

THE 3-PART OF CLASS NUMBERS OF QUADRATIC FIELDS

L. B. PIERCE

ABSTRACT

We prove that the 3-part of the class number of a quadratic field $\mathbb{Q}(\sqrt{D})$ is $O(|D|^{55/112+\epsilon})$ in general and $O(|D|^{5/12+\epsilon})$ if $|D|$ has a divisor of size $|D|^{5/6}$. These bounds follow as results of nontrivial estimates for the number of solutions to the congruence $x^a \equiv y^b$ modulo q in the ranges $x \leq X$ and $y \leq Y$, where a, b are nonzero integers and q is a square-free positive integer. Furthermore, we show that the number of elliptic curves over \mathbb{Q} with conductor N is $O(N^{55/112+\epsilon})$ in general and $O(N^{5/12+\epsilon})$ if N has a divisor of size $N^{5/6}$. These results are the first improvements to the trivial bound $O(|D|^{1/2+\epsilon})$ and the resulting bound $O(N^{1/2+\epsilon})$ for the 3-part and the number of elliptic curves, respectively.

1. Introduction

Consider the quadratic field $\mathbb{Q}(\sqrt{D})$ with class group $CL(D)$ and class number $h(D)$ for a nonzero integer D . Let $h_3(D)$ represent the 3-part of the class number, the number of elements in the class group whose cube is the principal ideal class. It is conjectured that $h_3(D) \ll |D|^\epsilon$ for any $\epsilon > 0$. Previously, the only known unconditional bound was the trivial bound:

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

We prove the following two nontrivial bounds for $h_3(D)$:

Theorem 1. *Let D be a nonzero integer. 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 .

Note that if 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 $\theta < 1/2$. Theorem 1 is most efficient when $d_0 = |D|^{5/6}$, in which case the bound is

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

for any $\epsilon > 0$.

In general, we prove:

Theorem 2. *Let D be a nonzero integer. Then*

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

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

Theorems 1 and 2 follow as corollaries to results for the following more general

problem. Let $N_q(X, Y)$ denote the number of solutions to the congruence

$$x^a \equiv y^b \pmod{q} \quad (1.1)$$

in the ranges $x \leq X$, $y \leq Y$, with $(x, q) = (y, q) = 1$. Here $X, Y \geq 1$, a and b are nonzero integers, and q is a square-free positive integer.

A trivial upper bound is

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

One could hope to improve on this trivial bound when $X, Y \leq q$ in the following ways:

$$N_q(X, Y) = o(\min(X, Y)); \quad (1.2)$$

$$N_q(X, Y) = O(XYq^{-1}). \quad (1.3)$$

If furthermore both a and b are positive integers, one may define $N'_q(X, Y)$ to be the number of positive integer solutions (x, y) to the congruence (1.1) in the bounded region $x \leq X$ and $y \leq Y$ without assuming the relative primality conditions $(x, q) = 1$ and $(y, q) = 1$. An identical trivial bound holds for $N'_q(X, Y)$.

We prove the following two nontrivial bounds for $N_q(X, Y)$ and $N'_q(X, Y)$.

Theorem 3. *Let q be a square-free positive integer and let a, b be nonzero integers with $(a, b) = 1$ 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 explicitly on a, b . If furthermore both a and b are positive integers, an identical bound holds for $N'_q(X, Y)$.

For $X = q^\alpha$, $Y = q^\beta$, with $\alpha, \beta \leq 1$, Theorem 3 achieves (1.2) if $1/2 < \alpha, \beta < 1$ and (1.3) if $\alpha + \beta \geq 3/2$, disregarding factors of size q^ϵ .

Theorem 4. *Let q be a square-free positive integer and let a, b be nonzero integers with $(b, q) = 1$ and such that $a/b \notin \mathbb{Z}^+$. If $X \leq q^{\frac{k+1}{2k}}$ and $Y \leq q/2$, then*

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

for any integer $k \geq 1$, where τ_k and the implied constant depend explicitly on a, b, k . If furthermore both a and b are positive integers, an identical bound holds for $N'_q(X, Y)$.

Note that in Theorem 4 it is advantageous to choose X to be the smaller of the two ranges. It is then clear that Theorem 4 achieves (1.2) and (1.3) for X and Y in certain ranges, with corresponding choice of $k \geq 1$.

We prove Theorems 3 and 4 for $N_q(X, Y)$; the bounds for $N'_q(X, Y)$ may be proved with very similar but slightly simpler arguments. Theorem 3 follows from a standard application of the well-known bound for exponential sums resulting from Weil's proof of the Riemann hypothesis for curves over finite fields. We prove Theorem 4, which is the most innovative work of this paper, using mean value properties of exponential sums. Our methods follow those of Heath-Brown in [6], which in turn follows work of Hooley [8] and extends Burgess's methods for character sums [2]. However, our methods are significantly more involved; in particular we must choose the averaging set of auxiliary primes more carefully, and we must handle the vanishing of certain polynomials both over \mathbb{C} and modulo primes with some delicacy.

We apply the bounds for $N'_q(X, Y)$ given in Theorems 3 and 4 to obtain the two nontrivial bounds for $h_3(D)$ presented in Theorems 1 and 2. Finally, we show the

corresponding bounds for the number of elliptic curves over \mathbb{Q} with fixed conductor, following Brumer and Silverman [1]. The resulting theorem is as follows:

Theorem 5. *The number of elliptic curves over \mathbb{Q} with conductor N is $O(N^{55/112+\epsilon})$ in general and $O(N^{5/12+\epsilon})$ if N has a divisor of size $N^{5/6}$.*

2. Notation

The notation $A \ll B$ indicates that $A \leq cB$ for a positive constant c depending only on certain variables as indicated. We denote by $[x]$ the greatest integer part of x and by $\|x\|$ the distance from x to the nearest integer. By $(A, B]$ we mean the set of integers $A < n \leq B$.

