(D) \ll |D|^{\theta}$ gives the corresponding bound

$$\mathcal{N}_3^{\pm}(X) \gg X^{1-\theta};$$

in particular, the conjectured bound $h_3(D) \ll |D|^{\epsilon}$ would give the desired bound (1.5). This follows from a striking result of Davenport and Heilbronn [11] on the

asymptotic density of discriminants of cubic fields, which gives as a corollary the mean value of the 3-part of class numbers of quadratic fields.[2] In the imaginary case, this states that

$$\sum_{-X\leq D<0} h_3(D) \sim 2 \sum_{-X\leq D<0} 1$$

as $X \to \infty$, where both sums consider only square-free values D. Thus

$$\sum_{-X\leq D<0} (h_3(D)-1) \sim \frac{6}{\pi^2} X. \tag{1.6}$$

Define $\mathbf{N}_3^-(X)$ to be the set of square-free integers $-X \leq D < 0$ such that $CL(D)$ contains an element of order 3, so that $\mathcal{N}_3^-(X) = \#\mathbf{N}_3^-(X)$. Then $(h_3(D)-1)$ is nonzero only for $D \in \mathbf{N}_3^-(X)$, so we may restrict the sum in (1.6) to $D \in \mathbf{N}_3^-(X)$. Then assuming that $h_3(D) \ll |D|^\theta$,

$$\sum_{D\in\mathbf{N}_3^-(X)} (h_3(D)-1) \leq \sum_{D\in\mathbf{N}_3^-(X)} h_3(D) \ll \sum_{D\in\mathbf{N}_3^-(X)} |D|^\theta \ll X^\theta \mathcal{N}_3^-(X).$$

Comparison with (1.6) then shows immediately that

$$\mathcal{N}_3^-(X) \gg X^{1-\theta}.$$

In the real case, the result of Davenport and Heilbronn states that

$$\sum_{0<D\leq X} h_3(D) \sim \frac{4}{3} \sum_{0<D\leq X} 1$$

as $X \to \infty$. Reasoning as above, it is clear that a bound $h_3(D) \ll |D|^\theta$ also yields the corresponding bound

$$\mathcal{N}_3^+(X) \gg X^{1-\theta}.$$

Thus any nontrivial bound for $h_3(D)$ gives a bound for $\mathcal{N}_3^\pm(X)$. In particular, our work shows that $\mathcal{N}_3^\pm(X) \gg X^{29/56-\epsilon}$. However, as we will see in Sections 2.3.3 and 2.3.4, a number of methods have succeeded in attacking $\mathcal{N}_3^\pm(X)$ directly, producing quite good lower bounds. Substantial improvements will have to be made to the bound for $h_3(D)$ in order for the resulting bound for $\mathcal{N}_3^\pm(X)$ to overtake known bounds for $\mathcal{N}_3^\pm(X)$ resulting from direct methods.

1.4.4 A note on $h_g(D)$ for $g \geq 5$

We note that although the methods presented in this thesis do not appear at first sight to depend crucially upon the fact that we consider the 3-part of the

[2] We note that analogous results for the asymptotic density of discriminants of quartic fields and the mean value of the 2-class group of cubic fields have recently been given in the thesis of Bhargava [4].

class number, rather than the 5-part, or the g-part for any $g \geq 5$, these methods do not extend to higher values g. For $g \geq 5$, one must consider increased ranges for integer points on a variety analogous to (1.2); these increased ranges are too large to be handled by the methods presented in this thesis. We discuss this in more detail in Chapter 6.

1.5 Outline of the Thesis

We begin in Chapter 2 with a brief history of research on class numbers of quadratic fields. Not only is the history of class numbers fascinating, it also serves to put the work of this thesis in context. In Chapter 3 we present some preliminary material, specifying notational conventions and stating a number of results for exponential sums and congruences that will be critical to the remainder of the thesis.

In Chapter 4 we begin the work of this thesis, proving two upper bounds for the least s-power-free positive integer in an arithmetic progression, for any integer $s \geq 2$. While these results do not in themselves pertain directly to class numbers, we present this work as an introduction to the methods we then develop in Chapter 5 to estimate the number of solutions in a bounded region to a congruence of the general form (1.4). In Chapter 6 we then use the results of Chapter 5 to prove our first two nontrivial bounds for $h_3(D)$.

In Chapter 7 we use the square sieve and the q-analogue of van der Corput's method to prove our third nontrivial bound for $h_3(D)$. Finally, in Chapter 8, we use our bounds for $h_3(D)$ to refine the known bound for the number of elliptic curves over $\mathbb{Q}$ with conductor N.

Chapter 2

A brief history

2.1 Class numbers of quadratic fields

Research on class numbers of quadratic fields has a long history, beginning with Gauss's study of class numbers of quadratic forms. To put the results of this thesis in the context of what is known or conjectured about class numbers of quadratic fields, we give in this chapter a description of some of the most important developments of this history, stating several of the nicest results that have been proven so far, as well as the most tantalising conjectures that remain unproven.

In Section 2.2 we discuss the problem of bounding the class numbers themselves; in the case of imaginary quadratic fields, this was famously solved in the 1980's, while in the case of real quadratic fields, little is known, although much is conjectured. In Section 2.3 we study the divisibility properties of class numbers, reviewing the work of Gauss on genus theory and the divisibility of class numbers by 2, and summarising the conjectures of Cohen and Lenstra for divisibility by any odd prime p. We also outline recent results on the divisibility of class numbers by any integer $g \geq 3$. This fascinating work illustrates the many beautiful properties we expect class numbers to possess, as well as how little we still know. In Section 2.4 we mention current research on the 3-part specifically.

2.2 Bounding the class number

Let D be a square-free integer and consider the quadratic field $\mathbb{Q}(\sqrt{D})$ with class number $h(D)$. In both the real and imaginary cases, the class number admits the trivial upper bound

$$h(D) \leq |D|^{1/2+\epsilon},$$

as we prove in Section 3.2.

In the case of imaginary fields, the so-called class number conjecture of Gauss states that only finitely many imaginary quadratic fields have any specified class number h. The companion problem to this conjecture, the class number problem, asks for an effective method of computing all the imaginary quadratic fields with class number h; thus the problem is to find an effective lower bound for $h(D)$ when $D < 0$. The class number conjecture was proved to be true in 1934, and an effective method of computation was proved in 1983. We give a brief summary of this work in Section 2.2.1.

The situation for real fields is conjectured to be much different: it is conjectured that for $D > 0$, $h(D)$ is usually very small, and in particular that $h(D) = 1$ infinitely often. However, the real case is still not well understood. We mention several partial results in Section 2.2.2.

2.2.1 The class number problem: imaginary quadratic fields

In 1801, Gauss enunciated the class number conjecture in *Disquisitiones Arithmeticae*. In 1918, Landau [45] published a theorem of Hecke showing that the generalised Riemann hypothesis implies the class number conjecture. (In particular, Hecke's theorem showed that the nonexistence of a Siegel zero would imply that $h(D) \to \infty$ as $|D| \to \infty$.) Then in 1933, Deuring [14] showed that if the classical Riemann hypothesis is false, $h(D) \geq 2$ for $|D|$ sufficiently large. Mordell [48] improved this in 1934 to the statement that if the classical Riemann hypothesis is false, then $h(D) \to \infty$ as $|D| \to \infty$. Then Heilbronn [34], also in 1934, finally showed that if the generalised Riemann hypothesis is false, then $h(D) \to \infty$ as $|D| \to \infty$. Thus the statement

$$h(D) \to \infty \quad \text{as} \quad |D| \to \infty$$

was finally shown to be true unconditionally, proving Gauss's conjecture.

It still remained to find an effective means of computing the finitely many imaginary quadratic fields with class number h. In 1936, Siegel [59] proved that for every $\epsilon > 0$ there exists a constant $c > 0$ such that

$$h(D) > c|D|^{1/2-\epsilon}. \tag{2.1}$$

However, this constant is not effectively computable. (Interestingly, Tatuzawa [64] was able to show that there is a computable constant c such that (2.1) holds for all except possibly one value D.)

The class number problem was first solved, after a good deal of effort, in the case of class number 1. In 1934, Heilbronn and Linfoot [35] showed that there could be at most one more square-free integer $D < 0$ such that $\mathbb{Q}(\sqrt{D})$ has class number 1, aside from the nine known values

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

In particular, the existence of a tenth such value would imply the falsity of the generalised Riemann hypothesis. In 1952, Heegner [33] published the first proof that no such tenth value existed. His paper contained some flaws and, at the time, was disregarded. In 1966, Baker [2] showed that no such tenth value existed, using the independence of three logarithms, and in 1967, Stark [62] used a method similar to Heegner's to prove that no tenth field existed. The problem continued to arouse interest for several years, as Deuring and others continued to study Heegner's original proof (see the summary of Goldfeld [20] for more details).

The next obvious problem was to find all imaginary quadratic fields with class number 2, and indeed, in 1971 both Baker [3] and Stark [63] showed that there are exactly eighteen imaginary quadratic fields with class number 2, using the linear independence of logarithms.

Yet the general class number problem remained open. Then in 1975-76, Goldfeld [19] reduced the problem to showing that the Birch–Swinnerton-Dyer conjecture holds true in a specific case, namely that there is an elliptic curve over $\mathbb{Q}$ with Mordell-Weil rank 3 such that its L-series has a zero of rank 3 at $s = 1$. Finally, in 1983, Gross and Zagier [22] used the theory of Heegner points to show that such a curve exists. The resulting theorem, due to the combined work of Goldfeld, Gross and Zagier, is that for every $\epsilon > 0$ there exists an effectively computable constant $c > 0$ such that

$$h(D) > c(\log |D|)^{1-\epsilon}.$$

Oesterlé [53] showed specifically that

$$h(D) \geq \frac{1}{7000}(\log |D|) \prod_{\substack{p||D| \\ p \neq |D|}} \left(1 - \frac{2\sqrt{p}}{p+1}\right).$$

This completely solved the class number problem for imaginary quadratic fields. In reality, it is still not easy to compute all discriminants with a specific class number, as a large (but finite) amount of computation is necessary; nevertheless all fields with class number 3 (of which there are 16) and class number 4 (of which there are 54) have been computed.

2.2.2 The class number problem: real quadratic fields

The situation for real fields is significantly less well understood; Siegel's theorem [59] for real quadratic fields states that

$$h(D)R_D > D^{1/2-\epsilon}$$

for any $\epsilon > 0$ and sufficiently large D, where R_D is the regulator of the field $\mathbb{Q}(\sqrt{D})$. The key lies in the presence of the regulator, whose behaviour is not

predictable by current methods. It is conjectured that the regulator is usually about size $D^{1/2}$, which would indicate that $h(D)$ is usually very small.

Computational evidence by Wada [65], Mollin and Williams [47], and Jacobson [42] supports the conjecture that $h(D) = 1$ infinitely often. Cohen and Lenstra [9] have also presented heuristic arguments for the observed frequency of class number 1 for real quadratic fields.

2.3 Divisibility properties

Divisibility properties of class numbers of quadratic fields are usually phrased in terms of the following quantities. Denote by $h_g(D)$ the g-part of the class number,

$$h_g(D) = \#\{[\mathfrak{a}] \in CL(D) : [\mathfrak{a}]^g = 1\}.$$

Denote by $\mathcal{N}_g^-(X)$ the number of square-free integers $-X \leq D < 0$ such that $CL(D)$ contains a nontrivial element of order g; define $\mathcal{N}_g^+(X)$ equivalently for real fields. These quantities are closely related; as we saw in Section 1.4, a bound for $h_3(D)$ gives a bound for $\mathcal{N}_3^{\pm}(X)$. Until recently, most successes in proving divisibility properties of $h(D)$ by an integer $g \geq 3$ have been achieved by attacking $\mathcal{N}_g^{\pm}(X)$ directly. Although the main results of this thesis are for $h_g(D)$ itself, with $g = 3$, we digress for the moment to discuss important background material concerning $\mathcal{N}_g^{\pm}(X)$.

It is conjectured that for each integer $g \geq 2$,

$$\mathcal{N}_g^-(X) \sim C_g^- X \quad \text{and} \quad \mathcal{N}_g^+(X) \sim C_g^+ X$$

for constants C_g^- in the imaginary case and C_g^+ in the real case.

2.3.1 Gauss's genus theory

Genus theory, developed by Gauss, shows that this is true for $g = 2$, with $C_2^{\pm} = 6/\pi^2$. Gauss was motivated by the problem of determining those primes represented by a given quadratic form with fundamental discriminant. Let $h^*(D)$ indicate the number of proper equivalence classes of quadratic forms with discriminant D. The goal of genus theory is to distinguish, in the case that $h^*(D) > 1$, which class contains forms that represent a given prime p, by collecting proper equivalence classes into larger sets, the genera. Most importantly in the context of this thesis, Gauss showed that there are 2^{r-1} genera, where r is the number of distinct prime divisors of the fundamental discriminant D. The genera partition the set of proper equivalence classes, hence the number of classes in each genus is $h^*(D)/2^{r-1}$. Thus 2^{r-1} divides $h^*(D)$.

Thus genus theory shows that $CL(D)$ contains $\mathbb{Z}/2\mathbb{Z}$ as a subgroup if the square-free integer D has more than three distinct prime factors.[1] In particular, this holds for almost all square-free $|D| \leq X$, so that

$$\mathcal{N}_2^{\pm}(X) \sim \frac{6}{\pi^2} X.$$

(For a summary from the historical perspective, see the memoir of Ribenboim [56]. For more modern references, see [52] or Hasse's text [27].)

2.3.2 Cohen and Lenstra heuristics

For $g \geq 3$, $h_g(D)$ and $\mathcal{N}_g^{\pm}(X)$ are not well understood. Cohen and Lenstra [9] have presented heuristics suggesting that for odd primes p, in the imaginary case

$$C_p^- = \frac{6}{\pi^2} \left(1 - \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^k} \right) \right),$$

and in the real case

$$C_p^+ = \frac{6}{\pi^2} \left(1 - \prod_{k=2}^{\infty} \left(1 - \frac{1}{p^k} \right) \right).$$

(Although we will not discuss this in detail, they also obtain conjectures for the probability that the p-rank of the class group is equal to an integer $n \geq 1$, and in the imaginary case they further obtain heuristic probabilities that the class group is a product of various cyclic groups.)

These conjectures are based on experimental observations of three phenomena, as summarised in [9]: firstly, that the odd part of the class group of imaginary quadratic fields appears rarely to be non-cyclic; secondly, that for odd primes p, the proportion of imaginary quadratic fields with class number divisible by p appears to be significantly greater than $1/p$; and thirdly, that a positive proportion of real quadratic fields with prime discriminant appear to have class number 1. Reasoning that the lack of cyclic groups may be due to the fact that such groups have many automorphisms, Cohen and Lenstra weighted isomorphism classes G of abelian groups by $1/\#\mathrm{Aut}(G)$. This, along with several other heuristic assumptions, allowed them to make accurate predictions about properties of class numbers. For example, they predict that approximately 43.987% of

[1] In the case of imaginary quadratic fields, $h^*(D) = h(D)$, so if $D < 0$ is a fundamental discriminant, then $2|h(D)$ if D has at least 2 distinct prime divisors. In the case of real quadratic fields, $h^*(D) = h(D)$ or $2h(D)$, depending if there is a unit of norm -1 in the field or not. Furthermore, the fundamental discriminant D associated to the square-free radicand d of a quadratic field $\mathbb{Q}(\sqrt{d})$ can have at most one more prime divisor (namely the prime 2) than d. Thus in all cases, if D is a square-free integer it is sufficient that D has more than three distinct prime divisors for $h(D)$ to be divisible by 2.

imaginary quadratic fields should have class number divisible by 3, and approximately 75.446% of real quadratic fields with prime discriminant should have class number 1, both of which predictions are in agreement with experimental evidence.[2]

2.3.3 Recent work: imaginary quadratic fields

So far the conjectures of Cohen and Lenstra remain out of reach; for $g \geq 3$ it remains to show even that $\mathcal{N}_g^- X \gg X^{1-\epsilon}$ for any $\epsilon > 0$. A number of partial results have been obtained. Gut [23] generalised Gauss's result to show that infinitely many imaginary quadratic fields have class number divisible by 3. In general, Ankeny and Chowla [1] showed (as did Nagell [51]) that for any $g \geq 2$ there are infinitely many imaginary quadratic fields with class group containing a nontrivial element of order g, so that $\mathcal{N}_g^-(X) \to \infty$ as $X \to \infty$. In fact, as Soundararajan points out in [61], their method shows that $\mathcal{N}_g^-(X) \gg X^{1/2}$.

Murty [50] then showed that $\mathcal{N}_g^-(X) \gg X^{1/2+1/g}$, which was improved in the cases $g = 4, 8$ by Morton [49] to $\mathcal{N}_g^-(X) \gg X^{1-\epsilon}$, using class field theory. More recently, Soundararajan [61] has shown that

$$\mathcal{N}_g^-(X) \gg \begin{cases} X^{1/2+2/g-\epsilon} & \text{if } g \equiv 0 \pmod 4 \\ X^{1/2+3/(g+2)-\epsilon} & \text{if } g \equiv 2 \pmod 4, \end{cases}$$

for sufficiently large X. Since $\mathcal{N}_g^-(X) \geq \mathcal{N}_{2g}^-(X)$, this also provides a bound when g is odd.

The complementary question of when the class number is not divisible by a prime p has also been studied. Recently, Kohnen and Ono [44] have shown that for any prime $p > 3$, the number of square-free integers $-X \leq D < 0$ such that $p \nmid h(D)$ is $\gg \sqrt{X}/\log X$ for sufficiently large X.

In the specific case of $p = 3$, Hartung [25] has shown that there are infinitely many $D < 0$ with $3 \nmid h(D)$. A result of Davenport and Heilbronn [11] further shows that at least half of the square-free integers $-X \leq D < 0$ have $3 \nmid h(D)$.

2.3.4 Recent work: real quadratic fields

Honda [38] first showed that there are infinitely many real quadratic fields with class numbers divisible by 3. (In [37] he also gives a criterion for the class number of a quadratic field, real or imaginary, to be divisible by 3, using isogenies of elliptic curves.) More generally, Yamamoto [70] and Weinberger [68] have shown that there are infinitely many real quadratic fields with class number divisible

[2] In [10], Cohen and Martinet provide analogous heuristics for number fields of higher degree, recently verified in the case of the mean size of the 2-class group of cubic fields in the thesis of Bhargava [4].

by g for any positive integer g. Ankeny and Chowla [1] have shown that if D is a square-free positive integer of the form $D = n^{2g} + 1$ with $n > 4$, then the class group of $\mathbb{Q}(\sqrt{D})$ contains a nontrivial element of order g. However, as it is unknown whether there are infinitely many square-free integers of the form $n^{2g} + 1$, this does not give a result for $\mathcal{N}_g^+(X)$ parallel to their result in the imaginary case.

Murty [50] has shown that $\mathcal{N}_g^+(X) \gg X^{1/2g-\epsilon}$ for any positive integer g. Recently, Yu [71] sharpened this result to $\mathcal{N}_g^+(X) \gg X^{1/g-\epsilon}$, using a result of Yamamoto [70]. In the specific case $g = 3$, Chakraborty and Murty [8] have also used the result of Yamamoto [70] to obtain the bound $\mathcal{N}_3^+(X) \gg X^{5/6}$. Byeon and Koh [7] have further improved this to $\mathcal{N}_3^+(X) \gg X^{7/8}$, using the result of Soundararajan [61] for imaginary quadratic fields.

Concerning indivisibility properties for class numbers of real quadratic fields, a result of Davenport and Heilbronn [11] shows that $3 \nmid h(D)$ for at least $5/6$ of the square-free integers $0 < D \leq X$.

2.4 Bounding the 3-part

Thus we arrive at the problem of bounding the 3-part $h_3(D)$. Several conditional results are known, as we will discuss in more detail in Section 8.3. Soundararajan has shown (as communicated in [36]) that if χ_D is the quadratic Dirichlet character associated with $\mathbb{Q}(\sqrt{D})$, the Riemann hypothesis for only the specific L-function $L(\chi_D, s)$ implies $h_3(D) \ll |D|^{1/3+\epsilon}$. Wong [69] has shown that the Birch–Swinnerton-Dyer conjecture, together with the Riemann hypothesis, gives the result $h_3(D) \ll |D|^{1/4+\epsilon}$.

In this thesis, we give three nontrivial bounds for $h_3(D)$. Independently and simultaneously with the work of this thesis, Helfgott and Venkatesh [36] have also improved on the trivial bound for $h_3(D)$, using a new method for counting integer points on elliptic curves. Their result is that $h_3(D) \ll |D|^{0.44178\ldots+\epsilon}$ for both real and imaginary quadratic fields. While this work occurred at the same time as the work leading to this thesis, it was entirely independent; indeed the methods used in this thesis are quite different from those of Helfgott and Venkatesh. In particular, the work of Chapter 5 covers a much broader problem than simply bounding $h_3(D)$. We discuss the work of Helfgott and Venkatesh in more detail in Chapter 8.

Chapter 3

Preliminaries

3.1 Notation

Throughout the thesis, the notation $A \ll B$ indicates that $A \leq cB$ for some positive constant c that depends only on certain variables as stated. We denote by $[x]$ the greatest integer part of x and by $\|x\|$ the distance from x to the nearest integer, i.e. $\|x\| = \min\{x - [x], [x] + 1 - x\}$. By $(A, B]$ we mean the set of integers $\{A < n \leq B\}$.

We will also use a number of arithmetic functions. The functions $\phi(n)$ and $\mu(n)$ represent the Euler totient function and the Möbius function, respectively. Also, $\nu(n)$ represents the number of distinct prime divisors of n, $d(n)$ represents the divisor function, and $d_k(n)$ represents the k-th generalised divisor function, i.e. the number of ways of expressing n as the product of k factors, including ordering.

The exponential function $e(x)$ represents $e^{2\pi ix}$ and $e_q(x)$ represents $e^{2\pi ix/q}$. Also, we denote by $\overline{n}$ the unique solution to $\overline{n}n \equiv 1 \pmod{q}$ with $1 \leq \overline{n} \leq q$. If a is a negative integer, then n^a denotes $\overline{n}^{|a|}$. By convention, whenever $\overline{n}$ appears, it is implicit that only values of n with $(n, q) = 1$ are considered in the expression. The letter p always denotes a prime.

3.2 The trivial bound for the class number

We briefly sketch the trivial bound for the class number h_K of an algebraic number field K. We use the following elementary lemma (Lemma 4.2 of [52]).

Lemma 3.1. *Let $R(n)$ be the number of distinct ideals with norm n in a given algebraic number field K of degree N. Then*

$$R(n) \leq d_N(n) = O(n^\epsilon),$$

for any $\epsilon > 0$.

Proof. The function R is multiplicative, since every ideal of norm mn with $(m, n) = 1$ is a unique product of ideals with norm m and n respectively. Thus we need only consider the case when n is a prime power. Let $n = p^a$ be a prime power, with

$$pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

where $\mathfrak{p}_i$ are prime ideals in O_K. If I is an ideal of norm $\mathfrak{N}(I) = p^a$ and $\mathfrak{p}|I$, then $\mathfrak{N}(\mathfrak{p})|\mathfrak{N}(I)$, so that $\mathfrak{N}(\mathfrak{p})$ must be a power of p. Hence $p \in \mathfrak{p}$ and so $\mathfrak{p}$ coincides with one of the ideals $\mathfrak{p}_i$. Thus

$$I = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_s^{b_s},$$

with suitable $0 \leq b_i \leq e_i$. Thus every such I induces a factorisation of p^a into s factors:

$$p^a = \mathfrak{N}(I) = \mathfrak{N}(\mathfrak{p}_1^{b_1}) \cdots \mathfrak{N}(\mathfrak{p}_s^{b_s}).$$

If J is another ideal of norm p^a inducing the same factorisation, then

$$J = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_s^{c_s},$$

and $\mathfrak{N}(\mathfrak{p}_i^{b_i}) = \mathfrak{N}(\mathfrak{p}_i^{c_i})$ for all $i = 1, \ldots, s$, whence $b_i = c_i$ and thus $I = J$. Thus $R(p^a)$ cannot exceed $d_s(p^a)$. There are at most $[K : \mathbb{Q}]$ prime ideals in the integral closure of O_K, so that $s \leq N$, and hence $R(p^a) \leq d_N(p^a)$. □

As a result of this lemma, we have the following trivial bound for the class number h_K of an algebraic number field K of degree N. (This proof is originally due to Landau; see Theorem 4.4 of [52].)

Theorem 3.1. *If K is an algebraic number field of degree $N > 1$, then*

$$h_K = O(|D_K|^{1/2} \log^{N-1} |D_K|),$$

where D_K is the discriminant of the field.

Proof. By the Minkowski bound, in every ideal class there is an integral ideal of norm

$$\mathfrak{N}(\mathfrak{b}) \leq c_N \sqrt{|D_K|},$$

for a constant c_N. Thus

$$h_K \leq \sum_{n \leq c_N |D_K|^{1/2}} R(n) \leq \sum_{n \leq c_N |D_K|^{1/2}} d_N(n).$$

One can prove by induction on N that

$$\sum_{n \leq x} d_N(n) = O(x \log^{N-1} x),$$

and the result follows. □

In the specific case of quadratic fields, we have:

Lemma 3.2. *For $h(D)$ the class number of a quadratic field $\mathbb{Q}(\sqrt{D})$,*

$$h(D) \ll |D|^{1/2+\epsilon}$$

for any $\epsilon > 0$.

We will refer to this as the trivial bound for the class number.

3.3 Congruences

We will frequently bound the number of solutions to simple congruences of the following form.

Lemma 3.3. *For $l > 0$ an integer and a number a modulo q, if $(b, q) = 1$, then*

$$\#\{n \ (mod\, q) : an^l \equiv b \ (mod\, q)\} \leq 2l^{\nu(q)}.$$

Proof. If $(a, q) \neq 1$ then there are no solutions since $(b, q) = 1$. Thus we may reduce to the case of a congruence $n^l \equiv c \pmod{q}$ where $(c, q) = 1$. Let $f(x) = x^l - c$. For $q = p_1^{r_1} \cdots p_m^{r_m}$, then by the Chinese remainder theorem, the number of solutions of $f(x) \equiv 0$ modulo q is the product of the number of solutions of $f(x) \equiv 0$ modulo $p_i^{r_i}$ for each $i = 1, \ldots, m$. Let $N(p^r)$ denote the number of solutions n of $f(x) \equiv 0$ modulo p^r.

First suppose that $p > 2$. Then there is a primitive root g modulo p^r, so we may write $c \equiv g^u$ and $n \equiv g^v$ modulo p^r for some u, v. Finding a solution n of $f(x) \equiv 0 \pmod{p^r}$ is then equivalent to finding a solution v of

$$lv \equiv u \pmod{\phi(p^r)},$$

and hence

$$N(p^r) \leq (l, \phi(p^r)).$$

For our purposes, it is sufficient that $N(p^r) \leq l$.

If $p = 2$, then the fact that $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong C_2 \times C_{2^{r-2}}$ enables us to write $c = (-1)^e 5^f$ and $n = (-1)^u 5^v$ where $e, u = 0$ or 1, and $0 \leq f, v \leq 2^{r-2}$. Then the problem is to find solutions u, v such that

$$(-1)^{ul} 5^{vl} \equiv (-1)^e 5^f \pmod{2^r},$$

or equivalently such that

$$\begin{aligned} ul &\equiv e \pmod{2} \\ vl &\equiv f \pmod{2^{r-2}}. \end{aligned}$$

There are $(l, 2^{r-2})$ solutions modulo 2^{r-2} to the second congruence, and at most 2 solutions modulo 2 to the first congruence. Thus $N(p^r) \leq 2(l, 2^{r-2}) \leq 2l$. $\square$

3.4 Bounds for exponential sums

We will use a number of bounds for exponential sums. As these are either classical results to be found in any number theory text or are quite deep results resulting from Weil's proof of the Riemann hypothesis for curves over finite fields, we state these results without proof, giving references and brief explanations where appropriate.

3.4.1 Incomplete sums

The first result is an elementary bound for incomplete exponential sums (see, for example, Chapter 7 of [41]).

Lemma 3.4. *For an integer a and positive integers M, N, q, let*

$$A(q; M, a) = \sum_{N<n\leq N+M} e_q(na).$$

Then

$$|A(q; M, a)| \leq \min(M, \|a/q\|^{-1}).$$

3.4.2 Gauss sums

The classical bounds for Gauss sums and for exponential sums of higher degree monomials will be used frequently (see Chapter 7 of [41]).

Lemma 3.5. *For an integer a and a prime $p > 2$ with $p \nmid a$,*

$$\left|\sum_{x=1}^{p} e_p(ax^2)\right| \leq p^{1/2}.$$

Lemma 3.6. *For an integer a, a positive integer k, and a prime $p > k$ with $p \nmid a$ and $d = (k, p-1)$,*

$$\left|\sum_{x=1}^{p} e_p(ax^k)\right| \leq (d-1)p^{1/2}.$$

3.4.3 Weil's bound for exponential sums

It is a well-known result of Weil's proof of the Riemann hypothesis [66] for curves over finite fields that exponential sums of certain polynomials with respect to a prime modulus may be bounded by the square-root of the modulus.

Lemma 3.7. *For a prime p and a polynomial $f(x) = c_n x^n + \cdots + c_0$ with integer coefficients having $0 < n < p$ and $p \nmid c_n$,*

$$\left|\sum_{x=1}^{p} e_p(f(x))\right| \leq (n-1)p^{1/2}.$$

Lemma 3.8. *Let χ be a nontrivial multiplicative character of order l modulo a prime p and ψ a nontrivial additive character of $\mathbb{F}_p$. Let $f(x)$ be a polynomial over $\mathbb{F}_p$ of degree d with $(d,l) = 1$ and with all distinct roots in the algebraic closure $\overline{\mathbb{F}}_p$. Let $g(x)$ be a polynomial over $\mathbb{F}_p$ of degree e with $(e,p) = 1$. Then*

$$\left|\sum_{x=1}^{p} \chi(f(x))\psi(g(x))\right| \leq (d+e-1)p^{1/2}.$$

These are quite deep results. We briefly outline the general idea behind the proof, but we refer the reader to Weil's note [67] or Schmidt's treatment in Chapter II of [57] for a complete discussion.

For a prime power $q = p^r$, consider the finite field k of q elements and $k(t)$ the field of rational functions in a transcendental element t, which may be regarded as the function field over k of a projective line. Given a character ψ of the additive group k and a character χ of the multiplicative group k^*, it is possible to define an abelian character ϕ over $k(t)$ whose L-series is a polynomial of degree M with roots α_i such that a sum of the form $\sum \psi\chi$ may be expressed as a sum of the roots of ϕ, i.e. as $(-1)^r \sum \alpha_i$ for some positive integer r.

Since by class field theory the character ϕ belongs to an abelian extension of $k(t)$ and its L-series divides the zeta function of that extension, the truth of the Riemann hypothesis implies that all the roots α_i have modulus $\sqrt{q}$. Thus it follows that the sum $\sum \psi\chi$ is bounded in modulus by $M\sqrt{q}$. Specific choices of the characters ψ and χ yield bounds for exponential sums of different types, such as the bounds for exponential sums of polynomials given above, or bounds for Kloosterman sums, as considered in the following section.

3.4.4 Kloosterman sums

In [12], Deligne proves the so-called Weil bound for exponential sums of rational functions of one variable. We state a specific case of Deligne's general result below, along with the resulting lemma we will require later.

Let p be a prime and let X_0 be an absolutely irreducible smooth projective curve of genus g over $\mathbb{F}_p$. Let f be a rational function, $f : X_0 \to \mathbb{P}^1$, not identically equal to infinity. Let $\nu_x(f)$ represent the order of the pole of f at x if $f(x) = \infty$, and set $\nu_x(f) = 0$ otherwise. Let S represent the sum

$$S = \sum_{x \in X_0} e_p(f(x)).$$

Deligne's result shows that

$$|S| \leq \left(2g - 2 + \sum_{\nu_x(f) \neq 0} (1 + \nu_x(f))\right) p^{1/2}. \tag{3.1}$$

As in the case of the Weil bound for exponential sums of polynomials described in the previous section, this is proved by expressing the character sum under consideration as a sum of roots of a function governed by the Riemann hypothesis for curves over finite fields (see Section 3 of [12]). We will use the following instance of this result.

Lemma 3.9. *For integers a, b with $a < 0$, $b > 0$, integers h, l and a prime p with $p \nmid h, l$ and $p > |a|, b$,*

$$\left| \sum_{x=1}^{p} e_p(hx^a + lx^b) \right| \leq (|a| + b)p^{1/2}.$$

Proof. We simply take $f(x) = hx^a + lx^b$, which has a pole of order $|a|$ at zero and a pole of order b at infinity. Here we recall that if $a < 0$, then x^a denotes $\overline{x}^{|a|}$ modulo p. Summing over $\mathbb{P}^1$, with genus zero, (3.1) immediately gives the result. □

3.5 Multiplicative properties

We will frequently find it convenient to use multiplicative properties of exponential sums. We prove two such properties here. The first is quite general, following Lemma 3 of [40].

Lemma 3.10. *Let $\psi(q; a, b)$ be a condition on a positive integer q and integers a and b such that*
(i) $\psi(q; a_1, b_1)$ is equivalent to $\psi(q; a_2, b_2)$ if $a_1 \equiv a_2 \pmod q$ and $b_1 \equiv b_2 \pmod q$;
(ii) if $(q_1, q_2) = 1$ then $\psi(q_1 q_2; a, b)$ is equivalent to the conjunction of the conditions $\psi(q_1; a, b)$ and $\psi(q_2; a, b)$.
For integers x, y and a positive integer q, define the exponential sum

$$S(q; x, y) = \sum_{\substack{a,b \pmod q \\ \psi(q;a,b)}} e_q(ax + by).$$

Then if $(q_1, q_2) = 1$, the following multiplicative property holds:

$$S(q_1 q_2; x, y) = S(q_1; x\overline{q_2}, y\overline{q_2}) S(q_2; x\overline{q_1}, y\overline{q_1}),$$

where $\overline{q_1}$ and $\overline{q_2}$ are defined modulo q_2 and q_1 respectively by

$$\begin{aligned} q_1\overline{q_1} &\equiv 1 \pmod{q_2} \\ q_2\overline{q_2} &\equiv 1 \pmod{q_1}. \end{aligned}$$

Proof. First note that given pairs $x_1, y_1 \pmod{q_1}$ and $x_2, y_2 \pmod{q_2}$, there is a unique pair x, y modulo q_1q_2 such that

$$\begin{aligned} x &\equiv x_1 \pmod{q_1} \\ x &\equiv x_2 \pmod{q_2} \end{aligned}$$

and

$$\begin{aligned} y &\equiv y_1 \pmod{q_1} \\ y &\equiv y_2 \pmod{q_2}, \end{aligned}$$

namely

$$\begin{aligned} x &\equiv q_2\overline{q_2}x_1 + q_1\overline{q_1}x_2 \pmod{q_1q_2} \\ y &\equiv q_2\overline{q_2}y_1 + q_1\overline{q_1}y_2 \pmod{q_1q_2}. \end{aligned}$$

Thus if the conditions $\psi(q_1; x_1, y_1)$ and $\psi(q_2; x_2, y_2)$ both hold, then $\psi(q_1; x, y)$ and $\psi(q_2; x, y)$ both hold and hence $\psi(q_1q_2; x, y)$ holds, and conversely. Therefore, simply multiplying the exponential sums $S(q_1; x\overline{q_2}, y\overline{q_2})$ and $S(q_2; x\overline{q_1}, y\overline{q_1})$ and expressing the resulting product as a double sum modulo q_1q_2 proves the lemma. □

In our work with the square sieve in Chapter 7 we will also need the following more specific multiplicative property for exponential sums involving Jacobi symbols $\left(\frac{n}{r}\right)$.

Lemma 3.11. *For integers k, z, an odd positive integer r, and a square-free positive integer d with $r \nmid d$, let*

$$S(d, r; k, z) = \sum_{\alpha=1}^{r} \left(\frac{4\alpha^3 - dz^2}{r}\right) e_r(k\alpha).$$

Then if $(r_0, r_1) = 1$, the following multiplicative property holds:

$$S(d, r_0r_1; k, z) = S(d, r_0; k\overline{r_1}, z)S(d, r_1; k\overline{r_0}, z),$$

where $r_0\overline{r_0} \equiv 1 \pmod{r_1}$ and $r_1\overline{r_1} \equiv 1 \pmod{r_0}$.

Proof. We may verify this directly. Write $\alpha = \alpha_1 r_0 + \alpha_0 r_1$ modulo r_0r_1. Then

$$\begin{aligned} S(d, r_0r_1; k, z) &= \sum_{\substack{\alpha_0 \pmod{r_0} \\ \alpha_1 \pmod{r_1}}} \left(\frac{4(\alpha_1 r_0 + \alpha_0 r_1)^3 - dz^2}{r_0r_1}\right) e_{r_0r_1}(k(\alpha_1 r_0 + \alpha_0 r_1)) \\ &= \sum_{\substack{\alpha_0 \pmod{r_0} \\ \alpha_1 \pmod{r_1}}} \left(\frac{4(\alpha_0 r_1)^3 - dz^2}{r_0}\right)\left(\frac{4(\alpha_1 r_0)^3 - dz^2}{r_1}\right) e_{r_0}(k\alpha_0)e_{r_1}(k\alpha_1). \end{aligned}$$

Making the transformations

$$\begin{aligned} \alpha_0 &\mapsto \alpha_0\overline{r_1} \pmod{r_0}, \\ \alpha_1 &\mapsto \alpha_1\overline{r_0} \pmod{r_1}, \end{aligned}$$

and separating the double sum over $\alpha_0 \pmod{r_0}$ and $\alpha_1 \pmod{r_1}$ into two sums, we then obtain the desired factorisation

$$S(d, r_0; k\overline{r_1}, z)S(d, r_1; k\overline{r_0}, z).$$

□

Chapter 4

The least s-power-free number in an arithmetic progression

4.1 Introduction

In this chapter we present upper bounds for the least s-power-free positive integer $n_s(a,q)$ occurring in an arithmetic progression $a \pmod q$, for any integer $s \geq 2$. These results are an extension of a result of Heath-Brown [30] giving the best known upper bound for the least square-free positive integer in an arithmetic progression. While the results of this chapter do not relate directly to class numbers of quadratic fields, the methods presented here are the basis for our approach to counting the number of solutions in a bounded region to a congruence of the form $x^a \equiv y^b \pmod q$, as presented in Chapter 5.

