# A BOUND FOR THE 3-PART OF CLASS NUMBERS OF QUADRATIC FIELDS BY MEANS OF THE SQUARE SIEVE

LILLIAN B. PIERCE

Abstract. We prove a nontrivial bound of $O(|D|^{27/56+\epsilon})$ for the 3-part of the class number of a quadratic field $\mathbb{Q}(\sqrt{D})$ by using a variant of the square sieve and the $q$-analogue of van der Corput's method to count the number of squares of the form $4x^3 - dz^2$ for a square-free positive integer $d$ and bounded $x, z$.

## 1. Introduction

Consider the quadratic field $\mathbb{Q}(\sqrt{D})$ with class group $CL(D)$ and class number $h(D)$ for a nonzero integer $D$. The 3-part $h_3(D)$ of the class number is defined to be the number of elements in the class group whose cube is the principal ideal class. The trivial bound for the 3-part is

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

for any $\epsilon > 0$. It is conjectured that $h_3(D) \ll |D|^{\epsilon}$ for any $\epsilon > 0$.

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

**Theorem 1.1.** *Let $D$ be a nonzero integer. The 3-part $h_3(D)$ of the class number of the quadratic field $\mathbb{Q}(\sqrt{D})$ admits the bound*

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

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

We reduce the problem of bounding the 3-part to counting squares as follows. Let $d$ be a square-free positive integer. By the Scholz reflection principle [13], $\log_3(h_3(-d))$ 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 $[\mathfrak{a}] \in CL(-d)$ is a nontrivial element such that $[\mathfrak{a}]^3$ is the principal ideal class. By the Minkowski bound, there is an integral ideal $\mathfrak{b}$ in $[\mathfrak{a}]$ with norm

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

where $\Delta$ is the discriminant of the field. Furthermore, 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 cubic surface

$$4x^3 = y^2 + dz^2 \tag{1.1}$$

*Date*: 10 January 2005.

1991 *Mathematics Subject Classification.* Primary 11R29; Secondary 11A07.

specifies at most $O(d^\epsilon)$ ideals $\mathfrak{b}$, so we may obtain an upper bound for $h_3(-d)$ by counting the number of integer points on (1.1) in the region $x \le L$, $y \le M$, and $z \le N$, where

$$L = (4/\pi)d^{1/2}, \qquad M = (16/\pi^{3/2})d^{3/4}, \qquad N = (16/\pi^{3/2})d^{1/4}. \tag{1.2}$$

We obtain a nontrivial bound for $h_3(-d)$ by counting the number of squares of the form

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

with $x \le L$, $z \le N$, using a variant of the square sieve [6] that allows us to employ the $q$-analogue of van der Corput's method [4], [7] to bound certain sums resulting from the square sieve. Furthermore, we use estimates for exponential sums resulting from Weil's proof of the Riemann hypothesis for curves over finite fields (as in [12] or [14]), and an estimate of Katz [10] using Deligne's results [2] for exponential sums in several variables. It is the use of the $q$-analogue of van der Corput's method in combination with the variant of the square sieve that is the most innovative aspect of this paper, allowing us to achieve a savings over the trivial bound for smaller ranges of $x, z$ than the square sieve alone could accommodate effectively.

In Section 2 we apply the square sieve variant, obtaining a main sieve term, two prime sieve terms, and two error terms. In Section 3 we bound the main sieve term, and in Section 4 we bound the two prime sieve terms. In Section 5 we choose certain parameters optimally, obtaining our final bound. In Section 6 we estimate the error terms, showing that they are dominated by the final bound. In Section 7 we note several immediate results of a nontrivial bound for $h_3(D)$.

Recent work by the author [11] has shown that $h_3(D)$ 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 results were obtained working modulo the square-free kernel of $D$, using cancellation of certain exponential sums, as in [5]. Furthermore, Helfgott and Venkatesh [8] have recently shown that $h_3(D)$ is $O(|D|^{0.44178\ldots})$, using a new method for counting integral points on elliptic curves, and a result for sphere-packings.

We also note two conditional results for $h_3(D)$. Assuming the Riemann hypothesis for the single $L$-function $L(\chi_D, s)$ associated to the quadratic Dirichlet character $\chi_D$ of the field $\mathbb{Q}(\sqrt{D})$, Soundararajan has shown, as outlined in [8], that $h_3(D)$ is $O(|D|^{1/3+\epsilon})$. Assuming both the Birch–Swinnerton-Dyer conjecture and the generalized Riemann hypothesis, Wong [15] has shown that $h_3(D)$ is $O(|D|^{1/4+\epsilon})$.

1.1. **Notation.** In this paper we use the following notational conventions. The notation $A \ll B$ indicates that $A \le cB$ for a positive constant $c$ that depends only on certain variables as indicated. The notation $A \approx B$ indicates that $A \ll B$ and $B \ll A$. We denote by $[x]$ the greatest integer part of $x$ and by $\|x\|$ the distance from $x$ to the nearest integer. We use the standard notation $e(x)$ for $e^{2\pi i x}$ and $e_q(x)$ for $e^{2\pi i x/q}$. Also, we denote by $\bar{n}$ the unique solution to $\bar{n}n \equiv 1 \pmod q$ with $1 \le \bar{n} \le q$. 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. The Legendre symbol $\left(\frac{n}{p}\right)$ is defined to be 0 if $n$ is zero modulo $p$, $+1$ if $n$ is a quadratic residue modulo $p$, and $-1$ otherwise. The Jacobi symbol $\left(\frac{n}{m}\right)$ for a positive integer $m = p_1^{a_1} \cdots p_r^{a_r}$ is defined in terms of Legendre symbols as $\left(\frac{n}{p_1}\right)^{a_1} \cdots \left(\frac{n}{p_r}\right)^{a_r}$.