The function $\nu(n)$ represents the number of distinct prime divisors of n , $d(n)$ represents the divisor function, and $d_k(n)$ represents the k -th generalized divisor function. We use the standard notation $e(x)$ for $e^{2\pi ix}$ and $e_q(x)$ for $e^{2\pi ix/q}$. Also, we denote by \bar{n} the unique solution to $\bar{n}n \equiv 1 \pmod{q}$ with $1 \leq \bar{n} \leq q$. If $a < 0$, n^a denotes $\bar{n}^{|a|}$. By convention, whenever \bar{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. Theorem 3: The Weil Bound

We proceed to bound $N_q(X, Y)$ for $X, Y \leq q$ by counting solutions (x, y) to (1.1) within dyadic ranges with respect to x . Note that since we only consider solutions with $(x, q) = 1$, $(y, q) = 1$, it is sufficient to restrict b to be a positive integer, while a may be any nonzero integer with $(a, b) = 1$. Let

$$U(w, M, q) = \sum_{\substack{w < n \leq 2w \\ (n, q) = 1}} \#\{m \leq M : m^b \equiv n^a \pmod{q}\}, \quad (3.1)$$

where $M \leq q/2$. Define

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

where $\delta_1(x) = 1$ if $\|x\| \leq Mq^{-1}$ and zero otherwise. Then

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

Defining

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

with $H = [(q/2)M^{-1}]$, we then have

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

Therefore

$$U(w, M, q) \ll H^{-1} \sum_{h=0}^{H-1} \left| \sum_{\substack{w < n \leq 2w \\ (n, q) = 1}} \sum_{\substack{m \pmod{q} \\ m^b \equiv n^a \pmod{q}}} e_q(hm) \right|. \quad (3.2)$$

We may extend the inner sum over $w < n \leq 2w$ to a sum over a set of residues modulo q ,

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

where the sum over k only considers $(k, q) = 1$. Let

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

where again the sum only considers $(k, q) = 1$. Then

$$U(w, M, q) \ll H^{-1} q^{-1} \sum_{h=0}^{H-1} \sum_{l=1}^q \min(w, \|l/q\|^{-1}) |V(q; h, l)|. \quad (3.3)$$

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

It is a result of Weil's proof of the Riemann hypothesis for curves over finite fields that the sum $V(q; h, l)$ admits the following bound:

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

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

where $\eta = 2(|a| + b)$.

Proof.

The sum $V(q; h, l)$ is multiplicative (for example, by Lemma 3 of [9]), in the sense that:

$$V(q_1 q_2; h, l) = V(q_1; h \bar{q}_2, l \bar{q}_2) V(q_2; h \bar{q}_1, l \bar{q}_1),$$

for $(q_1, q_2) = 1$. Since q is square-free we thus need only bound $V(p; h, l)$ for each prime $p|q$. Since $(a, b) = 1$, there exist integers r, s such that $ar + bs = 1$. For $k \not\equiv 0 \pmod{p}$, set $\alpha \equiv m^r k^s \pmod{p}$ so that $\alpha^a \equiv m$ and $\alpha^b \equiv k$ modulo p . Then

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

If $a > 0$, the Weil bound (see for example Chapter II of [11], [14]) 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 (see Section 3 of [3]) shows that for $p \nmid hl$ with $p > \max(|a|, b)$,

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

Supposing that $p|h$ but $p \nmid l$, then

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

Here we let $\psi_b(n) = 1$ if $n \equiv 0 \pmod{p}$, $\psi_b(n) = (b, p-1)$ if $n \equiv x^b \pmod{p}$ for some x , and $\psi_b(n) = 0$ otherwise. Note that since $(a, b) = 1$, $\psi_b(k^a) = \psi_b(k)$. Therefore

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

The classical bound for such sums (see for example Chapter 7 of [10]) 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 $p \leq \max(|a|, b)$.

3.2. Bounding $U(w, M, q)$

Applying Lemma 1 to (3.3), we obtain

$$\begin{aligned} U(w, M, q) &\ll \eta^{\nu(q)} H^{-1} q^{-1/2} \left[\sum_{l=1}^{q-1} \|l/q\|^{-1} (q, l)^{1/2} + wq^{1/2} \right. \\ &\quad \left. + \sum_{l=1}^{q-1} \|l/q\|^{-1} \sum_{h=1}^{H-1} (q, h, l)^{1/2} + w \sum_{h=1}^{H-1} (q, h)^{1/2} \right]. \end{aligned} \quad (3.4)$$

We may bound the double sum in (3.4) as follows:

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

Similarly,

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

and

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

Hence

$$U(w, M, q) \ll q^{1/2} d(q)^\tau \log q + q^{-1} M d(q)^\tau w + q^{1/2} d(q)^\tau w, \quad (3.5)$$

where we may take $\tau \geq \log \eta / \log 2 + 1$. Thus

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

This completes the proof of Theorem 3.

4. Theorem 4: The Mean Value Problem

To prove Theorem 4, we again examine $U(w, M, q)$, now using mean value properties of exponential sums, as in [6]. In this section we allow all implicit constants to depend on a, b and an integer $k \geq 1$ we introduce below. We further assume that $(a, b) = 1$, $(b, q) = 1$, and $a/b \notin \mathbb{Z}^+$. Throughout it is implicit that we only consider n such that $(n, q) = 1$.

Applying Hölder's inequality to (3.2),

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

for any integer $k \geq 1$. Define the function

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

for any finite set of integers \mathcal{I} and fixed $\alpha \in (\mathbb{Z}/q\mathbb{Z})^\times$. Equivalently, we may write

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

We will denote $N_1(\mathcal{I})$ simply by $N(\mathcal{I})$. It is clear that for $\mathcal{I} = (w, 2w]$,

$$U(w, M, q) \ll M^{\frac{1}{2k}} N(\mathcal{I})^{\frac{1}{2k}}. \quad (4.1)$$

Thus our main goal is to estimate $N(\mathcal{I})$.

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

When \mathcal{I} is a set of I consecutive positive integers, we may bound $N(\mathcal{I})$ by

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} (Iq^{-1} + 1),$$

where σ_k is a positive integer dependent only on a, b, k . We will refer to this as the trivial bound. We may see this as follows. There are at most I^{2k-1} choices for

n_1, \dots, n_{2k-1} , and these determine $\ll (b^{\nu(q)})^{2k-1}$ choices for m_1, \dots, m_{2k-1} modulo q . There is then one value of m_{2k} modulo q satisfying

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

and this determines $\ll |a|^{\nu(q)}$ 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 $n_{2k} \in \mathcal{I}$. We may thus choose the exponent $\sigma_k \geq b(2k-1) + |a|$. (Since any power of $d(q)$ will only contribute a factor of size q^ϵ to the final bound, we need not try to minimize our choice of σ_k .)

We may see in (4.1) that this trivial bound for $N(\mathcal{I})$ then gives

$$U(w, M, q) \ll M^{1/2k} [d(q)^{\sigma_k} (I^{2k} q^{-1} + I^{2k-1})]^{1/2k},$$

and hence

$$N_q(X, Y) \ll d(q)^{\sigma_k} \left[XY^{\frac{1}{2k}} q^{-\frac{1}{2k}} + X^{1-\frac{1}{2k}} Y^{\frac{1}{2k}} \right],$$

which is only as good as the trivial bound for $N_q(X, Y)$ when $X, Y \leq q$.