In studying the least s-power-free positive integer in an arithmetic progression $a \pmod q$, one must first assume that (a,q) is itself s-power-free, otherwise no such number exists. In the case $s = 2$, Prachar [55] was the first to provide an upper bound for $n_2(a,q)$, namely

$$n_2(a,q) \ll q^{\frac{3}{2}} \exp\left(c\frac{\log q}{\log\log q}\right),$$

for $(a,q) = 1$, with a specified constant c. Erdös [15] subsequently refined this to

$$n_2(a,q) \ll q^{\frac{3}{2}}(\log q)^{-1}$$

in the case $(a,q) = 1$ and

$$n_2(a,q) \ll q^{\frac{3}{2}}(\log\log q)(\log q)^{-1}$$

in general. In [39], Hooley used exponential sum techniques, employing the Weil bound, to prove the further result that for any $\epsilon > 0$, the numbers q for which

$$\max_{(a,q)=1} n_2(a,q) \leq q^{\frac{4}{3}+\epsilon}$$

have positive lower density. In [30], Heath-Brown extended the methods of Hooley, obtaining the upper bound

$$n_2(a,q) \ll (d(q)\log q)^6 (qq_0^{1/2} + q^2 q_0^{-1}) \tag{4.1}$$

for any divisor $q_0|q$. This result is most efficient for a divisor of size $q_0 \approx q^{2/3}$, in which case one obtains an exponent of $4/3 + \epsilon$ for $n_2(a,q)$. Heath-Brown furthermore extended ideas of Burgess [6] for character sums to prove the general result

$$n_2(a,q) \ll (d(q)\log q)^6 q^{13/9}, \tag{4.2}$$

where both bounds hold uniformly in a.

4.2 Statement of the Theorems

Following Heath-Brown, we prove two analogous bounds for $n_s(a,q)$ for any integer $s \geq 2$.

Theorem 4.1. *For any integer $s \geq 2$, if (a,q) is s-power-free, then*

$$n_s(a,q) \ll (qq_0^{\frac{1}{2}} + q^{\frac{s}{s-1}} q_0^{-\frac{1}{s-1}})(a,q)^{\frac{s-2}{2(s-1)}} q^{\epsilon}$$

for any $\epsilon > 0$, for any divisor $q_0|q$ with $q_0 \geq q^{1/s}$.

The implied constant depends only on s and ϵ, and the factor q^{ϵ} may be expressed explicitly in terms of powers of $d(q)$ and $\log q$. This theorem reduces to (4.1) in the case $s = 2$, and as is to be expected, the bound for $n_s(a,q)$ becomes weaker as s increases. Note that the theorem is least efficient when q is a prime, or when q is the product of two factors each of size $\approx q^{1/2}$. The best case occurs when the divisor $q_0 \approx q^{\frac{2}{s+1}}$; for example, if $q = k^{s+1}$ or $q = k!$.

Theorem 4.2. *For any integer $s \geq 2$, if q is square-free, then*

$$n_s(a,q) \ll q^{1+\frac{1}{s}\left(\frac{2s^2}{2s^2+s-1}\right)+\epsilon}$$

for any $\epsilon > 0$.

Again, the implied constant depends only on s and ϵ, and the factor q^{ϵ} may be expressed explicitly in terms of powers of $d(q)$ and $\log q$. This theorem reduces to (4.2) in the case $s = 2$. Some of the power of this theorem is lost by assuming q is square-free. In the main part of the discussion that follows

we make only the necessary assumption that (a, q) is s-power-free; it is only in the last stage of the proof of Theorem 4.2 that we must make the further assumption that q is square-free. However, this is the case of most interest to us, as we will only be concerned with square-free moduli q when we extend these methods in Chapter 5.

Both Theorems 4.1 and 4.2 are improvements over the trivial bound

$$n_s(a, q) \ll q^{1+\frac{1}{s}+\epsilon}, \tag{4.3}$$

which we derive in Section 4.4.1. Both theorems are straightforward extensions of the methods of Heath-Brown in [30]. We prove Theorem 4.1 using exponential sums, employing Weil's bound for exponential sums with prime moduli, and elementary methods for exponential sums with composite moduli. We prove Theorem 4.2 using mean value properties of exponential sums.

In Section 4.3 we reduce both theorems to bounding a certain sum over a finite interval. In Section 4.4 we prove Theorem 4.1, except for the bound of an exponential sum $V(q; m, b)$, which we derive in Section 4.5. In Section 4.6 we describe the mean value methods for Theorem 4.2. We derive several key estimates in Section 4.7, and then finally prove Theorem 4.2 in Section 4.8.

4.3 Reduction of the problem

We begin by expressing the problem of bounding $n_s(a, q)$ in terms of the number of solutions to a congruence modulo q.

Definition 4.1. For an integer $s \geq 2$, let

$$\eta_s(n) = \begin{cases} 1 & \text{if for all primes } p, \quad p^s \nmid n \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\eta_2(n) = \mu^2(n)$. Set $t = (\log q)^{1/s}$ and let

$$P = \prod_{\substack{p \leq t \\ \text{or } p \mid q}} p.$$

Then $\eta_s((n, P^s)) = \eta_s(n)$ if $n \leq t$. If $n > t$ then $\eta_s(n) = \eta_s((n, P^s)) = 1$ if no $p^s | n$. But if there is a prime p such that $p^s | n$ but neither $p \leq t$ nor $p | q$, then $\eta_s((n, P^s)) = 1$, yet $\eta_s(n) = 0$. As a result,

$$\eta_s((n, P^s)) - \eta_s(n) \leq \sum_{\substack{p^s \mid n \\ p \nmid q,\ p > t}} 1.$$

Thus it follows that

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \eta_s(n) \geq \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \eta_s((n, P^s)) - \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \sum_{\substack{p^s \mid n \\ p \nmid q,\ p > t}} 1. \tag{4.4}$$

Definition 4.2. Let

$$S(d,q,a,x,s) = \#\{m \leq xd^{-s} : md^s \equiv a \pmod q\}.$$

It is easy to prove by multiplicativity that

$$\eta_s((n,P^s)) = \sum_{\substack{d^s|n \\ d|P}} \mu(d).$$

Then

$$\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \eta_s((n,P^s)) = \sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \sum_{\substack{d^s|n \\ d|P}} \mu(d) = \sum_{d|P} \mu(d) S(d,q,a,x,s).$$

Also,

$$\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \sum_{\substack{p^s|n \\ p\nmid q, p>t}} 1 \leq \sum_{\substack{t<p\leq x^{1/s} \\ p\nmid q}} \sum_{\substack{n\leq x \\ n\equiv a \pmod q \\ p^s|n}} 1 = \sum_{\substack{t<p\leq x^{1/s} \\ p\nmid q}} S(p,q,a,x,s).$$

Thus we may write (4.4) as:

Proposition 4.1.

$$\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \eta_s(n) \geq \sum_{d|P} \mu(d) S(d,q,a,x,s) - \sum_{\substack{t<p\leq x^{1/s} \\ p\nmid q}} S(p,q,a,x,s).$$

In order to find an upper bound for $n_s(a,q)$ it is thus sufficient to find a lower bound for x such that the left hand side in Proposition 4.1 is strictly positive. While bounding the first term on the right in Proposition 4.1 from below is relatively simple, bounding the second term on the right from above is the main goal of this chapter.

We begin by finding a lower bound for the first term on the right hand side in Proposition 4.1.

Lemma 4.1.

$$S(d,q,a,x,s) = \begin{cases} xd^{-s}q^{-1}(d^s,q) + O(1) & \text{if } (d^s,q)|a \\ 0 & \text{if } (d^s,q) \nmid a. \end{cases}$$

Proof. First, if $(d^s,q) \nmid a$ then there are no solutions m to the congruence

$$md^s \equiv a \pmod q.$$

Next let $h = (d^s,q)$ and suppose $h|a$. Then for any $m \leq xd^{-s}$ such that $md^s \equiv a \pmod q$,

$$md^s h^{-1} \equiv ah^{-1} \pmod{qh^{-1}}.$$

Any such solution m may be written as

$$m = N \cdot qh^{-1} + L$$

for some $0 \leq N \leq xd^{-s}q^{-1}h$ and $0 \leq L \leq qh^{-1}$, and the result follows. □

A lower bound for the sum under consideration then follows easily:

Proposition 4.2. *Assume* $q^{1+\frac{1}{2s}} \leq x \leq q^2$. *Then*

$$\sum_{d|P} \mu(d) S(d,q,a,x,s) \gg x\phi(q)q^{-2}.$$

Proof. By Lemma 4.1,

$$\sum_{d|P} \mu(d) S(d,q,a,x,s) = \frac{x}{q} \sum_{\substack{d|P \\ (d^s,q)|a}} \mu(d) d^{-s}(d^s,q) + O(\sum_{d|P} 1).$$

First note that the number of divisors of P is at most the number of possible products composed of primes $p \leq t$, times the number of prime divisors of q. Thus P has at most $2^t d(q)$ divisors. For each $d|P$,

$$(d^s,q) = \prod_{p|d} (p^s,q),$$

so by multiplicativity, we have the product formula

$$\sum_{\substack{d|P \\ (d^s,q)|a}} \mu(d) d^{-s}(d^s,q) = \prod_{\substack{p|P \\ (p^s,q)|a}} (1 - p^{-s}(p^s,q)).$$

Therefore

$$\sum_{d|P} \mu(d) S(d,q,a,x,s) = \frac{x}{q} \prod_{\substack{p \leq t \text{ or } p|q \\ (p^s,q)|a}} (1 - p^{-s}(p^s,q)) + O(2^t d(q)).$$

Denote the product on the right hand side by $C(a,q,s)$. Our goal is to bound $C(a,q,s)$ from below. First assume that $(a,q) = 1$ so that $C(a,q,s)$ only includes $p|P$ such that $(p^s,q) = 1$. Then

$$\begin{aligned} C(a,q,s) &= \prod_{\substack{p \leq t \text{ or } p|q \\ (p^s,q)=1}} (1 - p^{-s}) \\ &\geq \prod_{p} (1 - p^{-s}) \\ &= \frac{1}{\zeta(s)}, \end{aligned}$$

which is a strictly positive number for any integer $s \geq 2$.

More generally, for (a,q) an s-power-free integer > 1, we have

$$C(a,q,s) \geq \prod_{\substack{p \nmid q \\ p \leq t}} (1 - p^{-s}(p^s,q)) \prod_{\substack{p|q \\ (p^s,q)|a}} (1 - p^{-s}(p^s,q)).$$

In the first product, $(p^s,q) = 1$ since $p \nmid q$. In the second product, since $(p^s,q)|a$ and (a,q) is s-power-free then $(p^s,q) < p^s$. But also (p^s,q) is a strictly positive

power of p, since $p|q$. Thus the least value a factor $(1-p^{-s}(p^s,q))$ can achieve is $(1-p^{-1})$. Therefore,

$$\begin{aligned} C(a,q,s) &\geq \prod_{p\nmid q}(1-p^{-s})\prod_{p|q}(1-p^{-1}) \\ &\geq \prod_{p}(1-p^{-s})\prod_{p|q}(1-p^{-1}) \\ &= \frac{1}{\zeta(s)}\prod_{p|q}(1-p^{-1}) \\ &= \frac{1}{\zeta(s)}\cdot\frac{\phi(q)}{q}. \end{aligned}$$

Thus in general if (a,q) is s-power-free,

$$C(a,q,s) \gg \phi(q)q^{-1}.$$

Recall that

$$\sum_{d|P}\mu(d)S(d,q,a,x,s) = \frac{x}{q}C(a,q,s) + O(2^t d(q)).$$

Assuming, as we will for the remainder of the discussion, that

$$q^{1+\frac{1}{2s}} \leq x \leq q^2, \tag{4.5}$$

this is then certainly sufficient to give

$$\sum_{d|P}\mu(d)S(d,q,a,x,s) \gg x\phi(q)q^{-2}.$$

□

This completes our lower bound for the first term on the right hand side in Proposition 4.1. In order to find an upper bound for the second term on the right hand side in Proposition 4.1 we will break the sum of $S(p,q,a,x,s)$ over primes $p \nmid q$ in the interval $t < p \leq x^{1/s}$ into three parts, summing over the intervals $t < p \leq y$, $y < p \leq z$, and $z < p \leq x^{1/s}$, for appropriately chosen values of x, y, z. We will accomplish bounds for the sums over the first and third intervals relatively easily. The sum over the second interval requires a more detailed analysis; it is the bound for this term that distinguishes the results of Theorems 4.1 and 4.2.

We bound the sum over the first interval $t < p \leq y$ as follows. All implied constants depend only upon s unless otherwise noted.

Proposition 4.3. *If $y = xq^{-1}$, then*

$$\sum_{\substack{t<p\leq y \\ p\nmid q}} S(p,q,a,x,s) \ll xq^{-1}(\log q)^{-1/s}.$$

Proof. By Lemma 4.1,

$$\sum_{\substack{t<p\le y\\ p\nmid q}} S(p,q,a,x,s) \ll \frac{x}{q}\sum_{\substack{t<p\le y\\ p\nmid q\\ (p^s,q)\mid a}} p^{-s}(p^s,q) + \sum_{\substack{t<p\le y\\ p\nmid q\\ (p^s,q)\mid a}} 1$$

Noting that $(p^s,q)=1$ since $p\nmid q$, we then have:

$$\begin{aligned}\sum_{\substack{t<p\le y\\ p\nmid q}} S(p,q,a,x,s) &\ll \frac{x}{q}\sum_{\substack{t<p\le y\\ p\nmid q}} p^{-s} + \sum_{\substack{t<p\le y\\ p\nmid q}} 1\\ &\ll \frac{x}{q}\sum_{t<p\le y} p^{-s} + y(\log y)^{-1},\end{aligned}$$

by the prime number theorem. Note that

$$\sum_{t<p\le y} p^{-s} \le \sum_{p>t} p^{-s} \ll t^{-1}.$$

Thus

$$\sum_{\substack{t<p\le y\\ p\nmid q}} S(p,q,a,x,s) \ll xq^{-1}(\log q)^{-1/s} + y(\log y)^{-1}.$$

In order to bound this expression by $xq^{-1}(\log q)^{-1/s}$, it is sufficient to choose

$$y = xq^{-1}. \tag{4.6}$$

This completes the proof. □

We next bound the sum over the third interval $z < p \le x^{1/s}$.

Definition 4.3. Let

$$T(m,q,a,z,x,s) = \#\{z < p \le x^{1/s}, p\nmid q : mp^s \equiv a \pmod q\}.$$

Then immediately

$$\begin{aligned}\sum_{\substack{z<p\le x^{1/s}\\ p\nmid q}} S(p,q,a,x,s) &= \sum_{\substack{z<p\le x^{1/s}\\ p\nmid q}} \#\{m \le xp^{-s} : mp^s \equiv a \pmod q\}\\ &\le \sum_{m\le xz^{-s}} T(m,q,a,z,x,s). \end{aligned}\tag{4.7}$$

Note that any solution m of

$$mp^s \equiv a \pmod q$$

must have $(a,q)\mid mp^s$, but $p\nmid q$, hence $(a,q)\mid m$. Thus $T(m,q,a,z,x,s)=0$ unless $(a,q)\mid m$. In particular, if $z > x^{1/s}(a,q)^{-1/s}$, the sum (4.7) is zero, since then $m < (a,q)$ for each $m \le xz^{-s}$.

Let $d = (a, q)$ and write $q = dq_1$, $a = da_1$, and $m = dm_1$. Then

$$T(m, q, a, z, x, s) \leq (1 + x^{1/s} q_1^{-1}) \#\{u \pmod{q_1} : m_1 u^s \equiv a_1 \pmod{q_1}\}.$$

Using Lemma 3.3 to count the number of solutions to this congruence, it follows immediately that

$$T(m, q, a, z, x, s) \ll s^{\nu(q)}(1 + x^{1/s} q_1^{-1}).$$

We now use this to choose a value of z and obtain an upper bound for the sum of $S(p, q, a, x, s)$ over the interval $z < p \leq x^{1/s}$.

Proposition 4.4. *Let*

$$z = \min(2x^{\frac{1}{s}}(a, q)^{-\frac{1}{s}}, s^{\frac{\nu(q)}{s}}(\log q)(x^{\frac{1}{s^2}} + q^{\frac{1}{s}}(a, q)^{-\frac{1}{s}})). \tag{4.8}$$

Then

$$\sum_{\substack{z < p \leq x^{1/s} \\ p \nmid q}} S(p, q, a, x, s) \ll xq^{-1}(\log q)^{-s}.$$

Proof. Abbreviate (4.8) as $z = \min(A, B)$. If A is the minimal expression, so that $z > x^{1/s}(a, q)^{-1/s}$, then the sum (4.7) is zero. Thus we need only consider the case when $z = B$. In this case we have:

$$\begin{aligned}
\sum_{\substack{z < p \leq x^{1/s} \\ p \nmid q}} S(p, q, a, x, s) &\leq \sum_{m \leq xz^{-s}} T(m, q, a, z, x, s) \\
&\ll s^{\nu(q)}(1 + x^{1/s} q_1^{-1}) \sum_{\substack{m \leq xz^{-s} \\ (a,q) \mid m}} 1 \\
&\ll s^{\nu(q)}(1 + x^{1/s} q_1^{-1})(xz^{-s}(a, q)^{-1} + 1).
\end{aligned}$$

Using the explicit expression $z = B$ we then obtain:

$$\begin{aligned}
\sum_{\substack{z < p \leq x^{1/s} \\ p \nmid q}} S(p, q, a, x, s) &\ll \frac{s^{\nu(q)} x(a, q)^{-1}(1 + x^{1/s} q_1^{-1})}{\left[s^{\nu(q)/s}(\log q)(x^{\frac{1}{s^2}} + q^{\frac{1}{s}}(a, q)^{-\frac{1}{s}})\right]^s} \\
&\ll \frac{x(a, q)^{-1}(1 + x^{1/s} q^{-1}(a, q))}{(\log q)^s (x^{1/s} + q(a, q)^{-1})} \\
&\ll xq^{-1}(\log q)^{-s}.
\end{aligned}$$

□

We have now chosen y and z such that the sum of $S(p, q, a, x, s)$ over the interval $t < p \leq y$ is bounded above by $xq^{-1}(\log q)^{-1/s}$ and the sum over the interval $z < p \leq x^{1/s}$ is bounded above by $xq^{-1}(\log q)^{-s}$, for some appropriate value of x not yet explicitly chosen. Suppose we have a lower bound for x such

that the sum of $S(p,q,a,x,s)$ over the middle interval $y < p \leq z$ is also bounded above by $xq^{-1}(\log q)^{-s}$. Then we would have a lower bound for x for which

$$\begin{aligned}\sum_{\substack{n\leq x\\ n\equiv a \pmod q}} \eta_s(n) &\geq \sum_{d|P} S(d,q,a,x,s) - \sum_{\substack{t<p\leq x^{1/s}\\ p\nmid q}} S(p,q,a,x,s)\\ &\gg x\phi(q)q^{-2} - xq^{-1}(\log q)^{-1/s} - xq^{-1}(\log q)^{-s}\\ &\gg x\phi(q)q^{-2}.\end{aligned}$$

The last line follows since $\phi(n)/n^{1-\epsilon} \gg 1$ for every $\epsilon > 0$ and sufficiently large n (see Theorem 327 of [24], for example). In other words, we would have the desired upper bound for $n_s(a,q)$.

It remains to bound the middle sum,

$$\sum_{\substack{y<p\leq z\\ p\nmid q}} S(p,q,a,x,s). \tag{4.9}$$

We could obviate the need to bound (4.9) by choosing $y \geq z$, but this would only allow us to choose

$$x \gg \min(q^{\frac{s}{s-1}}(a,q)^{-\frac{1}{s-1}}, q^{\frac{s^2}{s^2-1}} + q^{1+\frac{1}{s}}(a,q)^{-1})q^{\epsilon}.$$

Note that this does improve as (a,q) increases; however, our goal is to save a power of q over the trivial bound (4.3).

4.4 Theorem 4.1: the Weil bound

We will prove a nontrivial bound for the remaining sum (4.9) using exponential sums. It will be easier to manipulate the following closely related function:

Definition 4.4. For $y < w \leq z$, let

$$U(w,M,q,a,s) = \sum_{\substack{w<n\leq 2w\\ (n,q)=1}} \#\{m \leq M : mn^s \equiv a \pmod q\}$$

where $(a,q) = 1$ and $M \leq q/2$.

It follows that:

Lemma 4.2.

$$\sum_{\substack{w<p\leq 2w\\ p\nmid q}} S(p,q,a,x,s) \leq U(w, xw^{-s}(a,q)^{-1}, q(a,q)^{-1}, a(a,q)^{-1}, s).$$

Proof. It is easily verified that

$$xw^{-s}(a,q)^{-1} \leq \frac{q}{2}(a,q)^{-1},$$

for $w > y$, recalling from (4.5) and (4.6) that we have chosen $q^{1+\frac{1}{2s}} \leq x \leq q^2$ and $y = xq^{-1}$.

Letting $d = (a, q)$,

$$\begin{aligned}\sum_{\substack{w<p\leq 2w\\ p\nmid q}} S(p,q,a,x,s) &= \sum_{\substack{w<p\leq 2w\\ p\nmid q}} \#\{m \leq xp^{-s} : mp^s \equiv a \pmod q\}\\ &\leq \sum_{\substack{w<n\leq 2w\\ (n,q)=1}} \#\{m \leq xn^{-s} : mn^s \equiv a \pmod q\}\\ &\leq \sum_{\substack{w<n\leq 2w\\ (n,qd^{-1})=1}} \#\{md^{-1} \leq xw^{-s}d^{-1} : md^{-1}n^s \equiv ad^{-1} \pmod{qd^{-1}}\}\\ &= U(w, xw^{-s}(a,q)^{-1}, q(a,q)^{-1}, a(a,q)^{-1}, s).\end{aligned}$$

□

4.4.1 The trivial bound for $n_s(a, q)$

It is at this point that it is easy to see that the trivial bound for $n_s(a, q)$ is $O(q^{1+1/s+\epsilon})$. Suppose for convenience that $(a, q) = 1$, so that

$$\begin{aligned}\sum_{\substack{w<p\leq 2w\\ p\nmid q}} S(p,q,a,x,s) &\leq U(w, xw^{-s}, q, a, s)\\ &= \#\{n, m : w < n \leq 2w,\ m \leq xw^{-s},\ mn^s \equiv a \pmod q\}.\end{aligned}$$

Fixing m and counting the possible values of n for each m, we obtain

$$U(w, xw^{-s}, q, a, s) \ll s^{\nu(q)}(xq^{-1}w^{1-s} + xw^{-s}). \tag{4.10}$$

Alternatively, fixing n and counting the possible values of m for each n we obtain

$$U(w, xw^{-s}, q, a, s) \ll xq^{-1}w^{1-s} + w. \tag{4.11}$$

If $w \geq x^{\frac{1}{s+1}}$, then to bound (4.9) by $xq^{-1}(\log q)^{-s}$, we see by (4.10) that we must have $xw^{-s} \ll xq^{-1}(\log q)^{-s}$, which is true as long as $x \gg q^{1+1/s+\epsilon}$. If $w \leq x^{\frac{1}{s+1}}$, then we see by (4.11) that we must have $w \ll xq^{-1}(\log q)^{-s}$, which is true as long as $x \gg q^{1+1/s+\epsilon}$. Thus

$$n_s(a, q) \ll q^{1+\frac{1}{s}+\epsilon},$$

which we refer to as the trivial bound. A similar analysis shows that the same trivial bound applies when $(a, q) > 1$.

4.4.2 Expressing $U(w, M, q, a, s)$ as an exponential sum

We improve on this trivial bound using exponential sum techniques. Define $\delta(n) = 1$ if there exists an m with $1 \leq m \leq M$ such that $m \equiv a\overline{n}^s \pmod q$, and

let $\delta(n) = 0$ otherwise. Then

$$U(w, M, q, a, s) = \sum_{w<n\leq 2w} \delta(n).$$

Define

$$\delta_1(x) = \begin{cases} 1 & \text{if } \|x\| \leq Mq^{-1} \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, let

$$\delta_2(x) = \left(\frac{\sin(\pi Hx)}{H\sin(\pi x)}\right)^2 = \left|\sum_{h=1}^{H} e(hx)\right|^2 = H^{-2} \sum_{|h|<H} (H - |h|)e(hx)$$

with $H = [(q/2)M^{-1}]$. We obtain the following relation between the functions δ, δ_1 and δ_2.

Lemma 4.3.

$$\delta(n) \leq \delta_1\left(\frac{a\overline{n}^s}{q}\right) \ll \delta_2\left(\frac{a\overline{n}^s}{q}\right).$$

Proof. For the first inequality, it is sufficient to show that if $\delta(n) = 1$ then $\delta_1(a\overline{n}^s/q) = 1$. If $\delta(n) = 1$, then for some integer k,

$$1 \leq m = a\overline{n}^s + kq \leq M$$

and hence

$$\left\|\frac{a\overline{n}^s}{q}\right\| \leq Mq^{-1},$$

so that $\delta_1(a\overline{n}^s/q) = 1$.

For the second inequality, it is sufficient to show that if $\delta_1(x) = 1$ then $\delta_2(x) \geq c > 0$ for a constant c independent of x. The function $\delta_2(x)$ is an even function with period 1, hence $\delta_2(x) = \delta_2(\|x\|)$. Also, $\delta_2(x)$ can be defined at $x = 0$ so that it is continuous for all x. Now suppose $\delta_1(x) = 1$ so that $\|x\| \leq Mq^{-1}$ and thus $\|x\| \leq 1/(2H)$. On the interval $0 \leq t \leq \pi/2$, we have $2t/\pi \leq \sin t \leq t$. Therefore if $\|x\| \leq 1/(2H)$,

$$\frac{\sin(\pi H\|x\|)}{H\sin(\pi\|x\|)} \geq \frac{2H\|x\|}{\pi H\|x\|} = \frac{2}{\pi}.$$

□

We may now express the function $U(w, M, q, a, s)$ in terms of the following exponential sum.

Proposition 4.5.

$$U(w, M, q, a, s) \ll H^{-1} \sum_{h=0}^{H-1} \left| \sum_{w<n\leq 2w} e_q(ha\overline{n}^s) \right|.$$

Proof. Using Lemma 4.3 and the Fourier transform for δ_2 we see immediately that

$$\begin{aligned} U(w,M,q,a,s) &= \sum_{w<n\leq 2w} \delta(n) \\ &\ll \sum_{w<n\leq 2w} \delta_2\left(\frac{a\overline{n}^s}{q}\right) \\ &= \sum_{w<n\leq 2w}\left[H^{-2}\sum_{|h|<H}(H-|h|)e_q(ha\overline{n}^s)\right] \\ &\ll H^{-1}\sum_{h=0}^{H-1}\left|\sum_{w<n\leq 2w} e_q(ha\overline{n}^s)\right|. \end{aligned}$$

□

4.4.3 Bounding the inner sum $N(w,q,ha,s)$

Let

$$N(w,q,ha,s) = \sum_{w<n\leq 2w} e_q(ha\overline{n}^s)$$

so that

$$U(w,M,q,a,s) \ll H^{-1}\sum_{h=0}^{H-1}|N(w,q,ha,s)|. \tag{4.12}$$

Let $m = ha$. Then we may extend $N(w,q,m,s)$ to a sum over a complete set of residues modulo q as follows:

$$\begin{aligned} N(w,q,m,s) &= \sum_{k=1}^{q} e_q(m\overline{k}^s)\sum_{w<n\leq 2w}\frac{1}{q}\sum_{b=1}^{q} e_q(b(k-n)) \\ &= \frac{1}{q}\sum_{b=1}^{q}\sum_{w<n\leq 2w} e_q(-bn)\sum_{k=1}^{q} e_q(m\overline{k}^s+bk). \end{aligned}$$

As in Lemma 3.4, let

$$A(q;w,-b) = \sum_{w<n\leq 2w} e_q(-bn),$$

so that

$$|A(q;w,-b)| \leq \min(w, \|b/q\|^{-1}).$$

Definition 4.5. Let

$$V(q;m,b) = \sum_{k=1}^{q} e_q(m\overline{k}^s+bk).$$

Then

$$|N(w,q,m,s)| \leq \frac{1}{q}\sum_{b=1}^{q}|V(q;m,b)||A(q;w,-b)|.$$

Assume the following bound for $V(q;m,b)$:

Lemma 4.4. *If $(m,q)=1$ then*

$$|V(q;m,b)| \ll d(q)^{\sigma}q^{1/2},$$

where σ is a positive integer dependent only on s.

We prove this lemma in the following section, but for now we proceed with the proof of Theorem 4.1.

Proposition 4.6.

$$|N(w,q,ha,s)| \ll d(q)^{\sigma_1}\left[q^{-1/2}(h,q)^{1/2}w + q^{1/2}\log q\right],$$

where $\sigma_1 = \sigma + 1$.

Proof. First suppose that $(h,q)=1$. Recall that the function U only considers values of a such that $(a,q)=1$. Thus defining $m=ha$, we have $(m,q)=1$ and so by Lemma 4.4,

$$\begin{aligned}
|N(w,q,ha,s)| &\ll q^{-1}(d(q)^{\sigma}q^{1/2})\sum_{b=1}^{q}\min(w,\|b/q\|^{-1}) \\
&\ll d(q)^{\sigma}q^{-1/2}\left[w + 2q\sum_{1\leq b\leq q/2} b^{-1}\right] \\
&\ll d(q)^{\sigma}\left[q^{-1/2}w + q^{1/2}\log q\right]. \qquad (4.13)
\end{aligned}$$

In the general case where $(h,q)=\delta$, write $q=\delta q_1$ and $ha=\delta m$ so that $(m,q_1)=1$. Let D be the product of primes p such that $p|\delta$ and $p\nmid q_1$. Then

$$\begin{aligned}
N(w,q,ha,s) &= \sum_{w<n\leq 2w} e\left(\frac{\delta m\overline{n}^s}{dq_1}\right) \\
&= \sum_{\substack{w<n\leq 2w \\ (n,D)=1}} e\left(\frac{m\overline{n}^s}{q_1}\right) \\
&= \sum_{j|D}\mu(j)\sum_{\substack{w<n\leq 2w \\ j|n}} e\left(\frac{m\overline{n}^s}{q_1}\right) \\
&= \sum_{j|D}\mu(j)\sum_{w<jl\leq 2w} e\left(\frac{m\overline{j}^s\overline{l}^s}{q_1}\right).
\end{aligned}$$

Note that since $j|D$ then $(j, q_1) = 1$ and so $(m\overline{j}^s, q_1) = 1$. Thus we may apply the bound (4.13) of the previous case, obtaining

$$|N(w, q, ha, s)| \ll d(D)d(q)^{\sigma} \left[q_1^{-1/2}w + q_1^{1/2}\log q_1\right].$$

Since $d(D) \ll d(q)$, we define $\sigma_1 = \sigma + 1$ and we have the final bound

$$|N(w, q, ha, s)| \ll d(q)^{\sigma_1} \left[q^{-1/2}(h, q)^{1/2}w + q^{1/2}\log q\right].$$

□

This immediately gives a bound for $U(w, M, q, a, s)$:

Proposition 4.7.

$$U(w, M, q, a, s) \ll d(q)^{\sigma_1} \left[q^{1/2}\log q + wq^{-1}M + wq^{-1/2}d(q)\right].$$

Proof. Applying the bound of the previous proposition to (4.12),

$$\begin{aligned}
&U(w, M, q, a, s)\\
&\quad\ll\quad H^{-1}\sum_{h=0}^{H-1}|N(w, q, ha, s)|\\
&\quad\ll\quad H^{-1}\sum_{h=0}^{H-1}d(q)^{\sigma_1}\left[q^{-1/2}(h, q)^{1/2}w + q^{1/2}\log q\right]\\
&\quad\ll\quad d(q)^{\sigma_1}\left[q^{1/2}\log q + wq^{-1/2}H^{-1}\sum_{h=0}^{H-1}(h, q)^{1/2}\right]\\
&\quad\ll\quad d(q)^{\sigma_1}\left[q^{1/2}\log q + wH^{-1} + wq^{-1/2}H^{-1}\sum_{h=1}^{H-1}(h, q)^{1/2}\right].
\end{aligned}$$

We may estimate the sum in the last term by:

$$H^{-1}\sum_{h=1}^{H-1}(h, q)^{1/2} = H^{-1}\sum_{d|q}d^{1/2}\sum_{\substack{h=1\\ d|h}}^{H-1}1 \ll H^{-1}\sum_{d|q}d^{1/2}(H/d) = \sum_{d|q}d^{-1/2} \ll d(q).$$

Recalling that $H = [(q/2)M^{-1}]$, this gives

$$U(w, M, q, a, s) \ll d(q)^{\sigma_1} \left[q^{1/2}\log q + wq^{-1}M + wq^{-1/2}d(q)\right].$$

□

4.4.4 The assumption of a divisor q_0

Proposition 4.7 is not sufficient to prove Theorem 4.1 in itself, as it would only allow us to choose $x \gg q^{1+1/s+\epsilon}$, giving the trivial bound $n_s(a, q) \ll q^{1+1/s+\epsilon}$. However, we may refine this to a non-trivial bound for $n_s(a, q)$, assuming that

q has a factor q_0 of suitable size. Write $q_1 = q(a,q)^{-1}$ and $q_2 = (q_0, q_1)$. By definition,

$$U(w, M, q_1, a, s) = \sum_{\substack{w<n\le 2w \\ (n,q_1)=1}} \#\{m \le M : m\overline{n}^s \equiv a \pmod{q_1}\}.$$

Any solution m of $m\overline{n}^s \equiv a$ modulo q_1 is also a solution modulo q_2, so trivially

$$U(w, M, q_1, a, s) \le U(w, M, q_2, a, s). \tag{4.14}$$

Thus by Lemma 4.2,

$$\sum_{\substack{w<p\le 2w \\ p\nmid q}} S(p, q, a, x, s) \le U(w, xw^{-s}(a,q)^{-1}, q_2, a(a,q)^{-1}, s).$$

Note that the requirement $M = xw^{-s}(a,q)^{-1} \le q_2/2$ is satisfied for $y < w \le z$ with y and z chosen as in (4.6) and (4.8), as long as

$$x \gg q^{\frac{s}{s-1}} q_0^{-\frac{1}{s-1}}. \tag{4.15}$$

Applying Proposition 4.7,

$$U(w, M, q_2, a, s) \ll d(q_2)^{\sigma_1} \left[q_2^{1/2} \log q_2 + w q_2^{-1} M + w q_2^{-1/2} d(q_2) \right].$$

Thus

$$\begin{aligned} \sum_{\substack{w<p\le 2w \\ p\nmid q}} S(p, q, a, x, s) &\ll d(q)^{\sigma_1} \left[q_0^{1/2} \log q + x w^{1-s} q_2^{-1} (a,q)^{-1} + w q_0^{-1/2} d(q) (a,q)^{1/2} \right] \\ &\ll d(q)^{\sigma_1} \left[q_0^{1/2} \log q + x w^{1-s} q_0^{-1} + w q_0^{-1/2} d(q) (a,q)^{1/2} \right]. \end{aligned}$$

Let J be the least integer such that $J \ge (\log z - \log y)/\log 2$. Summing over dyadic intervals,

$$\begin{aligned} \sum_{\substack{y<p\le z \\ p\nmid q}} S(p, q, a, x, s) &\le \sum_{j=0}^{J-1} \sum_{\substack{w<p\le 2w \\ w=2^j y \\ p\nmid q}} S(p, q, a, x, s) \\ &\ll \sum_{j=0}^{J-1} d(q)^{\sigma_1} \left[q_0^{1/2} \log q + 2^{-j} x y^{1-s} q_0^{-1} + 2^j y q_0^{-1/2} d(q) (a,q)^{1/2} \right]. \end{aligned}$$

Thus

$$\sum_{\substack{y<p\le z \\ p\nmid q}} S(p, q, a, x, s) \ll d(q)^{\sigma_1} \left[q_0^{1/2} (\log q)^2 + x y^{1-s} q_0^{-1} + z q_0^{-1/2} d(q) (a,q)^{1/2} \right].$$

It remains to choose x so that this is bounded by $xq^{-1}(\log q)^{-s}$. With y and z as chosen in (4.6) and (4.8), is sufficient to choose x such that

$$d(q)^{\sigma_1} \left[q_0^{1/2} (\log q)^2 + x^{2-s} q^{s-1} q_0^{-1} + x^{1/s} q_0^{-1/2} d(q) (a,q)^{1/2-1/s} \right] \ll x q^{-1} (\log q)^{-s},$$

or

$$x \gg d(q)^{\sigma_2}(\log q)^2(a,q)^{\frac{s-2}{2(s-1)}} \max(qq_0^{\frac{1}{2}}, q^{\frac{s}{s-1}}q_0^{-\frac{1}{s-1}}),$$

where σ_2 is a positive integer dependent only on s. This satisfies the previously stated requirements (4.5) and (4.15) for x, so long as the divisor q_0 satisfies $q_0 \geq q^{1/s}$. Thus we have the final bound

$$n_s(a,q) \ll (qq_0^{\frac{1}{2}} + q^{\frac{s}{s-1}}q_0^{-\frac{1}{s-1}})(a,q)^{\frac{s-2}{2(s-1)}}q^{\epsilon}$$

for any divisor $q_0 \geq q^{1/s}$, and for any $\epsilon > 0$, where the implied constant depends only upon s and ϵ. Aside from the bound for $V(q;m,b)$ derived in the following section, this completes the proof of Theorem 4.1.

4.5 Bounding the sum $V(q;m,b)$

In this section we prove Lemma 4.4. $V(q;m,b)$ is multiplicative by Lemma 3.10 in the sense that

$$V(q_1q_2;m,b) = V(q_1;m\overline{q_2},b\overline{q_2})V(q_2;m\overline{q_1},b\overline{q_1})$$

for $(q_1,q_2)=1$, where $q_1\overline{q_1} \equiv 1 \pmod{q_2}$ and $q_2\overline{q_2} \equiv 1 \pmod{q_1}$. Thus it suffices to bound $V(q;m,b)$ for prime powers $q = p^f$. Throughout this section we will assume that $(m,q)=1$.

4.5.1 Prime moduli

In the case $q=p$, $V(p;m,b)$ is a Kloosterman sum,

$$V(p;m,b) = \sum_{n=1}^{p} e\left(\frac{m\overline{n}^s + bn}{p}\right).$$

For $p > s$, since $p \nmid m$, the Weil bound given in Lemma 3.9 shows that

$$|V(p;m,b)| \leq (s+1)p^{1/2}.$$

For $p \leq s$, the trivial bound

$$|V(p;m,b)| \leq p \leq (s+1)p^{1/2}$$

is sufficient.

4.5.2 Composite moduli

We will bound $V(p^f;m,b)$ for $f \geq 2$ by elementary methods, following Heath-Brown in [30] (who in turn follows methods of Hooley used in an unpublished proof of Theorem 3 in [39]).