## 2. The square sieve

The square sieve was introduced by Heath-Brown in [6] 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 a sequence $(\omega(n))$ where $\omega$ is a non-negative integer-valued function defined for each integer $n$, with $\sum\omega(n) < \infty$. We use the following variant of the square sieve with a sieving set $\mathcal{A}$ of positive integers that are products of two primes, rather than a sieving set of primes, as in [6].

**Lemma 2.1** (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, and in particular, if $n = m^2$, then

$$\sum_{f\in\mathcal{A}}\left(\frac{n}{f}\right) = \sum_{f\in\mathcal{A}}\left(\frac{m^2}{f}\right) = \sum_{\substack{f\in\mathcal{A}\\(f,m)=1}} 1 \geq A - \sum_{\substack{f\in\mathcal{A}\\(f,m)\neq 1}} 1 \gg A,$$

since $\omega(n) = 0$ for $|n| \geq \exp(\min(U, V))$. Thus

$$\Sigma \gg A^2\sum_n \omega(n^2). \tag{2.1}$$

But also

$$\begin{aligned}\Sigma &= \sum_{f,g\in\mathcal{A}}\sum_n \omega(n)\left(\frac{n}{fg}\right)\\ &= \sum_{f\in\mathcal{A}}\sum_n \omega(n)\left(\frac{n}{f^2}\right) + \sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)=1}}\sum_n \omega(n)\left(\frac{n}{fg}\right)\\ &\quad + \sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)\neq 1}}\sum_n \omega(n)\left(\frac{n}{fg}\right).\end{aligned} \tag{2.2}$$

The last term in (2.2) may be broken into the two terms

$$S(\mathcal{U})+S(\mathcal{V}) = \sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v\nmid n}}\omega(n)\left(\frac{n}{uu'}\right) + \sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u\nmid n}}\omega(n)\left(\frac{n}{vv'}\right).$$

Furthermore, $S(\mathcal{U})$ may be written as a main term $M(\mathcal{U})$, 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 $S(\mathcal{V}) = M(\mathcal{V}) - E(\mathcal{V})$. Thus (2.2) becomes:

$$\begin{aligned}|\Sigma| &\ll A\sum_n \omega(n) + \sum_{\substack{f\neq g\in\mathcal{A}\\(f,g)=1}}\left|\sum_n \omega(n)\left(\frac{n}{fg}\right)\right|\\ &\quad + V\sum_{u\neq u'\in\mathcal{U}}\left|\sum_n \omega(n)\left(\frac{n}{uu'}\right)\right| + |E(\mathcal{U})|\\ &\quad + U\sum_{v\neq v'\in\mathcal{V}}\left|\sum_n \omega(n)\left(\frac{n}{vv'}\right)\right| + |E(\mathcal{V})|.\end{aligned}$$

The result then follows by comparison with (2.1). □

Let

$$T(d) = \#\{x,y,z\in\mathbb{N} : y^2 = 4x^3 - dz^2 : x\leq L, y\leq M, z\leq N\},$$

where $L, M, N$ are as defined in (1.2). Then

$$h_3(-d) \ll d^{\epsilon}T(d). \tag{2.3}$$

Furthermore, let

$$\omega(n) = \#\{x,z\in\mathbb{N} : n = 4x^3 - dz^2 : x\leq L, z\leq N\}, \tag{2.4}$$

so that

$$T(d) = \sum_{n=1}^{\infty}\omega(n^2).$$

Our main goal is thus to obtain a nontrivial bound $T(d)\ll d^{1/2-\theta}$, for some constant $\theta>0$.

Let $Q$ be a positive number we will choose later; for now we assume only that $c\log d \le Q \le d$ for some constant $c$. Let $\alpha, \beta \in (0,1)$ be positive real numbers with $\alpha+\beta = 1$. Let $\mathcal{U}, \mathcal{V}, \mathcal{A}$ be sets of cardinalities $U, V, A$, 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 later see that it is sufficient to choose the constants to be $c_0 = 2, c_1 = 1$ in order that the sets $\mathcal{U}$ and $\mathcal{V}$ be 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 $Q \ge c\log d$ 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 $A = UV \gg Q(\log Q)^{-2}$.