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

We improve upon the trivial bound for $N(\mathcal{I})$ by averaging over a set of auxiliary primes. Let $\mathcal{I} = \{1 \leq n \leq I\}$ and fix a prime $p \nmid q$ with $Q < p \leq 2Q$ and $Q < I \leq q$, where Q is a parameter we will choose later. We may then see that

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + \frac{1}{q} \sum_{h=1}^q \left| \sum_{\substack{n \in \mathcal{I} \\ p \nmid n}} \sum_{\substack{m \pmod{q} \\ m^b \equiv n^a \pmod{q}}} e_q(hm) \right|^{2k}. \quad (4.2)$$

In fact, 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 $\ll Ip^{-1}$ choices for n_1 and these determine $\ll b^{\nu(q)}$ choices for m_1 . There are at most I^{2k-2} choices for n_2, \dots, n_{2k-1} and similarly these determine $\ll (b^{\nu(q)})^{2k-2}$ choices for m_2, \dots, m_{2k-1} . There is then one choice for m_{2k} modulo q and hence $\ll |a|^{\nu(q)}$ choices for n_{2k} modulo q . Thus, in total the contribution to $N(\mathcal{I})$ from (\mathbf{n}, \mathbf{m}) with $p|n_1$ is $\ll d(q)^{\sigma_k} I^{2k-1} Q^{-1}$, where as before we may take $\sigma_k \geq b(2k-1) + |a|$.

Consider the sum in (4.2) over $n \in \mathcal{I}$ with $p \nmid n$. Since $p \nmid q$, these remaining n fall into the $p-1$ nonzero residue classes

$$n \equiv fq \pmod{p},$$

with $0 < f < p$. Thus by Hölder's inequality,

$$\left| \sum_{\substack{n \in \mathcal{I} \\ p \nmid n}} \sum_{\substack{m \pmod{q} \\ m^b \equiv n^a \pmod{q}}} e_q(hm) \right|^{2k} \leq (p-1)^{2k-1} \sum_{f=1}^{p-1} \left| \sum_{\substack{n \in \mathcal{I} \\ n \equiv fq \pmod{p}}} \sum_{\substack{m \pmod{q} \\ m^b \equiv n^a \pmod{q}}} e_q(hm) \right|^{2k}.$$

Define the interval

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

and write $n = fq + ps$, so that $s \in \mathcal{I}(p, f)$. The congruence $m^b \equiv n^a \pmod{q}$ is then equivalent to $m^b \equiv p^a s^a \pmod{q}$. Temporarily, let

$$S(q; p, f) = \frac{1}{q} \sum_{h=1}^q \left| \sum_{s \in \mathcal{I}(p, f)} \sum_{\substack{m \pmod{q} \\ m^b \equiv p^a s^a \pmod{q}}} e_q(hm) \right|^{2k}.$$

For square-free q , the prime p belongs to one of the at most $b^{\nu(q)}$ cosets of Γ/Γ^b , where Γ denotes $(\mathbb{Z}/q\mathbb{Z})^\times$. Let $R_1 = 1, R_2, \dots, R_{b^{\nu(q)}}$ be a fixed set of coset representatives. Then if $p = R_t g^b$, set $m = g^a u$ so that the congruence $m^b \equiv p^a s^a \pmod{q}$ is equivalent to $u^b \equiv R_t^a s^a \pmod{q}$. Then

$$S(q; p, f) = \frac{1}{q} \sum_{h=1}^q \left| \sum_{s \in \mathcal{I}(p, f)} \sum_{\substack{u \pmod{q} \\ u^b \equiv R_t^a s^a \pmod{q}}} e_q(hg^a u) \right|^{2k},$$

so that

$$S(q; p, f) = \frac{1}{q} \sum_{l=1}^q \left| \sum_{s \in \mathcal{I}(p, f)} \sum_{\substack{u \pmod{q} \\ u^b \equiv R_t^a s^a \pmod{q}}} e_q(lu) \right|^{2k}.$$

Setting $\alpha = R_t^a$, then

$$S(q; p, f) = N_\alpha(\mathcal{I}(p, f)).$$

Thus

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha(\mathcal{I}(p, f)). \quad (4.3)$$

This result is of crucial importance, as it removes any dependence on the auxiliary prime p from the argument of the exponential sum; therefore we may average over a large set of primes.

4.3. Averaging for the good set

We first distinguish between “good” and “bad” $2k$ -tuples (n_1, \dots, n_{2k}) , as in [6]. We will average $N_\alpha(\mathcal{I}(p, f))$ only for the set of good $2k$ -tuples, since the set of bad $2k$ -tuples will be small enough to admit a trivial bound. For notational convenience, define $\mathcal{I}(t) = (-qt, IQ^{-1} - qt]$.

Suppose G and B are disjoint sets partitioning the set of all $2k$ -tuples (n_1, \dots, n_{2k}) . Define

$$N_\alpha^G(t) = \#\{(\mathbf{n}, \mathbf{m}), \mathbf{n} \in G, n_i \in \mathcal{I}(t), m_i \pmod{q} : \\ m_i^b \equiv \alpha n_i^a \pmod{q} \text{ for } 1 \leq i \leq 2k, \text{ and } \sum_{i=1}^k m_i \equiv \sum_{i=1}^k m_{i+k} \pmod{q}\}.$$

Define $N_\alpha^B(t)$ equivalently and let

$$K_\alpha = \max_t N_\alpha^B(t).$$

Then

$$N_\alpha(\mathcal{I}(p, f)) \leq N_\alpha(\mathcal{I}(f/p)) = N_\alpha^B(f/p) + N_\alpha^G(f/p),$$

so that

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + Q^{2k-1} \sum_{f=1}^{p-1} N_\alpha^G \left(\frac{f}{p} \right).$$

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 . Consider the largest of the sets \mathcal{P}_t ,

$$\mathcal{P}_t = \{Q < p \leq 2Q, p \nmid q : p \in R_t \Gamma^b\}.$$

Assuming $Q \geq c \log q$ for some constant c , then the largest set \mathcal{P}_t is at least of size $\gg Q(b^{\nu(q)} \log Q)^{-1}$. Therefore