Let $g = [f/2]$. Write $n = u + p^g v$ with $1 \le u \le p^g$, $1 \le v \le p^{f-g}$. Then

$$\overline{n}^s = (\overline{u + p^g v})^s \equiv \overline{u}^s - sp^g v\overline{u}^{s+1} + \frac{s(s-1)}{2}p^{2g}v^2\overline{u}^{s+2} \pmod{p^f}.$$

For convenience let $\beta = \frac{s(s-1)}{2}$; then

$$V(p^f; m, b) = \sum_{u=1}^{p^g}\sum_{v=1}^{p^{f-g}} e\left(\frac{m\overline{u}^s + bu}{p^f}\right) e\left(\frac{p^g(bv - smv\overline{u}^{s+1} + p^g\beta mv^2\overline{u}^{s+2})}{p^f}\right),$$

so that

$$|V(p^f; m, b)| \le \sum_{u=1}^{p^g}\left|\sum_{v=1}^{p^{f-g}} e\left(\frac{(b - sm\overline{u}^{s+1})v + p^g\beta mv^2\overline{u}^{s+2}}{p^{f-g}}\right)\right|.$$

In the case $f = 2g$, the inner sum reduces to

$$\sum_{v=1}^{p^g} e\left(\frac{(b - sm\overline{u}^{s+1})v}{p^g}\right) = \begin{cases} p^g & \text{if } p^g | (b - sm\overline{u}^{s+1}) \\ 0 & \text{if } p^g \nmid (b - sm\overline{u}^{s+1}). \end{cases}$$

Therefore

$$|V(p^f; m, b)| \le p^g N_p, \tag{4.16}$$

where we define N_p by

$$N_p = \#\{u \pmod{p^g} : b \equiv sm\overline{u}^{s+1} \pmod{p^g}\}.$$

In the case $f = 2g+1$, then $1 \le v \le p^{g+1}$ so we may write $v = w + pk$ where $1 \le w \le p$ and $1 \le k \le p^g$. Then

$$|V(p^f; m, b)| \le \sum_{u=1}^{p^g}\left|\sum_{w=1}^{p} e\left(\frac{(b - sm\overline{u}^{s+1})w + p^g\beta w^2 m\overline{u}^{s+2}}{p^{g+1}}\right)\sum_{k=1}^{p^g} e\left(\frac{(b - sm\overline{u}^{s+1})k}{p^g}\right)\right|.$$

The innermost sum vanishes unless $p^g | (b - sm\overline{u}^{s+1})$, so we need only consider u such that $b - sm\overline{u}^{s+1} = p^g\theta_u$ for some θ_u. Then

$$|V(p^f; m, b)| \le p^g \sum_{\substack{u=1 \\ p^g | (b - sm\overline{u}^{s+1})}}^{p^g}\left|\sum_{w=1}^{p} e\left(\frac{\theta_u w + \beta m\overline{u}^{s+2}w^2}{p}\right)\right|.$$

Let T_p represent the bound for the absolute value of the inner sum. Then in the case $f = 2g + 1$,

$$|V(p^f; m, b)| \le p^g N_p T_p. \tag{4.17}$$

It remains to bound N_p and T_p.

Lemma 4.5. *Assume $(m, q) = 1$. For any prime divisor $p|q$,*

$$N_p = \#\{u \,(mod\, p^g) : b \equiv sm\overline{u}^{s+1} \,(mod\, p^g)\} \ll (s+1)^2.$$

Proof. First assume that $p \nmid s(s+1)$. Then $p \nmid sm\overline{u}^{s+1}$, so $N_p = 0$ unless $p \nmid b$. Then N_p is bounded above by the number of solutions of

$$f(u) = u^{s+1} - sm\overline{b} \equiv 0 \pmod{p^g}$$

with $(u, q) = 1$. The formal derivative of f is $f'(u) = (s+1)u^s$. By assumption $p \nmid (s+1)$ so the only solutions of $f'(u) \equiv 0 \pmod{p}$ are congruent to 0 modulo p. Thus $f(u)$ and $f'(u)$ share no solutions modulo p and hence $f(u)$ has exactly as many solutions modulo p^g as modulo p, hence no more than $s+1$.

If $p|s(s+1)$ then p can divide at most one of $s, s+1$. Suppose that $p|s$, $p \nmid (s+1)$. By assumption $(u, q) = 1$, so we may think of

$$N_p = \#\{u \pmod{p^g}, (u, p^g) = 1 : bu^{s+1} \equiv sm \pmod{p^g}\}.$$

Define β so that $p^\beta = (b, p^g)$. Then we must have $p^\beta | s$, or else there are no solutions. Write $b = p^\beta b_1$, $s = p^\beta s_1$ and $g_1 = g - \beta$. If $g_1 = 0$, then $N_p \leq p^g = p^\beta \leq s$. Thus suppose that $g_1 \geq 1$. Examine the congruence

$$b_1 u^{s+1} \equiv s_1 m \pmod{p^{g_1}}, \tag{4.18}$$

where $(b_1, p) = 1$. For any s_1, the solutions u of this congruence are obtained by lifting solutions of the corresponding congruence modulo p, of which there are at most $s+1$. Thus there are at most $s+1$ solutions modulo p^{g_1} to (4.18), giving $\ll p^\beta(s+1)$ total solutions modulo p^g. Thus $N_p \ll (s+1)^2$.

If $p \nmid s$ but $p|(s+1)$ then we may argue as in Lemma 3.3 to obtain the result that $N_p \ll 2(s+1) \leq (s+1)^2$. This concludes the proof. □

Lemma 4.6. *Assume $(m, q) = 1$. For any prime divisor $p|q$,*

$$T_p = \left| \sum_{w=1}^{p} e_p(\theta_u w + \beta m \overline{u}^{s+2} w^2) \right| \ll \sqrt{s(s-1)} p^{1/2}.$$

Proof. Let p be any prime with $p|q$, $p > 2$. First assume that $p \nmid s(s-1)$. Then $p \nmid \beta$ and $p \nmid m$ so we may complete the square. Then

$$T_p = \left| \sum_{w=1}^{p} e_p(\beta m \overline{u}^{s+2}(w + \overline{2\beta m} u^{s+2} \theta_u)^2) \right| \leq p^{1/2}$$

by the classical bound for Gauss sums given in Lemma 3.5.

If $p|s(s-1)$, then trivially $T_p \leq p$. But p can divide only one of s and $s-1$, so that $p \ll \sqrt{s(s-1)}$. In the case $p = 2$, we use the trivial bound

$$T_p \leq 2 \leq \sqrt{s(s-1)} p^{1/2},$$

for any $s \geq 2$. □

It follows from these two lemmas that in the case $f = 2g$, by (4.16),

$$|V(p^f; m, b)| \ll (s+1)^2 p^{f/2}.$$

In the case $f = 2g+1$, by (4.17),

$$|V(p^f; m, b)| \ll p^g (s+1)^2 \sqrt{s(s-1)} p^{1/2} \ll s^3 p^{f/2}.$$

By the multiplicativity of $V(q; m, b)$ we then have the bound:

$$|V(q; m, b)| \leq c^{\nu(q)} s^{3\nu(q)} q^{1/2},$$

for a constant c depending only on s. For convenience we will express $c^{\nu(q)} s^{3\nu(q)}$ as $d(q)^\sigma$ for a positive integer σ depending only on s, using the fact that for any positive integer q, $n^{\nu(q)} \leq d(q)^{\log n / \log 2}$. This completes the proof of Lemma 4.4.

4.6 Theorem 4.2: the mean value problem

We next consider the scenario of Theorem 4.2, in which we do not assume that q has a divisor q_0 of appropriate size. In the following discussion, all implied constants depend only on s and the variable $k \geq 1$ we introduce below.

Recall from Proposition 4.5 that

$$U(w, M, q, a, s) \ll H^{-1} \sum_{h=0}^{H-1} \left| \sum_{w < n \leq 2w} e_q(ha\overline{n}^s) \right|,$$

where $H = [(q/2)M^{-1}]$. We would like to average over h, so we need to consider a full set of residues h modulo q. Therefore we apply Hölder's inequality, whereby

$$U(w, M, q, a, s) \ll M^{\frac{1}{2k}} \left(\frac{1}{q} \sum_{h=1}^{q} \left| \sum_{w < n \leq 2w} e_q(h\overline{n}^s) \right|^{2k} \right)^{\frac{1}{2k}} \tag{4.19}$$

for any integer $k \geq 1$. We will specify k in terms of s later, but for now we proceed to examine the general case. Note that here we have assumed that $(a, q) = 1$, which we may do since we will apply the bound we derive, as in Lemma 4.2, to $U(w, xw^{-s}(a,q)^{-1}, q(a,q)^{-1}, a(a,q)^{-1}, s)$.

Definition 4.6. For a finite set of integers $\mathcal{I}$, let

$$N(\mathcal{I}) = \frac{1}{q} \sum_{h=1}^{q} \left| \sum_{n \in \mathcal{I}} e_q(h\overline{n}^s) \right|^{2k}.$$

We may then write (4.19) as

$$U(w, M, q, a, s) \ll M^{\frac{1}{2k}} N(\mathcal{I})^{\frac{1}{2k}}, \tag{4.20}$$

with the set of integers $\mathcal{I} = (w, 2w]$. (Recall that we have defined the notation $(A, B]$ to indicate the set of integers $\{A < n \leq B\}$.) It will be more convenient to work with $N(\mathcal{I})$ in the following equivalent form.

Lemma 4.7. *For a finite set of integers $\mathcal{I}$,*

$$N(\mathcal{I}) = \#\{(n_1, \ldots, n_{2k}),\ n_i \in \mathcal{I} : \sum_{i=1}^{k} \overline{n}_i^s \equiv \sum_{i=1}^{k} \overline{n}_{i+k}^s \ (mod\ q)\}.$$

Proof. Let

$$S(q, h) = \sum_{n \in \mathcal{I}} e_q(h\overline{n}^s).$$

Then

$$\begin{aligned}
N(\mathcal{I}) &= \frac{1}{q} \sum_{h=1}^{q} |S(q,h)|^{2k} \\
&= \frac{1}{q} \sum_{h=1}^{q} S(q,h)^k \overline{S(q,h)}^k \\
&= \frac{1}{q} \sum_{h=1}^{q} \sum_{n_1,\ldots,n_k \in \mathcal{I}} e_q\left(\sum_{i=1}^{k} h\overline{n}_i^s\right) \sum_{n_1,\ldots,n_k \in \mathcal{I}} e_q\left(-\sum_{j=1}^{k} h\overline{n}_j^s\right) \\
&= \sum_{n_1,\ldots,n_{2k} \in \mathcal{I}} \frac{1}{q} \sum_{h=1}^{q} e_q\left(h\left(\sum_{i=1}^{k} \overline{n_i}^s - \sum_{i=1}^{k} \overline{n}_{i+k}^s\right)\right) \\
&= \#\{(n_1, \ldots, n_{2k}), n_i \in \mathcal{I} : \sum_{i=1}^{k} \overline{n}_i^s \equiv \sum_{i=1}^{k} \overline{n}_{i+k}^s \ (\text{mod } q)\}.
\end{aligned}$$

□

4.6.1 The trivial bound for $N(\mathcal{I})$

From the expression given for $N(\mathcal{I})$ in Lemma 4.7 we can immediately obtain the following trivial bound for $N(\mathcal{I})$.

Proposition 4.8. *For the set of integers $\mathcal{I} = \{1 \leq n \leq I\}$,*

$$N(\mathcal{I}) \ll s^{\nu(q)}(I^{2k} q^{-1} + I^{2k-1}).$$

Proof. There are I^{2k-1} ways of choosing $n_1, \ldots, n_{2k-1}$. Once $n_1, \ldots, n_{2k-1}$ have been chosen, n_{2k} must be such that

$$\overline{n}_{2k}^s \equiv \sum_{i=1}^{k} \overline{n}_i^s - \sum_{i=1}^{k-1} \overline{n}_{i+k}^s \ (\text{mod } q),$$

so that there are $\ll s^{\nu(q)}$ choices for n_{2k} modulo q, and hence $\ll (Iq^{-1}+1)$ choices for $n_{2k} \in \mathcal{I}$. Thus

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1}(Iq^{-1}+1).$$

□

Using this trivial bound in (4.20) we see that

$$U(w, M, q, a, s) \ll w\left[s^{\nu(q)} M(w^{-1}+q^{-1})\right]^{\frac{1}{2k}}.$$

Dyadic summation then gives a final bound for the sum of $S(p, q, a, x, s)$:

$$\sum_{\substack{y<p\leq z \\ p\nmid q}} S(p, q, a, x, s) \ll s^{\frac{\nu(q)}{2k}} x^{\frac{1}{2k}}\left[z^{1-\frac{s}{2k}} q^{-\frac{1}{2k}} + z^{1-\frac{1}{2k}-\frac{s}{2k}}\right].$$

In order to bound this by $xq^{-1}(\log q)^{-s}$ as desired, with z as in (4.8), we would have to choose

$$x \gg q^{1+\frac{1}{s}+\epsilon}.$$

Thus this gives only the trivial bound for $n_s(a, q)$. Hence we must bound $N(\mathcal{I})$ more effectively; this is the main goal of the rest of the chapter.

4.6.2 Bounding $N(\mathcal{I})$ by averaging

We will improve on the trivial bound for $N(\mathcal{I})$ by taking advantage of averaging over h, which then allows us to average further over a set of auxiliary primes $p \nmid q$. Let $\mathcal{I} = \{1 \leq n \leq I\}$, where $I \leq q$. In the following discussion, suppose p is a prime in the range $Q < p \leq 2Q$ with $p \nmid q$. We will choose Q explicitly later, but for now we only specify $Q < I$.

Proposition 4.9.

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + \frac{1}{q}\sum_{h=1}^{q}\left|\sum_{\substack{n\in\mathcal{I} \\ p\nmid n}} e\left(\frac{h\overline{n}^s}{q}\right)\right|^{2k}.$$

Proof. It is sufficient to show that $2k$-tuples $(n_1, \ldots, n_{2k})$ with at least one n_i divisible by p contribute only a term of magnitude $s^{\nu(q)} I^{2k-1} Q^{-1}$ to $N(\mathcal{I})$. Without loss of generality, consider $2k$-tuples $(n_1, \ldots, n_{2k})$ with $p|n_1$. There are at most $Ip^{-1} < IQ^{-1}$ choices of n_1 such that $p|n_1$ and $1 \leq n_1 \leq I$. There are I^{2k-2} possible choices for $n_2, \ldots, n_{2k-1}$, and hence at most $I^{2k-1}Q^{-1}$ possible choices for $n_1, \ldots, n_{2k-1}$. These choices for $n_1, \ldots, n_{2k-1}$ determine $\ll s^{\nu(q)}$ possible choices for n_{2k} modulo q. Since $I \leq q$, these are all the choices for $n_{2k} \in \mathcal{I}$ as well. Thus in total the contribution of terms where p divides at least one entry in the $2k$-tuple $(n_1, \ldots, n_{2k})$ is $\ll s^{\nu(q)} I^{2k-1} Q^{-1}$, where the implied constant depends only on k. □

Define for each $0 < f < p$,

$$\mathcal{I}(p,f) = \left(\frac{-fq}{p}, \frac{I-fq}{p}\right].$$

Proposition 4.10.

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + Q^{2k-1} \sum_{f=1}^{p-1} N(\mathcal{I}(p,f)).$$

Proof. Examine the inner sum in Proposition 4.9 over $n \in \mathcal{I}$ such that $p \nmid n$. Since by assumption the auxiliary prime $p \nmid q$, these remaining n fall into the $p-1$ residue classes

$$n \equiv fq \pmod{p}, \quad 0 < f < p.$$

Thus

$$\left|\sum_{\substack{n\in\mathcal{I}\\ p\nmid n}} e_q(h\overline{n}^s)\right|^{2k} = \left|\sum_{f=1}^{p-1} \sum_{\substack{n\in\mathcal{I}\\ n\equiv fq \pmod p}} e_q(h\overline{n}^s)\right|^{2k}.$$

Applying Hölder's inequality,

$$\left|\sum_{\substack{n\in\mathcal{I}\\ p\nmid n}} e_q(h\overline{n}^s)\right|^{2k} \leq (p-1)^{2k-1} \sum_{f=1}^{p-1} \left|\sum_{\substack{n\in\mathcal{I}\\ n\equiv fq \pmod p}} e_q(h\overline{n}^s)\right|^{2k}.$$

Write $n = fq + p\alpha$ so that $\alpha \in \mathcal{I}(p,f)$ as defined above. Then $\overline{n} \equiv \overline{p\alpha} \pmod q$. Thus for each $f = 1, \ldots, p-1$, we have

$$\sum_{h=1}^{q} \left|\sum_{\substack{n\in\mathcal{I}\\ n\equiv fq \pmod p}} e_q(h\overline{n}^s)\right|^{2k} = \sum_{h=1}^{q} \left|\sum_{\alpha\in\mathcal{I}(p,f)} e_q(h\overline{p}^s\overline{\alpha}^s)\right|^{2k}.$$

Since $(\overline{p}^s, q) = 1$, $h\overline{p}^s$ ranges over a complete set of residues modulo q as h does, so we may write this as:

$$\sum_{h=1}^{q} \left|\sum_{\alpha\in\mathcal{I}(p,f)} e_q(h\overline{\alpha}^s)\right|^{2k}.$$

This step is critical: averaging over h has allowed us to remove the specific auxiliary prime p from the argument of the exponential.

We now have

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + (p-1)^{2k-1} \sum_{f=1}^{p-1} \frac{1}{q} \sum_{h=1}^{q} \left|\sum_{\alpha\in\mathcal{I}(p,f)} e\left(\frac{h\overline{\alpha}^s}{q}\right)\right|^{2k}.$$

Recalling that $Q < p \leq 2Q$, we may conclude

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + Q^{2k-1} \sum_{f=1}^{p-1} N(\mathcal{I}(p,f)).$$

□

4.6.3 Averaging the good set over primes

In order to bound the sum of $N(\mathcal{I}(p,f))$ over $f = 1,\dots,p-1$ appearing in Proposition 4.10, we partition all $2k$-tuples $(n_1,\dots,n_{2k})$ into two disjoint sets G and B, which we call, after Heath-Brown, the "good" set and the "bad" set. We will specify these sets later; for now, we define a version of the function $N(\mathcal{I})$ restricted to each of these sets. For notational convenience, define for a positive real number t,

$$\mathcal{I}(t) = (-qt, IQ^{-1} - qt].$$

Then $\mathcal{I}(p,f) \subseteq \mathcal{I}(f/p)$, since $p > Q$. Since $N(\mathcal{I})$ is an increasing function on the set $\mathcal{I}$, $N(\mathcal{I}(p,f)) \le N(\mathcal{I}(f/p))$.

Definition 4.7. For two disjoint sets G and B partitioning the set of all $2k$-tuples $\mathbf{n} = (n_1,\dots,n_{2k})$, define

$$\begin{aligned} N_G(t) &= \#\{\mathbf{n} \in G, n_i \in \mathcal{I}(t) : \sum_{i=1}^{k} \overline{n}_i^s \equiv \sum_{i=1}^{k} \overline{n}_{i+k}^s \pmod q\}, \\ N_B(t) &= \#\{\mathbf{n} \in B, n_i \in \mathcal{I}(t) : \sum_{i=1}^{k} \overline{n}_i^s \equiv \sum_{i=1}^{k} \overline{n}_{i+k}^s \pmod q\}. \end{aligned}$$

We will average only $N_G(t)$ over primes; the bad set B will be sufficiently small for $N_B(t)$ to admit a trivial bound.

Definition 4.8. Let

$$K = \max_t N_B(t).$$

Then for any $0 < f < p$,

$$N(\mathcal{I}(p,f)) \le N(\mathcal{I}(f/p)) = N_B(f/p) + N_G(f/p) \le K + N_G(f/p).$$

Thus from Proposition 4.10,

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + Q^{2k} K + Q^{2k-1} \sum_{f=1}^{p-1} N_G\left(\frac{f}{p}\right).$$

We now proceed to average over all $p \nmid q$ with $Q < p \le 2Q$.

Proposition 4.11. *Assume $Q \ge c \log q$ for a constant c. Then*

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + Q^{2k} K + Q^{2k-2} (\log Q) \sum_{\substack{Q < p \le 2Q \\ p \nmid q}} \sum_{f=1}^{p-1} N_G\left(\frac{f}{p}\right).$$

Proof. By the prime number theorem, the number of primes p in the range $Q < p \le 2Q$ is $\gg Q(\log Q)^{-1}$. Since

$$\nu(q) = O\left(\frac{\log q}{\log\log q}\right)$$

(see for example Section 22.10 of [24]), we see that $O(\log q/\log\log q)$ of the primes $Q < p \le 2Q$ are factors of q. Suppose we impose the condition

$$Q \ge c \log q$$

for some constant c. Then under this condition, the number of primes p with $Q < p \le 2Q$ and $p \nmid q$ is $\gg Q(\log Q)^{-1}$. Averaging $N(\mathcal{I})$ over these primes, we obtain the result. □

We next focus on bounding the sum of $N_G(f/p)$ over $f = 1, \dots, p-1$. It is convenient to define

$$J\left(\frac{f}{p}\right) = \frac{fq}{p},$$

and

$$\mathcal{I}'(t) = (-qt, 2IQ^{-1} - qt].$$

We also define $N'_G(t)$ in a manner analogous to $N_G(t)$:

Definition 4.9. Let

$$N'_G(t) = \#\{\mathbf{n} \in G, n_i \in \mathcal{I}'(t) : \sum_{i=1}^{k} \overline{n}_i^s \equiv \sum_{i=1}^{k} \overline{n}_{i+k}^s \pmod q\}.$$

N_G and N'_G are related by the following inequality.

Proposition 4.12.

$$N_G\left(\frac{f}{p}\right) \le QI^{-1} \sum_{0 \le j \le IQ^{-1}} N'_G\left(\frac{j + J\left(\frac{f}{p}\right)}{q}\right).$$

Proof. First note that

$$\mathcal{I}(t) \subseteq \mathcal{I}'\left(t + \frac{j}{q}\right)$$

for any integer $0 \le j \le IQ^{-1}$, since

$$(-qt, IQ^{-1} - qt] \subseteq (-qt - j, IQ^{-1} - qt + (IQ^{-1} - j)] \subseteq (-qt - j, 2IQ^{-1} - qt - j].$$

Thus for each $f = 1, \dots, p-1$,

$$\mathcal{I}\left(\frac{f}{p}\right) \subseteq \mathcal{I}'\left(\frac{f}{p} + \frac{j}{q}\right) \subseteq \mathcal{I}'\left(\frac{j + J(f/p)}{q}\right).$$

Then since N increases as a function of the interval,

$$N_G\left(\frac{f}{p}\right) \le N'_G\left(\frac{j + J\left(\frac{f}{p}\right)}{q}\right)$$

for any integer $0 \le j \le IQ^{-1}$. Averaging over j we obtain the desired result,

$$N_G\left(\frac{f}{p}\right) \le QI^{-1} \sum_{0 \le j \le IQ^{-1}} N'_G\left(\frac{j + J\left(\frac{f}{p}\right)}{q}\right).$$

□

We next express the sum of N_G averaged over p and f given in Proposition 4.11 in terms of N'_G.

Proposition 4.13. *Assume that* $8IQ \le q$. *Then*

$$\sum_{p,f} N_G\left(\frac{f}{p}\right) \le QI^{-1} \sum_{j=0}^{2q-1} N'_G\left(\frac{j}{q}\right),$$

where the sum on the left hand side is over all primes $Q < p \le 2Q$, $p \nmid q$, *and* $0 < f < p$.

Proof. This results from the following two facts. First observe that if either $p \ne p'$ or $f \ne f'$, or both, then

$$\left|J\left(\frac{f}{p}\right) - J\left(\frac{f'}{p'}\right)\right| = \left|\frac{fq}{p} - \frac{f'q}{p'}\right| = q\left|\frac{fp' - f'p}{pp'}\right| \ge \frac{q}{pp'} \ge \frac{q}{4Q^2} \ge \frac{2I}{Q},$$

assuming that $8IQ \le q$. Thus if $p \ne p'$ or $f \ne f'$ then $\mathcal{I}'(j + J(f/p))$ and $\mathcal{I}'(j + J(f'/p'))$ are intervals of length $2IQ^{-1}$ (with open left endpoint) shifted away from each other by at least $2IQ^{-1}$, and hence they are disjoint. Secondly, for any integer $0 \le j \le IQ^{-1}$,

$$0 \le j + J\left(\frac{f}{p}\right) \le IQ^{-1} + \frac{fq}{p} < 2q$$

since $0 < f < p$ and $I \le q$. Thus all possible values of $j + J(f/p)$ are within the range $[0, 2q)$, and the result follows. □

For a fixed integer $0 \le j \le 2q - 1$, $N'_G(j/q)$ is the number of solutions to the congruence

$$\sum_{i=1}^{k} \overline{n}_i^s \equiv \sum_{i=1}^{k} \overline{n}_{i+k}^s \pmod q,$$

with $(n_1, \dots, n_{2k}) \in G$, where $n_i \in \mathcal{I}'(j/q) = (-j, 2IQ^{-1} - j]$. Making the change of variables $n_i \mapsto n_i - j$, we can equivalently consider $N'_G(j/q)$ as the number of solutions to the congruence

$$\sum_{i=1}^{k} (\overline{n_i - j})^s \equiv \sum_{i=1}^{k} (\overline{n_{i+k} - j})^s \pmod q, \tag{4.21}$$

with $(n_1 - j, \dots, n_{2k} - j) \in G$, where $n_i \in (0, 2IQ^{-1}]$. Note that the congruence (4.21) is identical for $0 \le j, j' < 2q$ if $j \equiv j' \pmod q$. Thus it suffices to consider values $0 \le j < q$. Therefore we define:

Definition 4.10. Let L denote the number of solutions to the congruence

$$\sum_{i=1}^{k}(\overline{n_i - j})^s \equiv \sum_{i=1}^{k}(\overline{n_{i+k} - j})^s \pmod{q},$$

where $0 \leq j < q$ and $(n_1 - j, \ldots, n_{2k} - j) \in G$ with $0 < n_i \leq 2IQ^{-1}$.

It follows immediately that:

Proposition 4.14.

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + Q^{2k} K + Q^{2k-1} I^{-1} (\log Q) L.$$

We have now bounded $N(\mathcal{I})$ in terms of L and K, where these are defined in terms of the good and bad sets G and B. In the following section we proceed to estimate L and K individually; in the process of doing so it becomes clear how the sets G and B should be defined.

4.7 Estimating L and K for q square-free

Decompose L as

$$L = \sum_{\mathbf{n} \in G} L(\mathbf{n}; q),$$

where $L(\mathbf{n}; q)$ is the number of solutions $0 \leq j < q$ of the congruence (4.21) for a fixed $2k$-tuple $\mathbf{n}$. Then $L(\mathbf{n}; q)$ is multiplicative with respect to q, so that for $q = \prod p^f$,

$$L(\mathbf{n}; q) = \prod L(\mathbf{n}; p^f).$$

The methods for bounding $L(\mathbf{n}; p^f)$ we present here are only effective if $f = 1$; therefore from this point onward we assume that q is square-free.

We first show that if we assume certain restrictions on the elements n_i, we may bound $L(\mathbf{n}; p)$ by a constant independent of p.

Lemma 4.8. *Suppose $\exists i \leq k$ such that for all $h = k+1, \ldots, 2k$, we have $n_i \not\equiv n_h \pmod{p}$. Then*

$$L(\mathbf{n}; p) \leq s(2k-1) - 1.$$

Proof. Consider the congruence

$$\sum_{i=1}^{k}(\overline{n_i - j})^s \equiv \sum_{i=1}^{k}(\overline{n_{i+k} - j})^s \pmod{p}. \tag{4.22}$$

We may relabel the k-tuple $(n_1, \ldots, n_k)$ so that $n_1 \not\equiv n_h \pmod{p}$ for each $h = k+1, \ldots, 2k$. Furthermore, label any of $n_2, \ldots, n_k$ that are congruent to n_1 modulo p so that they are the first elements following n_1 in the k-tuple

$(n_1, \ldots, n_k)$. Suppose there are a total of k_0 elements congruent to n_1 modulo p, including n_1. Then we may write the congruence (4.22) as

$$k_0(\overline{n_1 - j})^s + \sum_{i=k_0+1}^{k} (\overline{n_i - j})^s \equiv \sum_{i=1}^{k} (\overline{n_{i+k} - j})^s \pmod{p}$$

where $1 \leq k_0 \leq k$. Let $l = n_1 - j$. Then this becomes

$$k_0\bar{l}^s + \sum_{i=k_0+1}^{k} (\overline{n_i - n_1 + l})^s \equiv \sum_{i=1}^{k} (\overline{n_{i+k} - n_1 + l})^s \pmod{p}. \tag{4.23}$$

Define $m_i = n_i - n_1$ for each $i = k_0 + 1, \ldots, 2k$. Note that in each case $m_i \not\equiv 0 \pmod{p}$ since we have ordered $n_1, \ldots, n_{2k}$ so that $n_i \not\equiv n_1$ for all $i = k_0 + 1, \ldots, 2k$. Define

$$m = \prod_{j=k_0+1}^{2k} m_j,$$

so that $p \nmid m$. Now multiply the congruence (4.23) by

$$l^s \prod_{j=k_0+1}^{2k} (m_j + l)^s$$

to obtain

$$k_0 \prod_{j=k_0+1}^{2k} (m_j + l)^s \quad + \quad l^s \sum_{i=k_0+1}^{k} \overline{(m_i + l)}^s \prod_{j=k_0+1}^{2k} (m_j + l)^s$$
$$- \; l^s \sum_{i=k+1}^{2k} \overline{(m_i + l)}^s \prod_{j=k_0+1}^{2k} (m_j + l)^s \equiv 0 \pmod{p}.$$

Note that in each of the two sums, for each i the term $\overline{(m_i + l)}^s$ cancels with one of the factors $(m_j + l)^s$ in the product. In effect, we have rid the congruence of denominators, so it is now a polynomial in l. Moreover, note that all the highest order terms (of degree $s(2k - k_0)$) cancel exactly, so the degree of the polynomial is in fact at most $s(2k - k_0) - 1$. For $1 \leq k_0 \leq k$, this means that we have a polynomial in l of degree at most $s(2k-1) - 1$. The constant term of the polynomial is $k_0 m^s$. Since $p \nmid m$, this term can only vanish if $p | k_0$, in which case we must have $p \leq k_0 \leq k$.

First suppose that $p > k$. Then the constant term does not vanish, so the polynomial is not identically zero, and hence it can have at most $s(2k-1) - 1$ roots. Since $l = n_1 - j$, each root l is in one-to-one correspondence with a solution j of the original congruence defining $L(\mathbf{n}; p)$, hence

$$L(\mathbf{n}; p) \leq s(2k - 1) - 1.$$

Next suppose that $p \leq k$. Then trivially $p \leq s(2k-1)-1$ for $s \geq 2,\ k \geq 2$. Of course a congruence modulo p can have at most p solutions, so again

$$L(\mathbf{n}; p) \leq s(2k-1) - 1.$$

This completes the proof of the lemma. □

4.7.1 The good and bad sets

We use the key assumption that enabled us to prove Lemma 4.8 to define the sets G and B.

Definition 4.11. Define

$$\begin{aligned} B &= \{\mathbf{n} : \forall i \leq k\ \exists h > k \text{ s.t. } n_i = n_h\} \\ G &= \{\mathbf{n} \notin B\}. \end{aligned}$$

A bound for K follows immediately.

Proposition 4.15.

$$K = \max_t N_B(t) \ll (IQ^{-1})^k.$$

Proof. Consider an element $\mathbf{n} \in B$. There are IQ^{-1} ways to choose each of the entries $n_h \in \mathcal{I}(t) = (-qt, IQ^{-1} - qt]$ for $h = k+1, \ldots, 2k$. Then each of the entries n_i for $i = 1, \ldots, k$ must be chosen from these k possible values. Hence

$$N_B(t) \leq k^k (IQ^{-1})^k.$$

This bound is independent of t, so the result follows, with an implicit constant dependent on k. □

Consider the set G. For each $i = 1, \ldots, k$, define

$$A_i(\mathbf{n}) = \prod_{h=k+1}^{2k} (n_i - n_h).$$

If $\mathbf{n} = (n_1, \ldots, n_{2k}) \in G$ then for some $i \leq k$ we have $A_i(\mathbf{n}) \neq 0$. Let

$$G_i = \{\mathbf{n} : A_i(\mathbf{n}) \neq 0\},$$

so that

$$G = \bigcup_{i=1}^{k} G_i.$$

Proposition 4.16. *For* $\mathbf{n} \in G_i$,

$$L(\mathbf{n}; p) \leq d_{s(2k-1)-1}(p) \cdot (p, A_i(\mathbf{n})).$$

Proof. If $p \nmid A_i(\mathbf{n})$ then there exists $k < h \leq 2k$ such that $n_i \not\equiv n_h \pmod{p}$, so by Lemma 4.8,

$$L(\mathbf{n}; p) \leq s(2k-1) - 1.$$

If $p | A_i(\mathbf{n})$ then trivially

$$L(\mathbf{n}; p) \leq (p, A_i(\mathbf{n})).$$

Thus, regardless of whether p divides $A_i(\mathbf{n})$ or not,

$$L(\mathbf{n}; p) \leq d_{s(2k-1)-1}(p) \cdot (p, A_i(\mathbf{n})).$$

□

It follows immediately that for square-free q,

$$\begin{aligned} L &= \sum_{\mathbf{n} \in G} L(\mathbf{n}; q) \\ &\leq \sum_{i=1}^{k} \sum_{\mathbf{n} \in G_i} L(\mathbf{n}; q) \\ &= \sum_{i=1}^{k} \sum_{\mathbf{n} \in G_i} \prod_{p|q} L(\mathbf{n}; p) \\ &\ll \sum_{i=1}^{k} d_{s(2k-1)-1}(q) \sum_{\mathbf{n} \in G_i} (q, A_i(\mathbf{n})). \end{aligned} \tag{4.24}$$

We bound the innermost sum by the following argument, as in Lemma 2 of [28].

Proposition 4.17. *For each $1 \leq i \leq k$,*

$$\sum_{\mathbf{n} \in G_i} (q, A_i(\mathbf{n})) \ll d(q)^k (IQ^{-1})^{2k}.$$

Proof. Without loss of generality, let $i = 1$. Since $\mathbf{n} \in G_1$, then $A_1(\mathbf{n}) \neq 0$. Let $\alpha_j = (q, n_1 - n_j)$ for each $j = k+1, \ldots, 2k$, so that

$$(q, A_1(\mathbf{n})) = \left(q, \prod \alpha_j\right).$$

Then,

$$\sum_{\mathbf{n} \in G_1} (q, A_1(\mathbf{n})) \leq \sum_{\alpha_j | q} \prod \alpha_j \sum_{\substack{\mathbf{n} \\ \alpha_j | (n_1 - n_j)}} 1.$$

Since $A_1(\mathbf{n}) \neq 0$ then $n_j \neq n_1$ for all $j = k+1, \ldots, 2k$. So for a fixed value of n_1, of which there are $2IQ^{-1}$ possible choices, the conditions $0 < n_j \leq 2IQ^{-1}$ and $\alpha_j | (n_1 - n_j)$ give $\ll 2IQ^{-1}\alpha_j^{-1}$ choices for each n_j, since we are assuming $n_j \neq n_1$. Thus

$$\sum_{\mathbf{n} \in G_1} (q, A_1(\mathbf{n})) \ll \sum_{\alpha_j | q} \prod \alpha_j \cdot (2IQ^{-1}) \left(\prod_{j=k+1}^{2k} \left(\frac{2IQ^{-1}}{\alpha_j} \right) \right) (2IQ^{-1})^{k-1}.$$

The last factor of $(2IQ^{-1})^{k-1}$ accounts for all possible combinations of n_h, with $1 < h \leq k$. Therefore

$$\begin{aligned}\sum_{\mathbf{n}\in G_1}(q, A_1(\mathbf{n})) &\ll (IQ^{-1})^{2k} \sum_{\substack{\alpha_j \mid q \\ j=k+1,\ldots,2k}} 1 \\ &\ll d(q)^k (IQ^{-1})^{2k}.\end{aligned}$$

□

Applying this result in (4.24) immediately gives the final bound for L:

Proposition 4.18.

$$L \ll d(q)^{\tau_{s,k}}(IQ^{-1})^{2k},$$

where $\tau_{s,k} = (2s+1)k - (s+1)$.

We conclude this section with a proposition combining all these results into our final bound for $N(\mathcal{I})$.

Proposition 4.19. *Assume q is square-free. Let $\mathcal{I} = \{1 \leq n \leq I\}$ where $I \leq q^{\frac{k+1}{2k}}$. Choose $Q = \frac{1}{8}I^{\frac{k-1}{k+1}}$. Then for any $k \geq 2$,*

$$N(\mathcal{I}) \ll d(q)^{\tau_{s,k}}(\log q) I^{\frac{2k^2}{k+1}},$$

where the implied constant depends only on s and k.

Proof. By the bounds for K and L given in Propositions 4.15 and 4.18,

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{2k-1} Q^{-1} + Q^{2k}(IQ^{-1})^k + Q^{2k-1} I^{-1} (\log Q) d(q)^{\tau_{s,k}} (IQ^{-1})^{2k},$$

assuming that

$$\begin{aligned} c \log q &\leq Q < I \leq q, \\ 8IQ &\leq q. \end{aligned}$$

These conditions are satisfied with I and Q as chosen in the hypothesis. Thus

$$N(\mathcal{I}) \ll s^{\nu(q)} I^{\frac{2k^2}{k+1}} + I^{\frac{2k^2}{k+1}} + d(q)^{\tau_{s,k}} I^{\frac{2k^2}{k+1}} \log q.$$

Note that for square-free q, $s^{\nu(q)} = d(q)^{\frac{\log s}{\log 2}} \ll d(q)^{\tau_{s,k}}$. We may conclude that

$$N(\mathcal{I}) \ll d(q)^{\tau_{s,k}}(\log q) I^{\frac{2k^2}{k+1}}.$$

□

4.8 Proof of Theorem 4.2

In order to complete the proof of Theorem 4.2, it remains only to bound the sum

$$\sum_{\substack{y<p\leq z\\ p\nmid q}} S(p,q,a,x,s).$$

Recall from Lemma 4.2 that

$$\sum_{\substack{w<p\leq 2w\\ p\nmid q}} S(p,q,a,x,s) \leq U(w, xw^{-s}(a,q)^{-1}, q(a,q)^{-1}, a(a,q)^{-1}, s).$$

From (4.20),

$$U(w,M,q,a) \ll M^{\frac{1}{2k}} N(\mathcal{I})^{\frac{1}{2k}},$$

where $\mathcal{I} = \{w < n \leq 2w\}$. Since $N(\mathcal{I})$ increases as a function of the interval, we may instead take $\mathcal{I} = \{1 \leq n \leq 2w\}$ and apply the bound for $N(\mathcal{I})$ given in Proposition 4.19, simply including any resulting factors of 2 in the implied constant. We obtain

$$\begin{aligned} &U(w, xw^{-s}(a,q)^{-1}, q(a,q)^{-1}, a(a,q)^{-1}, s) \\ &\qquad \ll (xw^{-s}(a,q)^{-1})^{\frac{1}{2k}} \left[d(q)^{\tau_{s,k}} (\log q) w^{\frac{2k^2}{k+1}} \right]^{\frac{1}{2k}}. \end{aligned} \tag{4.25}$$

Let J be the least integer such that $J \geq (\log z - \log y)/\log 2$. Then

$$\begin{aligned} \sum_{\substack{y<p\leq z\\ p\nmid q}} S(p,q,a,x,s) &\leq \sum_{j=0}^{J-1} \sum_{\substack{w<p\leq 2w,\ p\nmid q\\ w=2^j y}} S(p,q,a,x,s) \\ &\ll \sum_{j=0}^{J-1} U(2^j y, x(2^j y)^{-s}(a,q)^{-1}, q(a,q)^{-1}, a(a,q)^{-1}, s) \\ &\ll \sum_{j=0}^{J-1} (x(2^j y)^{-s}(a,q)^{-1})^{\frac{1}{2k}} \left[d(q)^{\tau_{s,k}} (\log q) (2^j y)^{\frac{2k^2}{k+1}} \right]^{\frac{1}{2k}} \\ &\ll x^{\frac{1}{2k}} (a,q)^{-\frac{1}{2k}} d(q)^{\frac{\tau_{s,k}}{2k}} (\log q)^{\frac{1}{2k}} \sum_{j=0}^{J-1} (2^j y)^{\frac{k}{k+1}-\frac{s}{2k}} \qquad (4.26) \\ &\ll x^{\frac{1}{2k}} z^{\frac{k}{k+1}-\frac{s}{2k}} (a,q)^{-\frac{1}{2k}} d(q)^{\frac{\tau_{s,k}}{2k}} (\log q)^{\frac{1}{2k}}. \qquad (4.27) \end{aligned}$$

Note that in applying the bound (4.25) we must have $I = 2w = 2^{j+1}y \leq q^{\frac{k+1}{2k}}$ in each case, so in particular we must have $2^J y \approx z \leq q^{\frac{k+1}{2k}}$, which is always satisfied for z as in (4.8).