For positive integers $a, b$ with $(a,b) = 1$, define

$$C(d,a,b) = \sum_n \omega(n) \left(\frac{n}{ab}\right).$$

Applying Lemma 2.1 with the function $\omega(n)$ as defined in (2.4) and the sets $\mathcal{A}, \mathcal{U}, \mathcal{V}$ as defined above, we obtain

$$\begin{aligned} T(d) \ll\ & A^{-1}\sum_n \omega(n) + A^{-2} \sum_{\substack{f\ne g\in\mathcal{A}\\(f,g)=1}} |C(d,f,g)| \\ & + VA^{-2} \sum_{u\ne u'\in\mathcal{U}} |C(d,u,u')| + A^{-2}|E(\mathcal{U})| \\ & + UA^{-2} \sum_{v\ne v'\in\mathcal{V}} |C(d,v,v')| + A^{-2}|E(\mathcal{V})|. \end{aligned} \tag{2.5}$$

The first term on the right hand side in (2.5), to which we will refer as the leading term, is bounded trivially by

$$A^{-1}\sum_n \omega(n) \ll A^{-1}LN \ll d^{3/4}Q^{-1}(\log Q)^2. \tag{2.6}$$

Thus it is clear that in order to attain a nontrivial bound for $T(d)$, we must choose $Q = d^{1/4+\delta}$ for some $\delta > 0$.

We will refer to the sum in (2.5) 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. Sieving over products of primes, rather than over primes alone, is a critical innovation of our methods. We will 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 product of the larger primes alone, thus enabling us to achieve a nontrivial bound for $T(d)$, despite the relatively small range of the variable $z$.

2.1. **The general term $C(d,a,b)$.** Our main goal is to estimate the term $C(d,a,b)$, which may be written as

$$C(d,a,b) = \sum_{\substack{x \leq L \\ z \leq N}} \left( \frac{4x^3 - dz^2}{ab} \right),$$

where as before $\left(\frac{n}{ab}\right)$ is the Jacobi symbol. In order to obtain a nontrivial bound for $T(d)$, we require an estimate of the form $|C(d,a,b)| \ll d^{1/2-\theta}$ for some $\theta > 0$.

In order to accomplish such a bound, we will extend the ranges of the variables $x$ and $z$ to complete sets of residues and then use exponential sum techniques. 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 of size $\sqrt{ab}$. In the case of the main sieve, $\sqrt{ab}$ is of size $Q = d^{1/4+\delta}$, where $\delta$ is a small positive constant. Thus the range $L \approx d^{1/2}$ of the variable $x$ is sufficiently large, while the range $N \approx d^{1/4}$ of the variable $z$ is not. Extending the ranges of both $x$ and $z$ at this point would only obtain a bound of size $|C(d,a,b)| \ll d^{1/2+2\delta}$.

Therefore at this stage we only extend the range of $x$ to a full set of residues modulo $ab$. We later use the $q$-analogue of van der Corput's method to reduce the effective modulus of the resulting exponential sum so that we may then finally extend the range of $z$ to a full set of residues modulo the new, smaller modulus. Extending the range of $x$, we obtain:

$$\begin{aligned} C(d,a,b) &= \sum_{z \leq N} \sum_{\alpha=1}^{ab} \left( \frac{4\alpha^3 - dz^2}{ab} \right) \sum_{\substack{x \leq L \\ x \equiv \alpha \pmod{ab}}} 1 \\ &= \sum_{z \leq N} \sum_{\alpha=1}^{ab} \left( \frac{4\alpha^3 - dz^2}{ab} \right) \frac{1}{ab} \sum_{x \leq L} \sum_{k=1}^{ab} e_{ab}(k(\alpha - x)). \end{aligned}$$

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

$$\mathbf{S}(d,r;k,N) = \sum_{z \leq N} S(d,r;k,z). \tag{2.7}$$

Then

$$|C(d,a,b)| \leq \frac{1}{ab} \sum_{k=1}^{ab} \min(L, \|k/ab\|^{-1}) |\mathbf{S}(d,ab;k,N)|. \tag{2.8}$$

Thus the main problem is to bound sums of the form $\mathbf{S}(d,r;k,N)$. Using simply the trivial bound $|S(d,r;k,z)| \leq r$ for each term in (2.7), we obtain a trivial bound of $|\mathbf{S}(d,r;k,N)| \leq Nr$, which in the case of the main sieve is of size $d^{1/4}Q^2 = d^{3/4+2\delta}$. Even assuming square-root cancellation for each individual term $S(d,r;k,z)$ in (2.7) only results in a bound of size $|\mathbf{S}(d,r;k,N)| \ll d^{1/2+\delta}$. In order to obtain a nontrivial bound for $T(d)$, we require a bound of the form $|\mathbf{S}(d,r;k,N)| \ll d^{1/2-\theta}$ for some $\theta > 0$. Auxiliary cancellation over the $z$ variable gives the critical savings.

## 3. The main sieve

We first 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 factorization $r = r_0 r_1$, where $r_0 = uu'$ and $r_1 = vv'$, so that $r_0 \approx Q^{2\alpha}$ and $r_1 \approx Q^{2\beta}$.