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-2} (\log Q) \sum_p \sum_{f=1}^{p-1} N_\alpha^G \left(\frac{f}{p} \right), \quad (4.4)$$

where the sum is over primes p in the chosen set \mathcal{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 $n_i \in \mathcal{I}'(t)$. As shown in [6], assuming $8IQ \leq q$, we may rearrange the intervals we consider so that the sum of $N_\alpha^G(t)$ in (4.4) is only dependent on the set \mathcal{P}_t of primes over which we average in terms of the value of α . We obtain

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-1} I^{-1} (\log Q) \sum_{j=1}^{2q-1} N_\alpha^{G'} \left(\frac{j}{q} \right). \quad (4.5)$$

Let L_α denote the number of solutions $(\mathbf{n}, \mathbf{m}, j)$ with $\mathbf{n} \in G$ and

$$\begin{aligned} n_i &\in (0, 2IQ^{-1}] \text{ for } i = 1, \dots, 2k, \\ m_i &\in \mathbb{Z}/q\mathbb{Z} \text{ for } i = 1, \dots, 2k, \\ 0 &\leq j < q \end{aligned}$$

such that

$$m_i^b \equiv \alpha(n_i - j)^a \pmod{q}$$

for each $i = 1, \dots, 2k$, and

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

Then we may write (4.5) as

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + Q^{2k} K_\alpha + b^{\nu(q)} Q^{2k-1} I^{-1} (\log Q) L_\alpha, \quad (4.6)$$

where $\alpha = R_t^a$, with R_t a fixed representative for the largest set \mathcal{P}_t .

5. The Good and Bad Sets

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 proceed to estimate $L_\alpha(\mathbf{n}; p)$ for each prime $p|q$ by bounding the number of roots of certain polynomials $H_\alpha(\mathbf{n}, j)$ in the case $a > 0$ and $\bar{H}_\alpha(\mathbf{n}, j)$ in the case $a < 0$. Studying when $H_\alpha(\mathbf{n}, j)$ and $\bar{H}_\alpha(\mathbf{n}, j)$ vanish identically over \mathbb{C} and modulo primes then shows how we may define the good and bad sets G and B .

5.1. Positive exponent: the polynomial $H_\alpha(\mathbf{n}, j)$

We first consider the case when $a > 0$. Let $\beta = b$ if b is even and $\beta = 2b$ if b is odd. Let $F(\mathbf{Y})$ be the polynomial in $\mathbb{Z}[X_1, \dots, X_{2k}, Y_1, \dots, Y_{2k}, Z]$ defined by

$$F(\mathbf{Y}) = \prod_{\{\omega\}} F_{\{\omega\}}(\mathbf{Y}) = \prod_{\{\omega_1=0, \omega_2, \dots, \omega_{2k}\}} (\xi^{\omega_1} Y_1 + \xi^{\omega_2} Y_2 + \dots + \xi^{\omega_{2k}} Y_{2k}), \quad (5.1)$$

where ξ is a primitive β th root of unity and $\omega_i \in \{0, \dots, \beta - 1\}$. Informally, if we were to fix \mathbf{n} and substitute $\alpha^{1/b}(\mathbf{n} - j)^{a/b}$ for \mathbf{Y} , one factor of $F(\alpha^{1/b}(\mathbf{n} - j)^{a/b})$ would vanish whenever

$$\sum_{i=1}^k \alpha^{1/b} (n_i - j)^{a/b} \equiv \sum_{i=1}^k \alpha^{1/b} (n_{i+k} - j)^{a/b} \pmod{p}.$$

We cannot take fractional powers modulo p , but note that $F(\mathbf{Y})$ is in fact a polynomial in $\mathbf{Y}^b = (Y_1^b, \dots, Y_{2k}^b)$. Therefore if $Y_i^b = \alpha(X_i - Z)^a$ 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 to bound $L_\alpha(\mathbf{n}; p)$ it is sufficient to bound the number of roots j of $H_\alpha(\mathbf{n}, j)$ modulo p for each prime $p|q$.

5.2. The vanishing of $H_\alpha(\mathbf{n}, z)$ over \mathbb{C}

Suppose that $H_\alpha(\mathbf{n}, z)$ is identically zero for $z \in \mathbb{C}$. Then a factor of $H_\alpha(\mathbf{n}, z)$ must vanish identically, so for some set of exponents $\{\omega_1 = 0, \dots, \omega_{2k}\}$,

$$\sum_{i=1}^{2k} \xi^{\omega_i} (n_i - z)^{a/b} = 0 \quad (5.2)$$

for all $z \in \mathbb{C}$. In the power series expansion of each term in (5.2),

$$(n_i - z)^{a/b} = (-z)^{a/b} (1 - n_i/z)^{a/b} = c_0 (-z)^{a/b} + c_1 (-z)^{a/b-1} n_i + c_2 (-z)^{a/b-2} n_i^2 + \dots,$$

the coefficients c_m are nonzero for all $m \geq 0$, since $a/b \notin \mathbb{Z}^+$. Thus in order for all coefficients of z to vanish in (5.2),

$$E(m) = \sum_{i=1}^{2k} \xi^{\omega_i} n_i^m = 0,$$

for all integers $m \geq 0$.

Regarding $E(0) = 0, \dots, E(2k-1) = 0$ as a system of linear equations in variables $t_i = \xi^{\omega_i}$ for $1 \leq i \leq 2k$,

$$\begin{aligned} t_1 n_1^0 + t_2 n_2^0 + \cdots + t_{2k} n_{2k}^0 &= 0 \\ &\vdots \\ t_1 n_1^{2k-1} + t_2 n_2^{2k-1} + \cdots + t_{2k} n_{2k}^{2k-1} &= 0, \end{aligned}$$

and constructing the corresponding matrix

$$\mathbf{A} = \begin{pmatrix} n_1^0 & n_2^0 & \cdots & n_{2k}^0 \\ n_1^1 & n_2^1 & \cdots & n_{2k}^1 \\ \vdots & \vdots & \ddots & \vdots \\ n_1^{2k-1} & n_2^{2k-1} & \cdots & n_{2k}^{2k-1} \end{pmatrix},$$

the Vandermonde determinant then shows that

$$\prod_{i < h} (n_i - n_h) = 0.$$

Thus for some pair $i \neq h$, $n_i - n_h = 0$. Reducing the dimension of the matrix \mathbf{A} (either by writing the variables t_i and t_h as one variable, if $\xi^{\omega_i} + \xi^{\omega_h} \neq 0$, or omitting the i th and h th columns of \mathbf{A} , if $\xi^{\omega_i} + \xi^{\omega_h} = 0$), we may apply this reasoning again to the resulting lower dimensional matrix to find that two more values n_i, n_h with $i \neq h$ must be equal. Proceeding in this fashion, one sees that if $H_\alpha(\mathbf{n}, z)$ vanishes identically over \mathbb{C} , then for each $i = 1, \dots, 2k$, there exists $h \neq i$ such that $n_i - n_h = 0$.