To obtain a nontrivial bound it is sufficient[1] to choose $k = s$. Then

$$\sum_{\substack{y<p\le z\\ p\nmid q}} S(p,q,a,x,s) \ll x^{\frac{1}{2s}} z^{\frac{s-1}{2(s+1)}} (a,q)^{-\frac{1}{2s}} (\log q)^{\frac{1}{2s}} d(q)^{\frac{2s^2-1}{2s}}.$$

Recall from (4.8) that

$$z = \min(2x^{\frac{1}{s}}(a,q)^{-\frac{1}{s}}, s^{\frac{\nu(q)}{s}}(\log q)(x^{\frac{1}{s^2}} + q^{\frac{1}{s}}(a,q)^{-\frac{1}{s}})).$$

Then

$$\sum_{\substack{y<p\le z\\ p\nmid q}} S(p,q,a,x,s) \ll x^{\frac{1}{2s}} (\log q)^{\frac{s^2+1}{2s(s+1)}} d(q)^{\frac{2s^2-1}{2s}} s^{\frac{\nu(q)(s-1)}{2s(s+1)}} \left[x^{\frac{s-1}{2s^2(s+1)}} + q^{\frac{s-1}{2s(s+1)}}\right].$$

Recalling $x \le q^2$ and approximating

$$s^{\frac{\nu(q)(s-1)}{2s(s+1)}} \le d(q)^{\frac{s-1}{s+1}},$$

we then obtain

$$\sum_{\substack{y<p\le z\\ p\nmid q}} S(p,q,a,x,s) \ll x^{\frac{1}{2s}} (\log q)^{\frac{s^2+1}{2s(s+1)}} d(q)^{\frac{2s^3+4s^2-3s-1}{2s(s+1)}} q^{\frac{s-1}{2s(s+1)}},$$

where the implied constant depends only upon s.

In order that this sum may be bounded by $xq^{-1}(\log q)^{-s}$, it is sufficient to choose x such that

$$x \gg (\log q)^{\frac{2s^3+3s^2+1}{(2s-1)(s+1)}} d(q)^{\frac{2s^3+4s^2-3s-1}{(2s-1)(s+1)}} q^{\frac{2s^2+3s-1}{(2s-1)(s+1)}}.$$

This then gives the result of Theorem 4.2:

$$n_s(a,q) \ll q^{\frac{2s^2+3s-1}{(2s-1)(s+1)}+\epsilon} = q^{1+\frac{1}{s}\left(\frac{2s^2}{2s^2+s-1}\right)+\epsilon}. \tag{4.28}$$

In fact, if we expand the exponent of q in (4.28), we obtain a main term of

$$q^{1+\frac{1}{s}-\frac{1}{2s^2}+\frac{3}{4s^3}-\frac{5}{8s^4}+\cdots}.$$

Thus it is clear that the improvement over the trivial bound comes from the higher order terms in the expansion of the exponent. This completes the discussion of Theorem 4.2.

[1] In fact, the optimal choice is approximately $k \approx s/2$ for sufficiently large s. This can be seen by noting that in order for (4.27) to be bounded above by $xq^{-1}(\log q)^{-s}$, we must choose

$$x \gg q^{1+\frac{1}{s}\left(\frac{2k^2}{2k^2+k-1}\right)+\epsilon}.$$

The exponent gives the trivial bound for $k = 1$, decreases for several small values of $k > 1$, and then increases to 1 with large k. We would thus in general choose the smallest k such that the exponent of $2^j y$ in (4.26) is positive.

Chapter 5

Solutions to a congruence

5.1 Introduction

Consider the congruence

$$x^a \equiv y^b \pmod{q} \tag{5.1}$$

where q is a square-free positive integer and a and b are nonzero integers.[1] Let $N_q(X,Y)$ denote the number of positive integer solutions (x,y) to this congruence with $(x,q)=1$, $(y,q)=1$, in the bounded region $x \leq X$ and $y \leq Y$, where $X,Y \geq 1$.

Given y with $(y,q)=1$, there are $O(|a|^{\nu(q)})$ solutions x modulo q to (5.1). Thus there are $O(|a|^{\nu(q)}(Xq^{-1}+1))$ solutions $x \leq X$. Alternatively, given x with $(x,q)=1$, there are $O(|b|^{\nu(q)}(Yq^{-1}+1))$ solutions $y \leq Y$. Thus in total

$$N_q(X,Y) = O(q^{\epsilon}(XYq^{-1} + \min(X,Y))).$$

We will refer to this as the trivial bound. In particular, if $X,Y \leq q$ then the trivial bound is

$$N_q(X,Y) = O(q^{\epsilon}\min(X,Y)).$$

One could hope to improve on this trivial bound when $X,Y \leq q$ by showing either of the following bounds:

Bound 1.

$$N_q(X,Y) = o(q^{\epsilon}\min(X,Y)).$$

Bound 2.

$$N_q(X,Y) = O(XYq^{-1+\epsilon}).$$

[1] Recall that if $a<0$, then n^a denotes $\overline{n}^{|a|}$.

Note that Bound 2 implies Bound 1. In this chapter we extend the methods presented in Chapter 4 to prove two bounds for $N_q(X,Y)$, each of which is better than the trivial bound, for X and Y in certain ranges.

While $N_q(X,Y)$ is interesting in its own right, in the next chapter we demonstrate that our bounds for $N_q(X,Y)$ give nontrivial bounds for the 3-part of class numbers of quadratic fields. With this application in mind, we restrict our attention to square-free moduli q.

5.2 Statement of the Theorems

In this chapter we prove the following theorems.

Theorem 5.1. *Let q be square-free and let a, b be nonzero integers such that $(a,b) = 1$ and $a \neq b$. If $X \leq q$ and $Y \leq q/2$ then*

$$N_q(X,Y) \ll q^{1/2} d(q)^\tau (\log q)^2 + q^{-1} XY d(q)^\tau + q^{-1/2} X d(q)^\tau,$$

where τ and the implied constant depend on a, b.

Suppose $X = q^\alpha$ and $Y = q^\beta$, with $\alpha, \beta \leq 1$. Then Theorem 5.1 achieves the trivial bound $O(q^\epsilon \min(X,Y))$, disregarding comparison of factors of size q^ϵ, as long as $1/2 \leq \alpha, \beta \leq 1$. Theorem 5.1 achieves Bound 1 whenever both $1/2 < \alpha < 1$ and $1/2 < \beta < 1$. Theorem 5.1 achieves Bound 2 whenever $\alpha + \beta \geq 3/2$.[2,3]

Theorem 5.2. *Let q be square-free and let a, b be nonzero integers such that $a/b \notin \mathbb{Z}^+$ and $(b,q) = 1$. Let $k \geq 1$ be any integer. If $X \leq q^{\frac{k+1}{2k}}$ and $Y \leq q/2$, then*

$$N_q(X,Y) \ll X^{\frac{k}{k+1}} Y^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}}$$

where τ_k and the implied constant depend on a, b, k.

Note that it is advantageous to choose X to be the smaller of the two ranges; suppose that $X = q^\alpha$ and $Y = q^\beta$ with $\alpha \leq \beta \leq 1$. Theorem 5.2 achieves Bound 1 if and only if

$$\frac{\beta}{\alpha} < \frac{2k}{k+1}$$

for some $k \geq 1$, and Bound 2 if and only if

$$\frac{\alpha k}{k+1} + \frac{\beta}{2k} \leq \alpha + \beta - 1$$

[2] In fact, a result similar to that of Theorem 5.1 holds whenever $a \neq b$, without assuming relative primality of a and b. The proof is more complicated in this more general case, and since Theorem 5.1 is more than sufficient for our purposes, we only consider the case $(a,b) = 1$.

[3] Note that we must exclude the case $a = b = 1$. In this case $N_q(X,Y)$ can attain the trivial bound, $N_q(X,Y) \gg q^\epsilon \min(X,Y)$; for example if q is a large prime.

for some $k \geq 1$. However, in applications it is more convenient simply to apply Theorem 5.2 for specific values α and β and then optimise the value of k accordingly.

If both a and b are positive integers, we may define $N'_q(X,Y)$ to be the number of positive integer solutions (x,y) to (5.1) in the bounded region $x \leq X$ and $y \leq Y$, without assuming the relative primality conditions $(x,q) = 1$ and $(y,q) = 1$. Then the following equivalent results hold for $N'_q(X,Y)$, which we state here for use in the next chapter.

Theorem 5.3. *Let q be square-free and let a, b be positive integers such that $(a,b) = 1$ and $a \neq b$. If $X \leq q$ and $Y \leq q/2$ then*

$$N'_q(X,Y) \ll q^{1/2} d(q)^\tau (\log q)^2 + q^{-1} XY d(q)^\tau + q^{-1/2} X d(q)^\tau,$$

where τ and the implied constant depend on a, b.

Theorem 5.4. *Let q be square-free and let a, b be positive integers such that $a/b \notin \mathbb{Z}^+$ and $(b,q) = 1$. Let $k \geq 1$ be an integer. If $X \leq q^{\frac{k+1}{2k}}$ and $Y \leq q/2$, then*

$$N'_q(X,Y) \ll X^{\frac{k}{k+1}} Y^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}}$$

where τ_k and the implied constant depend on a, b, k.

Theorems 5.3 and 5.4 are proved in the same manner as Theorems 5.1 and 5.2, with only minor modifications. Thus we will only give the proof in the case when we assume $(x,q) = 1$, $(y,q) = 1$.

We prove Theorem 5.1 in Section 5.3, using the Weil bound for certain key exponential sums, in a straightforward extension of the methods of Theorem 4.1. In Section 5.4 we describe the mean value methods we use to prove Theorem 5.2. While this approach is based on the methods of Theorem 4.2, which in turn are based on the methods of Heath-Brown [30], the proof is significantly more involved. In particular we must choose our averaging set of auxiliary primes more carefully. Moreover, in Section 5.5 we must handle the vanishing of two polynomials $H_\alpha(\mathbf{n}, j)$ and $\bar{H}_\alpha(\mathbf{n}, j)$ over $\mathbb{C}$ and modulo primes with some delicacy. This is the most novel feature of the work in this chapter.

5.3 Theorem 5.1: the Weil bound

Note that we may reduce the problem to considering a to be a nonzero integer and b a positive integer. We always require that $(x,q) = (y,q) = 1$. Thus if both $a < 0, b < 0$, solutions (x,y) of the congruence (5.1), which may be written as

$$\overline{x}^{|a|} \equiv \overline{y}^{|b|} \pmod{q},$$

are equivalent to solutions of the congruence

$$x^{|a|} \equiv y^{|b|} \pmod{q}.$$

If $a > 0, b < 0$, then solutions of the congruence (5.1), which may be written as

$$x^a \equiv \overline{y}^{|b|} \pmod{q},$$

are equivalent to solutions of the congruence

$$\overline{x}^a \equiv y^{|b|} \pmod{q}.$$

Thus from this point onward we restrict the integer $b \geq 1$ while a may be any nonzero integer with $(a, b) = 1$.

We begin by breaking the range $x \leq X$ into dyadic ranges $w < n \leq 2w$ and counting solutions within these partial ranges.

Definition 5.1. Let

$$U(w, M, q) = \sum_{\substack{w<n\leq 2w \\ (n,q)=1}} \#\{m \leq M : m^b \equiv n^a \pmod{q}\},$$

where $M \leq q/2$.

In order to express $U(w, M, q)$ more conveniently as an exponential sum, define for each $(n, q) = 1$,

$$\delta(n) = \sum_{\substack{m \pmod q \\ m^b \equiv n^a \pmod q}} \delta_1\left(\frac{m}{q}\right),$$

where

$$\delta_1(x) = \begin{cases} 1 & \text{if } \|x\| \leq Mq^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\delta(n) = \#\{m \pmod q : m^b \equiv n^a \pmod q,\ \|m/q\| \leq M/q\},$$

so that $\delta(n)$ counts m with $1 \leq m \leq M$, as well as m with $0 \leq (q - m) \leq M$. Thus we have the inequality

$$U(w, M, q) \leq \sum_{\substack{w<n\leq 2w \\ (n,q)=1}} \delta(n).$$

Define as before,

$$\delta_2(x) = \left(\frac{\sin(\pi H x)}{H \sin(\pi x)}\right)^2 = \left|\sum_{h=1}^{H} e(hx)\right|^2 = H^{-2} \sum_{|h|<H} (H - |h|)e(hx),$$

with $H = [(q/2)M^{-1}]$. By Lemma 4.3,

$$\delta_1\left(\frac{m}{q}\right) \ll \delta_2\left(\frac{m}{q}\right).$$

This immediately gives:

Proposition 5.1.

$$U(w,M,q) \ll H^{-1}\sum_{h=0}^{H-1}\left|\sum_{\substack{w<n\leq 2w\\(n,q)=1}}\sum_{\substack{m \pmod q\\ m^b\equiv n^a \pmod q}} e_q(hm)\right|.$$

We investigate the inner sum over n. We may extend this to a sum over a complete set of residues mod q as follows:

$$\begin{aligned}
&\sum_{\substack{w<n\leq 2w\\(n,q)=1}}\sum_{\substack{m \pmod q\\ m^b\equiv n^a \pmod q}} e_q(hm)\\
&\quad= \sum_{\substack{k \pmod q\\(k,q)=1}}\sum_{w<n\leq 2w}\frac{1}{q}\sum_{l=1}^{q} e_q(l(k-n))\sum_{\substack{m \pmod q\\ m^b\equiv k^a \pmod q}} e_q(hm)\\
&\quad= \frac{1}{q}\sum_{l=1}^{q}\sum_{w<n\leq 2w} e_q(-ln)\sum_{\substack{k,\,m \pmod q\\ m^b\equiv k^a \pmod q\\(k,q)=1}} e_q(hm+lk).
\end{aligned}$$

As in Lemma 3.4, let $A(q;w,-l)$ be the sum

$$A(q;w,-l) = \sum_{w<n\leq 2w} e_q(-ln),$$

so that

$$|A(q;w,-l)| \leq \min(w, \|l/q\|^{-1}).$$

Definition 5.2. Let

$$V(q;h,l) = \sum_{\substack{k,\,m \pmod q\\ m^b\equiv k^a \pmod q\\(k,q)=1}} e_q(hm+lk).$$

Then

$$U(w,M,q) \ll H^{-1}q^{-1}\sum_{h=0}^{H-1}\sum_{l=1}^{q}|V(q;h,l)||A(q;w,-l)|. \tag{5.2}$$

5.3.1 Bounding the sum $V(q;h,l)$

By Lemma 3.10, $V(q;h,l)$ is multiplicative in the sense that

$$V(q_1q_2;h,l) = V(q_1;h\overline{q_2},l\overline{q_2})V(q_2;h\overline{q_1},l\overline{q_1})$$

for $(q_1,q_2)=1$, where $q_1\overline{q_1}\equiv 1 \pmod{q_2}$ and $q_2\overline{q_2}\equiv 1 \pmod{q_1}$.

Lemma 5.1. *For q square-free and (a,b)=1 with $a \neq b$,*

$$|V(q;h,l)| \leq \eta_{a,b}^{\nu(q)} q^{1/2} (q,h,l)^{1/2},$$

where $\eta_{a,b} = 2(|a|+b)$.

Proof. Since q is square-free we need only consider $V(p;h,l)$ for each prime $p|q$:

$$V(p;h,l) = \sum_{\substack{m,\ k \pmod p \\ m^b \equiv k^a \pmod p \\ (k,p)=1}} e_p(hm+lk).$$

Suppose first that $p \nmid hl$. Since $(a,b)=1$, there exist integers r,s such that

$$ar + bs = 1.$$

For $k \not\equiv 0 \pmod p$ and hence $m \not\equiv 0 \pmod p$, set $\alpha \equiv m^r k^s \pmod p$ so that $\alpha^a \equiv m$, $\alpha^b \equiv k$ modulo p. Then

$$V(p;h,l) = \sum_{\alpha=1}^{p} e_p(h\alpha^a + l\alpha^b) - 1,$$

where we must subtract off the term $\alpha = p$. If $a > 0$, the Weil bound[4] (Lemma 3.7) then shows that for $p \nmid hl$ with $p > \max(a,b)$,

$$|V(p;h,l)| \leq (\max(a,b)-1)p^{1/2} + 1.$$

If $a < 0$, the Weil bound for such Kloosterman sums (Lemma 3.9) shows that for $p \nmid hl$ with $p > \max(|a|,b)$,

$$|V(p;h,l)| \leq (|a|+b)p^{1/2} + 1.$$

Now suppose that $p|h$ but $p \nmid l$. Then

$$\begin{aligned} V(p;h,l) &= \sum_{\substack{m,\ k \pmod p \\ m^b \equiv k^a \pmod p \\ (k,p)=1}} e_p(lk) \\ &= \sum_{\substack{k \pmod p \\ (k,p)=1}} e_p(lk) \sum_{\substack{m \pmod p \\ m^b \equiv k^a \pmod p}} 1 \\ &= \sum_{k \pmod p} e_p(lk)\psi_b(k^a) - 1, \end{aligned}$$

where again we subtract off the $k = p$ term. Here

$$\psi_b(n) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod p \\ (b, p-1) & \text{if } n \equiv x^b \pmod p \text{ for some } x \\ 0 & \text{otherwise.} \end{cases}$$

[4]It is to apply the Weil bound that we must assume $a \neq b$, so that the polynomial $h\alpha^a + l\alpha^b$ is indeed a nonzero polynomial.

Note that since $(a,b)=1$, $\psi_b(k^a)=\psi_b(k)$. Trivially, if k may be written as a bth power modulo p, so may k^a. In the other direction, if $k \not\equiv 0 \pmod p$ and $k^a \equiv x^b \pmod p$ for some x, then recall that $ar+bs=1$ and write $k^{ra} \equiv x^{rb} \pmod p$. Then $k^{ra}k^{bs} \equiv x^{rb}k^{bs}$, and hence $k \equiv (x^r k^s)^b \pmod p$, so that k may also be written as a bth power modulo p. Therefore

$$\begin{aligned} V(p;h,l) &= \sum_{k \pmod p} e_p(lk)\psi_b(k) - 1 \\ &= \sum_{t \pmod p} e_p(lt^b) - 1. \end{aligned}$$

The classical bound for such sums given in Lemma 3.6 with $p \nmid l$, $p > b$ then gives

$$|V(p;h,l)| \leq ((b,p-1)-1)p^{1/2}+1.$$

Alternatively, if $p|l$ but $p \nmid h$, then for $p > |a|$ we have

$$|V(p;h,l)| \leq ((|a|,p-1)-1)p^{1/2}+1.$$

If $p|l$ and $p|h$ then trivially

$$|V(p;h,l)| \leq p \leq p^{1/2}(p,h,l)^{1/2}.$$

The trivial bound

$$|V(p;h,l)| \leq p \leq \max(|a|,b)^{1/2}p^{1/2}$$

is also sufficient for those primes $p \leq \max(|a|,b)$.

Thus for any prime $p|q$,

$$|V(p;h,l)| \leq \eta_{a,b}p^{1/2}(p,h,l)^{1/2},$$

where we may take the constant $\eta_{a,b} = 2\max(|a|+b)$. By the multiplicative property of $V(q;h,l)$, we have the final bound

$$|V(q;h,l)| \leq \eta_{a,b}^{\nu(q)}q^{1/2}(q,h,l)^{1/2}.$$

□

5.3.2 Bounding $U(w,M,q)$

We may now bound $U(w,M,q)$. Recall from (5.2) that

$$U(w,M,q) \ll H^{-1}q^{-1}\sum_{h=0}^{H-1}\sum_{l=1}^{q}|V(q;h,l)||A(q;w,-l)|.$$

Applying the bound of Lemma 5.1 to $V(q;h,l)$, then:

$$U(w,M,q) \ll \eta_{a,b}^{\nu(q)} H^{-1} q^{-1/2} \left[\sum_{l=1}^{q} \min(w, \|l/q\|^{-1})(q,l)^{1/2} + \sum_{l=1}^{q} \min(w, \|l/q\|^{-1}) \sum_{h=1}^{H-1} (q,h,l)^{1/2} \right].$$

Only when $l = q$ is w the minimum, so we may write

$$U(w,M,q) \ll \eta_{a,b}^{\nu(q)} H^{-1} q^{-1/2} \left[\sum_{l=1}^{q-1} \|l/q\|^{-1} (q,l)^{1/2} + wq^{1/2} + \sum_{l=1}^{q-1} \|l/q\|^{-1} \sum_{h=1}^{H-1} ((q,h),(q,l))^{1/2} + w \sum_{h=1}^{H-1} (q,h)^{1/2} \right].$$

We may bound the three sums as follows.

Lemma 5.2.

$$\sum_{l=1}^{q-1} \|l/q\|^{-1} (q,l)^{1/2} \ll qd(q) \log q.$$

Proof.

$$\begin{aligned} \sum_{l=1}^{q-1} \|l/q\|^{-1} (q,l)^{1/2} &\leq 2 \sum_{1 \leq l \leq q/2} \frac{q}{l} (q,l)^{1/2} \\ &\leq 2q \sum_{d|q} d^{1/2} \sum_{\substack{1 \leq l \leq q/2 \\ d|l}} \frac{1}{l} \\ &= 2q \sum_{d|q} d^{-1/2} \sum_{1 \leq c \leq q/(2d)} \frac{1}{c} \\ &\ll qd(q) \log q. \end{aligned}$$

□

Lemma 5.3.

$$\sum_{l=1}^{q-1} \|l/q\|^{-1} \sum_{h=1}^{H-1} ((q,h),(q,l))^{1/2} \ll Hqd(q) \log q.$$

Proof.

$$\begin{aligned}
\sum_{l=1}^{q-1} \|l/q\|^{-1} \sum_{h=1}^{H-1} ((q,h),(q,l))^{1/2} &\leq 2 \sum_{1\leq l\leq q/2} \frac{q}{l} \sum_{h=1}^{H-1} ((q,h),(q,l))^{1/2} \\
&\leq 2q \sum_{1\leq l\leq q/2} \frac{1}{l} \sum_{d|(q,l)} d^{1/2} \sum_{\substack{h=1 \\ d|(q,h)}}^{H-1} 1 \\
&\leq 2q \sum_{1\leq l\leq q/2} \frac{1}{l} \sum_{d|(q,l)} d^{1/2} \sum_{\substack{h=1 \\ d|h}}^{H-1} 1 \\
&\ll q \sum_{1\leq l\leq q/2} \frac{1}{l} \sum_{d|(q,l)} d^{1/2}(H/d) \\
&\leq Hq \sum_{1\leq l\leq q/2} \frac{1}{l} \sum_{d|(q,l)} d^{-1/2} \\
&\leq Hqd(q) \sum_{1\leq l\leq q/2} \frac{1}{l} \\
&\ll Hqd(q)\log q.
\end{aligned}$$

□

Lemma 5.4.

$$\sum_{h=1}^{H-1} (q,h)^{1/2} \ll Hd(q).$$

Proof.

$$\begin{aligned}
\sum_{h=1}^{H-1} (q,h)^{1/2} &\leq \sum_{d|q} d^{1/2} \sum_{\substack{h=1 \\ d|h}}^{H-1} 1 \\
&\ll \sum_{d|q} d^{1/2}(H/d) \\
&\ll H \sum_{d|q} d^{-1/2} \\
&\ll Hd(q).
\end{aligned}$$

□

It follows from these three lemmas that

$$U(w,M,q) \ll \eta_{a,b}^{\nu(q)} \left[H^{-1}q^{1/2}d(q)\log q + H^{-1}w + q^{1/2}d(q)\log q + q^{-1/2}wd(q) \right].$$

Recall that $H = [(q/2)M^{-1}]$. For square-free q, $n^{\nu(q)} = d(q)^{\frac{\log n}{\log 2}}$, so let τ be the least integer with $\tau \geq \log \eta_{a,b}/\log 2 + 1$. We have:

Proposition 5.2.

$$U(w,M,q) \ll q^{1/2}d(q)^{\tau}\log q + q^{-1}Md(q)^{\tau}w + q^{-1/2}d(q)^{\tau}w.$$

5.3.3 Proof of Theorem 5.1

Dyadic summation quickly yields a bound for $N_q(X,Y)$. Let J be the least integer such that $J \geq \log X/\log 2$. Then if $Y \leq q/2$,

$$\begin{aligned} N_q(X,Y) &\leq \sum_{j=0}^{J-1} U(2^j,Y,q) \\ &\ll \sum_{j=0}^{J-1} \left[q^{1/2}d(q)^\tau \log q + q^{-1}Yd(q)^\tau 2^j + q^{-1/2}d(q)^\tau 2^j\right] \\ &\ll q^{1/2}(\log X)d(q)^\tau \log q + q^{-1}XYd(q)^\tau + q^{-1/2}Xd(q)^\tau. \end{aligned}$$

Since $X \leq q$ we may conclude

$$N_q(X,Y) \ll q^{1/2}d(q)^\tau(\log q)^2 + q^{-1}XYd(q)^\tau + q^{-1/2}Xd(q)^\tau.$$

This completes the proof of Theorem 5.1.

5.4 Theorem 5.2: the mean value problem

We again examine $U(w,M,q)$, this time using mean value properties of exponential sums. In the remainder of the discussion we will assume that a is any nonzero integer and that the integer $b \geq 1$ satisfies $(b,q) = 1$ and $a/b \notin \mathbb{Z}^+$. (In particular, if $a > 0$, we must assume $b \geq 2$.)

Recall from Proposition 5.1 that

$$U(w,M,q) \ll H^{-1} \sum_{h=0}^{H-1} \left| \sum_{\substack{w<n\leq 2w \\ (n,q)=1}} \sum_{\substack{m \pmod q \\ m^b \equiv n^a \pmod q}} e_q(hm) \right|.$$

As in Theorem 4.2, we wish to average over a complete set of residues h modulo q. Therefore, applying Hölder's inequality,

$$U(w,M,q) \ll M^{\frac{1}{2k}} \left(\frac{1}{q} \sum_{h=1}^{q} \left| \sum_{\substack{w<n\leq 2w \\ (n,q)=1}} \sum_{\substack{m \pmod q \\ m^b \equiv n^a \pmod q}} e_q(hm) \right|^{2k} \right)^{\frac{1}{2k}}$$

for any integer $k \geq 1$. We do not specify k, but prove the theorem for any integer $k \geq 1$. This allows for the choice of optimal k in applications such as those of Chapter 6. All implicit constants depend only upon a, b, k. We will assume unless otherwise noted that we only consider $(n,q) = 1$.

Definition 5.3. For any finite set of integers $\mathcal{I}$ and $\alpha \in (\mathbb{Z}/q\mathbb{Z})^\times$, let

$$N_\alpha(\mathcal{I}) = \frac{1}{q} \sum_{h=1}^{q} \left| \sum_{n\in\mathcal{I}} \sum_{\substack{m \pmod q \\ m^b \equiv \alpha n^a \pmod q}} e_q(hm) \right|^{2k}.$$

We will denote $N_1(\mathcal{I})$ simply by $N(\mathcal{I})$.

It follows immediately that

Proposition 5.3.

$$U(w, M, q) \ll M^{\frac{1}{2k}} N(\mathcal{I})^{\frac{1}{2k}},$$

where $\mathcal{I} = (w, 2w]$.

As in Chapter 4, we will bound $N(\mathcal{I})$ for a more general interval of the form $\mathcal{I} = [1, I]$. (Recall that we have defined the notation $(A, B]$ to denote the set of integers $\{A < n \leq B\}$.) In fact, $N(\mathcal{I})$ increases as a function of the interval $\mathcal{I}$; we will see that it is sufficient to use a bound for $N(\mathcal{I})$ with $I = [1, 2w]$ in Proposition 5.3.

We have the following equivalent representation for $N_\alpha(\mathcal{I})$.

Lemma 5.5.

$$\begin{aligned} N_\alpha(\mathcal{I}) &= \#\{(\mathbf{n}, \mathbf{m}) = (n_1, \ldots, n_{2k}, m_1, \ldots, m_{2k}), n_i \in \mathcal{I}, m_i \ (mod\, q) : \\ &\quad m_i^b \equiv \alpha n_i^a \ (mod\, q) \text{ for } 1 \leq i \leq 2k \text{ and } \sum_{i=1}^{k} m_i \equiv \sum_{i=1}^{k} m_{i+k} \ (mod\, q)\}. \end{aligned}$$

Proof. Let

$$S(q, h) = \sum_{n \in \mathcal{I}} \sum_{\substack{m \pmod q \\ m^b \equiv \alpha n^a \pmod q}} e_q(hm).$$

Then

$$\begin{aligned} N_\alpha(\mathcal{I}) &= \frac{1}{q} \sum_{h=1}^{q} |S(q, h)|^{2k} \\ &= \frac{1}{q} \sum_{h=1}^{q} S(q, h)^k \overline{S(q, h)}^k, \end{aligned}$$

so that

$$\begin{aligned} N_\alpha(\mathcal{I}) &= \frac{1}{q} \sum_{h=1}^{q} \left[\sum_{n_1, \ldots, n_k \in \mathcal{I}} \sum_{\substack{m_1, \ldots, m_k \\ m_i^b \equiv \alpha n_i^a \pmod q}} e_q\left(\sum_{i=1}^{k} h m_i \right) \right] \\ &\qquad \cdot \left[\sum_{n_1, \ldots, n_k \in \mathcal{I}} \sum_{\substack{m_1, \ldots, m_k \\ m_j^b \equiv \alpha n_j^a \pmod q}} e_q\left(-\sum_{j=1}^{k} h m_j \right) \right] \\ &= \sum_{n_1, \ldots, n_{2k} \in \mathcal{I}} \sum_{\substack{m_1, \ldots, m_{2k} \\ m_i^b \equiv \alpha n_i^a \pmod q}} \frac{1}{q} \sum_{h=1}^{q} e_q\left(h \left(\sum_{i=1}^{k} m_i - \sum_{i=1}^{k} m_{i+k} \right) \right). \end{aligned}$$

The result follows. □

5.4.1 The trivial bound for $N(\mathcal{I})$

We easily obtain the following trivial bound for $N(\mathcal{I})$ when $\mathcal{I}$ is a set of consecutive positive integers.

Proposition 5.4. *Let $\mathcal{I} = \{1 \leq n \leq I\}$. Then*

$$N(\mathcal{I}) \ll (b^{\nu(q)})^{2k-1}(|a|^{\nu(q)})(I^{2k}q^{-1} + I^{2k-1}).$$

Proof. Fix $n_1, \ldots, n_{2k-1}$, for which there are at most I^{2k-1} choices. Since q is square-free, these determine $\ll (b^{\nu(q)})^{2k-1}$ choices for $m_1, \ldots, m_{2k-1}$ modulo q. There is then one value of $m_{2k} \pmod q$ that satisfies the congruence

$$m_{2k} \equiv \sum_{i=1}^{k} m_i - \sum_{i=1}^{k-1} m_{i+k} \pmod q.$$

For this value of m_{2k} there are $\ll |a|^{\nu(q)}$ values of n_{2k} modulo q such that

$$m_{2k}^b \equiv n_{2k}^a \pmod q.$$

Hence there are $\ll (|a|^{\nu(q)})(Iq^{-1} + 1)$ values for $n_{2k} \in \mathcal{I}$. Thus in total we obtain

$$N(\mathcal{I}) \ll (b^{\nu(q)})^{2k-1}(|a|^{\nu(q)})I^{2k-1}(Iq^{-1} + 1).$$

□

We may easily see that this bound for $N(\mathcal{I})$ gives no more than the trivial bound for $N_q(X, Y)$. Writing the factor $(b^{\nu(q)})^{2k-1}(|a|^{\nu(q)})$ as q^ϵ, it follows from Proposition 5.3 that

$$U(w, M, q) \ll w(q^\epsilon M(w^{-1} + q^{-1}))^{\frac{1}{2k}}.$$

This then gives the result that

$$N_q(X, Y) \ll Y^{\frac{1}{2k}}(X^{1-\frac{1}{2k}} + Xq^{-\frac{1}{2k}})q^\epsilon.$$

This is never better than $O(q^\epsilon \min(X, Y))$, for $X, Y \leq q$ and $k \geq 1$, disregarding comparison of factors of size q^ϵ. Thus our goal is to improve on this trivial bound for $N(\mathcal{I})$.

5.4.2 Bounding $N(\mathcal{I})$ by averaging

As in Theorem 4.2, we improve upon the trivial bound for $N(\mathcal{I})$ by taking advantage of averaging over h in order to average further over a set of auxiliary primes satisfying certain criteria. Let $\mathcal{I} = \{1 \leq n \leq I\}$. Fix a prime $p \nmid q$ with $Q < p \leq 2Q$ and $Q < I \leq q$, where we will specify the parameters I and Q later.

Proposition 5.5.

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + \frac{1}{q} \sum_{h=1}^{q} \left| \sum_{\substack{n \in \mathcal{I} \\ p \nmid n}} \sum_{\substack{m \pmod q \\ m^b \equiv n^a \pmod q}} e_q(hm) \right|^{2k}$$

where ω_k is a positive integer depending explicitly on a, b, k.

Proof. It suffices to bound the contribution to $N(\mathcal{I})$ from $4k$-tuples $(\mathbf{n}, \mathbf{m})$ where $p|n_i$ for some i. Without loss of generality, assume $p|n_1$. There are then $\ll Ip^{-1}$ possible values for n_1 and these determine $\ll b^{\nu(q)}$ choices for m_1, based on $m_1^b \equiv n_1^a \pmod q$. There are at most I^{2k-2} choices for $n_2, \ldots, n_{2k-1}$ and similarly these determine $\ll (b^{\nu(q)})^{2k-2}$ choices for $m_2, \ldots, m_{2k-1}$. There is then one choice for m_{2k} modulo q that satisfies the congruence

$$m_{2k} \equiv \sum_{i=1}^{k} m_i - \sum_{i=1}^{k-1} m_{i+k} \pmod q.$$

For this value of m_{2k} there are $\ll |a|^{\nu(q)}$ values of n_{2k} modulo q such that

$$m_{2k}^b \equiv n_{2k}^a \pmod q.$$

Since $I \leq q$, these are all the possible values of $n_{2k} \in \mathcal{I}$ as well. Thus, in total the contribution to $N(\mathcal{I})$ from $(\mathbf{n}, \mathbf{m})$ with $p|n_1$ is at most

$$\ll (b^{\nu(q)})^{2k-1} (|a|^{\nu(q)}) I^{2k-1} Q^{-1}.$$

For square-free q, $n^{\nu(q)} = d(q)^{\log n / \log 2}$. Therefore we could write

$$(b^{\nu(q)})^{2k-1} (|a|^{\nu(q)}) = d(q)^{\omega_k}$$

where ω_k is the least integer such that

$$\omega_k \geq (\log b / \log 2)(2k-1) + \log |a| / \log 2.$$

However, this is needlessly scrupulous, as any factor of $d(q)$ will contribute only q^ϵ to the final bound. Therefore we will use the trivial bound $b^{\nu(q)} \leq d(q)^b$ and simply take

$$\omega_k = b(2k-1) + |a|.$$

This completes the proof. □

We next consider the sum over $n \in \mathcal{I}$ such that $p \nmid n$. Since $p \nmid q$, these remaining n fall into the $p-1$ nonzero residue classes

$$n \equiv fq \pmod p, \quad 0 < f < p.$$

Note that for q square-free, the prime p is either expressible as a bth power modulo q or it belongs to another of the at most $b^{\nu(q)}$ cosets of Γ/Γ^b, where $\Gamma = (\mathbb{Z}/q\mathbb{Z})^\times$. Let $R_1 = 1, R_2, \ldots, R_{b^{\nu(q)}}$ be a fixed set of representatives for these cosets. Define

$$\mathcal{I}(p,f) = \left(\frac{-fq}{p}, \frac{I-fq}{p}\right].$$

Proposition 5.6.

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha(\mathcal{I}(p,f)),$$

where $\alpha = R_t^a$ according as p belongs to the coset of Γ/Γ^b represented by R_t.

Proof. Applying Hölder's inequality to the two innermost sums in Proposition 5.5 yields

$$\begin{aligned}\left|\sum_{\substack{n\in\mathcal{I}\\ p\nmid n}} \sum_{\substack{m \pmod q\\ m^b\equiv n^a \pmod q}} e_q(hm)\right|^{2k} &= \left|\sum_{f=1}^{p-1} \sum_{\substack{n\in\mathcal{I}\\ n\equiv fq \pmod p}} \sum_{\substack{m \pmod q\\ m^b\equiv n^a \pmod q}} e_q(hm)\right|^{2k}\\ &\le (p-1)^{2k-1} \sum_{f=1}^{p-1} \left|\sum_{\substack{n\in\mathcal{I}\\ n\equiv fq \pmod p}} \sum_{\substack{m \pmod q\\ m^b\equiv n^a \pmod q}} e_q(hm)\right|^{2k}.\end{aligned}$$

Write $n = fq + ps$ so that $s \in \mathcal{I}(p,f)$. Then the congruence $m^b \equiv n^a \pmod q$ is equivalent to $m^b \equiv p^a s^a \pmod q$. Temporarily let

$$S(p,f) = \frac{1}{q}\sum_{h=1}^{q} \left|\sum_{s\in\mathcal{I}(p,f)} \sum_{\substack{m \pmod q\\ m^b\equiv p^a s^a \pmod q}} e_q(hm)\right|^{2k}.$$

The prime p belongs to a coset $R_t\Gamma^b$ of the quotient group Γ/Γ^b and so may be written as $p = R_t g^b$ where both R_t and g are in $\Gamma = (\mathbb{Z}/q\mathbb{Z})^\times$. Set $m = g^a u$ so that the congruence $m^b \equiv p^a s^a \pmod q$ is equivalent to the congruence $u^b \equiv R_t^a s^a \pmod q$. Thus

$$S(p,f) = \frac{1}{q}\sum_{h=1}^{q} \left|\sum_{s\in\mathcal{I}(p,f)} \sum_{\substack{u \pmod q\\ u^b\equiv R_t^a s^a \pmod q}} e_q(hg^a u)\right|^{2k}.$$

Since $g \in (\mathbb{Z}/q\mathbb{Z})^\times$, then

$$S(p,f) = \frac{1}{q}\sum_{l=1}^{q} \left|\sum_{s\in\mathcal{I}(p,f)} \sum_{\substack{u \pmod q\\ u^b\equiv R_t^a s^a \pmod q}} e_q(lu)\right|^{2k}.$$

Setting $\alpha = R_t^a$, we thus have

$$S(p,f) = N_\alpha(\mathcal{I}(p,f)).$$

Summing $S(p,f)$ over all the residue classes corresponding to $f = 1,\ldots,p-1$, we finally obtain

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha(\mathcal{I}(p,f)).$$

□

This result is of critical importance, as it removes any dependence on the prime p from the argument of the exponential sum, so we may now average $N(\mathcal{I})$ over a large number of primes.