The sum $S(d, r; k, z)$ is multiplicative in the following sense:

**Lemma 3.1.** *If $(r_0, r_1) = 1$, then*

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

*where $r_0\overline{r_0} \equiv 1 \ (mod\, r_1)$ and $r_1\overline{r_1} \equiv 1 \ (mod\, r_0)$.*

*Proof.* We may verify this directly. Writing $\alpha = \alpha_1 r_0 + \alpha_0 r_1$ modulo $r_0 r_1$,

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

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 writing the double sum over $\alpha_0 \pmod{r_0}$ and $\alpha_1 \pmod{r_1}$ as two sums, we then obtain the desired factorization. □

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. Let $H = [N/r_1]$. Then

$$\begin{aligned} H\mathbf{S}(d, r; k, N) &= \sum_{h=1}^{H} \sum_{z} A(z + hr_1) \\ &= \sum_{1 - Hr_1 \leq z \leq N - r_1} \sum_{h=1}^{H} A_0(z + hr_1) A_1(z + hr_1) \\ &= \sum_{1 - Hr_1 \leq z \leq N - r_1} S(d, r_1; k\overline{r_0}, z) \sum_{h=1}^{H} A_0(z + hr_1), \end{aligned}$$

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

$$\begin{aligned}\Sigma_1 &= \sum_{1-Hr_1 \le z \le N-r_1} |S(d, r_1; k\overline{r_0}, z)|^2, \\ \Sigma_2 &= \sum_z \left| \sum_{h=1}^{H} A_0(z+hr_1) \right|^2.\end{aligned}$$

(Unless otherwise noted, the sum over $z$ is taken over all integers; the characteristic function $A_0$ effectively restricts the sum to the appropriate range.)

We may further separate the term $\Sigma_2$ 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

$$H^2 |\mathbf{S}(d, r; k, N)|^2 \ll \Sigma_1 \left(\Sigma_{2A} + \Sigma_{2B}\right). \tag{3.1}$$

3.1. **Bounding $\Sigma_1$ and $\Sigma_{2A}$.** By Lemma 3.1, it suffices to bound $S(d, p; t, z)$ for any odd prime $p \nmid d$ and positive integers $t, z$.

**Lemma 3.2.** *Let $p$ be an odd prime with $p \nmid d$. Then*

$$|S(d, p; t, z)| \le 3p^{1/2}.$$

*Proof.* First assume that $p > 3$. If $p \nmid z$ and $p \nmid t$, the Weil bound for hybrid sums of a multiplicative and an additive character modulo $p$ (see Chapter II of [12]) shows that

$$|S(d, p; t, z)| \le 3p^{1/2}.$$

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 $|a_p| \leq 2p^{1/2}$. Hence

$$|S(d,p;t,z)| \leq 2p^{1/2}.$$

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 $p = 3$, the trivial bound

$$|S(d,p;t,z)| \leq 3$$

is sufficient. □

This immediately gives the following bounds for $\Sigma_1$ and $\Sigma_{2A}$:

**Lemma 3.3.**

$$\begin{aligned} \Sigma_1 &\ll (N + Hr_1)r_1, \\ \Sigma_{2A} &\ll HNr_0. \end{aligned}$$

3.2. **Bounding $\Sigma_{2B}$.** Define

$$T(d,r_0;h,N) = \sum_{z} A_0(z + hr_1)\overline{A_0(z)}, \tag{3.2}$$

so that

$$\Sigma_{2B} = H \sum_{h=1}^{H-1} |T(d,r_0;h,N)|. \tag{3.3}$$

Using simply the trivial bound $|A_0(z)| \leq r_0$, we see that a trivial bound for (3.2) is $|T(d,r_0;h,N)| \leq Nr_0^2$. However, in order to obtain a nontrivial bound for $T(d)$, we require a bound significantly better than $|T(d,r_0;h,N)| \ll Nr_0$.

It is at this point that we extend the range of $z$ to a complete set of residues modulo the new modulus $r_0 \approx Q^{2\alpha}$. (We will later choose $Q$ and $\alpha$ so that $r_0$ is of size $d^{5/14}$. The range $N \approx d^{1/4}$ of the variable $z$ is then larger than $\sqrt{r_0}$, as desired.) Write

$$\begin{aligned} T(d,r_0;h,N) &= \sum_{l=1}^{r_0} S(d,r_0;k\overline{r_1},l + hr_1)\overline{S(d,r_0;k\overline{r_1},l)} \sum_{\substack{1 \leq z \leq N - hr_1 \\ z \equiv l \pmod{r_0}}} 1 \\ &= \sum_{l=1}^{r_0} S(d,r_0;k\overline{r_1},l + hr_1)\overline{S(d,r_0;k\overline{r_1},l)} \\ &\quad \cdot \sum_{1 \leq z \leq N - hr_1} \frac{1}{r_0} \sum_{m=1}^{r_0} e_{r_0}(m(l-z)). \end{aligned}$$

Thus

$$|T(d,r_0;h,N)| \leq \frac{1}{r_0}\sum_{m=1}^{r_0} \min(N, \|m/r_0\|^{-1})\,|W(d,r_0;h,m,k\overline{r_1})|\,, \tag{3.4}$$

where we define

$$\begin{aligned} &W(d,r_0;h,m,k\overline{r_1}) \\ &= \sum_{\substack{l,\alpha,\beta \\ (\mathrm{mod}\ r_0)}} \left(\frac{4\alpha^3-d(l+hr_1)^2}{r_0}\right)\left(\frac{4\beta^3-dl^2}{r_0}\right) e_{r_0}(k\overline{r_1}\alpha - k\overline{r_1}\beta + ml). \end{aligned}$$

A simple computation similar to that of Lemma 3.1 shows that $W(d,r_0;h,m,k\overline{r_1})$ is multiplicative in the following sense: 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 $p \nmid r_1$ and positive integers $h,s,t$. The following estimate is due to Katz [10], using a result of Deligne [2] for exponential sums in several variables.