5.3. Defining the good and bad sets

Therefore we choose the sets G and B as follows:

$$\begin{aligned} B &= \{\mathbf{n} : \forall i, 1 \leq i \leq 2k, \exists h \neq i, 1 \leq h \leq 2k, \text{ with } n_i = n_h\}, \\ G &= \{\mathbf{n} : \mathbf{n} \notin B\}. \end{aligned}$$

For each \mathbf{n} and each $1 \leq i \leq 2k$, define

$$A_i(\mathbf{n}) = \prod_{h \neq i} (n_i - n_h). \quad (5.3)$$

Then if $\mathbf{n} \in G$, there exists some $1 \leq i \leq 2k$ such that $A_i(\mathbf{n}) \neq 0$.

5.4. The vanishing of $H_\alpha(\mathbf{n}, j)$ modulo p

Suppose p is a prime with $p|q$. 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 of $H_\alpha(\mathbf{n}, j)$ modulo p , unless the polynomial vanishes identically modulo p . There is a constant $c_{b,k}$ such that if p divides all the coefficients of terms of the form $\alpha(n_i - j)^\alpha$ in the expanded product of $H_\alpha(\mathbf{n}, j)$, then $p \leq c_{b,k}$. For $p > c_{b,k}$, $H_\alpha(\mathbf{n}, j)$ may still vanish identically modulo p due to 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 2. *Suppose that for some $\mathbf{n} \in G$ the polynomial $H_\alpha(\mathbf{n}, j)$ vanishes identically modulo p for a prime $p > P_k$ for an explicit constant P_k . Then $p|A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$.*

Proof. Fixing \mathbf{n} and regarding $H_\alpha(\mathbf{n}, z)$ as a polynomial in $\mathbb{Z}[z]$, suppose $H_\alpha(\mathbf{n}, z)$ vanishes identically modulo a prime p . Set $d = a\beta^{2k-1}$ and consider the polynomial $J(z) = \alpha^{-N/b} z^{-d} H_\alpha(\mathbf{n}, z^b)$ in $\mathbb{Z}[z^{-b}]$, where $N = \beta^{2k-1}$ is the number of factors in the product (5.1). We may think of $J(z)$ as a product of N factors,

$$J(z) = \prod_{\{\omega\}} J_{\{\omega\}}(z), \quad (5.4)$$

over all possible sets of exponents $\{\omega\} = \{\omega_1 = 0, \dots, \omega_{2k}\}$. Here each factor is of the form

$$J_{\{\omega\}}(z) = \xi^{\omega_1} \left(1 - \frac{n_1}{z^b}\right)^{a/b} + \dots + \xi^{\omega_{2k}} \left(1 - \frac{n_{2k}}{z^b}\right)^{a/b},$$

which may be regarded as a formal power series over $\bar{\mathbb{Q}}$,

$$J_{\{\omega\}}(z) = \sum_{m=0}^{\infty} v_{\{\omega\},m} (z^{-b})^m.$$

Define the truncation

$$J_{\{\omega\}}^M(z) = \sum_{m=0}^M v_{\{\omega\},m} (z^{-b})^m,$$

for an integer $M \geq 1$, and let

$$J^M(z) = \prod_{\{\omega\}} J_{\{\omega\}}^M(z).$$

Furthermore, let \mathcal{K} be the field $\mathcal{K} = \mathbb{Q}(v_{\{\omega\},m})$, where $\{\omega\}$ ranges over all sets of exponents, and $0 \leq m \leq M$. 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 over $O_{\mathcal{K}}$, and $Q^M(z)$ is a polynomial over $O_{\mathcal{K}}$ with all terms of degree strictly greater than M .

Let \mathfrak{p} be a fixed prime ideal above p in \mathcal{K} . By assumption, $J(z)$ is identically zero modulo p . Equating coefficients in (5.4), one sees that each coefficient of $P^M(z)$ is zero modulo \mathfrak{p} . Thus there exists a factor $J_{\{\omega\}}^M(z)$ such that all the coefficients $v_{\{\omega\},m}$ with $m \leq M/N$ are zero modulo \mathfrak{p} . Choose $M = N(2k-1)$. Each coefficient v_m (where we understand the set $\{\omega\}$ to be fixed, and omit 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 the constant P_k to be greater than all of $c_{b,k}, b, 2k-1, a(a-b) \cdots (a-b(2k-2))$. Since $v_m = 0$ modulo \mathfrak{p} for each $0 \leq m \leq 2k-1$, then

$$E(m) = \sum_{i=1}^{2k} \xi^{\omega_i} n_i^m = 0$$

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} , the Vandermonde determinant of the matrix \mathbf{A} then 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} . Arguing as before, one shows that for each $1 \leq i \leq 2k$ there exists $h \neq i$, $1 \leq h \leq 2k$ 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 $1 \leq i \leq 2k$.

5.5. Negative exponent: the polynomial $\bar{H}_\alpha(\mathbf{n}, j)$

We next consider the case when $a < 0$. To simplify notation, we denote $|a|$ by \bar{a} , and we denote variables associated with \bar{a} with a bar. 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 $N = \beta^{2k-1}$ as before. If we have the relation

$$Y_i^b = \alpha(X_i - Z)^{-\bar{a}}$$

for each $i = 1, \dots, 2k$, then there exist polynomials \bar{G} and \bar{H}_α such that

$$\bar{F}(\mathbf{Y}) = \bar{G}(\mathbf{Y}^b) = \bar{G}(\alpha(\mathbf{X} - Z)^{-\bar{a}}) = \bar{H}_\alpha(\mathbf{X}, Z).$$

Informally, we may think of $\bar{H}_\alpha(\mathbf{n}, j)$ as the product

$$\begin{aligned} \bar{H}_\alpha(\mathbf{n}, j) &= \bar{H}_\alpha^{(1)}(\mathbf{n}, j) \bar{H}_\alpha^{(2)}(\mathbf{n}, j) \\ &= \left(\prod_{i=1}^{2k} \alpha^{-1/b} (n_i - j)^{\bar{a}/b} \right)^N \\ &\quad \cdot \prod_{\{\omega\}} \left(\xi^{\omega_1} \alpha^{1/b} (n_1 - j)^{-\bar{a}/b} + \dots + \xi^{\omega_{2k}} \alpha^{1/b} (n_{2k} - j)^{-\bar{a}/b} \right), \end{aligned}$$

or as

$$\bar{H}_\alpha(\mathbf{n}, j) = \alpha^{-(2k-1)N/b} \prod_{\{\omega\}} \left(\xi^{\omega_1} \prod_{i \neq 1} (n_i - j)^{\bar{a}/b} + \dots + \xi^{\omega_{2k}} \prod_{i \neq 2k} (n_i - j)^{\bar{a}/b} \right).$$

In particular, if \mathbf{n} is fixed and \mathbf{m} is such that

$$m_i^b \equiv \alpha(n_i - j)^{-\bar{a}} \pmod{p}$$

for each $i = 1, \dots, 2k$, 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 of $\bar{H}_\alpha(\mathbf{n}, j)$ modulo p for each prime $p|q$.