5.4.3 Averaging the good set over primes

As in Theorem 4.2, we first separate the quantity $N_\alpha(\mathcal{I}(p,f))$ into two parts, according to a distinction between "good" and "bad" $2k$-tuples $(n_1,\ldots,n_{2k})$. Define for any real number t,

$$\mathcal{I}(t) = (-qt, IQ^{-1} - qt]$$

and let $N_\alpha(t) = N_\alpha(\mathcal{I}(t))$. Since $\mathcal{I}(p,f) \subseteq \mathcal{I}(f/p)$ and $N_\alpha(\mathcal{I})$ increases with the set $\mathcal{I}$, then

$$N_\alpha(\mathcal{I}(p,f)) \le N_\alpha(\mathcal{I}(f/p)) = N_\alpha(f/p).$$

Definition 5.4. For disjoint sets G and B partitioning the set of $2k$-tuples $\mathbf{n} = (n_1,\ldots,n_{2k})$, define

$$\begin{aligned} N_\alpha^G(t) &= \#\{(\mathbf{n},\mathbf{m}), \mathbf{n} \in G, n_i \in \mathcal{I}(t), m_i \pmod q : (n,q) = 1, (m,q) = 1, \\ &\quad m_i^b \equiv \alpha n_i^a \pmod q \text{ for } 1 \le i \le 2k, \text{ and } \sum_{i=1}^{k} m_i \equiv \sum_{i=1}^{k} m_{i+k} \pmod q\}, \\ N_\alpha^B(t) &= \#\{(\mathbf{n},\mathbf{m}), \mathbf{n} \in B, n_i \in \mathcal{I}(t), m_i \pmod q : (n,q) = 1, (m,q) = 1, \\ &\quad m_i^b \equiv \alpha n_i^a \pmod q \text{ for } 1 \le i \le 2k, \text{ and } \sum_{i=1}^{k} m_i \equiv \sum_{i=1}^{k} m_{i+k} \pmod q\}. \end{aligned}$$

We will average only $N_\alpha^G(t)$ over primes, since the set B of bad $2k$-tuples will be sufficiently small for $N_\alpha^B(t)$ to admit a trivial bound.

From these definitions, we immediately obtain:

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha^B\left(\frac{f}{p}\right) + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha^G\left(\frac{f}{p}\right),$$

where $\alpha = R_t^a$, as in Proposition 5.6.

Definition 5.5. Let

$$K_\alpha = \max_t N_\alpha^B(t).$$

We have the following result:

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha^G\left(\frac{f}{p}\right).$$

We now average over a set of auxiliary primes p. By the prime number theorem, there are $O(Q(\log Q)^{-1})$ primes p in the range $Q < p \leq 2Q$. Of these, $O(\log q/\log\log q)$ are factors of q. We would like to average over as large a set of primes as possible; therefore given q and Q, consider the largest of the at most $b^{\nu(q)}$ sets

$$P_t = \{Q < p \leq 2Q, p \nmid q : p \in R_t \Gamma^b\}.$$

Assuming $Q \geq c \log q$ for some constant c, we are then averaging over a set of $\gg Q(b^{\nu(q)} \log Q)^{-1}$ primes. Therefore

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-2} (\log Q) \sum_p \sum_{f=1}^{p-1} N_\alpha^G\left(\frac{f}{p}\right),$$

where the sum is over primes p in the largest set P_t, with α accordingly defined to be $\alpha = R_t^a$.

Let $\mathcal{I}'(t) = (-qt, 2IQ^{-1} - qt]$ and define $N_\alpha^{G'}(t)$ in analogy to $N_\alpha^G(t)$, the only alteration being that we require $n_i \in \mathcal{I}'(t)$. It follows exactly as in Propositions 4.11 and 4.13 of Section 4.6.3 that we may rearrange the intervals we consider so that the sum of $N_\alpha^G(t)$ is only dependent on the set P_t of auxiliary primes over which we average in terms of the value of α. We obtain

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-1} I^{-1} (\log Q) \sum_{j=1}^{2q-1} N_\alpha^{G'}\left(\frac{j}{q}\right).$$

Definition 5.6. Let L_α denote the number of solutions $(\mathbf{n}, \mathbf{m}, j)$ with $\mathbf{n} \in G$ and

$$\begin{aligned} n_i &\in (0, 2IQ^{-1}] \quad \text{for} \quad i = 1, \ldots, 2k, \\ m_i &\pmod q \quad \text{for} \quad i = 1, \ldots, 2k, \\ 0 &\leq j < q \end{aligned}$$

such that for each $i = 1, \ldots, 2k$, $(n_i, q) = 1$, $(m_i, q) = 1$,

$$m_i^b \equiv \alpha (n_i - j)^a \pmod q,$$

and

$$\sum_{i=1}^{k} m_i \equiv \sum_{i=1}^{k} m_{i+k} \pmod q.$$

We summarise the results of this section with the following proposition:

Proposition 5.7.

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-1} I^{-1} (\log Q) L_\alpha,$$

where $\alpha = R_t^a$, with R_t a fixed representative for the largest set P_t.

5.5 The good and bad sets

It remains to estimate L_α and K_α. The difficulty lies in defining the sets G and B and estimating L_α. Let $L_\alpha(\mathbf{n}; q)$ represent the number of solutions $(\mathbf{m}, j)$ corresponding to a fixed $2k$-tuple $\mathbf{n} \in G$. Then $L_\alpha(\mathbf{n}; q)$ is multiplicative with respect to q, thus for square-free $q = \prod p$ we may write

$$L_\alpha(\mathbf{n}; q) = \prod L_\alpha(\mathbf{n}; p).$$

We will bound $L_\alpha(\mathbf{n}; p)$ for each prime $p|q$ by bounding the number of roots of a certain polynomial. Once we have determined the conditions we must impose on $\mathbf{n}$ for the polynomial to have a small number of roots in a certain sense, it will be clear how to define the good and bad sets G and B. For technical reasons we consider the cases when the exponent $a > 0$ and $a < 0$ separately.

5.5.1 Positive exponent: defining the polynomial $H_\alpha(\mathbf{n}, j)$

First assume that $a > 0$. Let

$$\beta = \begin{cases} b & \text{for } b \text{ even}, \\ 2b & \text{for } b \text{ odd}. \end{cases}$$

Let $F(\mathbf{Y})$ be the polynomial in $\mathbb{Z}[X_1, \dots, X_{2k}, Y_1, \dots, Y_{2k}, Z]$ defined by

$$F(\mathbf{Y}) = \prod_{\{\omega\}} F_{\{\omega\}}(\mathbf{Y}) = \prod_{\omega_2, \dots, \omega_{2k}} (Y_1 + \xi^{\omega_2} Y_2 + \cdots + \xi^{\omega_{2k}} Y_{2k}),$$

where ξ is a primitive βth root of unity and the $(2k-1)$-tuples of exponents $\omega_2, \dots, \omega_{2k}$ range over all values in the set $\{0, \dots, \beta - 1\}$. Thus the coefficients $\xi^{\omega_2}, \dots, \xi^{\omega_{2k}}$ attain all possible sequences of $\{+1, -1\}$ of length $2k-1$. In particular, one factor $F_{\{\omega\}}(\mathbf{Y})$ of the polynomial $F(\mathbf{Y})$ has coefficients of $+1$ for $Y_1, \dots, Y_k$, and coefficients of -1 for $Y_{k+1}, \dots, Y_{2k}$. It is this factor in which we are most interested.

Imagine for the moment that we could take fractional powers modulo a prime p; fix $\mathbf{n}$ and substitute $\alpha^{1/b}(\mathbf{n} - j)^{a/b}$ for $\mathbf{Y}$. Then this particular factor $F_{\{\omega\}}(\alpha^{1/b}(\mathbf{n} - j)^{a/b})$ would vanish whenever

$$\sum_{i=1}^{k} \alpha^{1/b}(n_i - j)^{a/b} - \sum_{i=1}^{k} \alpha^{1/b}(n_{i+k} - j)^{a/b} \equiv 0 \pmod{p}.$$

Thus we can think of the number of roots of $F(\alpha^{1/b}(\mathbf{n}-j)^{a/b})$ as giving an upper bound for the number of values j for which there is a vector $\mathbf{m}$ such that $(\mathbf{n},\mathbf{m},j)$ is a solution satisfying the criteria given in the definition of L_α.

As we cannot actually take such fractional powers modulo p, we have to be more careful. However, the polynomial F as defined does have a special property that allows us to proceed with this line of argument. For note that $F(\mathbf{Y})$ is in fact a polynomial in $\mathbf{Y}^b = (Y_1^b,\dots,Y_{2k}^b)$. Therefore if we have the relation

$$Y_i^b = \alpha(X_i - Z)^a$$

for each $i = 1,\dots,2k$, then there exist polynomials G and H_α such that

$$F(\mathbf{Y}) = G(\mathbf{Y}^b) = G(\alpha(\mathbf{X}-Z)^a) = H_\alpha(\mathbf{X},Z).$$

Specifically, for a fixed vector $\mathbf{n}$, if $\mathbf{m}$ is such that

$$m_i^b \equiv \alpha(n_i - j)^a \pmod p$$

for each $i = 1,\dots,2k$, and if

$$F(\mathbf{m}) \equiv 0 \pmod p,$$

then

$$H_\alpha(\mathbf{n},j) \equiv 0 \pmod p.$$

Therefore it is sufficient to bound the number of roots j of $H_\alpha(\mathbf{n},j)$ modulo p, as then

$$L_\alpha(\mathbf{n};p) \le b^{2k}\#\{\text{roots } j \text{ of } H_\alpha(\mathbf{n},j) \text{ modulo } p\}, \tag{5.3}$$

where the factor of b^{2k} arises from the number of ways of choosing the $2k$-tuple $\mathbf{m}$ modulo p.

5.5.2 The vanishing of $H_\alpha(\mathbf{n},j)$ over $\mathbb{C}$

Studying those $\mathbf{n}$ for which $H_\alpha(\mathbf{n},j)$ can vanish identically over $\mathbb{C}$ makes it clear how to define the good set G of those $\mathbf{n}$ for which $H_\alpha(\mathbf{n},j)$ has few roots, and the bad set B of those $\mathbf{n}$ for which $H_\alpha(\mathbf{n},j)$ can have arbitrarily many roots. In the following section we then study the number of roots $H_\alpha(\mathbf{n},j)$ can have modulo a prime p, for $\mathbf{n} \in G$.

Suppose that $H_\alpha(\mathbf{n},z)$ is identically zero for $z \in \mathbb{C}$. Then one of the factors in the product defining $H_\alpha(\mathbf{n},z)$ must vanish identically over $\mathbb{C}$, so for some set of exponents $\omega_1,\dots,\omega_{2k}$, with $\omega_1 = 0$,

$$\sum_{i=1}^{2k} \xi^{\omega_i}(n_i - z)^{a/b} = 0 \tag{5.4}$$

for all $z \in \mathbb{C}$. Expand each term in (5.4) as a power series,

$$\begin{aligned}(n_i - z)^{a/b} &= (-z)^{a/b}(1 - n_i/z)^{a/b} \\ &= c_0(-z)^{a/b} + c_1(-z)^{a/b-1}n_i + c_2(-z)^{a/b-2}n_i^2 + \cdots,\end{aligned}$$

where $c_l \neq 0$ for all $l \geq 0$.[5] We then see that in order for all the coefficients of z in (5.4) to be zero, we must have

$$E(m) = \sum_{i=1}^{2k} \xi^{\omega_i} n_i^m = 0,$$

for all integers $m \geq 0$.

Regard $E(0) = 0, \ldots, E(2k-1) = 0$ as a system of linear equations in variables $t_i = \xi^{\omega_i}$ for $1 \leq i \leq 2k$:

$$\begin{aligned} t_1 n_1^0 + t_2 n_2^0 + \cdots + t_{2k} n_{2k}^0 &= 0 \\ &\vdots \\ t_1 n_1^{2k-1} + t_2 n_2^{2k-1} + \cdots + t_{2k} n_{2k}^{2k-1} &= 0. \end{aligned}$$

Construct the corresponding matrix

$$\mathbf{A} = \begin{pmatrix} n_1^0 & n_2^0 & \cdots & n_{2k}^0 \\ n_1^1 & n_2^1 & \cdots & n_{2k}^1 \\ \vdots & \vdots & & \vdots \\ n_1^{2k-1} & n_2^{2k-1} & \cdots & n_{2k}^{2k-1} \end{pmatrix}.$$

Since the vector $(\xi^{\omega_1}, \ldots, \xi^{\omega_{2k}})$ of all nonzero values is a solution to the equation $\mathbf{A}(t_1, \ldots, t_{2k}) = (0, \ldots, 0)$, the Vandermonde determinant shows that

$$\prod_{1 \leq i < h \leq 2k} (n_i - n_h) = 0.$$

[5] We observe that since $a > 0$ we must require $b \neq 1$, since otherwise the coefficients c_l, of the form

$$c_l = \frac{\frac{a}{b}(\frac{a}{b} - 1) \cdots (\frac{a}{b} - (l-1))}{l!},$$

vanish for $l > a$. The proof could proceed if the exponent a were sufficiently large, $a \geq 2k-1$, for the optimal choice of k. However, one would not know this were the case without already applying the result of the theorem.

In fact, this is an indication of a deeper problem. We may think informally of the requirement in the definition of $N(\mathcal{I})$ given in Lemma 5.5 as

$$\sum_{i=1}^{k} n_i^s \equiv \sum_{i=1}^{k} n_{i+k}^s \pmod{q},$$

where $s = a/b$ is a rational number. In general, this generates sufficiently many conditions to limit the number of allowable vectors $\mathbf{n}$ only if the resulting expansion is infinite, i.e. only if s is negative, or is a positive non-integer. If s is a positive integer, the resulting expansion is finite, and it is possible that too few conditions are generated to restrict the choice of $\mathbf{n}$ sufficiently.

Without loss of generality, suppose that $n_1 - n_2 = 0$. Let $n_{1,2} = n_1 = n_2$, so that in the set of linear equations we may collapse the two variables t_1 and t_2 into one variable; for example

$$t_1 n_1^0 + t_2 n_2^0 + \cdots + t_{2k} n_{2k}^0 = 0$$

becomes

$$(t_1 + t_2) n_{1,2}^0 + \cdots + t_{2k} n_{2k}^0 = 0.$$

(It is possible that more than two of the n_i are of equal value; if so one simply collapses all of the variables t_i with equal values n_i into one variable and the reasoning proceeds in a similar fashion.) If $\xi^{\omega_1} + \xi^{\omega_2} \neq 0$, then we obtain the $(2k-1) \times (2k-1)$ matrix

$$\mathbf{A}' = \begin{pmatrix} n_{1,2}^0 & n_3^0 & \cdots & n_{2k}^0 \\ n_{1,2}^1 & n_3^1 & \cdots & n_{2k}^1 \\ \vdots & \vdots & & \vdots \\ n_{1,2}^{2k-1} & n_3^{2k-1} & \cdots & n_{2k}^{2k-1} \end{pmatrix},$$

and again the Vandermonde determinant shows that $n_i - n_h = 0$ for some $i \neq h$. If $\xi^{\omega_1} + \xi^{\omega_2} = 0$, then examine the $(2k-2) \times (2k-2)$ matrix omitting the first two columns of $\mathbf{A}$ entirely. (Again, if more than two of the n_i are of equal value and the corresponding roots of unity ξ^{ω_i} sum to zero, simply omit all the appropriate columns of $\mathbf{A}$.) Proceeding in this fashion, one shows that if $H_\alpha(\mathbf{n}, z)$ vanishes identically over $\mathbb{C}$, then for each $i = 1, \ldots, 2k$, there exists $h \neq i$ such that $n_i - n_h = 0$.

Therefore we choose the sets B and G as follows.

Definition 5.7. Let

$$\begin{aligned} B &= \{\mathbf{n} : \forall i,\ 1 \leq i \leq 2k,\ \exists h \neq i, 1 \leq h \leq 2k,\ \text{s.t. } n_i = n_h\} \\ G &= \{\mathbf{n} : \mathbf{n} \notin B\}. \end{aligned}$$

For each $\mathbf{n}$ and each $1 \leq i \leq 2k$, define

$$A_i(\mathbf{n}) = \prod_{h \neq i} (n_i - n_h).$$

Then if $\mathbf{n} \in G$, there exists some $1 \leq i \leq 2k$ such that $A_i(\mathbf{n}) \neq 0$.

5.5.3 The vanishing of $H_\alpha(\mathbf{n}, j)$ modulo p

While $H_\alpha(\mathbf{n}, j)$ cannot vanish identically over $\mathbb{C}$ for $\mathbf{n} \in G$ as defined above, it is still possible that $H_\alpha(\mathbf{n}, j)$ could vanish identically modulo p for arbitrarily large primes p dividing q.

The highest degree possible for $H_\alpha(\mathbf{n}, j)$ with respect to j is $\delta_k = (a/b)\beta^{2k-1}$. There are thus at most δ_k roots j modulo p, unless the polynomial vanishes identically modulo p. Suppose a prime p divides all the coefficients of terms of the form $\alpha(n_i - j)^a$ in the expanded product $H_\alpha(\mathbf{n}, j)$. (Note that necessarily $\alpha = R_t^a \in (\mathbb{Z}/q\mathbb{Z})^\times$, so that $p \nmid \alpha$.) The coefficients of these terms arise from multiplying the β^{2k-1} factors of $H_\alpha(\mathbf{n}, j)$ and are hence dependent only upon b and k. Thus there exists a constant $c_{b,k}$ such that if p divides all the coefficients of terms of the form $\alpha(n_i - j)^a$ in the expanded product, then $p \leq c_{b,k}$.

For $p > c_{b,k}$, it is still possible that $H_\alpha(\mathbf{n}, j)$ could vanish identically modulo p because of congruences among the values n_i modulo p. We will show that if $H_\alpha(\mathbf{n}, j)$ vanishes identically modulo p for a sufficiently large prime p, then $\mathbf{n}$ is "bad" modulo p in the following sense:

Lemma 5.6. *Suppose the polynomial $H_\alpha(\mathbf{n}, j)$ vanishes identically modulo a prime $p > P_{a,b,k}$ for a constant $P_{a,b,k}$ explicitly dependent on a, b, k. Then $p|A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$.*

Proof. Fix $\mathbf{n}$ and regard $H_\alpha(\mathbf{n}, z)$ as a polynomial in $\mathbb{Z}[z]$. If $H_\alpha(\mathbf{n}, z)$ vanishes identically modulo p, then so does $H_\alpha(\mathbf{n}, z^b)$. Set $d = a\beta^{2k-1}$ and consider the polynomial $J(z) = \alpha^{-\beta^{2k-1}/b} z^{-d} H_\alpha(\mathbf{n}, z^b)$ in $\mathbb{Z}[z^{-b}]$. We may think of $J(z)$ as a product over all possible sets of exponents $\{\omega\} = \{\omega_1 = 0, \ldots, \omega_{2k}\}$,

$$J(z) = \prod_{\{\omega\}} J_{\{\omega\}}(z), \tag{5.5}$$

where each factor is of the form

$$J_{\{\omega\}}(z) = \xi^{\omega_1} \left(1 - \frac{n_1}{z^b}\right)^{a/b} + \cdots + \xi^{\omega_{2k}} \left(1 - \frac{n_{2k}}{z^b}\right)^{a/b}.$$

Each factor $J_{\{\omega\}}(z)$ may be regarded as a formal power series over $\overline{\mathbb{Q}}$,

$$J_{\{\omega\}}(z) = \sum_{m=0}^{\infty} v_{\{\omega\},m} (z^{-b})^m.$$

For each factor $J_{\{\omega\}}(z)$ and an integer $M \geq 1$ we will choose later, define the truncation

$$J_{\{\omega\}}^M(z) = \sum_{m=0}^{M} v_{\{\omega\},m} (z^{-b})^m,$$

and let

$$J^M(z) = \prod_{\{\omega\}} J_{\{\omega\}}^M(z). \tag{5.6}$$

Let $\mathcal{K}$ be the field $\mathcal{K} = \mathbb{Q}(v_{\{\omega\},m})$, where $\{\omega\}$ ranges over all sets of exponents, and $0 \leq m \leq M$ (i.e. we simply adjoin the coefficients of each truncated

factor $J^M_{\{\omega\}}$). Let $\mathfrak{p}$ be a fixed prime ideal above p in $\mathcal{K}$. Then $J^M(z)$ may be written as a sum

$$J^M(z) = P^M(z) + Q^M(z),$$

where $P^M(z)$ is a polynomial of degree M defined over $O_{\mathcal{K}}$, and $Q^M(z)$ is also a polynomial over $O_{\mathcal{K}}$, but of terms of degree strictly greater than M.

By assumption, $J(z)$ is identically zero modulo p. Equating coefficients in equation (5.5), one sees that each coefficient of $P^M(z)$ is zero modulo $\mathfrak{p}$. Thus there exists a factor $J^M_{\{\omega\}}(z)$ such that all its coefficients $v_{\{\omega\},m}$ with $0 \leq m \leq M/N$ are zero modulo $\mathfrak{p}$, where $N = \beta^{2k-1}$ is the number of factors in the product (5.6) defining $J^M(z)$. Each coefficient v_m (where we understand the set $\{\omega\}$ to be fixed, and drop the subscript) is of the form

$$v_m = (-1)^m \frac{\frac{a}{b}(\frac{a}{b}-1)\cdots(\frac{a}{b}-(m-1))}{m!} \sum_{i=1}^{2k} \xi^{\omega_i} n_i^m.$$

Choose $M = N(2k-1)$. We also require that the prime p satisfies $p > b$, $p > 2k-1$ and $p \nmid a(a-b)\cdots(a-b(2k-2))$. So for a sufficiently large constant $P_{a,b,k}$ defined in terms of a, b, k (which we also choose to be at least $c_{b,k}$), if $p > P_{a,b,k}$, then since $v_m = 0$ modulo $\mathfrak{p}$ for each $0 \leq m \leq 2k-1$, we have

$$E(m) = \sum_{i=1}^{2k} \xi^{\omega_i} n_i^m = 0$$

modulo $\mathfrak{p}$ for each $0 \leq m \leq 2k-1$.

As when studying the vanishing of $H_\alpha(\mathbf{n}, j)$ over $\mathbb{C}$, we construct the matrix

$$\mathbf{A} = \begin{pmatrix} n_1^0 & n_2^0 & \cdots & n_{2k}^0 \\ n_1^1 & n_2^1 & \cdots & n_{2k}^1 \\ \vdots & \vdots & & \vdots \\ n_1^{2k-1} & n_2^{2k-1} & \cdots & n_{2k}^{2k-1} \end{pmatrix}.$$

Once again, the Vandermonde determinant shows that

$$\prod_{i<h} (n_i - n_h) = 0 \text{ modulo } \mathfrak{p},$$

so that there exists $i \neq h$ such that $n_i - n_h = 0$ modulo $\mathfrak{p}$. Proceeding in the same fashion as before, one shows that for each $1 \leq i \leq 2k$ there exists some $h \neq i$, $1 \leq h \leq 2k$, such that $n_i - n_h = 0$ modulo $\mathfrak{p}$. In each case, since $n_i - n_h$ is a rational integer, in fact $p|(n_i - n_h)$. Thus $p|A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$. This completes the proof. □

5.5.4 Negative exponent: defining the polynomial $\bar{H}_\alpha(\mathbf{n}, j)$

We next consider the case when $a < 0$. We proceed with an argument similar to the case when the exponent $a > 0$, but slightly more complicated. We first

define a polynomial $\bar{H}_\alpha(\mathbf{n}, j)$ analogous to $H_\alpha(\mathbf{n}, j)$. Let β and $F(\mathbf{Y})$ be as before, and let

$$\bar{F}(\mathbf{Y}) = \left(\prod_{i=1}^{2k} Y_i^{-1} \right)^N F(\mathbf{Y}),$$

where $N = \beta^{2k-1}$ is the number of factors in the product over $\{\omega\}$ defining $F(\mathbf{Y})$. If we have the relation

$$Y_i^b = \alpha(X_i - Z)^{-|a|}$$

for each $i = 1, \ldots, 2k$, then there exist polynomials $\bar{G}$ and $\bar{H}_\alpha$ such that

$$\bar{F}(\mathbf{Y}) = \bar{G}(\mathbf{Y}^b) = \bar{G}(\alpha(\mathbf{X} - Z)^{-|a|}) = \bar{H}_\alpha(\mathbf{X}, Z).$$

Informally, we may think of the polynomial $\bar{H}_\alpha$ as the product

$$\begin{aligned} \bar{H}_\alpha(\mathbf{n}, j) &= \bar{H}_\alpha^{(1)}(\mathbf{n}, j) \bar{H}_\alpha^{(2)}(\mathbf{n}, j) \\ &= \left(\prod_{i=1}^{2k} \alpha^{-1/b} (n_i - j)^{|a|/b} \right)^N \\ &\quad \cdot \prod_{\{\omega\}} \left(\xi^{\omega_1} \alpha^{1/b} (n_1 - j)^{-|a|/b} + \cdots + \xi^{\omega_{2k}} \alpha^{1/b} (n_{2k} - j)^{-|a|/b} \right), \end{aligned}$$

or as

$$\bar{H}_\alpha(\mathbf{n}, j) = \prod_{\{\omega\}} \left(\xi^{\omega_1} \alpha^{-(2k-1)/b} \prod_{i \neq 1} (n_i - j)^{|a|/b} + \cdots + \xi^{\omega_{2k}} \alpha^{-(2k-1)/b} \prod_{i \neq 2k} (n_i - j)^{|a|/b} \right).$$

In particular, if $\mathbf{n}$ is fixed and $\mathbf{m}$ is such that

$$m_i^b \equiv \alpha(n_i - j)^{-|a|} \pmod{p}$$

for each $i = 1, \ldots, 2k$, and if

$$\bar{F}(\mathbf{m}) \equiv 0 \pmod{p},$$

then

$$\bar{H}_\alpha(\mathbf{n}, j) \equiv 0 \pmod{p}.$$

Therefore it is once again sufficient to bound the number of roots j of $\bar{H}_\alpha(\mathbf{n}, j)$ modulo p.

5.5.5 The vanishing of $\bar{H}_\alpha(\mathbf{n}, j)$ over $\mathbb{C}$

Suppose that $\bar{H}_\alpha(\mathbf{n}, z)$ is identically zero for $z \in \mathbb{C}$. Then either $\bar{H}_\alpha^{(1)}(\mathbf{n}, z)$ or $\bar{H}_\alpha^{(2)}(\mathbf{n}, z)$ must vanish identically over $\mathbb{C}$. Visibly the coefficient of $(-z)^{2kN(|a|/b)}$

in the expansion of $\bar{H}_\alpha^{(1)}(\mathbf{n}, z)$ is 1, thus it must be that $\bar{H}_\alpha^{(2)}(\mathbf{n}, z)$ vanishes identically over $\mathbb{C}$. As in the case $a > 0$, it follows that for some set of exponents $\omega_1, \ldots, \omega_{2k}$, with $\omega_1 = 0$,

$$\sum_{i=1}^{2k} \xi^{\omega_i} (n_i - z)^{-|a|/b} = 0 \tag{5.7}$$

for all $z \in \mathbb{C}$. Using an argument analogous[6] to that in the case $a > 0$, it follows that if $\bar{H}_\alpha^{(2)}(\mathbf{n}, z)$ vanishes identically over $\mathbb{C}$, then for each $i = 1, \ldots, 2k$, there exists $h \neq i$ such that $n_i - n_h = 0$. Therefore we may choose the sets B and G as before. We also define $A_i(\mathbf{n})$ for each $i = 1, \ldots, 2k$ as before.

5.5.6 The vanishing of $\bar{H}_\alpha(\mathbf{n}, j)$ modulo p

Thus $\bar{H}_\alpha(\mathbf{n}, j)$ cannot vanish identically over $\mathbb{C}$ for $\mathbf{n} \in G$, but it is still possible that $\bar{H}_\alpha(\mathbf{n}, j)$ could vanish identically modulo p for arbitrarily large primes p dividing q.

The highest degree possible for $\bar{H}_\alpha(\mathbf{n}, j)$ is $\bar{\delta}_k = (|a|/b)(2k-1)\beta^{2k-1}$. There are thus at most $\bar{\delta}_k$ roots j modulo p, unless the polynomial vanishes identically modulo p. Once again, there is a constant $\bar{c}_{b,k}$ such that if p divides all the coefficients of terms of the form $\alpha(n_i - j)^{|a|}$ in the expanded product of $\bar{H}_\alpha(\mathbf{n}, j)$, then $p \leq \bar{c}_{b,k}$. We may prove a lemma analogous to Lemma 5.6, showing that if $\bar{H}_\alpha(\mathbf{n}, j)$ vanishes identically modulo p for a sufficiently large prime p, then $\mathbf{n}$ is "bad" modulo p in the following sense:

Lemma 5.7. *Suppose the polynomial $\bar{H}_\alpha(\mathbf{n}, j)$ vanishes identically modulo a prime $p > \bar{P}_{a,b,k}$ for a constant $\bar{P}_{a,b,k}$ explicitly dependent on a, b, k. Then $p | A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$.*

Proof. Fix $\mathbf{n}$ and regard $\bar{H}_\alpha(\mathbf{n}, z)$ as a polynomial in $\mathbb{Z}[z]$. If $\bar{H}_\alpha(\mathbf{n}, z)$ vanishes identically modulo p, then so does $\bar{H}_\alpha(\mathbf{n}, z^b)$. Set $\bar{d} = |a|(2k-1)\beta^{2k-1}$ and consider the polynomial $\bar{J}(z) = \alpha^{(2k-1)N/b} z^{-\bar{d}} \bar{H}_\alpha(\mathbf{n}, z^b)$ in $\mathbb{Z}[z^{-b}]$. We may think of $\bar{J}(z)$ as a product over all sets of exponents $\{\omega\} = \{\omega_1 = 0, \ldots, \omega_{2k}\}$,

$$\bar{J}(z) = \prod_{\{\omega\}} \bar{J}_{\{\omega\}}(z), \tag{5.8}$$

where each factor is of the form

$$\begin{aligned} \bar{J}_{\{\omega\}}(z) &= \bar{J}^{(1)}_{\{\omega\}}(z) \bar{J}^{(2)}_{\{\omega\}}(z) \\ &= \left(\prod_{i=1}^{2k} \left(1 - \frac{n_i}{z^b}\right)^{|a|/b} \right) \\ &\quad \cdot \left(\xi^{\omega_1} \left(1 - \frac{n_1}{z^b}\right)^{-|a|/b} + \cdots + \xi^{\omega_{2k}} \left(1 - \frac{n_{2k}}{z^b}\right)^{-|a|/b} \right), \end{aligned}$$

[6] Note that in this case we may have $b = 1$, since the expansion of the resulting series is still infinite, since $a < 0$.

or alternatively,

$$\bar{J}_{\{\omega\}}(z) = \left(\xi^{\omega_1} \prod_{i \neq 1} \left(1 - \frac{n_i}{z^b}\right)^{|a|/b} + \cdots + \xi^{\omega_{2k}} \prod_{i \neq 2k} \left(1 - \frac{n_i}{z^b}\right)^{|a|/b} \right).$$

Each factor $\bar{J}_{\{\omega\}}(z)$ may be regarded as a product of the formal power series for $\bar{J}^{(1)}_{\{\omega\}}(z)$ and $\bar{J}^{(2)}_{\{\omega\}}(z)$ over $\overline{\mathbb{Q}}$. As before, we define Mth power truncations of each power series, which we denote by $\bar{J}^{(1),M}_{\{\omega\}}(z)$ and $\bar{J}^{(2),M}_{\{\omega\}}(z)$, and let

$$\bar{J}^M(z) = \prod_{\{\omega\}} \bar{J}^M_{\{\omega\}}(z) = \prod_{\{\omega\}} \bar{J}^{(1),M}_{\{\omega\}}(z) \bar{J}^{(2),M}_{\{\omega\}}(z). \tag{5.9}$$

Let $\mathcal{K}$ represent the field formed by adjoining the coefficients of each truncated factor to $\mathbb{Q}$, and let $\mathfrak{p}$ be a fixed prime ideal above p in $\mathcal{K}$. Then $\bar{J}^M(z)$ may be written as a sum

$$\bar{J}^M(z) = \bar{P}^M(z) + \bar{Q}^M(z),$$

where $\bar{P}^M(z)$ is a polynomial of degree M defined over $O_{\mathcal{K}}$, and $\bar{Q}^M(z)$ is also a polynomial over $O_{\mathcal{K}}$, but of terms of degree strictly greater than M.

By assumption, $\bar{J}(z)$ is identically zero modulo p. Equating coefficients in equation (5.8), it follows that each coefficient of $\bar{P}^M(z)$ is zero modulo $\mathfrak{p}$. Thus there exists a factor $\bar{J}^M_{\{\omega\}}(z)$ such the coefficients of all terms (in z^{-b}) with degree $0 \leq m \leq M/N$ are zero modulo $\mathfrak{p}$. Furthermore, for this specific factor, it must be that at least one of $\bar{J}^{(1),M}_{\{\omega\}}(z)$ and $\bar{J}^{(2),M}_{\{\omega\}}(z)$ has the property that the coefficients of all terms with degree $0 \leq m \leq M/2N$ are zero modulo $\mathfrak{p}$. Visibly, $\bar{J}^{(1),M}_{\{\omega\}}(z)$ has constant term 1, so it must be that all coefficients of terms in $\bar{J}^{(2),M}_{\{\omega\}}(z)$ with degree $0 \leq m \leq M/2N$ are zero modulo $\mathfrak{p}$.

Choosing $M = 2N(2k-1)$ and an appropriately large constant $\bar{P}_{\bar{a},b,k}$, we may argue as in the case $a > 0$ to conclude that for a prime $p|q$ with $p > \bar{P}_{\bar{a},b,k}$, if $\mathfrak{p}$ divides the coefficients of terms of degree $0 \leq m \leq 2k-1$ in the truncated expansion $\bar{J}^{(2),M}_{\{\omega\}}(z)$, then for each $1 \leq i \leq 2k$ there exists some $h \neq i$ such that $n_i - n_h = 0$ modulo $\mathfrak{p}$. In each case, since $n_i - n_h$ is a rational integer, in fact $p|(n_i - n_h)$. Thus $p|A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$. This completes the proof. □

5.6 Final bounds for L_α and K_α

We may now estimate L_α and K_α. We need no longer distinguish between the exponent a being positive or negative (other than in choosing certain constants), as we have seen that we may choose the sets G and B identically in each case.

5.6.1 Estimating L_α

For each $\mathbf{n} \in G$, $A_i(\mathbf{n}) \neq 0$ for at least one value $1 \leq i \leq 2k$. Let

$$G_i = \{\mathbf{n} \in G : A_i(\mathbf{n}) \neq 0\},$$

so that

$$G = \bigcup_{i=1}^{2k} G_i.$$

Proposition 5.8. *If $\mathbf{n} \in G_i$ then for any $p|q$,*

$$L_\alpha(\mathbf{n}; p) \leq d_{\eta_k}(p) b^{2k} (p, A_i(\mathbf{n})),$$

where $\eta_k = \max(P_{a,b,k}, \bar{P}_{\bar{a},b,k}, \delta_k, \bar{\delta}_k)$.

Proof. First consider the case $a > 0$. If $p \nmid A_i(\mathbf{n})$, then by Lemma 5.6, $H_\alpha(\mathbf{n}, j)$ can only vanish identically modulo p if $p \leq P_{a,b,k}$. If the polynomial is not identically zero modulo p then it has at most δ_k roots, where $\delta_k = (a/b)\beta^{2k-1}$ is its highest possible degree. Thus if $p \nmid A_i(\mathbf{n})$, then $H_\alpha(\mathbf{n}, j)$ has at most $\gamma_k = \max(P_{a,b,k}, \delta_k)$ roots. It then follows from (5.3) that

$$L_\alpha(\mathbf{n}; p) \leq d_{\gamma_k}(p) b^{2k},$$

using the fact that $l = d_l(p)$ for any integer $l \geq 1$. If $p|A_i(\mathbf{n})$ then there can be at most p roots of $H_\alpha(\mathbf{n}, j)$. Thus, regardless of whether p divides $A_i(\mathbf{n})$ or not,

$$L_\alpha(\mathbf{n}; p) \leq d_{\gamma_k}(p) b^{2k} (p, A_i(\mathbf{n})).$$

Alternatively, if $a < 0$, then using Lemma 5.7, we obtain the analogous result:

$$L_\alpha(\mathbf{n}; p) \leq d_{\bar{\gamma}_k}(p) b^{2k} (p, A_i(\mathbf{n})),$$

where $\bar{\gamma}_k = \max(\bar{P}_{a,b,k}, \bar{\delta}_k)$. □

We may thus bound L_α as follows:

$$\begin{aligned} L_\alpha &\leq \sum_{i=1}^{2k} \sum_{\mathbf{n} \in G_i} L_\alpha(\mathbf{n}; q) \\ &\ll \sum_{i=1}^{2k} \sum_{\mathbf{n} \in G_i} \prod L_\alpha(\mathbf{n}; p) \\ &\ll \sum_{i=1}^{2k} \sum_{\mathbf{n} \in G_i} \prod d_{\eta_k}(p) b^{2k} (p, A_i(\mathbf{n})) \\ &\ll \sum_{i=1}^{2k} d(q)^{\eta_k + 2kb} \sum_{\mathbf{n} \in G_i} (q, A_i(\mathbf{n})). \end{aligned}$$

We bound the inner sum over $\mathbf{n} \in G_i$ by an argument similar to that of Proposition 4.17 in Chapter 4.