**Lemma 3.4.** *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 use the following additional estimates in the cases when $p$ divides both $h$ and $s$.

**Lemma 3.5.** *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

$$|W(d,p;h,s,t)| \leq \sum_{l \ (\mathrm{mod}\ p)} \left| \sum_{\alpha \ (\mathrm{mod}\ p)} \left(\frac{4\alpha^3-dl^2}{p}\right) e_p(t\alpha)\right|^2.$$

We may bound the inner sum in absolute value by $3p^{1/2}$ using the Weil bound for hybrid sums of a multiplicative and an additive character modulo $p$ (as in [12]). Estimating the sum over $l$ trivially, we obtain a final bound of

$$|W(d,p;h,s,t)| \leq 9p^2.$$

□

**Lemma 3.6.** *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,

$$|W(d,p;h,s,t)| \leq \sum_{l \pmod p} \left| \sum_{\alpha \pmod p} \left( \frac{4\alpha^3 - dl^2}{p} \right) \right|^2. \tag{3.5}$$

If $p \equiv 2 \pmod 3$, then for each fixed $l$, $4\alpha^3 - dl^2$ ranges over a complete set of residues modulo $p$ as $\alpha$ does, so that the inner sum in (3.5) vanishes. If $p \equiv 1 \pmod 3$ we may argue, as in Lemma 3.2, that

$$p + \sum_{\alpha \pmod p} \left( \frac{4\alpha^3 - dl^2}{p} \right)$$

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 the inner sum in (3.5) is bounded in absolute value by $2p^{1/2}$, 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 combine all of these results in the following lemma:

**Lemma 3.7.** *Let $p$ be an odd prime with $p \nmid d$ and $p \nmid r_1$. Then*

$$|W(d,p;h,s,t)| \leq 24p^{3/2}(p,h,s)^{1/2}.$$

Applying this bound to $W(d, r_0; h, m, k\overline{r_1})$ in (3.4) gives

$$|T(d,r_0;h,N)| \ll r_0^{1/2} \sum_{m=1}^{r_0} (r_0,h,m)^{1/2} \min(N, \|m/r_0\|^{-1}).$$

By (3.3) we then have

$$\begin{aligned} \Sigma_{2B} &\ll H r_0^{1/2} \sum_{h=1}^{H-1} \sum_{m=1}^{r_0} (r_0,h,m)^{1/2} \min(N, \|m/r_0\|^{-1}) \\ &= N H r_0^{1/2} \sum_{h=1}^{H-1} (h,r_0)^{1/2} \\ &\quad + H r_0^{1/2} \sum_{h=1}^{H-1} \sum_{m=1}^{r_0-1} \|m/r_0\|^{-1} (r_0,h,m)^{1/2}. \end{aligned} \tag{3.6}$$

We may estimate the double sum in (3.6) by

$$\begin{aligned}\sum_{m=1}^{r_0-1}\|m/r_0\|^{-1}\sum_{h=1}^{H-1}(r_0,h,m)^{1/2} &\leq 2\sum_{1\leq m\leq r_0/2}\frac{r_0}{m}\sum_{h=1}^{H-1}((r_0,h),(r_0,m))^{1/2}\\ &\ll r_0\sum_{1\leq m\leq r_0/2}\frac{1}{m}\sum_{d|(r_0,m)}d^{1/2}\sum_{\substack{h=1\\ d|h}}^{H-1}1\\ &\ll Hr_0\sum_{1\leq m\leq r_0/2}\frac{1}{m}\sum_{d|(r_0,m)}d^{-1/2}\\ &\ll Hr_0d(r_0)\log r_0.\end{aligned}$$

Similarly, the first sum in (3.6) is bounded by

$$\sum_{h=1}^{H-1}(h,r_0)^{1/2}\ll Hd(r_0).$$

Thus the final bound for $\Sigma_{2B}$ is:

**Lemma 3.8.**

$$\Sigma_{2B}\ll H^2Nr_0^{1/2}d(r_0)+H^2r_0^{3/2}d(r_0)\log r_0.$$

3.3. **Bounding $\mathbf{S}(d,r;k,N)$.** Assembling the results of Lemmas 3.3 and 3.8 in (3.1), it follows that

$$\begin{aligned}|\mathbf{S}(d,r;k,N)|^2 &\ll H^{-1}N(N+Hr_1)r_0r_1\\ &\quad+(N+Hr_1)r_1\left[Nr_0^{1/2}d(r_0)+r_0^{3/2}d(r_0)\log r_0\right].\end{aligned}\tag{3.7}$$

Since $H=[N/r_1]$, we obtain:

$$|\mathbf{S}(d,r;k,N)|\ll Nr_0^{1/4}r_1^{1/2}(d(r_0))^{1/2}+N^{1/2}r_0^{1/2}r_1+N^{1/2}r_0^{3/4}r_1^{1/2}(d(r_0))^{1/2}(\log r_0)^{1/2}.$$

By (2.8), we may now achieve a bound for the term $C(d,f,g)$ in the main sieve:

**Proposition 3.1.** *For any $f\neq g\in\mathcal{A}$ with $(f,g)=1$,*

$$|C(d,f,g)|\leq\left[Q^{-2}L+\log Q\right]\left[NQr_0^{-1/4+\epsilon}+N^{1/2}Q^2r_0^{-1/2}+N^{1/2}Qr_0^{1/4+\epsilon}\right].$$

This completes our estimate for the main sieve.

