Distribution Agreement

Yan Sheng March 19, 2016

THE COHEN-LENSTRA HEURISTICS AND SOUNDARARAJAN'S THESIS

YAN SHENG

Ken Ono
Adviser

Department of Mathematics and Computer Science

Ken Ono
Adviser

David Zureick-Brown
Committee Member

John Duncan
Committee Member

Judy Raggi Moore
Committee Member

2016

THE COHEN-LENSTRA HEURISTICS AND SOUNDARARAJAN'S THESIS

YAN SHENG

Ken Ono
Adviser

An abstract of a thesis submitted to the Faculty of Emory College of Arts and Sciences of Emory University in partial fulfillment of the requirements of the degree of Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2016

THE COHEN-LENSTRA HEURISTICS AND SOUNDARARAJAN'S THESIS

YAN SHENG

Abstract. In this paper, we give an exposition of Kannan Soundararajan's Princeton Ph.D. thesis. His main theorem gives lower bounds on the number of torsion elements of the ideal class group $\mathrm{CL}(K)$ for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$. The proof relies on counting the number of square free d satisfying certain Diophantine conditions. These conditions are shown to be sufficient for the existence of elements of order g. Proofs of certain classical results from algebraic number theory, such as the finiteness of $\mathrm{CL}(K)$, are also included.

THE COHEN-LENSTRA HEURISTICS AND SOUNDARARAJAN'S THESIS

YAN SHENG

Ken Ono
Adviser

A thesis submitted to the Faculty of Emory College of Arts and Sciences of Emory University in partial fulfillment of the requirements of the degree of Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2016

Acknowledgments. I would like to thank Ken Ono for lending his expertise, guidance and support, and David Zureick-Brown for his encouragement to pursue this project.

Contents

1. Introduction and statement of results

The subject of algebraic number theory has two central goals: one is to develop an algebraic theory of numbers; that is, to understand their structure via equations and geometric intuition, and the other is to study the properties of algebraic numbers, objects arising from extensions of "ordinary" numbers to more general systems. Both interpretations will be discussed in this paper.

Let $L : K$ be a field extension. We say an element $\alpha \in L$ is *algebraic* over K if α is the root of some polynomial in $K[x]$. Furthermore, L is an *algebraic extension* if every $\alpha \in L$ is algebraic. L is said to be a *number field* if it is a field containing $\mathbb{Q}$ and is a finite dimensional $\mathbb{Q}$ vector space. Although many ideas from this area of study were first motivated by attempts to determine the extent to which the fundamental theorem of arithmetic prevailed in number fields - a question that was important to 19th century mathematicians' quest to resolve Fermat's Last Theorem - their relevance to our understanding of the integers remains crucial today. The primary goal of this paper is to give an exposition of open problems and recent results related to the class number of K. We begin with a definition:

Definition 1.1. Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Let $\mathcal{H}$ denote the set of all fractional ideals of K. Define the ***ideal class group*** of K, denoted $\mathrm{CL}(K)$, to be $\mathcal{H}/\sim$ where $A \sim B$ if there exist $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)A = (\beta)B$.

It is a well known fact that $\mathrm{CL}(K)$ is a finite abelian group; see Section 2 for a proof of finiteness. The order of this group is called the *class number*, denoted $h(K)$. For example, $h(\mathbb{Q}(i)) = h(\mathbb{Q}(\sqrt{-3})) = 1$ and $h(\mathbb{Q}(\sqrt{-5})) = 2$, so $\mathrm{CL}(\mathbb{Q}(i)) = \mathrm{CL}(\mathbb{Q}(\sqrt{-3})) = \{0\}$ and $\mathrm{CL}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Z}/2\mathbb{Z}$. See Examples 2.16 and 2.17 for details. For the remainder of this exposition, $d \neq 0$ is square free and $K = \mathbb{Q}(\sqrt{d})$ will denote a quadratic number field. K is called *imaginary* if $d < 0$ and *real* if $d > 0$. A famous problem of Gauss is to provide for every $h \geq 1$ a list of quadratic fields with class number $h(K) = h$. In 1952, K. Heegner [10] gave a proof, with some minor gaps, of a conjecture due to Gauss: the complete list of $d < 0$ for which $h(K) = 1$ is given by

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

H. Stark [6] was able to give a correct proof of this fact in 1967; during the same year, A. Baker [1] gave a completely different proof implying the same result. Since then, there has been extensive work in enumerating number fields by class number, for example see [2], [3] and [4]. For low class numbers - i.e. $h(K) \leq 100$, this problem has been solved for the case of imaginary quadratic fields, see [14]. However, Gauss conjectured that there are infinitely many *real* quadratic fields with class number one; this remains an open problem today.