5.6. *The vanishing of $\bar{H}_\alpha(\mathbf{n}, z)$ 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 $(-z)^{2kN(\bar{a}/b)}$ in the expansion of $\bar{H}_\alpha^{(1)}(\mathbf{n}, z)$ is 1, hence $\bar{H}_\alpha^{(2)}(\mathbf{n}, z)$ vanishes identically over \mathbb{C} , and as in the case $a > 0$, it follows that for some set of exponents $\{\omega_1 = 0, \dots, \omega_{2k}\}$,

$$\sum_{i=1}^{2k} \xi^{\omega_i} (n_i - z)^{-\bar{a}/b} = 0 \quad (5.5)$$

for all $z \in \mathbb{C}$. By an argument analogous to that of the case $a > 0$, it follows that for each $i = 1, \dots, 2k$, 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 $i = 1, \dots, 2k$ as before.

5.7. *The vanishing of $\bar{H}_\alpha(\mathbf{n}, j)$ modulo p*

Suppose p is a prime with $p|q$. The highest degree possible for $\bar{H}_\alpha(\mathbf{n}, j)$ with respect to j is $\bar{\delta}_k = (\bar{a}/b)(2k-1)N$. 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 $\alpha(n_i - j)^{\bar{a}}$ in the expanded product of $\bar{H}_\alpha(\mathbf{n}, j)$, then $p \leq \bar{c}_{b,k}$. We prove 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 3. *Suppose the polynomial $\bar{H}_\alpha(\mathbf{n}, j)$ vanishes identically modulo p for a prime $p > \bar{P}_k$ for an explicit constant \bar{P}_k . Then $p|A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$.*

Proof. Fixing \mathbf{n} and regarding $\bar{H}_\alpha(\mathbf{n}, z)$ as a polynomial in $\mathbb{Z}[z]$, suppose $\bar{H}_\alpha(\mathbf{n}, z)$ vanishes identically modulo a prime p . Setting $\bar{d} = \bar{a}(2k-1)\beta^{2k-1}$, 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 $\{\omega\} = \{\omega_1 = 0, \dots, \omega_{2k}\}$,

$$\bar{J}(z) = \prod_{\{\omega\}} \bar{J}_{\{\omega\}}(z), \quad (5.6)$$

where each factor is of the form

$$\begin{aligned} \bar{J}_{\{\omega\}}(z) &= \bar{J}_{\{\omega\}}^{(1)}(z) \bar{J}_{\{\omega\}}^{(2)}(z) \\ &= \left(\prod_{i=1}^{2k} \left(1 - \frac{n_i}{z^b}\right)^{\bar{a}/b} \right) \\ &\quad \cdot \left(\xi^{\omega_1} \left(1 - \frac{n_1}{z^b}\right)^{-\bar{a}/b} + \dots + \xi^{\omega_{2k}} \left(1 - \frac{n_{2k}}{z^b}\right)^{-\bar{a}/b} \right), \end{aligned}$$

or alternatively,

$$\bar{J}_{\{\omega\}}(z) = \left(\xi^{\omega_1} \prod_{i \neq 1} \left(1 - \frac{n_i}{z^b}\right)^{\bar{a}/b} + \dots + \xi^{\omega_{2k}} \prod_{i \neq 2k} \left(1 - \frac{n_i}{z^b}\right)^{\bar{a}/b} \right).$$

Each factor $\bar{J}_{\{\omega\}}(z)$ may be regarded as a product of formal power series for $\bar{J}_{\{\omega\}}^{(1)}(z)$ and $\bar{J}_{\{\omega\}}^{(2)}(z)$ over $\overline{\mathbb{Q}}$. As before, let $\bar{J}_{\{\omega\}}^{(1),M}(z)$ and $\bar{J}_{\{\omega\}}^{(2),M}(z)$ be M th power trunca-

tions of the power series, and let

$$\bar{J}^M(z) = \prod_{\{\omega\}} \bar{J}_{\{\omega\}}^M(z) = \prod_{\{\omega\}} \bar{J}_{\{\omega\}}^{(1),M}(z) \bar{J}_{\{\omega\}}^{(2),M}(z). \quad (5.7)$$

Let \mathcal{K} be 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 (5.6), it follows that each coefficient of $\bar{P}^M(z)$ is zero modulo \mathfrak{p} , and thus there exists a factor $\bar{J}_{\{\omega\}}^M(z)$ 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, at least one of $\bar{J}_{\{\omega\}}^{(1),M}(z)$ and $\bar{J}_{\{\omega\}}^{(2),M}(z)$ has the property that the coefficients of all terms with degree $0 \leq m \leq M/2N$ are zero modulo \mathfrak{p} . Visibly, $\bar{J}_{\{\omega\}}^{(1),M}(z)$ has constant term 1, hence all coefficients of terms in $\bar{J}_{\{\omega\}}^{(2),M}(z)$ 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}_k , we may argue as in the case $a > 0$ to conclude that for each $1 \leq i \leq 2k$ there exists some $i \neq h$ such that $n_i - n_h = 0$ modulo \mathfrak{p} . Thus $p|A_i(\mathbf{n})$ for all $1 \leq i \leq 2k$.

6. Proof of Theorem 2

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.