Proposition 5.9. *For each $i = 1, \ldots, 2k$,*

$$\sum_{\mathbf{n} \in G_i} (q, A_i(\mathbf{n})) \ll d(q)^{2k-1} (IQ^{-1})^{2k}.$$

Proof. Without loss of generality, let $i = 1$. Let $\alpha_h = (q, n_1 - n_h)$ for each $h > 1$, so that

$$(q, A_1(\mathbf{n})) = \left(q, \prod \alpha_h\right).$$

Then

$$\sum_{\mathbf{n}\in G_1} (q, A_1(\mathbf{n})) \leq \sum_{\alpha_h | q} \prod \alpha_h \sum_{\substack{\mathbf{n} \\ \alpha_h | (n_1 - n_h)}} 1.$$

Since $A_1(\mathbf{n}) \neq 0$ then $n_h \neq n_1$ for all $h > 1$. So for a fixed value of n_1, for which there are $2IQ^{-1}$ possible choices, the conditions $0 < n_h \leq 2IQ^{-1}$ and $\alpha_h | (n_1 - n_h)$ give $\ll 2IQ^{-1}\alpha_h^{-1}$ choices for each n_h, since necessarily $n_h \neq n_1$. Thus

$$\sum_{\mathbf{n}\in G_1} (q, A_1(\mathbf{n})) \ll \sum_{\alpha_h | q} \prod \alpha_h \cdot (2IQ^{-1}) \prod_{h>1} \left(\frac{2IQ^{-1}}{\alpha_h}\right)$$

Therefore

$$\begin{aligned} \sum_{\mathbf{n}\in G_1} (q, A_1(\mathbf{n})) &\ll (IQ^{-1})^{2k} \sum_{\substack{\alpha_h | q \\ h>1}} 1 \\ &\ll d(q)^{2k-1} (IQ^{-1})^{2k}. \end{aligned}$$

□

The final bound for L_α follows immediately.

Proposition 5.10.

$$L_\alpha \ll d(q)^{\eta_k + 2kb + 2k - 1} (IQ^{-1})^{2k}.$$

5.6.2 Estimating K_α

The bound for K_α follows easily from the definition of the set B.

Proposition 5.11.

$$K_\alpha \ll d(q)^{2kb} (IQ^{-1})^k.$$

Proof. Consider an element $\mathbf{n} \in B$. Since for each $i = 1, \ldots, 2k$ there exists $j \neq i$ such that $n_i = n_j$, then it is possible to choose only k distinct n_i, and then the remaining k values must be equal to one of those already chosen. There are at most $(IQ^{-1})^k$ ways to chose k of the n_i, and then there are at most $k!$ ways to choose the remaining k of the n_i. Once the $2k$-tuple $\mathbf{n}$ has been chosen, there are $\ll (b^{\nu(q)})^{2k}$ choices for the $2k$-tuple $\mathbf{m}$. This gives

$$N_\alpha^B(t) \ll k! (b^{\nu(q)})^{2k} (IQ^{-1})^k,$$

independent of t. Therefore,

$$K_\alpha = \max_t N_\alpha^B(t) \ll d(q)^{2kb} (IQ^{-1})^k.$$

□

5.6.3 The final bound for $N(\mathcal{I})$

We summarise these results in the following proposition, the final bound for $N(\mathcal{I})$.

Proposition 5.12. *Let q be a square-free positive integer. Let $\mathcal{I} = \{1 \leq n \leq I\}$ where $I \leq q^{\frac{k+1}{2k}}$. Choose $Q = \frac{1}{8} I^{\frac{k-1}{k+1}}$. Then for any $k \geq 1$,*

$$N(\mathcal{I}) \ll d(q)^{\tau_k} (\log q) I^{\frac{2k^2}{k+1}},$$

where τ_k depends only on a, b, k.

Proof. Recall from Proposition 5.7 that

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-1} I^{-1} (\log Q) L_\alpha.$$

The bounds for L_α and K_α given in Propositions 5.10 and 5.11 then show that

$$N(\mathcal{I}) \ll d(q)^{\omega_k} I^{2k-1} Q^{-1} + d(q)^{2kb} I^k Q^k + b^{\nu(q)} d(q)^{\eta_k + 2kb + 2k - 1} (\log Q) I^{2k-1} Q^{-1},$$

independent of the value of α. This was proved under the conditions

$$\begin{aligned} c \log q &\leq Q < I \leq q, \\ 8IQ &\leq q. \end{aligned}$$

Choosing I and Q as in the hypothesis of the proposition, these conditions are satisfied. To simplify notation, set

$$\tau_k = \max(\omega_k, 2kb, b + \eta_k + 2kb + 2k - 1).$$

We may conclude

$$N(\mathcal{I}) \ll d(q)^{\tau_k} (\log q) I^{\frac{2k^2}{k+1}}.$$

□

5.6.4 Proof of Theorem 5.2

We may now prove Theorem 5.2. By Proposition 5.3,

$$U(w, M, q) \ll M^{\frac{1}{2k}} N(\mathcal{I})^{\frac{1}{2k}},$$

where $\mathcal{I} = (w, 2w]$. Since $N(\mathcal{I})$ increases as a function of the interval, we may in fact take $\mathcal{I} = [1, 2w]$, so that applying the bound of Proposition 5.12,

$$U(w, M, q) \ll M^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}} w^{\frac{k}{k+1}},$$

where we must assume $I = 2w \leq q^{\frac{k+1}{2k}}$ and $M \leq q/2$.

We may now give the final bound for $N_q(X, Y)$. Assume that $X \leq q^{\frac{k+1}{2k}}$ so that the first condition given above is satisfied and $Y \leq q/2$ so that the second

condition is satisfied. Let J be the least integer such that $J \geq \log X / \log 2$. Then

$$\begin{aligned} N_q(X,Y) &\leq \sum_{j=0}^{J-1} U(2^j, Y, q) \\ &\ll \sum_{j=0}^{J-1} Y^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}} (2^j)^{\frac{k}{k+1}} \\ &\ll X^{\frac{k}{k+1}} Y^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}}. \end{aligned}$$

This concludes the proof of Theorem 5.2.

Chapter 6

Two bounds for the 3-part of class numbers of quadratic fields

6.1 Statement of the Theorems

In this chapter we present our first two nontrivial bounds for the 3-part of class numbers of quadratic fields. These bounds follow from the results for $N_q'(X,Y)$ given in Chapter 5. Let D be a square-free integer, positive or negative. Consider $h_3(D)$, the 3-part of the class number of the quadratic field $\mathbb{Q}(\sqrt{D})$.

Theorem 6.1. *For any positive divisor d_0 of $|D|$,*

$$h_3(D) \ll d_0^{1/2+\epsilon} + d_0^{-1}|D|^{5/4+\epsilon} + d_0^{-1/2}|D|^{1/2+\epsilon},$$

where the implied constant depends only upon ϵ. If the divisor d_0 satisfies $|D|^\alpha \ll d_0 \ll |D|^\beta$ with $\alpha > 3/4$ and $\beta < 1$, then

$$h_3(D) \ll |D|^\theta,$$

where $\theta < 1/2$. In particular, if $d_0 \approx |D|^{5/6}$, then

$$h_3(D) \ll |D|^{5/12+\epsilon},$$

for any $\epsilon > 0$.

In the general case, we prove:

Theorem 6.2. *For any square-free integer D,*

$$h_3(D) \ll |D|^{\frac{55}{112}+\epsilon}$$

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

These theorems are the first improvements on the known trivial bound.

6.2 Reduction of the problem

We begin by reducing the problem of bounding the 3-part to counting the number of integer points in a bounded region on a cubic surface, which we then further reduce to counting the number of solutions of a congruence of the form studied in Chapter 5. Theorems 6.1 and 6.2 then follow as corollaries to Theorems 5.3 and 5.4, respectively.

We now restrict our attention to imaginary quadratic fields. Let d be a square-free positive integer and consider the field $\mathbb{Q}(\sqrt{-d})$ with class group $CL(-d)$ and class number $h(-d)$. An integral basis for $\mathbb{Q}(\sqrt{-d})$ is given by $\{1, \frac{1}{2}(1+\sqrt{-d})\}$ if $-d \equiv 1 \pmod 4$ and $\{1, \sqrt{-d}\}$ if $-d \equiv 2, 3 \pmod 4$. The discriminant Δ of the field is equal to $-d$ if $-d \equiv 1 \pmod 4$ and $-4d$ if $-d \equiv 2, 3 \pmod 4$.

Suppose there is a nontrivial ideal class $[\mathfrak{a}] \in CL(-d)$ such that $[\mathfrak{a}]^3$ is the principal ideal class, so that $3|h(-d)$. By the Minkowski bound, there is an integral ideal $\mathfrak{b}$ in the ideal class $[\mathfrak{a}]$ with

$$\mathfrak{N}(\mathfrak{b}) \leq \frac{2}{\pi}\sqrt{|\Delta|}.$$

Since $\mathfrak{b}^3$ is principal, we may write

$$\mathfrak{N}(\mathfrak{b}^3) = \frac{y^2 + dz^2}{4}$$

for some $x, y \in \mathbb{N}$, or

$$4(\mathfrak{N}(\mathfrak{b}))^3 = y^2 + dz^2. \tag{6.1}$$

An integer point on the cubic surface

$$4x^3 = y^2 + dz^2 \tag{6.2}$$

specifies at most $O(d^\epsilon)$ ideals $\mathfrak{b}$ by Lemma 3.1. Thus we may obtain an upper bound for $h_3(-d)$ by bounding the number of integer points on the surface (6.2) with $x \leq L$, where $L = (4/\pi)d^{1/2}$, and hence $y \leq M$, and $z \leq N$, where $M = (16/\pi^{3/2})d^{3/4}$, and $N = (16/\pi^{3/2})d^{1/4}$.

Any such integer point (x, y, z) on the surface also provides a solution (x, y) of the congruence

$$4x^3 \equiv y^2 \pmod d \tag{6.3}$$

with $x \leq L$ and $y \leq M$. Conversely, any solution (x, y) of this congruence specifies at most 2 integer points (x, y, z) on the cubic surface. Therefore we may bound $h_3(-d)$ by estimating the number of solutions (x, y) to this congruence with x and y in the specified ranges. While studying the surface (6.2) in the form of the congruence (6.3) loses the information that z^2 is indeed a square, for now we will make this reduction.[1]

[1] In Chapter 7 we avoid this by counting the number of squares of the form $4x^3 - dz^2$.

As in Chapter 5, let

$$N'_d(L,M) = \#\{x \le L, y \le M : x^3 \equiv y^2 \pmod{d}\}.$$

Let $\bar{d} = d$ if d is odd and $\bar{d} = d/2$ if d is even. Then

$$h_3(-d) \ll d^{\epsilon} N'_{\bar{d}}(L', M'),$$

where $L' = 4L$, $M' = 4M$. Since $\bar{d}$ is odd and square-free, we may apply Theorems 5.3 and 5.4. (Note that the trivial bound $N'_{\bar{d}}(L', M') = O(d^{\epsilon} \min(L', M'))$ gives the trivial bound $h_3(-d) \ll d^{1/2+\epsilon}$.)

It is at this point that we observe that it is crucial to our methods that we consider imaginary, not real, quadratic fields. For suppose that we were to perform the same analysis for the real quadratic field $\mathbb{Q}(\sqrt{d})$, for d a positive square-free integer. We would then desire to bound the number of integer points on the cubic surface

$$4x^3 = y^2 - dz^2$$

with $x \le L$. However, in this case restricting the size of x does not restrict the sizes of y and z, so we are not able to consider only a bounded region.

Nevertheless, having obtained a bound for 3-part of class numbers of imaginary quadratic fields, an equivalent bound holds for the 3-part of class numbers of real quadratic fields, since the Scholz reflection principle [58] states that $\log_3 h_3(-d)$ and $\log_3 h_3(+3d)$ differ by at most one.

It might appear that one could apply the quite general bounds obtained in Chapter 5 in a similar manner to give a bound for the g-part $h_g(-d)$ for any $g \ge 3$. One would reduce the problem to counting the number of integer points on the variety

$$4x^g = y^2 + dz^2,$$

with the ranges $x \ll d^{1/2}$, $y \ll d^{g/4}$ and $z \ll d^{g/4-1/2}$. Thus one would require an upper bound for the number of solutions to the congruence

$$x^g \equiv y^2 \pmod{d}$$

with $x \ll d^{1/2}$ and $y \ll d^{g/4}$. However, neither Theorem 5.3 nor Theorem 5.4 may be applied for $g \ge 5$, since then the range of y is greater than the modulus d.[2] Thus the methods presented here are only applicable to bounding the 3-part of class numbers of quadratic fields.

6.3 Proof of Theorem 6.1

We first prove Theorem 6.1. By Theorem 5.3,

$$N'_{\bar{d}}(L', M') \ll d^{1/2+\epsilon} \log L + d^{-1+\epsilon} LM + d^{-1/2+\epsilon} L.$$

[2]For $g = 4$, we would examine the congruence $x^a \equiv y^b \pmod{d}$ with $a = 4$, $b = 2$. In this case we can apply neither Theorem 5.3, since $(a, b) \ne 1$, nor Theorem 5.4, since $a/b \in \mathbb{Z}^+$.

With $L \ll d^{1/2}$ and $M \ll d^{3/4}$, this gives

$$h_3(-d) \ll d^{1/2+\epsilon}.$$

Thus when applied directly, Theorem 5.3 gives only the trivial bound. However, if we assume that d has a divisor d_0 of appropriate size, we may apply Theorem 5.3 to obtain a nontrivial result. The assumption of a divisor is the most innovative aspect of Theorem 6.1.

For any divisor $d_0|d$, let $\bar{d_0} = d_0$ if d_0 is odd and $\bar{d_0} = d_0/2$ if d_0 is even, so that $\bar{d_0}|\bar{d}$. Then trivially,

$$N'_{\bar{d}}(L', M') \leq N'_{\bar{d_0}}(L', M').$$

If $\bar{d_0} \gg d^{3/4}$ then $L, M \ll d_0$ so that by Theorem 5.3,

$$h_3(-d) \ll d^{\epsilon} N'_{\bar{d_0}}(L', M') \ll d_0^{1/2+\epsilon} + d_0^{-1} d^{5/4+\epsilon} + d_0^{-1/2} d^{1/2+\epsilon}.$$

If $d_0 \ll d^{3/4}$ then even the trivial bound

$$h_3(-d) \ll d^{1/2+\epsilon}$$

is sufficient to obtain the result of Theorem 6.1. By the Scholz reflection principle, we also obtain an equivalent bound for $h_3(+3d)$. This completes the proof of Theorem 6.1.

6.4 Proof of Theorem 6.2

Theorem 6.2 is a direct corollary of Theorem 5.4. Note that L and M satisfy the requirements $L \leq (\bar{d})^{\frac{k+1}{2k}}$ and $M \leq \bar{d}/2$ for sufficiently large d. Thus Theorem 5.4 states that for any integer $k \geq 1$,

$$N'_{\bar{d}}(L', M') \ll M^{\frac{1}{2k}} L^{\frac{k}{k+1}} d(d)^{\frac{\tau_k}{2k}} (\log d)^{\frac{1}{2k}},$$

where τ_k and the implied constant depend only on k. Thus

$$N'_{\bar{d}}(L', M') \ll d^{\frac{4k^2+3k+3}{8k(k+1)}+\epsilon}.$$

Choosing $k = 6$ or $k = 7$ so as to minimise the exponent gives the result

$$N'_{\bar{d}}(L', M') \ll d^{\frac{55}{112}+\epsilon},$$

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

$$h_3(-d) \ll d^{\frac{55}{112}+\epsilon},$$

for any $\epsilon > 0$. Again by the Scholz reflection principle, an equivalent bound holds for $h_3(+3d)$. This completes the proof of Theorem 6.2.

Chapter 7

The square sieve: a third bound for the 3-part of class numbers

7.1 Introduction

In this chapter we prove a third nontrivial bound for the 3-part of class numbers of quadratic fields by employing the square sieve and the q-analogue of van der Corput's method. Once again we prove a bound for the 3-part $h_3(-d)$ of an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, where d is a square-free positive integer, and we obtain an equivalent result for real quadratic fields by the Scholz reflection principle.

In Chapter 6 we reduced the problem of bounding $h_3(-d)$ for a square-free positive integer d to counting the number of integer points within a bounded region on the cubic surface

$$4x^3 = y^2 + dz^2.$$

The methods we developed in Chapter 6 treated this equation as a congruence modulo d, losing the information that z^2 is in fact a square. In this chapter we count integer points on the cubic surface directly.

As in Chapter 6, let L, M, N describe the ranges of integer solutions (x, y, z) we consider on the cubic surface, i.e.

$$\begin{aligned} L &= (4/\pi)d^{1/2} \\ M &= (16/\pi^{3/2})d^{3/4} \\ N &= (16/\pi^{3/2})d^{1/4}. \end{aligned}$$

We could use the square sieve to count multiples of squares, dz^2, of the form

$$4x^3 - y^2, \tag{7.1}$$

or to count squares, y^2, of the form

$$4x^3 - dz^2. \tag{7.2}$$

We choose the latter approach, using the q-analogue of van der Corput's method to bound exponential sums resulting from the square sieve, as well as several key estimates resulting from Weil's proof of the Riemann hypothesis for curves over finite fields, and Deligne's results [13] for exponential sums in several variables.

The resulting theorem is as follows:

Theorem 7.1. *Let D be a square-free integer. Consider $h_3(D)$, the 3-part of the class number of the quadratic field $\mathbb{Q}(\sqrt{D})$. Then*

$$h_3(D) \ll |D|^{27/56+\epsilon}$$

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

Note that this gives a savings over the trivial bound of exactly twice that of Theorem 6.2; however, this appears to be no more than coincidence.

7.2 The square sieve

The square sieve was introduced by Heath-Brown in [31] as a method for determining the number of squares in a given sequence of integers using only information about the distribution of those integers with respect to a set of moduli. Specifically, consider the sequence $(\omega(n))$ where ω is a non-negative integer-valued function defined for each integer n, with $\sum \omega(n) < \infty$. Heath-Brown proves the following result:

Lemma 7.1 (The Square Sieve). *Let $\mathcal{P}$ be a set of P primes. Suppose that $\omega(n) = 0$ for $n = 0$ and for $|n| \geq e^P$. Then*

$$\sum_n \omega(n^2) \ll P^{-1} \sum_n \omega(n) + P^{-2} \sum_{p \neq q \in \mathcal{P}} \left| \sum_n \omega(n) \left(\frac{n}{pq} \right) \right|,$$

where the sums are over all positive integers n and $\left(\frac{n}{pq}\right)$ is the Jacobi symbol.

We prove the following variant of the square sieve for a set $\mathcal{A}$ of positive integers that are products of two primes.

Lemma 7.2 (Square Sieve Variant). *Let $\mathcal{A} = \{uv : u \in \mathcal{U}, v \in \mathcal{V}\}$ where $\mathcal{U}$ and $\mathcal{V}$ are disjoint sets of primes. Let $A = \#\mathcal{A}$, $U = \#\mathcal{U}$, and $V = \#\mathcal{V}$. Suppose that $\omega(n) = 0$ for $n = 0$ and for $|n| \geq \exp(\min(U, V))$. Then*

$$\begin{aligned}\sum_n \omega(n^2) \quad \ll \quad & A^{-1}\sum_n \omega(n) + A^{-2}\sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)=1}}\left|\sum_n \omega(n)\left(\frac{n}{fg}\right)\right| \\ & + VA^{-2}\sum_{u\neq u'\in\mathcal{U}}\left|\sum_n \omega(n)\left(\frac{n}{uu'}\right)\right| + A^{-2}|E(\mathcal{U})| \\ & + UA^{-2}\sum_{v\neq v'\in\mathcal{V}}\left|\sum_n \omega(n)\left(\frac{n}{vv'}\right)\right| + A^{-2}|E(\mathcal{V})|.\end{aligned}$$

The error terms $E(\mathcal{U})$ and $E(\mathcal{V})$ are defined by

$$\begin{aligned}E(\mathcal{U}) &= \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v|n}}\omega(n)\left(\frac{n}{uu'}\right), \\ E(\mathcal{V}) &= \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u|n}}\omega(n)\left(\frac{n}{vv'}\right).\end{aligned}$$

Proof. Let

$$\Sigma = \sum_n \omega(n)\left(\sum_{f\in\mathcal{A}}\left(\frac{n}{f}\right)\right)^2.$$

Each n is summed with non-negative weight. In particular, if $n = m^2$ then

$$\sum_{f\in\mathcal{A}}\left(\frac{n}{f}\right) = \sum_{f\in\mathcal{A}}\left(\frac{m^2}{f}\right) = \sum_{\substack{f\in\mathcal{A}\\(f,m)=1}} 1 \geq A - \sum_{\substack{f\in\mathcal{A}\\(f,m)\neq 1}} 1 \gg A,$$

where the last inequality holds as long as

$$\sum_{\substack{f\in\mathcal{A}\\(f,m)\neq 1}} 1 = o(A). \tag{7.3}$$

We may bound the sum in (7.3) by

$$\sum_{\substack{f\in\mathcal{A}\\(f,m)\neq 1}} 1 \leq V\#\{u \in \mathcal{U} : u|m\} \ll V\frac{\log m}{\log\log m},$$

or alternatively, by $U(\log m/\log\log m)$. Thus (7.3) holds as long as $w(n) = 0$ for $|n| \geq \exp(\min(U, V))$.

Then

$$\Sigma \gg A^2\sum_n \omega(n^2). \tag{7.4}$$

But also

$$\begin{aligned}\Sigma &= \sum_{f,g\in\mathcal{A}}\sum_n \omega(n)\left(\frac{n}{fg}\right)\\ &= \sum_{f\in\mathcal{A}}\sum_n \omega(n)\left(\frac{n}{f^2}\right) + \sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)=1}}\sum_n \omega(n)\left(\frac{n}{fg}\right)\\ &\quad + \sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)\neq 1}}\sum_n \omega(n)\left(\frac{n}{fg}\right). \end{aligned} \tag{7.5}$$

For $f = uv$ and $g = u'v'$, if $f \neq g$ and $(f, g) \neq 1$ then either $(f, g) = u$ or $(f, g) = v$. Thus the last term in (7.5) may be broken into two sums

$$S(\mathcal{U}) + S(\mathcal{V}) = \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v\dagger n}}\omega(n)\left(\frac{n}{uu'}\right) + \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u\dagger n}}\omega(n)\left(\frac{n}{vv'}\right).$$

The sum $S(\mathcal{U})$ may be written as a main term $M(\mathcal{U})$, summing over all positive integers n, minus a correction term $E(\mathcal{U})$:

$$S(\mathcal{U}) = M(\mathcal{U}) - E(\mathcal{U}) = V\sum_{u\neq u'\in\mathcal{U}}\sum_n \omega(n)\left(\frac{n}{uu'}\right) - \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v\mid n}}\omega(n)\left(\frac{n}{uu'}\right).$$

Analogously, we may write $S(\mathcal{V}) = M(\mathcal{V}) - E(\mathcal{V})$. Then in (7.5),

$$\begin{aligned}\Sigma &\ll A\sum_n \omega(n) + \sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)=1}}\left|\sum_n \omega(n)\left(\frac{n}{fg}\right)\right|\\ &\quad + V\sum_{u\neq u'\in\mathcal{U}}\left|\sum_n \omega(n)\left(\frac{n}{uu'}\right)\right| + |E(\mathcal{U})|\\ &\quad + U\sum_{v\neq v'\in\mathcal{V}}\left|\sum_n \omega(n)\left(\frac{n}{vv'}\right)\right| + |E(\mathcal{V})|.\end{aligned}$$

The result then follows by comparison with (7.4). □

Definition 7.1. Let

$$\omega(n) = \#\{x, z \in \mathbb{N} : n = 4x^3 - dz^2 : x \leq L, z \leq N\},$$

and

$$T(d) = \{x, y, z \in \mathbb{N} : y^2 = 4x^3 - dz^2 : x \leq L, y \leq M, z \leq N\}.$$

Then

$$h_3(-d) \ll d^{\epsilon}T(d). \tag{7.6}$$

Furthermore,

$$T(d) = \sum_{n=1}^{\infty}\omega(n^2).$$

We proceed to bound $T(d)$ using the variant of the square sieve we derived in Lemma 7.2.

We first define the set $\mathcal{A}$ over which we will sieve. Let Q be a parameter that we will fix later; for now think of $c \log d \le Q \le d$ for some constant c. Let α, β be two positive real numbers with $\alpha + \beta = 1$.

Definition 7.2. Let $\mathcal{U}, \mathcal{V}, \mathcal{A}$ be sets of sizes U, V, A, respectively, defined by

$$\begin{aligned} \mathcal{U} &= \{\text{primes } u \nmid d : c_0 Q^\alpha < u \le 2c_0 Q^\alpha\} \\ \mathcal{V} &= \{\text{primes } v \nmid d : c_1 Q^\beta < v \le 2c_1 Q^\beta\} \\ \mathcal{A} &= \{uv : u \in \mathcal{U}, v \in \mathcal{V}\}. \end{aligned}$$

We will choose the constants c_0, c_1 later so that the sets $\mathcal{U}$ and $\mathcal{V}$ are disjoint; we may further assume that $\mathcal{U}$ and $\mathcal{V}$ contain only odd primes. The number of primes in the range $c_0 Q^\alpha < u \le 2c_0 Q^\alpha$ is $O(Q^\alpha (\log Q)^{-1})$, and of these primes, $O(\log d / \log\log d)$ divide d. Assuming that $Q \ge c \log d$ for some constant c, then $U \gg Q^\alpha (\log Q)^{-1}$ and similarly $V \gg Q^\beta (\log Q)^{-1}$. Thus the set $\mathcal{A}$ is of cardinality $A = UV \gg Q (\log Q)^{-2}$.

Definition 7.3. For positive integers a, b with $(a, b) = 1$, let

$$C(d, a, b) = \sum_n \omega(n) \left(\frac{n}{ab}\right).$$

Applying Lemma 7.2 with the sets $\mathcal{A}, \mathcal{U}, \mathcal{V}$ as defined above, we obtain

$$\begin{aligned} T(d) \ll\ & A^{-1} \sum_n \omega(n) + A^{-2} \sum_{\substack{f \ne g \in \mathcal{A} \\ (f,g)=1}} |C(d, f, g)| \\ & + VA^{-2} \sum_{u \ne u' \in \mathcal{U}} |C(d, u, u')| + A^{-2} |E(\mathcal{U})| \\ & + UA^{-2} \sum_{v \ne v' \in \mathcal{V}} |C(d, v, v')| + A^{-2} |E(\mathcal{V})|. \end{aligned} \tag{7.7}$$

We will refer to the sum over $f \ne g \in \mathcal{A}$ with $(f, g) = 1$ as the main sieve, and to the sums over $u \ne u' \in \mathcal{U}$ and $v \ne v' \in \mathcal{V}$ as the prime sieves over the sets $\mathcal{U}$ and $\mathcal{V}$, respectively. The main sieve will dominate the contributions of both the prime sieves and the error terms.

The first term in (7.7), to which we will refer as the leading term, is bounded trivially by

$$A^{-1} \sum_n \omega(n) \ll A^{-1} LN \ll d^{3/4} Q^{-1} (\log Q)^2. \tag{7.8}$$

Thus it is clear that in order to attain a nontrivial bound $T(d) \ll d^\theta$, with $\theta < 1/2$, we must have at least $Q = d^{1/4+\delta}$ for some $\delta > 0$. We will choose the parameters Q and α, β so as to balance the contributions of the leading term and the main sieve.

It is at this point that we may see that an application of the original square sieve as stated in Lemma 7.1 results in only the trivial bound for $h_3(-d)$. In this case, the square sieve method would only give a savings over the trivial bound if both the ranges under consideration were greater than the square-root of the modulus (as the method relies on extending both ranges to a full set of residues). In the case of Lemma 7.1, the modulus is of size $\sqrt{pq} \approx Q$. The leading term in Lemma 7.1 is the same as in (7.7), therefore we would again have to choose Q to be at least of size $d^{1/4+\delta}$ for some $\delta > 0$. In our case, only the range $L \ll d^{1/2}$ would satisfy $L \geq \sqrt{pq}$; the range $N \ll d^{1/4}$ is too small.[1]

Sieving over products of primes, as in the square sieve variant of Lemma 7.2, is the critical innovation of our methods. We choose the sets $\mathcal{U}$ and $\mathcal{V}$ so that each element in $\mathcal{A}$ is the product of a "large" prime and a "small" prime. The q-analogue of van der Corput's method then allows us to reduce the effective modulus of certain exponential sums from the full modulus of an element in $\mathcal{A}$ to the comparatively smaller modulus of the larger prime. We choose the parameters Q and α, β so that even the smallest range $N \ll d^{1/4}$ is larger than the square-root of this new effective modulus.

7.2.1 The general term $C(d, a, b)$

Our main goal is to estimate the term $C(d, a, b)$. First note that

$$C(d,a,b) = \sum_{\substack{x \leq L \\ z \leq N}} \left(\frac{4x^3 - dz^2}{ab} \right),$$

where $\left(\frac{n}{ab}\right)$ is the Jacobi symbol. One approach to bounding this sum would be to extend the ranges of both x and z to complete sets of residues modulo ab. However, it is only advantageous to extend to a complete set of residues modulo ab if the initial range of the variable is at least $\sqrt{ab}$. If a, b are elements $f, g \in \mathcal{A}$, the range $L \ll d^{1/2}$ satisfies $L \geq \sqrt{fg}$, while $N \ll d^{1/4}$ does not. Therefore, at this stage we only extend the range of x.

Write

$$\begin{aligned} C(d,a,b) &= \sum_{z \leq N} \sum_{\alpha=1}^{ab} \left(\frac{4\alpha^3 - dz^2}{ab} \right) \sum_{\substack{x \leq L \\ x \equiv \alpha \pmod{ab}}} 1 \\ &= \sum_{z \leq N} \sum_{\alpha=1}^{ab} \left(\frac{4\alpha^3 - dz^2}{ab} \right) \frac{1}{ab} \sum_{x \leq L} \sum_{k=1}^{ab} e_{ab}(k(\alpha - x)). \end{aligned}$$

[1] We may also see that it is advantageous to count squares of the form (7.2) rather than counting multiplies of squares, dz^2, of the form (7.1) with $x \leq L$ and $y \leq M$. In this case the leading term in (7.7) would be of size $A^{-1}LM \approx d^{5/4}Q^{-1}(\log Q)^2$, which would force Q to be at least of size $d^{3/4+\delta}$ for some $\delta > 0$. Then not even the largest range $M \ll d^{3/4}$ would satisfy $M \geq \sqrt{pq}$.

For an odd positive integer $r \nmid d$, let

$$S(d, r; k, z) = \sum_{\alpha=1}^{r} \left(\frac{4\alpha^3 - dz^2}{r} \right) e_r(k\alpha)$$

and let

$$\mathbf{S}(d, r; k, N) = \sum_{z \leq N} S(d, r; k, z).$$

As before, let

$$A(ab; L, -k) = \sum_{x \leq L} e_{ab}(-kx),$$

so that

$$|A(ab; L, -k)| \leq \min(L, \|k/ab\|^{-1}).$$

Then

$$|C(d, a, b)| \leq \frac{1}{ab} \sum_{k=1}^{ab} |\mathbf{S}(d, ab; k, N)||A(ab; L, -k)|. \tag{7.9}$$

Thus the main problem is to bound sums of the form $\mathbf{S}(d, r; k, N)$. We achieve a nontrivial bound for the sum $\mathbf{S}(d, r; k, N)$ by employing the q-analogue of van der Corput's method, which allows us to extend the sum over z to a complete set of residues modulo r_0, for a divisor $r_0|r$. This gives the critical savings in the bound for $C(d, a, b)$.

In order to bound the term $C(d, f, g)$ occurring in the main sieve, we consider $\mathbf{S}(d, r; k, N)$ in the case where $r = fg = uu'vv'$ is a product of four primes. To bound $C(d, u, u')$ and $C(d, v, v')$ in the prime sieves, we consider the slightly easier case when $r = uu'$, or equivalently $r = vv'$, is a product of two primes.

In Section 7.3 we introduce the q-analogue of van der Corput's method. In Section 7.4 we estimate the contribution of the main sieve, and then in Section 7.5 we are able to estimate the contributions of the prime sieves quite quickly, using the main results of Section 7.4. The estimates for the main sieve and the prime sieves use both Weil's bound for certain exponential sums and Deligne's results [13] for exponential sums in several variables. In Section 7.6 we then choose Q and the parameters α and β so as to balance the contributions of the leading term and the main sieve. We are then able to bound the error terms in Section 7.7 using simpler arguments, involving the Weil bounds for exponential sums, but not requiring the q-analogue of van der Corput's method. Finally, in Section 7.8 we present the final bound for $T(d)$.

Before proceeding to the main body of the proof, we note that the methods we present here do not give a nontrivial bound for the g-part $h_g(-d)$ for $g > 3$. The corresponding problem is to bound

$$T_g(d) = \{x, y, z \in \mathbb{N} : y^2 = 4x^g - dz^2 : x \leq L_g, y \leq M_g, z \leq N_g\},$$

where $L_g = (4/\pi)d^{1/2}$ as before, but $M_g \ll d^{g/4}$ and $N_g \ll d^{g/4-1/2}$. Applying the variant of the square sieve as above, we obtain a bound for $T_g(d)$ equivalent to (7.7), and we may even carry through the technical analysis of the term corresponding to $C(d, a, b)$. But the range N_g is too large. In order for the leading term in (7.7), which in the general case is of size $Q^{-1}L_gN_g(\log Q)^2$, to be less than the trivial bound $d^{1/2+\epsilon}$, we would need to choose Q to be at least of size $d^{g/4-1/2+\delta}$, for some $\delta > 0$. As we will see in the following analysis, the main sieve cannot accommodate such a large value for Q and still give a nontrivial answer, if $g > 3$. Thus these methods give a nontrivial bound only for $h_3(-d)$.

7.3 The q-analogue of van der Corput's method

The simplest version of van der Corput's method for bounding exponential sums is based on the idea that in order to bound a sum of the form

$$\mathbf{S} = \sum_{A<n\leq B} e(f(n))$$

for some real valued function $f(n)$, one may instead study the quantity

$$H\mathbf{S} = \sum_{h=1}^{H} \sum_{A-h<n\leq B-h} e(f(n+h)),$$

for an arbitrary positive integer H. Applying Cauchy's inequality, one then obtains

$$H^2|\mathbf{S}|^2 \leq (B-A+H) \sum_{|h|<H} (H-|h|) \sum_{n\in I_h} e(f(n+h)\overline{e(f(n))}, \tag{7.10}$$

where $I_h = \{n : A < n, n+h \leq B\}$. In many cases the differenced function

$$e(f(n+h) - f(n))$$

is simpler to handle than the original function $e(f(n))$; for example, if $f(n)$ is a polynomial, then $f(n+h) - f(n)$ has lower degree than $f(n)$ itself. (For a full exposition of the method, see [21].)

The q-analogue of van der Corput's method was introduced by Heath-Brown in [29], [32] to handle exponential sums involving not $e(f(n))$ but the periodic function $e_q(f(n))$. This method uses an inequality similar to (7.10), of the form

$$H^2|\mathbf{S}|^2 \leq (B-A+H) \sum_{|h|<H} (H-|h|) \sum_{n\in I_h} e_q(f(n+hq_0))\overline{e_q(f(n))},$$

where q_0 is a divisor of q and $I_h = \{n : A < n, n+hq_0 \leq B\}$. This serves not only to average over h but also to reduce the effective period of the function

in the summand from q to q/q_0, thus sharpening the bound. We will see that this method is sufficient to attain a nontrivial bound for the main sieve and the prime sieve terms.

7.4 The main sieve

We now apply the q-analogue of van der Corput's method to the term $\mathbf{S}(d, r; k, N)$ appearing in the main sieve. To fix notation, elements $f \neq g \in \mathcal{A}$ with $(f, g) = 1$ will be written as $f = uv$ and $g = u'v'$, where $u \neq u' \in \mathcal{U}$, $v \neq v' \in \mathcal{V}$. We further set $r = fg$, with the factorisation $r = r_0 r_1$, where $r_0 = uu'$ and $r_1 = vv'$, so that $r_0 \approx Q^{2\alpha}$ and $r_1 \approx Q^{2\beta}$.

First note that by Lemma 3.11 the sum $S(d, r; k, z)$ is multiplicative in the sense that

$$S(d, r_0 r_1; k, z) = S(d, r_0; k\overline{r_1}, z) S(d, r_1; k\overline{r_0}, z), \tag{7.11}$$

for $(r_0, r_1) = 1$, where $r_0\overline{r_0} \equiv 1 \pmod{r_1}$ and $r_1\overline{r_1} \equiv 1 \pmod{r_0}$.

Temporarily define

$$A(z) = \begin{cases} S(d, r; k, z) & \text{if } 1 \leq z \leq N \\ 0 & \text{otherwise.} \end{cases}$$

Similarly define $A_0(z)$ to be equal to $S(d, r_0; k\overline{r_1}, z)$ if $1 \leq z \leq N$ and zero otherwise, and $A_1(z)$ to be equal to $S(d, r_1; k\overline{r_0}, z)$ if $1 \leq z \leq N$ and zero otherwise.

Then for a positive integer H, which we will choose later,

$$\begin{aligned} H\mathbf{S}(d, r; k, N) &= \sum_{h=1}^{H} \sum_{z} A(z + hr_1) \\ &= \sum_{1 - Hr_1 \leq z \leq N - r_1} \sum_{h=1}^{H} A_0(z + hr_1) A_1(z + hr_1) \\ &= \sum_{1 - Hr_1 \leq z \leq N - r_1} S(d, r_1; k\overline{r_0}, z) \sum_{h=1}^{H} A_0(z + hr_1), \end{aligned}$$

since $S(d, r_1; k\overline{r_0}, z + hr_1) = S(d, r_1; k\overline{r_0}, z)$ for all values of h. Thus by Cauchy's inequality,

$$H^2 |\mathbf{S}(d, r; k, N)|^2 \leq \Sigma_1 \Sigma_2,$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{1 - Hr_1 \leq z \leq N - r_1} |S(d, r_1; k\overline{r_0}, z)|^2, \\ \Sigma_2 &= \sum_{z} \left| \sum_{h=1}^{H} A_0(z + hr_1) \right|^2. \end{aligned}$$

(Unless otherwise noted, the sum over z is taken to be over all integers; the characteristic function A_0 effectively restricts the sum to the appropriate range.) We will further separate the sum Σ_2 into two parts. Observe that

$$\begin{aligned}\Sigma_2 &= \sum_{h_1=1}^{H}\sum_{h_2=1}^{H}\sum_z A_0(z+h_1r_1)\overline{A_0(z+h_2r_1)}\\ &= \sum_{h_1=1}^{H}\sum_{h_2=1}^{H}\sum_z A_0(z+(h_1-h_2)r_1)\overline{A_0(z)}\\ &= \sum_{|h|<H}(H-|h|)\sum_z A_0(z+hr_1)\overline{A_0(z)}.\end{aligned}$$

Thus in absolute value,

$$|\Sigma_2| \le 2H\sum_{h=0}^{H-1}\left|\sum_z A_0(z+hr_1)\overline{A_0(z)}\right|.$$

Let

$$\begin{aligned}\Sigma_{2A} &= H\sum_z |A_0(z)|^2,\\ \Sigma_{2B} &= H\sum_{h=1}^{H-1}\left|\sum_z A_0(z+hr_1)\overline{A_0(z)}\right|.\end{aligned}$$

Then

$$H^2|\mathbf{S}(d,r;k,N)|^2 \ll \Sigma_1\left(\Sigma_{2A}+\Sigma_{2B}\right). \tag{7.12}$$

In Section 7.4.1 we bound Σ_1 and Σ_{2A}, and in Section 7.4.2 we bound Σ_{2B}.