Fundamentally, Gauss' class number problem is a question about the algebraic properties of number fields for certain values of $h(K)$. There are, however, other interesting questions that can be asked about the arithmetic properties of $h(K)$ itself. H. Cohen and H. W. Lenstra give an important conjecture in this direction.

Conjecture 1.2 (Cohen-Lenstra)**.** *Let p be an odd prime,*

(1) if K is an imaginary quadratic field, then the probability that $p|h(K)$ is

$$1 - \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right).$$

(2) if K is a real quadratic field, then the probability that $p|h(K)$ is

$$1 - \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{p^i}\right)}{1 - 1/p}.$$

A table giving some numerics associated with these conjectures is displayed. These values were computed using SAGE. In the notation below,

$$h_p^-(X) = \#\{d : p|h(K),\ d \leq X \text{ is square free},\ K = \mathbb{Q}(\sqrt{-d})\},$$

$$h_p^+(X) = \#\{d : p|h(K),\ d \leq X \text{ is square free},\ K = \mathbb{Q}(\sqrt{d})\},$$

$$\mathscr{D} = \#\{d : d \leq X \text{ is square free}\}.$$

X	$\frac{h_3^-(X)}{\mathscr{D}}$	$\frac{h_5^-(X)}{\mathscr{D}}$	$\frac{h_7^-(X)}{\mathscr{D}}$	$\frac{h_3^+(X)}{\mathscr{D}}$	$\frac{h_5^+(X)}{\mathscr{D}}$	$\frac{h_7^+(X)}{\mathscr{D}}$
500	.261	.179	.071	.049	.009	.000
1,000	.300	.189	.093	.057	.009	.001
10,000	.353	.207	.141	.091	.026	.009
50,000	.378	.222	.150	.108	.034	.014
C-L prediction	.439	.239	.163	.159	.049	.023

Following the notation in [11], let $\mathscr{N}_g(X)$ be the number of square free $d \leq X$ such that $\mathrm{CL}(K)$ contains an element of order g. Here $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary field. Due to Gauss' genus theory, if d has at least two odd prime factors, then $\mathrm{CL}(K)$ contains $\mathbb{Z}/2\mathbb{Z}$ as a subgroup. Since d is square free, if d has at least three prime factors, then $\mathrm{CL}(K)$ contains an element of order two, and there are no elements of order two when d is prime. Since "most" numbers have more than three prime factors, we expect almost all square free d to give rise to elements of order two in $\mathrm{CL}(K)$. The proportion of square free integers is given by

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2},$$

where $\zeta(s)$ is the Riemann zeta function. This implies $\mathscr{N}_2(X) \sim \frac{6X}{\pi^2}$. However, virtually nothing is known about Conjecture 1.2 beyond this. Namely, the behavior of $\mathscr{N}_g(X)$ for $g \geq 3$ is not well understood. H. Davenport and H. Heilbronn [5] showed that the proportion of d for which $3 \nmid h(K)$ is at least $1/2$. More precisely, for any $\epsilon > 0$ and sufficiently large $X > 0$,

$$\frac{\#\{0 < d < X : h(K) \not\equiv 0 \mod 3\}}{\#\{0 < d < X\}} \geq \frac{1}{2} - \epsilon.$$

An estimate for the case of primes $p > 3$ is given by the work of W. Kohnen and K. Ono [18], which says that for $\epsilon > 0$ and sufficiently large X,

$$\#\{0 < d < X : h(K) \not\equiv 0 \mod p\} \geq \left(\frac{2(p-2)}{\sqrt{3}(p-1)} - \epsilon\right) \frac{\sqrt{X}}{\log(X)}.$$

This result uses the theory of modular forms mod p, and is obtained by bounding the largest d that is a multiple of some prime $q \not\equiv \left(\frac{-4}{q}\right) \mod p$ for which $p \nmid h(K)$.