6.1. Estimating K_α

For an element $\mathbf{n} \in B$, only k distinct n_i may be chosen, so there are $\ll k!(IQ^{-1})^k$ ways to choose $\mathbf{n} \in B$. There are then $\ll (b^{\nu(q)})^{2k}$ choices for the $2k$ -tuple \mathbf{m} , hence

$$K_\alpha = \max_t N_\alpha^B(t) \ll d(q)^{2kb} (IQ^{-1})^k.$$

6.2. 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 $G = \bigcup G_i$. If $\mathbf{n} \in G_i$ then it follows from Lemmas 2 and 3 that for each prime $p|q$,

$$L_\alpha(\mathbf{n}; p) \leq d_{\eta_k}(p) b^{2k}(p, A_i(\mathbf{n})),$$

where $\eta_k = \max(P_k, \bar{P}_k, \delta_k, \bar{\delta}_k)$, and the factor of b^{2k} results from the number of ways to choose \mathbf{m} . Recall that

$$L_\alpha = \sum_{\mathbf{n} \in G} L_\alpha(\mathbf{n}; q) = \sum_{\mathbf{n} \in G} \prod_{p|q} L_\alpha(\mathbf{n}; p).$$

Therefore

$$L_\alpha \ll \sum_{i=1}^{2k} d(q)^{\eta_k+2kb} \sum_{\mathbf{n} \in G_i} (q, A_i(\mathbf{n})). \quad (6.1)$$

We bound the inner sum over $\mathbf{n} \in G_i$ following Lemma 2 of [5].

Lemma 4. *For each $i = 1, \dots, 2k$,*

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

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 , of which there are at most $2IQ^{-1}$ 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 . 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

$$\begin{aligned} \sum_{\mathbf{n} \in G_1} (q, A_1(\mathbf{n})) &\ll 2^{2k} (IQ^{-1})^{2k} \sum_{\substack{\alpha_h | q \\ h>1}} 1 \\ &\ll d(q)^{2k-1} (IQ^{-1})^{2k}. \end{aligned}$$

The final bound for L_α then follows immediately from (6.1),

$$L_\alpha \ll d(q)^{\eta_k+2kb+2k-1} (IQ^{-1})^{2k}.$$

6.3. The final bound for $N(\mathcal{I})$

It follows from (4.6) that

$$N(\mathcal{I}) \ll d(q)^{\sigma_k} I^{2k-1} Q^{-1} + d(q)^{2kb} I^k Q^k + b^{\nu(q)} d(q)^{\eta_k+2kb+2k-1} (\log Q) I^{2k-1} Q^{-1},$$

independent of the value of α . This was proved under the conditions

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

Setting $I \leq q^{\frac{k+1}{2k}}$ and $Q = \frac{1}{8} I^{\frac{k-1}{k+1}}$, we have the final bound

$$N(\mathcal{I}) \ll d(q)^{\tau_k} (\log q) I^{\frac{2k^2}{k+1}}, \quad (6.2)$$

where τ_k is a constant dependent only on a, b, k . Note that $N(\mathcal{I})$ increases as a function of the interval \mathcal{I} . Thus applying (6.2) to (4.1) with $\mathcal{I} = [1, 2w]$, we obtain

$$U(w, M, q) \ll M^{\frac{1}{2k}} d(q)^{\frac{\tau_k}{2k}} (\log q)^{\frac{1}{2k}} w^{\frac{k}{k+1}},$$

as long as $2w \leq q^{\frac{k+1}{2k}}$ and $M \leq q/2$. Thus assuming $X \leq q^{\frac{k+1}{2k}}$ and $Y \leq q/2$,

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

This concludes the proof of Theorem 4.

7. Two Nontrivial Bounds for $h_3(D)$

We now prove two nontrivial bounds for $h_3(D)$. Let d be a square-free positive integer. By the Scholz reflection principle [12], $\log_3(h_3(-d))$ and $\log_3(h_3(+3d))$ differ by at most one, hence we may restrict our attention to imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$. Suppose there is a nontrivial ideal class $[\mathfrak{a}] \in CL(-d)$ such that $[\mathfrak{a}]^3$ is the principal ideal class. There is an integral ideal \mathfrak{b} in $[\mathfrak{a}]$ with norm

$$\mathfrak{N}(\mathfrak{b}) \leq \frac{2}{\pi} \sqrt{|\Delta|},$$

where Δ is the discriminant of the field. Since \mathfrak{b}^3 is principal, we may write

$$4(\mathfrak{N}(\mathfrak{b}))^3 = y^2 + dz^2$$

for some $y, z \in \mathbb{N}$. An integer point on the surface

$$4x^3 = y^2 + dz^2 \tag{7.1}$$

specifies at most d^ϵ ideals \mathfrak{b} , so we may obtain an upper bound for $h_3(-d)$ by bounding the number of integer points (x, y, z) on the cubic surface (7.1) in the region $x \leq L$, $y \leq M$, and $z \leq N$, where $L = (4/\pi)d^{1/2}$, $M = (16/\pi^{3/2})d^{3/4}$, and $N = (16/\pi^{3/2})d^{1/4}$. Any integer point on this surface also provides a solution of the congruence

$$4x^3 \equiv y^2 \pmod{d}, \tag{7.2}$$

and conversely, any solution of this congruence specifies at most 2 integer points on the cubic surface. Therefore it is sufficient to estimate the number of solutions (x, y) to (7.2) with $x \leq L$ and $y \leq M$.

Let

$$N'_d(L, M) = \#\{x \leq L, y \leq M : x^3 \equiv y^2 \pmod{d}\}.$$

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 $L' = 4L$, $M' = 4M$. Theorems 1 and 2 now follow as corollaries to Theorems 3 and 4 with the odd square-free modulus \bar{d} .

7.1. Proof of Theorem 1

By Theorem 3,

$$N'_{\bar{d}}(L', M') \ll d^{1/2+\epsilon} + d^{-1+\epsilon} LM + d^{-1/2+\epsilon} L.$$

Thus when applied directly, Theorem 3 gives only the trivial bound,

$$h_3(-d) \ll d^{1/2+\epsilon}.$$

However, if we assume that d has a divisor d_0 of appropriate size, we may apply

Theorem 3 to obtain a nontrivial result. 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 $\bar{d}_0|\bar{d}$. Trivially,

$$N'_{\bar{d}}(L', M') \leq N'_{\bar{d}_0}(L', M').$$

If $\bar{d}_0 \gg d^{3/4}$ then $L', M' \ll \bar{d}_0$ so we may apply Theorem 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 $\bar{d}_0 \ll d^{3/4}$ then even the trivial bound

$$h_3(-d) \ll d^{1/2+\epsilon}$$

is sufficient for Theorem 1. By the Scholz reflection principle, we also obtain an equivalent bound for $h_3(+3d)$. This completes the proof of Theorem 1.

7.2. Proof of Theorem 2

By Theorem 4,

$$N'_{\bar{d}}(L', M') \ll M^{\frac{1}{2k}} L^{\frac{k}{k+1}} d(d)^{\frac{\tau_k}{2k}} (\log d)^{\frac{1}{2k}}$$

for any integer $k \geq 1$, 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 equivalently $k = 7$, we obtain an exponent of $55/112 + \epsilon$. Thus

$$h_3(-d) \ll d^{\frac{55}{112}+\epsilon}$$

for any $\epsilon > 0$. Again, by the Scholz reflection principle, we obtain an equivalent bound for $h_3(+3d)$. This completes the proof of Theorem 2.