## 4. The prime sieves

We briefly consider the term $\mathbf{S}(d,r;k,N)$ in 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 factorize 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 outline the argument only for the set $\mathcal{U}$.

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 $H_u = [N/u']$. Applying the $q$-analogue of van der Corput's method as in Section 3, we obtain an expression analogous to that of equation (3.1), namely

$$H_u^2 |\mathbf{S}(d, uu'; k, N)|^2 \ll \Sigma_1 \left(\Sigma_{2A} + \Sigma_{2B}\right), \tag{4.1}$$

where

$$\begin{aligned}
\Sigma_1 &= \sum_{1-H_u u' \le z \le N-u'} |S(d, u'; k\overline{u}, z)|^2, \\
\Sigma_{2A} &= H_u \sum_z |A_0(z)|^2, \\
\Sigma_{2B} &= H_u \sum_{h=1}^{H_u - 1} \left| \sum_z A_0(z + hu') \overline{A_0(z)} \right|.
\end{aligned}$$

By Lemma 3.2 it follows immediately that:

**Lemma 4.1.**

$$\begin{aligned}
\Sigma_1 &\ll (N + H_u u')u', \\
\Sigma_{2A} &\ll H_u N u.
\end{aligned}$$

Let

$$T(d, u; h, N) = \sum_z A_0(z + hu') \overline{A_0(z)},$$

so that

$$\Sigma_{2B} = H_u \sum_{h=1}^{H_u - 1} |T(d, u; h, N)|. \tag{4.2}$$

Define $W(d, u; h, m, k\overline{u'})$ as before, so that

$$|T(d, u; h, N)| \le \frac{1}{u} \sum_{m=1}^{u} \min(N, \|m/u\|^{-1}) \left| W(d, u; h, m, k\overline{u'}) \right|.$$

It follows immediately from Lemma 3.7 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 (4.2) 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 4.2.**

$$\Sigma_{2B} \ll H_u^2 N u^{1/2} d(u) + H_u^2 u^{3/2} d(u) \log u.$$

Applying the bounds for $\Sigma_1, \Sigma_{2A}$, and $\Sigma_{2B}$ given in Lemmas 4.1 and 4.2 to (4.1), it then follows that

$$|\mathbf{S}(d, uu'; k, N)|^2 \ll H_u^{-1} N(N + H_u u')uu' + (N + H_u u')u' \left[ N u^{1/2} d(u) + u^{3/2} d(u) \log u \right].$$

Since $H_u = [N/u']$, we then obtain

$$|\mathbf{S}(d, uu'; k, N)| \ll N u^{1/4} u'^{1/2} (d(u))^{1/2} + N^{1/2} u^{1/2} u' + N^{1/2} u^{3/4} u'^{1/2} (d(u))^{1/2} (\log u)^{1/2}.$$

We thus obtain a bound for $C(d,u,u')$ by (2.8). For reference we state the corresponding result for $C(d,v,v')$ as well:

**Proposition 4.1.** *For any $u \neq u' \in \mathcal{U}$ and $v \neq v' \in \mathcal{V}$ ,*

$$\begin{aligned} |C(d,u,u')| &\leq \left[Q^{-2\alpha}L + \log Q\right]\left[NQ^{(3/4)\alpha+\epsilon} + N^{1/2}Q^{(3/2)\alpha} + N^{1/2}Q^{(5/4)\alpha+\epsilon}\right], \\ |C(d,v,v')| &\leq \left[Q^{-2\beta}L + \log Q\right]\left[NQ^{(3/4)\beta+\epsilon} + N^{1/2}Q^{(3/2)\beta} + N^{1/2}Q^{(5/4)\beta+\epsilon}\right], \end{aligned}$$

*for any $\epsilon > 0$, where all implied constants depend only on $\epsilon$.*

This completes our bounds for the prime sieve terms.

## 5. The final bound for $T(d)$

Applying the bounds of Propositions 3.1 and 4.1 to (2.5), we obtain

$$\begin{aligned} T(d) \ll\ & Q^{-1}LN(\log Q)^2 \\ & + \left[Q^{-2}L + \log Q\right]\left[NQr_0^{-1/4+\epsilon} + N^{1/2}Q^2r_0^{-1/2} + N^{1/2}Qr_0^{1/4+\epsilon}\right] \\ & + V^{-1}\left[Q^{-2\alpha}L + \log Q\right]\left[NQ^{(3/4)\alpha+\epsilon} + N^{1/2}Q^{(3/2)\alpha} + N^{1/2}Q^{(5/4)\alpha+\epsilon}\right] \\ & + U^{-1}\left[Q^{-2\beta}L + \log Q\right]\left[NQ^{(3/4)\beta+\epsilon} + N^{1/2}Q^{(3/2)\beta} + N^{1/2}Q^{(5/4)\beta+\epsilon}\right] \\ & + A^{-2}|E(\mathcal{U})| + A^{-2}|E(\mathcal{V})|. \end{aligned}$$