The main result to be explained in this paper is a theorem from K. Soundararajan's Ph.D. thesis at Princeton, which was published in the Journal of the London Mathematical Society in 2000 [11].

Theorem 1.3 (Soundararajan)**.** *For large X we have*

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

It should be noted that Theorem 1.3 includes cases when g is odd since $\mathscr{N}_g(X) \geq \mathscr{N}_{2g}(X)$. The proof of Theorem 1.3 depends on certain Diophantine conditions on

d that give rise to elements of order g in $\mathrm{CL}(K)$. Tools for counting the frequency with which such d occur are explained in this paper.

In Section 2, we present preliminary facts and definitions from algebraic number theory that are necessary to understand Theorem 1.3. Section 3 contains the Diophantine conditions mentioned above, as well as bounds on the number of admissible d satisfying these conditions. Together with some technical details, these estimates are enough to prove Theorem 1.3.

2. Preliminaries

In order to talk about the divisibility properties of $h(K)$, we state and prove the following theorem:

Theorem 2.1. *If K is a number field, then $h(K)$ is finite.*

We recall some necessary definitions and facts. An element α of a commutative ring R, with $1 \in R$, is said to be *integral* over a subring $A \subseteq R$ if α satisfies a monic polynomial over A. In our case, we are interested in the $\alpha \in \mathbb{C}$ that are integral over $\mathbb{Z}$, i.e. the *algebraic integers*. Let $\mathscr{A}$ denote the set of all such α. From the definition, one can show that $\alpha \in \mathscr{A}$ is equivalent to saying $\mathbb{Z}[\alpha]$ is finitely generated. Thus $\mathscr{A}$ is a ring since for any $\alpha, \beta \in \mathscr{A}$, all powers of $\alpha + \beta$ and $\alpha\beta$ can be expressed as integer linear combinations of $\alpha^i \beta^j$, which lie in $\mathbb{Z}[\alpha]\mathbb{Z}[\beta]$. Now for any number filed K, we can define the *integers of* K to be $\mathcal{O}_K := K \cap \mathscr{A}$. Since K is a field, it is clear that $\mathcal{O}_K$ is a ring.

Definitions 2.2. Let K be a number field of degree n over $\mathbb{Q}$, and $\mathcal{O}_K$ its ring of integers.

(1) Define the ***norm of an ideal*** $\mathfrak{a}$ to be $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$.

(2) If $\sigma_i : K \to \mathbb{C}$ are the n embeddings of K, define the ***norm of an element*** $\alpha \in K$ to be $N(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha)$.

(3) If $\{\theta_1, \ldots, \theta_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$ then define $\Delta[\theta_1, \ldots, \theta_n] := \det(A)^2$, where $A = (\sigma_i(\theta_j))$.

(4) The ***discriminant*** of K is defined as $d_K := \Delta[\alpha_1, \ldots, \alpha_n]$, where $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

Facts 2.3. Let $\mathcal{O}_K$ and $\{\theta_1, \ldots, \theta_n\}$ be as above, and $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then,

(1) $\mathfrak{a}$ contains a non-zero rational integer. That is, $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$.

(2) The norm of $\mathfrak{a}$ is finite.

(3) $\mathfrak{a}$ contains exactly one rational prime p.

(4) Let $\mathfrak{a} = (\alpha)$ be a principal ideal, then $N(\mathfrak{a}) = N(\alpha)$.

(5) If $\mathfrak{p}$ is a prime ideal, then $N(\mathfrak{p})$ is a power of a rational prime.

(6) $\Delta[\theta_1, \ldots, \theta_n] = N(\mathfrak{a})^2 d_K$.

(7) The norm of ideals is multiplicative. That is, if $\mathfrak{a}, \mathfrak{b}$ are two ideals, then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

(8) $\mathfrak{a}$ factors uniquely into prime ideals.

For proofs of these facts, see [13] and [7].