7.4.1 Bounding the sums Σ_1 and Σ_{2A}

By definition,

$$\Sigma_1 = \sum_{1-Hr_1\le z\le N-r_1}|S(d,r_1;k\overline{r_0},z)|^2.$$

Consider

$$S(d,r_1;k\overline{r_0},z) = \sum_{\alpha=1}^{r_1}\left(\frac{4\alpha^3-dz^2}{r_1}\right)e_{r_1}(k\overline{r_0}\alpha).$$

Since $r_1 = vv'$ with primes $v \ne v'$, this further factorises as

$$S(d,vv';k\overline{r_0},z) = S(d,v;k\overline{r_0}\overline{v'},z)S(d,v';k\overline{r_0v},z),$$

where $v\overline{v} \equiv 1 \pmod{v'}$ and $v'\overline{v'} \equiv 1 \pmod{v}$.

Similarly, for

$$\Sigma_{2A} = H\sum_{1\le z\le N}|S(d,r_0;k\overline{r_1},z)|^2,$$

where $r_0 = uu'$ with primes $u \neq u'$, we have the factorisation

$$S(d, uu'; k\overline{r_1}, z) = S(d, u; k\overline{r_1}\,\overline{u'}, z)S(d, u'; k\overline{r_1 u}, z).$$

Thus it suffices to bound the sum

$$S(d, p; t, z) = \sum_{\alpha=1}^{p} \left(\frac{4\alpha^3 - dz^2}{p}\right) e_p(t\alpha),$$

for any odd prime $p \nmid d$ and positive integers t, z.

Lemma 7.3. *Let p be any odd prime $p \nmid d$. Then*

$$|S(d, p; t, z)| \leq 3p^{1/2}.$$

Proof. First assume that $p > 3$. In the case that $p \nmid z$ and $p \nmid t$, the Weil bound for hybrid sums of a multiplicative and an additive character modulo p, given as Lemma 3.8, shows that

$$|S(d, p; t, z)| \leq 3p^{1/2}.$$

If $p \nmid z$ but $p|t$ then

$$\begin{aligned} p + S(d, p; t, z) &= \sum_{\alpha=1}^{p} \left[1 + \left(\frac{4\alpha^3 - dz^2}{p}\right)\right] \\ &= \#\{\alpha, \beta \pmod p : \beta^2 \equiv 4\alpha^3 - dz^2 \pmod p\} \\ &= p + a_p, \end{aligned}$$

where a_p is the usual quantity associated with counting points on elliptic curves over finite fields, with $|a_p| \leq 2p^{1/2}$. (Note that we do not count the point at infinity.) It follows that

$$|S(d, p; t, z)| \leq 2p^{1/2}.$$

If $p|z$ but $p \nmid t$, then

$$S(d, p; t, z) = \sum_{\alpha=1}^{p} \left(\frac{\alpha}{p}\right) e_p(t\alpha),$$

so that

$$|S(d, p; t, z)| \leq \sqrt{p}.$$

If $p|z$ and $p|t$, then

$$S(d, p; t, z) = \sum_{\alpha=1}^{p} \left(\frac{4\alpha^3}{p}\right) = \sum_{\alpha=1}^{p} \left(\frac{\alpha}{p}\right) = 0.$$

For $p = 3$ we simply use the trivial bound

$$|S(d, p; t, z)| = 3.$$

Thus in all cases,

$$|S(d,p;t,z)| \leq 3p^{1/2}.$$

□

This immediately gives the following lemma:

Lemma 7.4.

$$\begin{aligned}\Sigma_1 &\ll (N+Hr_1)r_1,\\ \Sigma_{2A} &\ll HNr_0.\end{aligned}$$

7.4.2 Bounding the sum Σ_{2B}

Define

$$T(d,r_0;h,N) = \sum_z A_0(z+hr_1)\overline{A_0(z)},$$

so that

$$\Sigma_{2B} = H\sum_{h=1}^{H-1}|T(d,r_0;h,N)|. \tag{7.13}$$

By definition,

$$T(d,r_0;h,N) = \sum_{1\leq z\leq N-hr_1} S(d,r_0;k\overline{r_1},z+hr_1)\overline{S(d,r_0;k\overline{r_1},z)}.$$

It is at this point that we extend the range of the sum over z to a complete set of residues. While extending the range to the full modulus $r \approx Q^2$ would be too great a loss, our hope is that we will be able to choose the parameters Q and α so that extending the range to the modulus r_0, where $r_0 \approx Q^{2\alpha}$, is not. Therefore we write

$$\begin{aligned}T(d,r_0;h,N) &= \sum_{l=1}^{r_0} S(d,r_0;k\overline{r_1},l+hr_1)\overline{S(d,r_0;k\overline{r_1},l)}\\ &\quad\cdot\sum_{1\leq z\leq N-hr_1}\frac{1}{r_0}\sum_{m=1}^{r_0} e_{r_0}(m(l-z)).\end{aligned}$$

Thus

$$|T(d,r_0;h,N)| \leq \frac{1}{r_0}\sum_{m=1}^{r_0}|W(d,r_0;h,m,k\overline{r_1})|\,|A(r_0;N,-m)|\,, \tag{7.14}$$

where $A(r_0;N,-m)$ is as before and

$$\begin{aligned}&W(d,r_0;h,m,k\overline{r_1}) \qquad (7.15)\\ &= \sum_{\substack{l,\alpha,\beta\\ (\mathrm{mod}\ r_0)}}\left(\frac{4\alpha^3-d(l+hr_1)^2}{r_0}\right)\left(\frac{4\beta^3-dl^2}{r_0}\right)e_{r_0}(k\overline{r_1}\alpha-k\overline{r_1}\beta+ml).\end{aligned}$$

A simple computation similar to that of Lemma 3.11 shows that $W(d, r_0; h, m, k\overline{r_1})$ is multiplicative in the sense that for $r_0 = uu'$ with $(u, u') = 1$,

$$W(d, r_0; h, m, k\overline{r_1}) = W(d, u; h, m\overline{u'}, k\overline{r_1}\,\overline{u'})W(d, u'; h, m\overline{u}, k\overline{r_1 u}),$$

where $u\overline{u} \equiv 1 \pmod{u'}$ and $u'\overline{u'} \equiv 1 \pmod{u}$. Thus it is sufficient to bound the sum

$$W(d, p; h, s, t) = \sum_{\substack{l,\alpha,\beta \\ (\mathrm{mod}\ p)}} \left(\frac{4\alpha^3 - d(l + hr_1)^2}{p}\right)\left(\frac{4\beta^3 - dl^2}{p}\right) e_p(t\alpha - t\beta + sl)$$

for any odd prime p with $p \nmid d$ and $p \nmid r_1$.

The following key estimate, due to Katz [43], uses Deligne's estimates for exponential sums in several variables [13].

Lemma 7.5. *Let $p > 3$ be a prime with $p \nmid d$ and $p \nmid r_1$. If $p \nmid h$ or $p \nmid s$, then*

$$|W(d, p; h, s, t)| \leq 24p^{3/2}.$$

We make the following simpler estimates in the cases when p divides both h and s.

Lemma 7.6. *Let $p > 3$ be a prime with $p \nmid d$ and $p \nmid r_1$. If $p|h$ and $p|s$, but $p \nmid t$, then*

$$|W(d, p; h, s, t)| \leq 9p^2.$$

Proof. In this case

$$W(d, p; h, s, t) = \sum_{\substack{l,\alpha,\beta \\ (\mathrm{mod}\ p)}} \left(\frac{4\alpha^3 - dl^2}{p}\right)\left(\frac{4\beta^3 - dl^2}{p}\right) e_p(t\alpha - t\beta),$$

so that

$$|W(d, p; h, s, t)| \leq \sum_{l \pmod p} \left| \sum_{\alpha \pmod p} \left(\frac{4\alpha^3 - dl^2}{p}\right) e_p(t\alpha)\right|^2.$$

We may bound the inner sum using the Weil bound for hybrid sums of a multiplicative and an additive character modulo p (Lemma 3.8), obtaining

$$|W(d, p; h, s, t)| \leq 9p^2.$$

□

Lemma 7.7. *Let $p > 3$ be a prime with $p \nmid d$ and $p \nmid r_1$. If $p|h$, $p|s$, and $p|t$, then:*

$$\begin{aligned} |W(d, p; h, s, t)| &= 0 \quad \text{if } p \equiv 2 \ (\mathit{mod}\ 3) \\ |W(d, p; h, s, t)| &\leq 4p^2 \quad \text{if } p \equiv 1 \ (\mathit{mod}\ 3). \end{aligned}$$

Proof. In this case

$$W(d,p;h,s,t) = \sum_{\substack{l,\alpha,\beta \\ (\mathrm{mod}\ p)}} \left(\frac{4\alpha^3 - dl^2}{p}\right)\left(\frac{4\beta^3 - dl^2}{p}\right),$$

so that

$$|W(d,p;h,s,t)| \leq \sum_{l\ (\mathrm{mod}\ p)} \left| \sum_{\alpha\ (\mathrm{mod}\ p)} \left(\frac{4\alpha^3 - dl^2}{p}\right)\right|^2.$$

If $p \equiv 2 \pmod 3$, then $4\alpha^3 - dl^2$ (for fixed l) ranges over a complete set of residues as α does, so that the inner sum is

$$\sum_{\alpha\ (\mathrm{mod}\ p)} \left(\frac{4\alpha^3 - dl^2}{p}\right) = \sum_{\beta\ (\mathrm{mod}\ p)} \left(\frac{\beta}{p}\right) = 0.$$

Thus

$$|W(d,p;h,s,t)| = 0.$$

If $p \equiv 1 \pmod 3$ we may argue, as in Lemma 7.3, that

$$p + \sum_{\alpha\ (\mathrm{mod}\ p)} \left(\frac{4\alpha^3 - dl^2}{p}\right)$$

is the number of points on the elliptic curve $\beta^2 = 4\alpha^3 - dl^2$ over $\mathbb{F}_p$, not counting the point at infinity, and hence is equal to $p + a_p$, where $|a_p| \leq 2p^{1/2}$. Thus

$$\left| \sum_{\alpha\ (\mathrm{mod}\ p)} \left(\frac{4\alpha^3 - dl^2}{p}\right)\right| \leq 2p^{1/2},$$

so that in total

$$|W(d,p;h,s,t)| \leq 4p^2.$$

□

For the prime $p = 3$ we may simply use the trivial bound

$$|W(d,p;h,s,t)| \leq 3.$$

We summarise all these results in the following lemma:

Lemma 7.8. *Let p be an odd prime with $p \nmid d$ and $p \nmid r_1$. Then*

$$|W(d,p;h,s,t)| \leq 24p^{3/2}(p,h,s)^{1/2}.$$

Since the prime u does not divide $\overline{r_1}, \overline{u'}$, and similarly u' does not divide $\overline{r_1}, \overline{u}$, it follows immediately that

$$\begin{aligned} |W(d,u;h,m\overline{u'},k\overline{r_1}\overline{u'})| &\leq 24u^{3/2}(u,h,m)^{1/2} \\ |W(d,u';h,m\overline{u},k\overline{r_1 u})| &\leq 24u'^{3/2}(u',h,m)^{1/2}, \end{aligned}$$

so that

$$|W(d, r_0; h, m, k\overline{r_1})| \ll r_0^{3/2}(r_0, h, m)^{1/2}.$$

Thus in (7.14),

$$|T(d, r_0; h, N)| \ll r_0^{1/2} \sum_{m=1}^{r_0} (r_0, h, m)^{1/2} \min(N, \|m/r_0\|^{-1}).$$

By (7.13) we then have

$$\begin{aligned} \Sigma_{2B} &\ll Hr_0^{1/2} \sum_{h=1}^{H-1} \sum_{m=1}^{r_0} (r_0, h, m)^{1/2} \min(N, \|m/r_0\|^{-1}) \\ &= NHr_0^{1/2} \sum_{h=1}^{H-1} (h, r_0)^{1/2} \qquad (7.16) \\ &\quad + Hr_0^{1/2} \sum_{h=1}^{H-1} \sum_{m=1}^{r_0-1} \|m/r_0\|^{-1} (r_0, h, m)^{1/2}. \qquad (7.17) \end{aligned}$$

Bounds for the sums (7.16) and (7.17) are given in Lemmas 5.4 and 5.3, respectively, of Section 5.3.2. It follows that:

Lemma 7.9.

$$\Sigma_{2B} \ll H^2 N r_0^{1/2} d(r_0) + H^2 r_0^{3/2} d(r_0) \log r_0.$$

7.4.3 Bounding the sum $\mathbf{S}(d, r; k, N)$

Assembling the results of Lemmas 7.4 and 7.9 in (7.12), it follows that

$$\begin{aligned} H^2 |\mathbf{S}(d, r; k, N)|^2 &\ll HN(N + Hr_1) r_0 r_1 \\ &\quad + (N + Hr_1) r_1 \left[H^2 N r_0^{1/2} d(r_0) + H^2 r_0^{3/2} d(r_0) \log r_0 \right]. \end{aligned}$$

Hence

$$\begin{aligned} |\mathbf{S}(d, r; k, N)|^2 &\ll H^{-1} N(N + Hr_1) r_0 r_1 \qquad (7.18) \\ &\quad + (N + Hr_1) r_1 \left[N r_0^{1/2} d(r_0) + r_0^{3/2} d(r_0) \log r_0 \right]. \end{aligned}$$

7.4.4 Choosing H

Suppose that $Hr_1 \geq N$. Then the right hand side of (7.18) is of the form

$$Nr_0 r_1^2 + HN r_0^{1/2} r_1^2 d(r_0) + Hr_0^{3/2} r_1^2 d(r_0) \log r_0.$$

This is increasing in H, so we choose H to be as small as possible, namely $H = [N/r_1]$. Next suppose that $Hr_1 \leq N$. Then the right hand side of (7.18) is of the form

$$H^{-1} N^2 r_0 r_1 + N^2 r_0^{1/2} r_1 d(r_0) + N r_0^{3/2} r_1 d(r_0) \log r_0.$$

This is decreasing in H, so we choose H to be as large as possible, namely $H = [N/r_1]$. Thus in either case we choose $H = [N/r_1]$ and (7.18) becomes

$$|\mathbf{S}(d, r; k, N)|^2 \ll Nr_0r_1^2 + N^2 r_0^{1/2} r_1 d(r_0) + Nr_0^{3/2} r_1 d(r_0) \log r_0.$$

Thus we finally obtain:

Proposition 7.1.

$$|\mathbf{S}(d, r; k, N)| \ll Nr_0^{1/4} r_1^{1/2} (d(r_0))^{1/2} + N^{1/2} r_0^{1/2} r_1 + N^{1/2} r_0^{3/4} r_1^{1/2} (d(r_0))^{1/2} (\log r_0)^{1/2}.$$

7.4.5 Bounding $C(d, f, g)$

We may now achieve a bound for the term $C(d, f, g)$ in the main sieve.

Proposition 7.2. *For any $f \neq g \in \mathcal{A}$ with $(f, g) = 1$,*

$$|C(d, f, g)| \leq \left[Q^{-2}L + \log Q\right] \left[NQr_0^{-1/4+\epsilon} + N^{1/2}Q^2 r_0^{-1/2} + N^{1/2}Qr_0^{1/4+\epsilon}\right].$$

Proof. By (7.9),

$$|C(d, f, g)| \leq \frac{1}{fg} \sum_{k=1}^{fg} |\mathbf{S}(d, fg; k, N)||A(fg; L, -k)|.$$

Recalling that $r = fg = r_0r_1$, and noting that the bound given for $|\mathbf{S}(d, r; k, N)|$ in Proposition 7.1 is independent of k,

$$\begin{aligned} |C(d, f, g)| &\leq \frac{1}{fg} \max_k |\mathbf{S}(d, r; k, N)| \left[L + \sum_{k=1}^{fg-1} \|k/fg\|^{-1}\right] \\ &\ll \frac{1}{fg} \max_k |\mathbf{S}(d, r; k, N)| \left[L + fg \sum_{1 \leq k \leq fg/2} k^{-1}\right] \\ &\ll \max_k |\mathbf{S}(d, r; k, N)| \left[Q^{-2}L + \log Q\right]. \end{aligned}$$

Recalling that $r_1r_0 \approx Q^2$, the result then follows from Proposition 7.1. □

This completes our estimate for the main sieve.

7.5 The prime sieves

We now consider briefly the term $\mathbf{S}(d, r; k, N)$ in the case of the prime sieves, when r is a product of two distinct primes. This merely requires using the machinery already developed for the main sieve, and is in fact simpler as we need only factorise the exponential sums under consideration once. The case where $r = uu'$ is the product of two distinct primes in the set $\mathcal{U}$ is analogous to

the case where $r = vv'$ is the product of two distinct primes in the set $\mathcal{V}$, so we will outline the argument only for the set $\mathcal{U}$.

Recall from (7.11) that $S(d, uu'; k, z)$ is multiplicative in the sense that

$$S(d, uu'; k, z) = S(d, u; k\overline{u'}, z)S(d, u'; k\overline{u}, z),$$

for primes $u \neq u' \in \mathcal{U}$. Define

$$A(z) = \begin{cases} S(d, uu'; k, z) & \text{if } 1 \leq z \leq N \\ 0 & \text{otherwise.} \end{cases}$$

Similarly define $A_0(z)$ to be equal to $S(d, u; k\overline{u'}, z)$ if $1 \leq z \leq N$ and zero otherwise, and $A_1(z)$ to be equal to $S(d, u'; k\overline{u}, z)$ if $1 \leq z \leq N$ and zero otherwise.

Let H_u be a positive integer, which we will specify later. Applying the q-analogue of van der Corput's method exactly as in Section 7.4, we obtain a bound equivalent to that of equation (7.12), namely

$$H_u^2 |\mathbf{S}(d, uu'; k, N)|^2 \ll \Sigma_1 \left(\Sigma_{2A} + \Sigma_{2B}\right), \tag{7.19}$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{1 - H_{\mathcal{U}} u' \leq z \leq N - u'} \left|S(d, u'; k\overline{u}, z)\right|^2, \\ \Sigma_{2A} &= H_u \sum_z \left|A_0(z)\right|^2, \\ \Sigma_{2B} &= H_u \sum_{h=1}^{H_{\mathcal{U}}-1} \left| \sum_z A_0(z + hu')\overline{A_0(z)} \right|. \end{aligned}$$

By Lemma 7.3 it follows immediately that:

Lemma 7.10.

$$\begin{aligned} \Sigma_1 &\ll (N + H_u u')u', \\ \Sigma_{2A} &\ll H_u N u. \end{aligned}$$

Again let

$$T(d, u; h, N) = \sum_z A_0(z + hu')\overline{A_0(z)},$$

so that

$$\Sigma_{2B} = H_u \sum_{h=1}^{H_{\mathcal{U}}-1} |T(d, u; h, N)|. \tag{7.20}$$

Define $W(d, u; h, m, k\overline{u'})$ as in (7.15), so that

$$|T(d, u; h, N)| \leq \frac{1}{u} \sum_{m=1}^{u} \left|W(d, u; h, m, k\overline{u'})\right| \left|A(u; N, -m)\right|. \tag{7.21}$$

It follows immediately from Lemma 7.8 that

$$|T(d,u;h,N)| \ll u^{1/2}\sum_{m=1}^{u}(u,h,m)^{1/2}\min(N,\|m/u\|^{-1}),$$

so that from (7.20) we have

$$\Sigma_{2B} \ll H_u u^{1/2}\sum_{h=1}^{H_u-1}\sum_{m=1}^{u}(u,h,m)^{1/2}\min(N,\|m/u\|^{-1}).$$

Thus:

Lemma 7.11.

$$\Sigma_{2B} \ll H_u^2 N u^{1/2} d(u) + H_u^2 u^{3/2} d(u)\log u.$$

Assembling the bounds for $\Sigma_1, \Sigma_{2A}, \Sigma_{2B}$, it then follows from (7.19) that

$$\begin{aligned} H_u^2|\mathbf{S}(d,uu';k,N)|^2 &\ll H_u N(N+H_u u')uu' \\ &\quad + (N+H_u u')u'\left[H_u^2 N u^{1/2}d(u) + H_u^2 u^{3/2}d(u)\log u\right]. \end{aligned}$$

Thus

$$|\mathbf{S}(d,uu';k,N)|^2 \ll H_u^{-1}N(N+H_u u')uu' + (N+H_u u')u'\left[Nu^{1/2}d(u) + u^{3/2}d(u)\log u\right].$$

Choosing $H_u = [N/u']$ analogously to H, we then finally obtain

$$|\mathbf{S}(d,r;k,N)| \ll Nu^{1/4}u'^{1/2}(d(u))^{1/2} + N^{1/2}u^{1/2}u' + N^{1/2}u^{3/4}u'^{1/2}(d(u))^{1/2}(\log u)^{1/2}.$$

As in Section 7.4.5, we then obtain a bound for $C(d,u,u')$, which we may write in terms of Q, using the fact that $u, u' \approx Q^{\alpha}$. For reference we state the corresponding result for $C(d,v,v')$ as well:

Proposition 7.3. *For any $u \neq u' \in \mathcal{U}$ and $v \neq v' \in \mathcal{V}$,*

$$\begin{aligned} |C(d,u,u')| &\leq \left[Q^{-2\alpha}L + \log Q\right]\left[NQ^{(3/4)\alpha+\epsilon} + N^{1/2}Q^{(3/2)\alpha} + N^{1/2}Q^{(5/4)\alpha+\epsilon}\right], \\ |C(d,v,v')| &\leq \left[Q^{-2\beta}L + \log Q\right]\left[NQ^{(3/4)\beta+\epsilon} + N^{1/2}Q^{(3/2)\beta} + N^{1/2}Q^{(5/4)\beta+\epsilon}\right]. \end{aligned}$$

This completes our bounds for the prime sieve terms.

7.6 Choosing the parameters Q, α, β

Recall from equation (7.7) that

$$\begin{aligned} T(d) \ll\ & A^{-1}LN + A^{-2}\sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)=1}}|C(d,f,g)| \\ & + VA^{-2}\sum_{u\neq u'\in\mathcal{U}}|C(d,u,u')| + A^{-2}|E(\mathcal{U})| \\ & + UA^{-2}\sum_{v\neq v'\in\mathcal{V}}|C(d,v,v')| + A^{-2}|E(\mathcal{V})|. \end{aligned}$$

Note that in each case the bounds we have proved for $|C(d,f,g)|$, $|C(d,u,u')|$ and $|C(d,v,v')|$ are independent of the specific elements chosen from the sets $\mathcal{A}$,$\mathcal{U}$ or $\mathcal{V}$. Therefore we need only estimate the number of terms in each sum. There are $\ll A^2$ terms in the sum over $f \neq g \in \mathcal{A}$ with $(f,g)=1$, since for each $f=uv$, of which there are UV choices, there are $(U-1)(V-1)$ choices for $g=u'v'$ with $u' \neq u, v' \neq v$. There are $\ll U^2$ terms in the sum over $u \neq u' \in \mathcal{U}$, and $\ll V^2$ terms in the sum over $v \neq v' \in \mathcal{V}$. Therefore, applying the bounds of Propositions 7.2 and 7.3, we obtain

$$\begin{aligned} T(d) \ll\ & Q^{-1}LN(\log Q)^2 \\ & + \left[Q^{-2}L + \log Q\right]\left[NQr_0^{-1/4+\epsilon} + N^{1/2}Q^2r_0^{-1/2} + N^{1/2}Qr_0^{1/4+\epsilon}\right] \\ & + V^{-1}\left[Q^{-2\alpha}L + \log Q\right]\left[NQ^{(3/4)\alpha+\epsilon} + N^{1/2}Q^{(3/2)\alpha} + N^{1/2}Q^{(5/4)\alpha+\epsilon}\right] \\ & + U^{-1}\left[Q^{-2\beta}L + \log Q\right]\left[NQ^{(3/4)\beta+\epsilon} + N^{1/2}Q^{(3/2)\beta} + N^{1/2}Q^{(5/4)\beta+\epsilon}\right] \\ & + A^{-2}|E(\mathcal{U})| + A^{-2}|E(\mathcal{V})|. \end{aligned}$$

We choose Q so as to balance the contributions of the leading term and the main sieve. For simplicity, consider temporarily the following expression, disregarding factors of size Q^ϵ:

$$T'(d) = Q^{-1}LN + \left[Q^{-2}L + \log Q\right]\left[NQr_0^{-1/4} + N^{1/2}Q^2r_0^{-1/2} + N^{1/2}Qr_0^{1/4}\right].$$

With $L \ll d^{1/2}$ and $N \ll d^{1/4}$, this gives

$$T'(d) \ll d^{3/4}Q^{-1} + \left[d^{1/2}Q^{-2} + \log Q\right]\left[d^{1/4}Qr_0^{-1/4} + d^{1/8}Q^2r_0^{-1/2} + d^{1/8}Qr_0^{1/4}\right].$$

We see from the leading term that in order to obtain a nontrivial bound, we must have at least $Q = d^{1/4+\delta}$ with $\delta > 0$. Then $d^{1/2}Q^{-2} = d^{-2\delta} \ll \log Q$, so it is sufficient to consider the expression

$$T''(d) \ll d^{3/4}Q^{-1} + d^{1/4}Qr_0^{-1/4} + d^{1/8}Q^2r_0^{-1/2} + d^{1/8}Qr_0^{1/4}.$$

Taking $r_0 = Q^{4/3}$ therefore gives

$$T''(d) \ll d^{1/2-\delta} + d^{5/12+(2/3)\delta} + d^{11/24+(4/3)\delta}.$$

It is optimal to choose

$$\delta = 1/56.$$

Then

$$T'(d) \ll d^\epsilon T''(d) \ll d^{1/2-1/56+\epsilon} \approx d^{0.48214\ldots+\epsilon}.$$

With the choices $Q = d^{1/4+1/56}$ and $r_0 = Q^{4/3}$, we then see that $\alpha = 2/3$ and $\beta = 1/3$. Note that we may now choose the constants c_0, c_1 in the definition of the sets $\mathcal{U}$ and $\mathcal{V}$ so that $\mathcal{U}$ and $\mathcal{V}$ are disjoint; it is sufficient to choose $c_0 = 2, c_1 = 1$.

The prime sieve over the set $\mathcal{U}$ is bounded by

$$d^{3/56+\epsilon}\left[NQ^{1/2+\epsilon}+N^{1/2}Q+N^{1/2}Q^{5/6+\epsilon}\right] \ll d^{25/56+\epsilon} \approx d^{0.44642\ldots+\epsilon},$$

and the prime sieve over the set $\mathcal{V}$ is bounded by

$$d^{1/7+\epsilon}\left[NQ^{1/4+\epsilon}+N^{1/2}Q^{1/2}+N^{1/2}Q^{5/12+\epsilon}\right] \ll d^{103/224+\epsilon} \approx d^{0.45982\ldots+\epsilon}.$$

Thus it is clear that the prime sieves are dominated by the leading term and the main sieve. Assuming that the error terms are also dominated by the leading term (as we show in the following section), we have the final bound

$$T(d) \ll d^{1/2-1/56+\epsilon}. \tag{7.22}$$

7.7 The error terms

It remains to estimate the contributions of the error terms $E(\mathcal{U})$ and $E(\mathcal{V})$ in the square sieve. The choices of Q and α, β made in the previous section determine the cardinalities U and V of the sets $\mathcal{U}$ and $\mathcal{V}$; while we could have estimated the error terms without this knowledge, it is convenient to know how sharp an estimate is required. We will see that it is sufficient to bound $E(\mathcal{V})$ with a trivial estimate, but $E(\mathcal{U})$ requires that we take advantage of cancellation in certain exponential sums.

Recall that the error terms $E(\mathcal{U})$ and $E(\mathcal{V})$ are defined by

$$\begin{aligned} E(\mathcal{U}) &= \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v|n}}\omega(n)\left(\frac{n}{uu'}\right), \\ E(\mathcal{V}) &= \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u|n}}\omega(n)\left(\frac{n}{vv'}\right). \end{aligned}$$

7.7.1 The trivial bound

We may estimate $E(\mathcal{U})$ trivially by

$$\begin{aligned} |E(\mathcal{U})| &\leq \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v|n}}\omega(n) \\ &\ll \sum_{u\neq u'\in\mathcal{U}}\sum_{n}\omega(n)\frac{\log n}{\log\log n} \\ &\ll U^2\min(U,V)LN, \end{aligned}$$

where the last step may be seen using Abel summation and noting that $\omega(n)$ is zero for $|n| \geq \exp(\min(U,V))$. Thus since $A = UV$,

$$A^{-2}|E(\mathcal{U})| \ll V^{-2}\min(U,V)LN. \tag{7.23}$$

With U and V as chosen in the previous section, (7.23) is on the order of $V^{-1}LN \ll d^{37/56+\epsilon}$, so this trivial bound is not sufficient. However, the equivalent bound for $E(\mathcal{V})$ gives

$$A^{-2}|E(\mathcal{V})| \ll U^{-2}\min(U,V)LN \ll U^{-2}VLN,$$

which is on the order of $d^{27/56+\epsilon}$. Thus the trivial bound is sufficient for the error term $E(\mathcal{V})$ (although a sharper bound analogous to the one we derive for $E(\mathcal{U})$ in the following section also applies).

7.7.2 Estimating $E(\mathcal{U})$

We will estimate $E(\mathcal{U})$ more precisely as follows. We may write

$$E(\mathcal{U}) = \sum_{u\neq u'\in\mathcal{U}}\sum_{v\in\mathcal{V}}\sum_{z\leq N}\sum_{\substack{x\leq L\\ 4x^3\equiv dz^2 \pmod v}}\left(\frac{4x^3-dz^2}{uu'}\right).$$

For a fixed odd prime $v \in \mathcal{V}$ and a fixed value $z \leq N$, there are $\delta = 0, 1$, or 3 solutions x modulo v to

$$4x^3 \equiv dz^2 \pmod v.$$

Thus we may divide the set of $x \leq L$ with $4x^3 \equiv dz^2 \pmod v$ into sets $\{x \leq L : x \equiv x_0 \pmod v\}$ for δ values x_0. Let

$$K = LV^{-1} \approx d^{1/2-5/56+\epsilon}.$$

Writing $x = x_0 + vt$ where $t \leq K$, we then have

$$E(\mathcal{U}) = \sum_{u\neq u'\in\mathcal{U}}\sum_{v\in\mathcal{V}}\sum_{z\leq N}\sum_{x_0}\sum_{t\leq K}\left(\frac{4(x_0+vt)^3-dz^2}{uu'}\right).$$

Define

$$D(d,uu';v,x_0,z,K) = \sum_{t\leq K}\left(\frac{4(x_0+vt)^3-dz^2}{uu'}\right),$$

so that

$$E(\mathcal{U}) \ll U^2VN\max|D(d,uu';v,x_0,z,K)|, \tag{7.24}$$

where the maximum is taken over all appropriate pairs u, u' and v, x_0, z.

7.7.3 Bounding $D(d, uu'; v, x_0, z, K)$

We may write $D(d,uu';v,x_0,z,K)$ as a sum over a complete set of residues modulo uu',

$$\begin{aligned} D(d,uu';v,x_0,z,K) &= \sum_{\alpha=1}^{uu'}\left(\frac{4(x_0+v\alpha)^3-dz^2}{uu'}\right)\sum_{\substack{t\leq K\\ t\equiv\alpha \pmod{uu'}}} 1 \\ &= \frac{1}{uu'}\sum_{h=1}^{uu'}\sum_{\alpha=1}^{uu'}\left(\frac{4(x_0+v\alpha)^3-dz^2}{uu'}\right)e_{uu'}(h\alpha)A(uu';K,-h), \end{aligned}$$

where $|A(uu';K,-h)| \leq \min(K, \|h/uu'\|^{-1})$ as usual.

Define

$$T(d,uu';v,x_0,z,h) = \sum_{\alpha=1}^{uu'} \left(\frac{4(x_0+v\alpha)^3 - dz^2}{uu'}\right) e_{uu'}(h\alpha),$$

so that

$$|D(d,uu';v,x_0,K)| \leq \frac{1}{uu'} \sum_{h=1}^{uu'} |T(d,uu';v,x_0,z,h)||A(uu';K,-h)|. \quad (7.25)$$

A simple computation similar to that of Lemma 3.11 shows that we have the factorisation

$$T(d,uu';v,x_0,z,h) = T(d,u;v,x_0,z,h\overline{u'})T(d,u';v,x_0,z,h\overline{u}),$$

for $(u,u')=1$, with $u\overline{u} \equiv 1 \pmod{u'}$ and $u'\overline{u'} \equiv 1 \pmod{u}$. Thus it is sufficient to bound $T(d,p;v,x_0,z,h)$ for an odd prime p with $p \nmid d$, $p \nmid v$.

Lemma 7.12. *For an odd prime p with $p \nmid d$, $p \nmid v$,*

$$|T(d,p;v,x_0,z,h)| \leq 3p^{1/2}.$$

Proof. First suppose that $p > 3$. If $p \nmid z$, $p \nmid h$, then applying the Weil bound for hybrid sums given as Lemma 3.8,

$$|T(d,p;v,x_0,z,h)| \leq 3p^{1/2}.$$

If $p \nmid z$ but $p|h$, then

$$T(d,p;v,x_0,z,h) = \sum_{\alpha=1}^{p} \left(\frac{4(x_0+v\alpha)^3 - dz^2}{p}\right).$$

Arguing as in Lemma 7.3, we note that $p + T(d,p;v,x_0,z,h)$ is the number of points on the elliptic curve $\beta^2 = 4(x_0+v\alpha)^3 - dz^2$ over the finite field $\mathbb{F}_p$ (not counting the point at infinity), so that

$$|T(d,p;v,x_0,z,h)| \leq 2p^{1/2}.$$

If $p|z$ then

$$T(d,p;v,x_0,z,h) = \sum_{\alpha=1}^{p} \left(\frac{4(x_0+v\alpha)^3}{p}\right) e_p(h\alpha) = \sum_{\alpha=1}^{p} \left(\frac{x_0+v\alpha}{p}\right) e_p(h\alpha).$$

Since $p \nmid v$ we may make the change of variables $\alpha \mapsto \alpha - \overline{v}x_0$ so that

$$T(d,p;v,x_0,z,h) = \left(\frac{v}{p}\right) e_p(-h\overline{v}x_0) \sum_{\alpha=1}^{p} \left(\frac{\alpha}{p}\right) e_p(h\alpha).$$

Then if $p \nmid h$, the classical bound for character sums (or Lemma 3.5) shows that

$$|T(d,p;v,x_0,z,h)| \le p^{1/2}.$$

If furthermore $p|h$, then

$$T(d,p;v,x_0,z,h) = \left(\frac{v}{p}\right)\sum_{\alpha=1}^{p}\left(\frac{a}{p}\right) = 0.$$

For $p = 3$ we simply use the trivial bound

$$|T(d,p;v,x_0,z,h)| \le 3.$$

This completes the proof. □

It follows immediately from Lemma 7.12 that

$$|T(d,uu';v,x_0,z,h)| \le 9u^{1/2}u'^{1/2}.$$

Applying this to (7.25),

$$\begin{aligned}|D(d,uu';v,x_0,z,K)| &\ll u^{-1/2}u'^{-1/2}\sum_{h=1}^{uu'}\min(K,\|h/uu'\|^{-1})\\ &\ll u^{-1/2}u'^{-1/2}K + u^{1/2}u'^{1/2}\sum_{1\le h\le uu'/2}h^{-1}\\ &\ll u^{-1/2}u'^{-1/2}K + u^{1/2}u'^{1/2}\log U.\end{aligned}$$

Therefore by (7.24),

$$|E(\mathcal{U})| \ll U^2VN(U^{-1}K + U\log U) \ll ULN + U^3VN\log U,$$

since $K = LV^{-1}$. Thus

$$A^{-2}|E(\mathcal{U})| \ll V^{-1}(A^{-1}LN) + UV^{-1}N\log U.$$

Both of these terms are smaller than the leading term (7.8), the first by a factor of $V^{-1} \approx d^{-5/56+\epsilon}$ and the second by a factor of $L^{-1}U^2\log U \approx d^{-1/7+\epsilon}$. Thus this estimate for the error term $E(\mathcal{U})$ is sufficiently sharp.

The analogous bound for $E(\mathcal{V})$ gives

$$A^{-2}|E(\mathcal{V})| \ll U^{-1}(A^{-1}LN) + VU^{-1}N\log V,$$

where the first of these terms is smaller than the leading term by a factor of $d^{-5/28+\epsilon}$ and the second by a factor of $d^{-9/28+\epsilon}$.

7.8 The final bound

We have thus shown that for Q and α, β as chosen in Section 7.6, the prime sieves and the error terms are dominated by the leading term and the main sieve. Thus the final bound for $T(d)$ is given by (7.22):

$$T(d) \ll d^{27/56+\epsilon}.$$

Therefore by (7.6),

$$h_3(-d) \ll d^{27/56+\epsilon}$$

for any $\epsilon > 0$, where the implied constant depends only on ϵ. By the Scholz reflection principle, an equivalent bound also holds for $h_3(+3d)$. Thus we obtain the final result that for any square-free integer D,

$$h_3(D) \ll |D|^{27/56+\epsilon},$$

for any $\epsilon > 0$. This completes the proof of Theorem 7.1.

Chapter 8

Elliptic curves with fixed conductor

8.1 Introduction

The 3-part of class numbers of quadratic fields is intimately related to the number of elliptic curves over $\mathbb{Q}$ with fixed conductor. This was first noted by Brumer and Silverman in [5], in which they show that the number of elliptic curves over $\mathbb{Q}$ with conductor N, which we will denote by $C(\mathbb{Q}, N)$, is $O(N^{1/2+\epsilon})$. Their proof proceeds by bounding the number of integer points on certain elliptic curves in terms of the 3-part of the class number of an associated quadratic field. At the time of Brumer and Silverman's original paper, only the trivial bound $h_3(D) \leq h(D) \ll |D|^{1/2+\epsilon}$ was known, hence the resulting exponent of $1/2 + \epsilon$ in the bound for $C(\mathbb{Q}, N)$. Any improvement to the bound for $h_3(D)$ gives a corresponding improvement to the bound for $C(\mathbb{Q}, N)$. In particular, the conjectured bound $h_3(D) \ll |D|^{\epsilon}$ would show that $C(\mathbb{Q}, N)$ is $O(N^{\epsilon})$, for any $\epsilon > 0$.