Balancing the contributions of the leading term and the main sieve, it is optimal to choose $Q = d^{1/4+\delta}$ with $\delta = 1/56$ and $r_0 = Q^{4/3}$, so that $\alpha = 2/3$ and $\beta = 1/3$. The prime sieve over the set $\mathcal{U}$ is then 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

$$d^{1/7+\epsilon}\left[NQ^{1/4+\epsilon} + N^{1/2}Q^{1/2} + N^{1/2}Q^{5/12+\epsilon}\right] \ll d^{103/224+\epsilon} \approx d^{0.45982\ldots+\epsilon}.$$

Assuming that the error terms are also dominated by the leading term and the main sieve (as we will show in the following section), we thus have the final bound

$$T(d) \ll d^{27/56+\epsilon} \approx d^{0.48214\ldots+\epsilon}. \tag{5.1}$$

Hence by (2.3), it follows that

$$h_3(-d) \ll d^{27/56+\epsilon}.$$

## 6. The error terms

We may estimate the error term $E(\mathcal{U})$ as follows. 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 the sets $\{x \leq L : x \equiv x_0 \pmod{v}\}$ for $\delta$ values $x_0$. Let

$$K = LV^{-1} \approx d^{1/2-5/56+\epsilon}.$$

Writing $x = x_0 + vt$ with $t \leq K$, 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

$$E(\mathcal{U}) \ll U^2 V N \max |D(d, uu'; v, x_0, z, K)|, \tag{6.1}$$

where the maximum is taken over all appropriate pairs $u, u'$ and $v, x_0, z$.

6.1. **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 $uu'$,

$$\begin{aligned} D(d, uu'; v, x_0, z, K) &= \sum_{\alpha=1}^{uu'} \left( \frac{4(x_0+v\alpha)^3 - dz^2}{uu'} \right) \sum_{\substack{t \leq K \\ t \equiv \alpha \pmod{uu'}}} 1 \\ &= \frac{1}{uu'} \sum_{h=1}^{uu'} \sum_{\alpha=1}^{uu'} \left( \frac{4(x_0+v\alpha)^3 - dz^2}{uu'} \right) e_{uu'}(h\alpha) \sum_{t \leq K} e_{uu'}(-ht). \end{aligned}$$

Define

$$Y(d, uu'; v, x_0, z, h) = \sum_{\alpha=1}^{uu'} \left( \frac{4(x_0+v\alpha)^3 - dz^2}{uu'} \right) e_{uu'}(h\alpha),$$

so that

$$|D(d, uu'; v, x_0, z, K)| \leq \frac{1}{uu'} \sum_{h=1}^{uu'} \min(K, \|h/uu'\|^{-1}) |Y(d, uu'; v, x_0, z, h)|. \tag{6.2}$$

A simple computation similar to that of Lemma 3.1 shows that we have the factorization

$$Y(d, uu'; v, x_0, z, h) = Y(d, u; v, x_0, z, h\overline{u'}) Y(d, u'; v, x_0, z, h\overline{u}),$$

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 $Y(d, p; v, x_0, z, h)$ for any odd prime $p$ with $p \nmid d$, $p \nmid v$.

**Lemma 6.1.** *For an odd prime $p$ with $p \nmid d$, $p \nmid v$,*

$$|Y(d, p; v, x_0, z, h)| \leq 3p^{1/2}.$$

*Proof.* First suppose that $p > 3$. If $p \nmid z$ and $p \nmid h$, then applying the Weil bound for hybrid sums (as given in [12]),

$$|Y(d, p; v, x_0, z, h)| \leq 3p^{1/2}.$$

If $p \nmid z$ but $p | h$, then

$$Y(d, p; v, x_0, z, h) = \sum_{\alpha=1}^{p} \left( \frac{4(x_0+v\alpha)^3 - dz^2}{p} \right).$$

Arguing as in Lemma 3.2, we obtain

$$|Y(d,p;v,x_0,z,h)| \leq 2p^{1/2}.$$

If $p|z$ then

$$Y(d,p;v,x_0,z,h) = \sum_{\alpha=1}^{p} \left(\frac{4(x_0+v\alpha)^3}{p}\right) e_p(h\alpha) = \sum_{\alpha=1}^{p} \left(\frac{x_0+v\alpha}{p}\right) e_p(h\alpha).$$

Since $p \nmid v$ we may make the change of variables $\alpha \mapsto \alpha - \overline{v}x_0$ so that

$$Y(d,p;v,x_0,z,h) = \left(\frac{v}{p}\right) e_p(-h\overline{v}x_0) \sum_{\alpha=1}^{p} \left(\frac{\alpha}{p}\right) e_p(h\alpha).$$

Then if $p \nmid h$, the classical bound for character sums (see Chapter 7 of [9]) shows that

$$|Y(d,p;v,x_0,z,h)| \leq p^{1/2}.$$

If furthermore $p|h$, then

$$Y(d,p;v,x_0,z,h) = \left(\frac{v}{p}\right) \sum_{\alpha=1}^{p} \left(\frac{a}{p}\right) = 0.$$