7.3. Remarks

It is an immediate consequence of Theorem 2 that there are at most $O(|D|^{55/112+\epsilon})$ cubic extensions of \mathbb{Q} with discriminant D , by Hasse's result [4]. Similarly, by Theorem 1, if 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 .

We also note two conditional results for $h_3(D)$. In [13], Soundararajan notes that it is possible to show $h_3(D) \ll |D|^{1/3+\epsilon}$ for all but $\ll X^\epsilon$ values D in a range $[X, 2X]$. Assuming both the Birch–Swinnerton-Dyer conjecture and the Riemann hypothesis, Wong [15] has shown that $h_3(D) \ll |D|^{1/4+\epsilon}$.

Finally, we remark that it might appear that one could apply the quite general estimates for $N'_q(X, Y)$ in Theorems 3 and 4 to bound the g -part $h_g(-d)$ for any $g \geq 3$. In this case one would desire to bound the number of integer points on the variety

$$4x^g = y^2 + dz^2,$$

within 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 3 nor Theorem 4 apply, since the range of y is greater than the modulus d , for $g > 3$.

8. *Elliptic Curves with Fixed Conductor*

The 3-part of class numbers of quadratic fields is intimately related to the number of elliptic curves over \mathbb{Q} with fixed conductor. In [1], Brumer and Silverman bound the number of elliptic curves over \mathbb{Q} with good reduction outside a given set of primes S . Their method is as follows: let S be a finite set of rational primes (including 2 and 3) and let M be the product of the primes in S . Let E/\mathbb{Q} be an elliptic curve with good reduction outside of S and with minimal Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then the invariants c_4 and c_6 have $c_4^3 - c_6^2 = 1728\Delta \in \mathbb{Z}_S^*$; 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

$$\mathcal{E}_A : y^2 = x^3 + A.$$

Then $(c_4/D^2, c_6/D^3)$ 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 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 and third bounds may be obtained by simple combinatorial arguments; 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. Brumer and Silverman show that

$$\#\mathcal{E}_A(\mathbb{Z}_S) \leq 2 \cdot 17^{14+2\#S} \cdot 3^{4\#S} h_3(-A).$$

Thus a bound $h_3(-A) \ll |\text{Disc}(\mathbb{Q}(\sqrt{-A}))|^{\theta+\epsilon}$ gives a bound of $O(M^{\theta+\epsilon})$ for $\#\mathcal{E}_A(\mathbb{Z}_S)$, and as a consequence, for the number of elliptic curves with good reduction outside of S . Since a curve with conductor N has good reduction outside the primes dividing N , it follows that the number of elliptic curves over \mathbb{Q} with conductor N may be bounded by $O(N^{1/2+\epsilon})$, and that a nontrivial bound $h_3(-A) \ll |\text{Disc}(\mathbb{Q}(\sqrt{-A}))|^{\theta+\epsilon}$ refines this to $O(N^{\theta+\epsilon})$. Thus Theorem 5 is an immediate result of the bounds for $h_3(D)$ given in Theorems 1 and 2.

Acknowledgements. The author was at the Mathematical Institute of the University of Oxford, supported by the Rhodes Trust, for duration of this work. The author would like to thank D. R. Heath-Brown for advising the thesis of which this work is a part, and J. H. Silverman, P. Sarnak, and N. Katz for their advice and encouragement.

Independently and simultaneously, H. Helfgott and A. Venkatesh also proved a nontrivial bound for $h_3(D)$ and the number of elliptic curves with conductor N . Specifically, they obtain the bounds $O(|D|^{0.44178\dots})$ for the 3-part and $O(N^{0.2238\dots})$ for the number of such elliptic curves. Their methods are presented in [7]; they are based on a new method for counting integral points on elliptic curves, using a result for sphere-packings. The author would like to thank Helfgott and Venkatesh for making a preprint of their paper available.

*Department of Mathematics,
Princeton University, Princeton,
NJ 08544 USA*

lbpierce@princeton.edu

References

1. A. BRUMER and J. H. SILVERMAN, 'The number of elliptic curves over \mathbb{Q} with conductor N ,' *Manuscripta Math.* 91 (1996) 95-102.
2. D. A. BURGESS, 'On character sums and L -series I,' *Proc. London Math. Soc.* (12) 3 (1962) 193-206.
3. 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), pp. 168-232.
4. H. HASSE, 'Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage,' *Math. Z.* 31 (1930) 565-582. Corrigendum, *Math. Z.* 31 (1930) 799.
5. D. R. HEATH-BROWN, 'Hybrid bounds for Dirichlet L -functions,' *Inventiones Math.* 47 (1978) 149-170.
6. D. R. HEATH-BROWN, 'The least square-free number in an arithmetic progression,' *J. Reine Angew. Math.* 332 (1982) 204-220.
7. H. HELFGOTT and A. VENKATESH, 'Integral points on elliptic curves and 3-torsion in class groups,' preprint, <http://www.arxiv.org/abs/math.NT/0405180>.
8. C. HOOLEY, 'A note on square-free numbers in arithmetic progressions,' *Bull. London Math. Soc.* 7 (1975), 133-138.
9. C. HOOLEY, 'On the representations of a number as the sum of four cubes: I,' *Proc. London Math. Soc.* (36) 3 (1978), 117-140.
10. L. K. HUA, *Introduction to Number Theory* (Berlin: Springer-Verlag, 1982).
11. W. SCHMIDT, *Equations over Finite Fields: An Elementary Approach* Lecture Notes in Mathematics 536 (Berlin: Springer-Verlag, 1976).
12. A. SCHOLZ, 'Über die Beziehung der Klassenzahlen quadratischer Körper zueinander,' *J. Reiner Angew. Math.* 166 (1932) 201-203.
13. K. SOUNDARARAJAN, 'Divisibility of class numbers of imaginary quadratic fields,' *J. London Math. Soc.* (61) 2 (2000) 681-690.
14. A. WEIL, 'On some exponential sums,' *Proc. Nat. Acad. Sci. USA* 34(1948) 204-207.
15. S. WONG, 'On the rank of ideal class groups,' *Number Theory*. (Ottawa, ON, 1996), pp. 377-383, *CRM Proc. Lecture Notes* 19 (Amer. Math. Soc., Providence, RI, 1999).