In Section 8.2 we review the argument of Brumer and Silverman and prove two improved bounds for $C(\mathbb{Q}, N)$ resulting from our bounds for $h_3(D)$:

Theorem 8.1. *Let $C(\mathbb{Q}, N)$ denote the number of elliptic curves over $\mathbb{Q}$ with conductor N. Then*

$$C(\mathbb{Q}, N) \ll N^{27/56+\epsilon},$$

for any $\epsilon > 0$. If the conductor N has a divisor $N_0 \approx N^{5/6}$, then

$$C(\mathbb{Q}, N) \ll N^{5/12+\epsilon},$$

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

In Section 8.3, we briefly examine a conditional bound for $C(\mathbb{Q}, N)$ as well as a resulting conditional bound for $h_3(D)$ of Wong [69] and a conditional bound for $h_3(D)$ of Soundararajan [61].

Work of Helfgott and Venkatesh [36] simultaneous with that of this thesis gives an improved method for counting integral points on elliptic curves, based on a result for sphere packings. Their methods refine Brumer and Silverman's bound for $C(\mathbb{Q}, N)$, showing that $C(\mathbb{Q}, N)$ is $O(N^{0.22377\ldots})$. In Section 8.4, we summarise the methods of Helfgott and Venkatesh. We further show that if N has a divisor N_0 of approximate size $N_0 \approx N^{5/6}$, then Theorem 6.1, combined with the methods of Helfgott and Venkatesh, yields the best known bound for $C(\mathbb{Q}, N)$:

Theorem 8.2. *If the conductor N has a divisor $N_0 \approx N^{5/6}$, then*

$$C(\mathbb{Q}, N) \ll N^{\lambda+\epsilon},$$

where $\lambda = 0.21105\ldots$ and the implied constant depends only on $\epsilon > 0$.

8.2 Improving the bound of Brumer and Silverman

More generally, in [5] Brumer and Silverman bound the number of elliptic curves over $\mathbb{Q}$ with good reduction outside a given set of primes S. This immediately gives the result for elliptic curves with conductor N, as a curve with conductor N has good reduction outside the primes dividing N. Their method is as follows: let S be a finite set of rational primes (containing 2 and 3) and let M be the product of the primes in S. For $E/\mathbb{Q}$ an elliptic curve with good reduction outside of S and with minimal Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

let

$$\begin{aligned} b_2 &= a_1^2 + 4a_1 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

and compute

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

Then $c_4^3 - c_6^2 = 1728\Delta \in \mathbb{Z}_S^*$ (where $\mathbb{Z}_S^*$ denotes the set of integers composed of primes in S). Moreover c_4 and c_6 determine E up to isomorphism over $\mathbb{Q}$. Writing $-1728\Delta = AD^6$ with A being 6-th power free, consider the elliptic curve

$$\mathcal{E}_A : y^2 = x^3 + A.$$

In particular $(c_4/D^2, c_6/D^3)$ is an S-integral point on $\mathcal{E}_A$.

Brumer and Silverman proceed to bound the number of elliptic curves over $\mathbb{Q}$ with good reduction outside of S by showing that each elliptic curve $E/\mathbb{Q}$ corresponds to an integer A and an S-integral point on $\mathcal{E}_A$ such that: first, the number of possible values for A is $\ll 6^{\log M/\log\log M}$; second, the number of S-integral points on each curve $\mathcal{E}_A$ is $\ll M^{1/2+\epsilon}$; and third, the number of (c_4, c_6) pairs associated to each S-integral point P of $\mathcal{E}_A$ (and hence the number of curves $E/\mathbb{Q}$ associated to each S-integral point) is $\ll 2^{\log M/\log\log M}$.

The first bound is simple: A is positive or negative, 6-th power free, and composed only of primes in S, so that there are $2 \cdot 6^{\#S}$ possibilities for A; it is an elementary result that

$$\#S = \nu(M) \ll \frac{\log M}{\log\log M}.$$

The third bound, for the number of (c_4, c_6) pairs associated to each S-integral point P of $\mathcal{E}_A$ may be seen as follows. Write P in lowest terms as $(a/\delta^2, b/\delta^3)$, so that if $P = (c_4/D^2, c_6/D^3)$, then $\delta | D$. Writing $D = \delta D_0$, then $c_4 = D_0^2 a$ and $c_6 = D_0^3 b$, so that the point P, along with D_0, determines c_4, c_6. Thus we need only count the number of possible values D_0. Since (c_4^3, c_6^2) is divisible by D_0, and it is known that (c_4^3, c_6^2) divides $2^{12} \cdot 3^6 \cdot M^{11}$ (see [5]), it follows that $D_0 | 2^{12} \cdot 3^6 \cdot M^{11}$. Since M is square-free by definition, it follows that $D_0 | 12M$, so that there are no more than $2^{\#S+3} \ll 2^{\log M/\log\log M}$ possible values D_0.

It is in bounding the number of S-integral points on the curve $\mathcal{E}_A$ that the 3-part of the class number appears. Let $\kappa_3(\mathbb{Q}(\sqrt{-A}))$ denote the 3-rank of the class group of $\mathbb{Q}(\sqrt{-A})$, so that

$$h_3(-A) = 3^{\kappa_3(\mathbb{Q}(\sqrt{-A}))}.$$

(Note that here A can be positive or negative.) Brumer and Silverman use a result of Evertse and Silverman [16] on uniform bounds for the number of solutions to an equation of the form $X^n = F(Y)$ with $n = 3$ to show that

$$\#\mathcal{E}_A(\mathbb{Z}_S) \leq 2 \cdot 17^{14+2\#S} \cdot 3^{4\#S+\kappa_3(\mathbb{Q}(\sqrt{-A}))}, \tag{8.1}$$

so that

$$\#\mathcal{E}_A(\mathbb{Z}_S) \leq 2 \cdot 17^{14+2\#S} \cdot 3^{4\#S} h_3(\mathbb{Q}(\sqrt{-A})). \tag{8.2}$$

Using the trivial bound $h_3(-A) \leq h(-A)$, Brumer and Silverman then find that

$$\#\mathcal{E}_A(\mathbb{Z}_S) \leq h(-A)|A|^\epsilon \ll |\mathrm{Disc}(\mathbb{Q}(\sqrt{-A}))|^{1/2}|A|^\epsilon.$$

Since A is 6-th power free and is divisible only by primes in S, then $|\mathrm{Disc}(\mathbb{Q}(\sqrt{-A}))|$ is at most $4M$, and $|A| \leq M^5$. Hence

$$\#\mathcal{E}_A(\mathbb{Z}_S) \ll M^{1/2+\epsilon}.$$

A nontrivial bound of the form $h_3(-A) \ll |\mathrm{Disc}(\mathbb{Q}(\sqrt{-A}))|^\theta$ with $\theta < 1/2$ thus immediately improves this bound for $\#\mathcal{E}_A(\mathbb{Z}_S)$, and as a consequence, the bound for the number of elliptic curves with good reduction outside of S, to $O(M^{\theta+\epsilon})$. Thus in particular the result of Theorem 7.1, namely

$$h_3(-A) \ll |\mathrm{Disc}(\mathbb{Q}(\sqrt{-A}))|^{27/56+\epsilon},$$

gives the bound

$$C(\mathbb{Q}, N) \ll N^{27/56+\epsilon}.$$

Theorem 6.1 sharpens this bound in the case that the conductor N has a divisor $N_0 \approx N^{5/6}$. To see this, we must examine more closely the values of A that define the curves $\mathcal{E}_A$ in the argument of Brumer and Silverman. Let S be the set of primes dividing N (and including 2 and 3). Then A, which is divisible only by primes in S and is 6-th power free, may take any value in the set

$$\mathcal{A} = \{\pm \prod_{p \in S} p^{\alpha_p} : 0 \leq \alpha_p \leq 5\}.$$

Lemma 8.1. *If N has a divisor $N_0 \approx N^{5/6}$ then*

$$h_3(-A) \ll N^{5/12+\epsilon}$$

for any $A \in \mathcal{A}$.

Proof. For each value $A \in \mathcal{A}$, let $\bar{A}$ be the square-free kernel,

$$\bar{A} = \pm \prod_{p \in S} p^{a_p}$$

where $a_p \equiv \alpha_p \pmod 2$, with $a_p = 0, 1$. Set $A_0 = |\bar{A}|$. First suppose that a prime p divides N with $p \approx N^{5/6}$. Then for each value A, if $p|A_0$ then by Theorem 6.1,

$$\begin{aligned} h_3(-A) = h_3(-\bar{A}) &\ll p^{1/2+\epsilon} + p^{-1} A_0^{5/4+\epsilon} + p^{-1/2} A_0^{1/2+\epsilon} \\ &\ll N^{5/12+\epsilon}. \end{aligned}$$

If $p \nmid A_0$ then $A_0 \ll N^{1/6}$ so that even applying the trivial bound we obtain

$$h_3(-A) = h_3(-\bar{A}) \ll A_0^{1/2+\epsilon} \ll N^{1/12+\epsilon}.$$

Next suppose that N has a divisor $N_0 \approx N^{5/6}$, not necessarily prime. Let $d_0 = (N_0, A_0)$. Then by Theorem 6.1,

$$\begin{aligned} h_3(-A) = h_3(-\bar{A}) &\ll d_0^{1/2+\epsilon} + d_0^{-1} A_0^{5/4+\epsilon} + d_0^{-1/2} A_0^{1/2+\epsilon} \\ &\ll N^{5/12+\epsilon} + \frac{A_0^{5/4+\epsilon}}{(N_0, A_0)} + \frac{A_0^{1/2+\epsilon}}{(N_0, A_0)^{1/2}}. \end{aligned} \tag{8.3}$$

Note that $A_0/(N_0, A_0)$ divides N/N_0. (It suffices to show that $A_0 N_0 | N(N_0, A_0)$. But $N(N_0, A_0) = (NN_0, NA_0)$, and since $A_0 | N$ then $A_0 N_0 | NN_0$, and since $N_0 | N$, then $A_0 N_0 | NA_0$.) Thus in (8.3),

$$\frac{A_0^{5/4}}{(N_0, A_0)} \leq A_0^{1/4} \left(\frac{N}{N_0} \right) \leq \frac{N^{5/4}}{N_0} \leq N^{5/12},$$

and

$$\frac{A_0^{1/2}}{(N_0, A_0)^{1/2}} \leq \frac{N^{1/2}}{N_0^{1/2}} \leq N^{1/12}.$$

Thus in conclusion, if $N_0 | N$ with $N_0 \approx N^{5/6}$, then

$$h_3(-A) = h_3(-\bar{A}) \ll N^{5/12+\epsilon}.$$

□

Thus we may apply the result of Theorem 6.1 for $h_3(\sqrt{-A})$ in (8.2) to give

$$\#\mathcal{E}_A(\mathbb{Z}_S) \ll N^{5/12+\epsilon}$$

and hence

$$C(\mathbb{Q}, N) \ll N^{5/12+\epsilon}$$

when N has a divisor of size $N_0 \approx N^{5/6}$. This completes the discussion of Theorem 8.1.

8.3 Conditional bounds

Brumer and Silverman also note the following conditional bound for $C(\mathbb{Q}, N)$, which, as we will see, may be used to derive a conditional bound for $h_3(D)$.

8.3.1 A conditional bound for $C(\mathbb{Q}, N)$

Let $L(\mathcal{E}_A, s)$ denote the L-series of the curve $\mathcal{E}_A$. Suppose that for all nonzero integers A, $L(\mathcal{E}_A, s)$ satisfies the generalised Riemann hypothesis, and that the order of vanishing of $L(\mathcal{E}_A, s)$ at $s = 1$ is greater than or equal to that of the rank of $\mathcal{E}_A(\mathbb{Q})$. Then Brumer and Silverman show (Theorem 4 of [5]) that

$$C(\mathbb{Q}, N) \ll N^{\epsilon} \tag{8.4}$$

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

This follows by the same method as the proof of the unconditional bound given in the previous section, but with a different bound for the number of S-integral points on each curve $\mathcal{E}_A$. A result of Silverman (Theorem A of [60]) states that for each curve $\mathcal{E}_A$,

$$\#\mathcal{E}_A(\mathbb{Z}_S) \leq c_1^{1+\#S+\operatorname{rank}\mathcal{E}_A(\mathbb{Q})}, \tag{8.5}$$

for some constant c_1. (All constants c_i used below are absolute.) A bound of Mestre [46] states that

$$\operatorname{rank}\mathcal{E}_A(\mathbb{Q}) \leq c_2 \frac{\log(\operatorname{cond}\mathcal{E}_A)}{\log\log(\operatorname{cond}\mathcal{E}_A)}, \tag{8.6}$$

under the assumptions that $L(\mathcal{E}_A, s)$ satisfies the generalised Riemann hypothesis and that the order of vanishing of $L(\mathcal{E}_A, s)$ at $s = 1$ is greater than or equal to $\operatorname{rank}\mathcal{E}_A(\mathbb{Q})$. The conductor $\operatorname{cond}\mathcal{E}_A$ is at most $1728M^2$, where M is the product of primes in the set S, as before. Therefore (8.6) gives

$$\operatorname{rank}\mathcal{E}_A(\mathbb{Q}) \leq c_3 \frac{\log M}{\log\log M}.$$

Since $\#S \ll \log M/\log\log M$ also, (8.5) becomes

$$\#\mathcal{E}_A(\mathbb{Z}_S) \leq c_4^{\log M/\log\log M}.$$

Using this in place of (8.1), and proceeding as in the proof of the unconditional bound, we obtain (8.4).

8.3.2 Conditional bounds for $h_3(D)$

Wong [69] uses the conditional estimate (8.4) for $C(\mathbb{Q}, N)$ to derive a conditional bound for the 3-part $h_3(D)$ as follows. A result of Hasse [26] states that the 3-part of the class number of a quadratic field with discriminant D is 1/6th the number of non-Galois cubic fields of discriminant D whose Galois closure contains $\mathbb{Q}(\sqrt{D})$. Wong notes that a cubic field of discriminant D can be generated by a polynomial f of discriminant $|\operatorname{Disc}(f)| \leq 2|D|^{3/2}$. Define F_D to be the set of monic, cubic, irreducible polynomials $f \in \mathbb{Z}[x]$ such that $|\operatorname{Disc}(f)| = |D|N^2$ for an integer N with $1 \leq N \leq \sqrt{2}|D|^{1/4}$, and let two polynomials in F_D be equivalent if they define isomorphic extensions of $\mathbb{Q}$. Then it follows that the 3-part of the class number of $\mathbb{Q}(\sqrt{D})$ is bounded by the number M_D of equivalence classes of polynomials in F_D.

For each $f \in F_D$, regard $y^2 = f(x)$ as the Weierstrass equation of an elliptic curve with discriminant $1728\operatorname{Disc}(f)$, and with conductor dividing $1728\operatorname{Disc}(f)$. The equivalence classes in F_D correspond to different elliptic curves, as the

2-division fields of the curves are distinct. Thus by (8.4),

$$\begin{aligned} M_D &\leq \sum_{1 \leq N \leq \sqrt{2}|D|^{1/4}} C(\mathbb{Q}, N) \\ &\ll \sum_{1 \leq N \leq \sqrt{2}|D|^{1/4}} (1728|D|N^2)^{\epsilon} \\ &\ll |D|^{\epsilon} \sum_{1 \leq N \leq \sqrt{2}|D|^{1/4}} N^{2\epsilon} \\ &\ll |D|^{1/4+\epsilon'}, \end{aligned}$$

where the implied constant depends only on $\epsilon' = 3\epsilon/2 > 0$. Therefore, under the assumptions given above,

$$h_3(D) \ll |D|^{1/4+\epsilon}$$

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

In fact, one may obtain a nontrivial bound for $h_3(D)$ by assuming the Riemann hypothesis for only a single L-function, as noted by Soundararajan in [61]. The proof, as communicated in [36], is as follows. Let χ_d be the quadratic Dirichlet character associated to $K = \mathbb{Q}(\sqrt{-d})$ for a positive integer d. Let $CL_3(-d) = \{[\mathfrak{a}] \in CL(-d) : [\mathfrak{a}]^3 = 1\}$, so that $h_3(-d) = \#CL_3(-d)$. Assuming $d \equiv 1 \pmod 4$ for simplicity, let σ be the Galois automorphism of K. Assuming the Riemann hypothesis for the L-function $L(\chi_d, s)$, there are $\gg d^{1/6-\epsilon}$ primes p with $p < d^{1/6}$ and $\chi_d(p) = 1$, and hence $\gg d^{1/6-\epsilon}$ prime ideals $\mathfrak{p}$ of O_K with $\mathfrak{N}(\mathfrak{p}) < d^{1/6}$ and $\mathfrak{N}(\mathfrak{p})$ prime. If $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct such ideals that represent the same ideal class in $CL(-d)/CL_3(-d)$, then $\mathfrak{p}_1^{\sigma}\mathfrak{p}_2 \in CL_3(-d)$ so that

$$4\mathfrak{N}(\mathfrak{p}_1^{\sigma}\mathfrak{p}_2)^3 = y^2 + dz^2$$

for some $y, z \in \mathbb{N}$, by the same argument leading to (6.1). However, since $\mathfrak{N}(\mathfrak{p}_1^{\sigma}\mathfrak{p}_2)^3 < d$, we must have $z = 0$, leading to a contradiction. Therefore $\#CL(-d)/CL_3(-d) \gg d^{1/6-\epsilon}$, so that

$$h_3(-d) = \#CL_3(-d) \ll d^{1/3+\epsilon},$$

where the implied constant depends only on ϵ. Again, by the Scholz reflection principle, an equivalent bound holds for $h_3(+3d)$, so that we obtain

$$h_3(D) \ll |D|^{1/3+\epsilon}$$

for any discriminant D, under the assumptions given above.

8.4 The work of Helfgott and Venkatesh

In [36], Helfgott and Venkatesh present a method for bounding the number of integral points on elliptic curves that yields the bounds $h_3(D) = O(|D|^{0.44178\ldots+\epsilon})$

and $C(\mathbb{Q}, N) = O(N^{0.22377\ldots+\epsilon})$ (Theorems 4.2 and 4.5 of [36]). Their methods are based on the idea that integer points on an elliptic curve that are v-adically close to one another tend to repel each other. This enables them to define a type of quasi-orthogonality, and thus state the problem of bounding the number of integral points on an elliptic curve as a problem of sphere-packings. It is quite interesting that this method also gives a nontrivial bound for $h_3(D)$. Before we discuss Helfgott and Venkatesh's result for $C(\mathbb{Q}, N)$, we therefore briefly examine their result for $h_3(D)$.

As before, let $\mathcal{E}_A$ represent the curve

$$\mathcal{E}_A : y^2 = x^3 + A$$

for any nonzero integer A. As we do in Section 6.2, Helfgott and Venkatesh consider the case of an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer and reduce the problem of bounding $h_3(-d)$ to counting the number of integer points on the surface

$$x^3 = y^2 + dz^2$$

with $2x, 2y, 2z \in \mathbb{Z}$ and $x \ll d^{1/2}, y \ll d^{3/4}, z \ll d^{1/4}$. They then deduce that

$$h_3(-d) \ll d^{1/4+\epsilon} \max_{z \ll d^{1/4}} \#\{(x, y) \in \mathcal{E}_{-dz^2}(\mathbb{Q}, \{\infty\}) : x \ll d^{1/2}, y \ll d^{3/4}\}.$$

The general bound they obtain for the number of S-integer points on a curve of the form $\mathcal{E}_A$ is as follows (Corollary 3.9 of [36]). Let K be a number field and let S be a finite set of s places of K, including all infinite places and all places at which $\mathcal{E}_A$ has bad reduction. Let $R \geq \max(1, \operatorname{rank}_{\mathbb{Z}} \mathcal{E}_A(\mathbb{Q}))$, where $\operatorname{rank}_{\mathbb{Z}} \mathcal{E}_A(\mathbb{Q})$ denotes the rank of $\mathcal{E}_A(\mathbb{Q})$ as a $\mathbb{Z}$-lattice. For each $h_0 \geq 1$, the number of S-integer points of $\mathcal{E}_A$ with canonical height (as defined in [36]) satisfying $\hat{h}(P) \leq h_0$ is at most

$$O_{\epsilon,[K:\mathbb{Q}]}\left(C^s \epsilon^{-2(s+[K:\mathbb{Q}])} s^{[K:\mathbb{Q}]} (1 + \log h_0) e^{R \cdot \left(\alpha\left(\frac{h_0[K:\mathbb{Q}]}{R}\right)+\epsilon\right)}\right), \tag{8.7}$$

for every sufficiently small $\epsilon > 0$. Here C is an absolute constant and $\alpha(x)$ is a computable function for which we refer the reader to [36].

A result of Fouvry (Proposition 2 of [17]) states that

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{E}_A(\mathbb{Q}) \leq a + b\nu(A) + 2\log_3 h_3(-A) \tag{8.8}$$

for absolute constants a, b. Defining

$$\gamma = \limsup_{d \to \infty} \frac{\log h_3(-d)}{\log d},$$

it follows from (8.8) that for any $z \ll d^{1/4}$,

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{E}_{-dz^2}(\mathbb{Q}) \leq R = \log d \left(\frac{2\gamma}{\log 3} + o(1)\right).$$

Defining the set $S = \{p : p|6dz^2\} \cup \{\infty\}$ and setting $h_0 = (\log d)/4 + O(1)$ in (8.7), Helfgott and Venkatesh then obtain

$$\#\{P \in \mathcal{E}_{-dz^2} : \hat{h}(P) \leq h_0\} \ll d^{\left(\frac{2\gamma}{\log 3}\right)\left(\alpha\left(\frac{\log 3}{8\gamma}\right)+\epsilon\right)},$$

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

$$\gamma \leq \frac{1}{4} + \frac{2\gamma}{\log 3}\alpha\left(\frac{\log 3}{8\gamma}\right).$$

Solving for γ computationally, with $\gamma < 1/2$, then gives the exponent

$$h_3(-d) \ll d^{\lambda+\epsilon}$$

with $\lambda = 0.44178....$ The Scholz reflection principle gives an equivalent result for $h_3(+3d)$.

Helfgott and Venkatesh's bound for $C(\mathbb{Q}, N)$ is more immediate, as one need only apply (8.7) to curves $\mathcal{E}_A$ with A being 6-th power free and divisible only by primes in S, where S is the set of primes dividing N (and including 2 and 3). Employing an upper bound for the height of S-integers on $\mathcal{E}_A$ and assembling this with (8.7), with canonical height $\hat{h}(P) \leq h_0 = cN^{c'\nu(N)}$, for some constants c, c', It is a result of Corollary 3.11 of [36] that

$$\#\mathcal{E}_A(\mathbb{Z}_S) \ll N^{\epsilon} \exp[\operatorname{rank}_{\mathbb{Z}}(\mathcal{E}_A(\mathbb{Q}))(\beta+\epsilon)],$$

where β is the numerical constant 0.278236.... Using (8.8) to bound the rank of $\mathcal{E}_A(\mathbb{Q})$, this becomes

$$\#\mathcal{E}_A(\mathbb{Z}_S) \ll N^{\epsilon} \exp[2\log_3(h_3(-A))(\beta+\epsilon)].$$

Thus a nontrivial bound $h_3(-A) \ll |N|^{\theta}$ gives a bound

$$\#\mathcal{E}_A(\mathbb{Z}_S) \ll N^{2\beta\theta/\log 3+\epsilon},$$

and hence

$$C(\mathbb{Q}, N) \ll N^{2\beta\theta/\log 3+\epsilon}. \tag{8.9}$$

By Theorem 7.1 we may take $\theta = 27/56 + \epsilon$ in (8.9), so that we obtain

$$C(\mathbb{Q}, N) \ll N^{0.24422...+\epsilon}.$$

Note that this is slightly weaker than the bound of Helfgott and Venkatesh, namely $C(\mathbb{Q}, N) = O(N^{\lambda+\epsilon})$ with $\lambda = 0.22377....$

However, if N has a divisor of size $N_0 = N^{5/6}$, by Theorem 6.1 and Lemma 8.1, we may take $\theta = 5/12 + \epsilon$ in (8.9), obtaining

$$C(\mathbb{Q}, N) \ll N^{0.21105...+\epsilon}.$$

This is the best known bound for $C(\mathbb{Q}, N)$. This concludes the discussion of Theorem 8.2.

Appendix A

Table A.1 gives the class numbers h of the real quadratic fields $\mathbb{Q}(\sqrt{D})$ for square-free integers $2 \leq D < 100$. Table A.2 gives the class numbers h of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ for square-free integers $0 < D < 500$. (Reference: [54].)

Table A.1: Real quadratic fields

D	h	D	h
2	1	51	2
3	1	53	1
5	1	55	2
6	1	57	1
7	1	58	2
10	2	59	1
11	1	61	1
13	1	62	1
14	1	65	2
15	2	66	2
17	1	67	1
19	1	69	1
21	1	70	2
22	1	71	1
23	1	73	1
26	2	74	2
29	1	77	1
30	2	78	2
31	1	79	3
33	1	82	4
34	2	83	1
35	2	85	2
37	1	86	1
38	1	87	2
39	2	89	1
41	1	91	2
42	2	93	1
43	1	94	1
46	1	95	2
47	1	97	1

Table A.2: Imaginary quadratic fields

D	h	D	h	D	h	D	h	D	h	D	h	D	
1	1	71	7	143	10	215	14	287	14	365	20	434	24
2	1	73	4	145	8	217	8	290	20	366	12	435	4
3	1	74	10	146	16	218	10	291	4	367	9	437	20
5	2	77	8	149	14	219	4	293	18	370	12	438	8
6	2	78	4	151	7	221	16	295	8	371	8	439	15
7	1	79	5	154	8	222	12	298	6	373	10	442	8
10	2	82	4	155	4	223	7	299	8	374	28	443	5
11	1	83	3	157	6	226	8	301	8	377	16	445	8
13	2	85	4	158	8	227	5	302	12	379	3	446	32
14	4	86	10	159	10	229	10	303	10	381	20	447	14
15	2	87	6	161	16	230	20	305	16	382	8	449	20
17	4	89	12	163	1	231	12	307	3	383	17	451	6
19	1	91	2	165	8	233	12	309	12	385	8	453	12
21	4	93	4	166	10	235	2	310	8	386	20	454	14
22	2	94	8	167	11	237	12	311	19	389	22	455	20
23	3	95	8	170	12	238	8	313	8	390	16	457	8
26	6	97	4	173	14	239	15	314	26	391	14	458	26
29	6	101	14	174	12	241	12	317	10	393	12	461	30
30	4	102	4	177	4	246	12	318	12	394	10	462	8
31	3	103	5	178	8	247	6	319	10	395	8	463	7
33	4	105	8	179	5	249	12	321	20	397	6	465	16
34	4	106	6	181	10	251	7	322	8	398	20	466	8
35	2	107	3	182	12	253	4	323	4	399	16	467	7
37	2	109	6	183	8	254	16	326	22	401	20	469	16
38	6	110	12	185	16	255	12	327	12	402	16	470	20
39	4	111	8	186	12	257	16	329	24	403	2	471	16
41	8	113	8	187	2	258	8	330	8	406	16	473	12
42	4	114	8	190	4	259	4	331	3	407	16	474	20
43	1	115	2	191	13	262	6	334	12	409	16	478	8
46	4	118	6	193	4	263	13	335	18	410	16	479	25
47	5	119	10	194	20	265	8	337	8	411	6	481	16
51	2	122	10	195	4	266	20	339	6	413	20	482	20
53	6	123	2	197	10	267	2	341	28	415	10	483	4
55	4	127	5	199	9	269	22	345	8	417	12	485	20
57	4	129	12	201	12	271	11	346	10	418	8	487	7
58	2	130	4	202	6	273	8	347	5	419	9	489	20
59	3	131	5	203	4	274	12	349	14	421	10	491	9
61	6	133	4	205	8	277	6	353	16	422	10	493	12
62	8	134	14	206	20	278	14	354	16	426	24	494	28
65	8	137	8	209	20	281	20	355	4	427	2	497	24
66	8	138	8	210	8	282	8	357	8	429	16	498	8
67	1	139	3	211	3	283	3	358	6	430	12	499	3
69	8	141	8	213	8	285	16	359	19	431	21		
70	4	142	4	214	6	286	12	362	18	433	12		

Bibliography

[1] N. C. ANKENY and S. CHOWLA, 'On the divisibility of the class number of quadratic fields,' *Pacific J. Math.* **5** (1955) 321-324.

[2] A. BAKER, 'Linear forms in the logarithms of algebraic numbers,' *Mathematika* **13** (1966) 204-216.

[3] A. BAKER, 'Imaginary quadratic fields with class number two,' *Ann. of Math.* **94** No. 2 (1971) 139-152.

[4] M. BHARGAVA, 'Higher Composition Laws,' Dissertation, Princeton University (2001).

[5] A. BRUMER and J. H. SILVERMAN, 'The number of elliptic curves over $\mathbb{Q}$ with conductor N,' *Manuscripta Math.* **91** (1996) 95-102.

[6] D. A. BURGESS, 'On character sums and L-series I,' *Proc. London Math. Soc.* **12** No. 3 (1962) 193-206.

[7] D. BYEON and E. KOH, 'Real quadratic fields with class number divisible by 3,' *Manuscripta Math.,* **111** No. 2 (2003) 261-263.

[8] K. CHAKRABORTY and R. MURTY, 'On the number of real quadratic fields with class number divisible by 3,' *Proc. Am. Math. Soc.* **131** No. 1 (2002) 41-44.

[9] H. COHEN and H. W. LENSTRA, 'Heuristics on class groups of number fields,' *Number Theory,* Noordwijkerhout 1983. Lecture Notes in Mathematics 1068. Berlin: Springer-Verlag (1984) 33-62.

[10] H. COHEN and J. MARTINET, 'Étude heuristique des groupes de classes des corps de nombres,' *J. Reine Angew. Math.* **404** (1990) 39-76.

[11] H. DAVENPORT and H. HEILBRONN, 'On the density of discriminants of cubic fields II,' *Proc. Roy. Soc. Lond. A.* **322** (1971) 405-420.

[12] P. DELIGNE, 'Sommes Trigonometrique' in *Cohomologie Etale*, Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$. Lecture Notes in Mathematics 569. New York: Springer-Verlag (1977) 168-232.

[13] P. DELIGNE, 'La Conjecture de Weil II,' *Pub. Math. I.H.E.S.* **52** (1981) 313-428.

[14] M. DEURING, 'Imaginär-quadratische Zahlkörper mit der Klassenzahl 1,' *Math. Z.* **37** (1933) 405-415.

[15] P. ERDÖS, 'Über die kleinste quadratfreie Zahl einer arithmetischen Reihe,' *Montash. Math.* **64** (1960) 314-316.

[16] J.-H. EVERTSE and J. H. SILVERMAN, 'Uniform bounds for the number of solutions to $Y^n = f(X)$,' *Math. Proc. Camb. Phil. Soc.* **100** No. 237 (1986) 237-248.

[17] É. FOUVRY, 'Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$,' *Séminaire de Théorie des Nombres, Paris, 1990-91, Progr. Math.,* 61-84. Boston: Birkhäuser Boston (1993).

[18] C. F. GAUSS, *Disquisitiones Arithmeticae* (1801). G. Fleischer, Leipzig. Trans. A. A. Clarke. New Haven: Yale University Press (1966).

[19] D. GOLDFELD, 'The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer,' *Ann. Scuola Norm. Sup. Pisa* **3** No. 4 (1976) 623-663.

[20] D. GOLDFELD, 'Gauss' class number problem for imaginary quadratic fields,' *Bull. Am. Math. Soc.* **13** No. 1 (1985) 23-37.

[21] S. W. GRAHAM and G. KOLESNIK, *Van der Corput's Method of Exponential Sums.* London Mathematical Society Lecture Notes Series 126. Cambridge: Cambridge University Press (1991).

[22] B. GROSS and D. ZAGIER, 'Heegner points and derivatives of L-series,' *Invent. Math.* **84** (1986) 225-320.

[23] M. GUT, 'Kubische Klassenkörper über quadratischimaginären Grundkörpen,' *Nieuw Arch. Wiskunde* **23** No. 2 (1951) 185-189.

[24] G. H. HARDY and E. M. WRIGHT, *An Introduction to the Theory of Numbers, 5th ed.* Oxford: Oxford University Press (2000).

[25] P. HARTUNG, 'Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3,' *J. Number Theory,* **6** (1974) 276-278.

[26] H. HASSE, 'Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage,' *Math. Z.* **31** (1930) 565-582. Corrigendum, *Math. Z.* **31** (1930) 799.

[27] H. HASSE, *Number Theory, 3rd ed.* Berlin: Springer-Verlag (1980).

[28] D. R. HEATH-BROWN, 'Hybrid bounds for Dirichlet L-functions,' *Inventiones Math.* **47** (1978) 149-170.

[29] D. R. HEATH-BROWN, 'Hybrid bounds for L-functions: a q-analogue of Van der Corput's method and a t-analogue of Burgess's method,' *Recent Progress in Analytic Number Theory,* ed. Halberstam and Hooley, London: Academic Press (1981) 121-126.

[30] D. R. HEATH-BROWN, 'The least square-free number in an arithmetic progression,' *J. Reine Angew. Math.* **332** (1982) 204-220.

[31] D. R. HEATH-BROWN, 'The square sieve and consecutive square-free numbers,' *Math. Ann.* **266** (1984) 251-259.

[32] D. R. HEATH-BROWN, 'The largest prime factor of X^3+2,' *Proc. London Math. Soc.,* **82** No. 3 (2001) 554-596.

[33] K. HEEGNER, 'Diophantische Analysis und Modulfunktionen,' *Math. Z.* **56** (1052) 227-253.

[34] H. HEILBRONN, 'On the class number in imaginary quadratic fields,' *Quart. J. Math. Oxford Ser. 2* **5** (1934) 150-160.

[35] H. HEILBRONN and E. H. LINFOOT, 'On the imaginary quadratic corpora of class number one,' *Quart. J. Math. Oxford* **5** No. 2 (1934) 293-301.

[36] H. HELFGOTT and A. VENKATESH, 'Integral points on elliptic curves and 3-torsion in class groups,' preprint available at http://www.arxiv.org/abs/math.NT/0405180.

[37] T. HONDA, 'Isogenies, rational points and section points of group varieties,' *Japan J. Math.* **30** (1960) 84-101.

[38] T. HONDA, 'On real quadratic fields whose class numbers are multiples of 3,' *J. Reine Angew. Math.* **223** (1968) 101-102.

[39] C. HOOLEY, 'A note on square-free numbers in arithmetic progressions.' *Bull. London Math. Soc.* **7** (1975), 133-138.

[40] C. HOOLEY, 'On the representations of a number as the sum of four cubes: I.' *Proc. London Math. Soc.* **36** No. 3 (1978), 117-140.

[41] L. K. HUA, *Introduction to Number Theory.* Berlin: Springer-Verlag (1982).

[42] M. J. JACOBSON, 'Experimental results on class groups of real quadratic fields (extended abstract),' *Algorithmic Number Theory.* Berlin: Springer-Verlag (1998) 463-474.

[43] N. M. KATZ, 'On a question of Lillian Pierce,' in preparation.

[44] W. KOHNEN and K. ONO, 'Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication,' *Invent. Math.* **135** (1999) 387-398.

[45] E. LANDAU, 'Über die Klassenzahl imaginär-quadratischer Zahlkörper,' *Göttinger Nachr.* (1918) 285-295.

[46] J. -F. MESTRE, 'Formules explicites et minorations des conducteurs de varietés algébriques,' *Compositio Math.* **58** (1986) 209-232.

[47] R. A. MOLLIN and H. C. WILLIAMS, 'Computation of the class number of a real quadratic field,' *Utilitas Math.* **41** (1992) 259-308.

[48] L. J. MORDELL, 'On the Riemann hypothesis and imaginary quadratic fields with a given class number,' *J. London Math. Soc.* **9** (1934) 289-298.

[49] P. MORTON, 'Density results for the 2-classgroups of imaginary quadratic fields,' *J. Reine Angew. Math.* **332** (1982) 156-187.

[50] M. H. MURTY, 'Exponents of class groups of quadratic fields,' *Topics in Number Theory: Mathematics and Its Applications 467.* Dordrecht: Kluwer Academic (1997) 229-239.

[51] T. NAGELL, 'Über die Klassenzahl imaginär-quadratischer Zahlkörper,' *Abh. Math. Sem. Univ. Hamburg* **1** (1922) 140-150.

[52] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers.* Berlin: Springer-Verlag (1980).

[53] J. OESTERLÉ, 'Nombres de classes des corps quadratiques imaginaires,' *Séminaire Nicolas Bourbaki* (1983-1984) Éxp. 631.

[54] A. N. PARSHIN and I. R. SHAFAREVICH, eds. *Number Theory II*, Encyclopaedia of Mathematical Sciences, Vol. 62. Berlin: Springer-Verlag (1991).

[55] K. PRACHAR, 'Über die kleinste quadratfreie Zahl einer arithmetischen Reihe,' *Montash. Math.* **62** (1958) 173-176.

[56] P. RIBENBOIM, *My Numbers, My Friends: Popular Lectures on Number Theory.* New York: Springer-Verlag (2000).

[57] W. SCHMIDT, *Equations over Finite Fields: An Elementary Approach.* Lecture Notes in Mathematics 536. Berlin: Springer-Verlag (1976).

[58] A. SCHOLZ, 'Über die Beziehung der Klassenzahlen quadratischer Körper zueinander,' *J. Reine Angew. Math.* **166** (1932) 201-203.

[59] C. L. SIEGEL, 'Über die Classenzahl quadratischer Zahlkörper,' *Acta Arith.* **1** (1936) 83-86.

[60] J. H. SILVERMAN, 'A quantitative version of Siegel's theorem,' *J. Reine Angew. Math.* **378** (1987) 60-100.

[61] K. SOUNDARARAJAN, 'Divisibility of class numbers of imaginary quadratic fields,' *J. London Math. Soc.* **61** No. 2 (2000) 681-690.

[62] H. M. STARK, 'A complete determination of the complex quadratic fields of class-number one,' *Michigan Math. J.* **14** (1967) 1-27.

[63] H. M. STARK, 'A transcendence theorem for class number problems,' *Ann. of Math.* **94** No. 2 (1971) 153-173.

[64] T. TATUZAWA, 'On a theorem of Siegel,' *Japan. J. Math.* **21** (1951) 163-178.

[65] H. WADA, 'A table of ideal class numbers of real quadratic fields,' *Sophia Kokyoroku in Mathematics.* No. 10 (1981).

[66] A. WEIL, 'Sur les courbes algébriques et les variétés qui s'en déduis,' *Pub. Inst. Math. Strasbourg* **7** Hermann et Cie., Paris (1948) 1-85.

[67] A. WEIL, 'On some exponential sums,' *Proc. Nat. Acad. Sci. USA* **34** (1948) 204-207.

[68] P. WEINBERGER, 'Real quadratic fields with class number divisible by n,' *J. Number Theory* **5** (1973) 237-241.

[69] S. WONG, 'On the rank of ideal class groups,' *Number Theory.* Ottawa, ON (1996) 377-383, *CRM Proc. Lecture Notes* 19. Amer. Math. Soc., Providence, RI, 1999.

[70] Y. YAMAMOTO, 'On unramified Galois extensions of quadratic number fields,' *Osaka J. Math.* **7** (1970) 57-76.

[71] G. YU, 'A note on the divisibility of class numbers of real quadratic fields,' *J. Number Theory* **97** No. 1 (2002) 35-44.