For $p = 3$, the trivial bound

$$|Y(d,p;v,x_0,z,h)| \leq 3$$

is sufficient. □

It follows immediately from Lemma 6.1 that

$$|Y(d,uu';v,x_0,z,h)| \leq 9u^{1/2}u'^{1/2}.$$

Applying this in (6.2), we obtain:

$$\begin{aligned} |D(d,uu';v,x_0,z,K)| &\ll u^{-1/2}u'^{-1/2} \sum_{h=1}^{uu'} \min(K, \|h/uu'\|^{-1}) \\ &\ll u^{-1/2}u'^{-1/2}K + u^{1/2}u'^{1/2} \sum_{1 \leq h \leq uu'/2} h^{-1} \\ &\ll u^{-1/2}u'^{-1/2}K + u^{1/2}u'^{1/2} \log U. \end{aligned}$$

Therefore in (6.1),

$$|E(\mathcal{U})| \ll U^2VN(U^{-1}K + U\log U) \ll ULN + U^3VN\log U.$$

Thus

$$A^{-2}|E(\mathcal{U})| \ll V^{-1}(A^{-1}LN) + UV^{-1}N\log U.$$

This estimate for the error term $E(\mathcal{U})$ is sufficiently sharp. The analogous bound for $E(\mathcal{V})$,

$$A^{-2}|E(\mathcal{V})| \ll U^{-1}(A^{-1}LN) + VU^{-1}N\log V,$$

is also sufficiently sharp. This completes the proof of Theorem 1.1.

## 7. Remarks

It is an immediate consequence of Theorem 1.1 that there are $O(|D|^{27/56+\epsilon})$ cubic extensions of $\mathbb{Q}$ with discriminant $D$, by Hasse's result [3]. Additionally, a result of Brumer and Silverman [1] shows that a bound for the 3-part of the form $h_3(D) \ll |D|^{\lambda+\epsilon}$ gives a bound of $O(N^{\lambda+\epsilon})$ for the number of elliptic curves over $\mathbb{Q}$ with conductor $N$. In particular, the trivial bound $h_3(D) \ll |D|^{1/2+\epsilon}$ gives the result that there are $O(N^{1/2+\epsilon})$ elliptic curves over $\mathbb{Q}$ with conductor $N$. Theorem 1.1 refines this to $O(N^{27/56+\epsilon})$. Furthermore, in [8], Helfgott and Venkatesh present a new method for counting integral points on elliptic curves that enables them to show that a bound of the form $h_3(D) \ll |D|^{\lambda+\epsilon}$ gives a bound of $O(N^{2\beta\lambda/\log 3+\epsilon})$ for the number of elliptic curves over $\mathbb{Q}$ with conductor $N$, where $\beta$ is the numerical constant 0.278236.... By Theorem 1.1, we may take $\lambda = 27/56+\epsilon$, yielding a bound of $O(N^{0.24422...+\epsilon})$. However, this is slightly weaker than the bound given by the methods of Helfgott and Venkatesh, namely $O(N^{0.22377...+\epsilon})$.

Finally, we note that our methods do not appear to extend to give a nontrivial bound for the $g$-part $h_g(-d)$ for $g > 3$. The general 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 our variant of the square sieve as above, we obtain a bound for $T_g(d)$ equivalent to (2.5), and we may even carry through the technical analysis of the term corresponding to $C(d, a, b)$. But in order for the leading term in (2.5), 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 $\delta > 0$. The main sieve cannot accommodate such a large value for $Q$ and give a nontrivial bound, for $g > 3$.

## 8. Acknowledgements

The author would like to thank D. R. Heath-Brown for advising the thesis of which this work is a part. The author would also like to thank N. Katz for proving a key estimate in [10], as well as P. Sarnak for his advice and encouragement, the referee for a number of helpful comments, and H. Helfgott and A. Venkatesh for providing a preprint of [8]. The author was supported by the Rhodes Trust for the duration of this work at the Mathematical Institute, Oxford University.

## 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] P. DELIGNE, 'La Conjecture de Weil II,' *Pub. Math. I.H.E.S.* **52** (1981) 313-428.

[3] H. HASSE, 'Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage,' *Math. Z.* **31** (1930) 565-582. Corrigendum, *Math. Z.* **31** (1930) 799.

[4] 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.

[5] D. R. HEATH-BROWN, 'The least square-free number in an arithmetic progression,' *J. Reine Angew. Math.* **332** (1982) 204-220.

[6] D. R. HEATH-BROWN, 'The square sieve and consecutive square-free numbers,' *Math. Ann.* **266** (1984) 251-259.

[7] D. R. HEATH-BROWN, 'The largest prime factor of $X^3 + 2$,' *Proc. London Math. Soc.,* **82** No. 3 (2001) 554-596.

[8] 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.
[9] L. K. HUA, *Introduction to Number Theory*. Berlin: Springer-Verlag (1982).
[10] N. M. KATZ, 'On a question of Lillian Pierce,' Forum Math., in press.
[11] L. B. PIERCE, 'The 3-Part of Class Numbers of Quadratic Fields,' J. London Math. Soc., in press.
[12] W. SCHMIDT, *Equations over Finite Fields: An Elementary Approach.* Lecture Notes in Mathematics 536. Berlin: Springer-Verlag (1976).
[13] A. SCHOLZ, 'Über die Beziehung der Klassenzahlen quadratischer Körper zueinander,' *J. Reiner Angew. Math.* **166** (1932) 201-203.
[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) 377-383, *CRM Proc. Lecture Notes* 19. Amer. Math. Soc., Providence, RI, 1999.

Department of Mathematics, Princeton University, Princeton NJ 08544 USA