Lemma 2.4. *For any fixed $m \in \mathbb{Z}_{>0}$, there are finitely many ideals $\mathfrak{a}$ of $\mathcal{O}_K$ such that $N(\mathfrak{a}) \leq m$.*

Proof. By Facts 2.3 (5), (7) and (8) it is sufficient to prove that there are at most finitely many prime ideals $\mathfrak{p}$ with $N(\mathfrak{p}) \leq m$. By Fact 2.3 (3), we know any prime ideal $\mathfrak{p}$ contains a rational prime p, and so $(p) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$. Then, by taking norms we have

$$N((p)) = p^n = N(\mathfrak{p})^e \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i} \Rightarrow N(\mathfrak{p}) = p^t, \quad t \geq 1.$$

This fact implies there are at most finitely many choices for $\mathfrak{p}$, since $k \leq n-1$. $\square$

Thus in order to prove Theorem 2.1, we need only show that each ideal class contains an integral ideal of bounded norm. Then by Lemma 2.4 we are done. To do this, we will require a geometric result due to Minkowski.

Definitions 2.5. Consider the set $\Omega \subseteq \mathbb{R}^n$,

(1) Ω is *convex* if $\forall x, y \in \Omega$ we have $tx + (1-t)y \in \Omega$, $0 \leq t \leq 1$.

(2) Ω is *centrally symmetric* if $x \in \Omega \Rightarrow -x \in \Omega$.

(3) A *convex body* is a non-empty, bounded, centrally symmetric convex set.

As a problem of independent interest, we wish to count the number of non-trivial integral points in a convex body Ω. Methods for doing so will be useful for the proof of Theorem 2.1.

Fact 2.6. Let $\Omega \subseteq \mathbb{R}^n$ be bounded and Jordan measurable. For $c \in \mathbb{Z}_{>0}$, define

$$L(c) := \#\{P \in \Omega : cP \in \mathbb{Z}^n\}.$$

Then,

$$\lim_{c\to\infty} \frac{L(c)}{c^n} = \mathrm{Vol}(\Omega).$$

A proof of this fact can be found in [15]. The basic idea is that we can count the number of $\frac{1}{c}$-lattice points of Ω in the n-cube $I^n := [-1,1]^n$, with scaling if necessary, by dividing I^n into $(2c)^n$ subcubes and counting the subcubes that contain such points. Doing so as $c \to \infty$ will produce a sequence of Riemann sums for χ_Ω, which converges to $\mathrm{Vol}(\Omega)$ since Ω is Jordan measurable.

Lemma 2.7. *Let $\Omega \subseteq \mathbb{R}^n$ be a convex body with $\mathrm{Vol}(\Omega) := \int_\Omega \chi(x)dx > 2^n$. Then $\Omega \cap \mathbb{Z}^n \neq \{0\}$.*

Proof. Notice that by scaling, $\frac{1}{2}\Omega$ is also a convex body, with volume $\mathrm{Vol}\left(\frac{1}{2}\Omega\right) = \frac{1}{2^n}\mathrm{Vol}(\Omega) > 1$. Furthermore, Ω contains a non-trivial integral point if and only if there is a $0 \neq P \in \frac{1}{2}\Omega$ such that $2P \in \mathbb{Z}^n$. Thus it suffices to show that there are *distinct* $S', T' \in \Omega$ such that $S' - T' \in \mathbb{Z}^n$, and let $P := \frac{1}{2}S' - \frac{1}{2}T' \in \frac{1}{2}\Omega$.

Adopting the same notation as Fact 2.6, we have $\lim_{c\to\infty} \frac{L(c)}{c^n} = \mathrm{Vol}(\Omega) > 1$. This means that for sufficiently large c we have $L(c) > c^n = \#\left(\mathbb{Z}/c\mathbb{Z}\right)^n$. So by the pigeonhole principle there are $S = (s_1, \dots, s_n)$, $T = (t_1, \dots, t_n) \in \mathbb{Z}^n$, $S \neq T$, such that $s_i \equiv t_i \mod c$ for all $1 \leq i \leq n$ and $S' := \frac{1}{c}S$, $T' := \frac{1}{c}T \in \Omega$. It then follows that $0 \neq S' - T' \in \mathbb{Z}^n$ and by convexity $\frac{1}{2}S' - \frac{1}{2}T' = \frac{1}{2}(S' - T') \in \frac{1}{2}\Omega$. □

Remark 2.8. The proof of Lemma 2.7 was taken from notes on the Four Squares Theorem by Pete L. Clark [16]. The main idea is similar to that of Fact 2.6: we can scale Ω and count the $\frac{1}{c}$-lattice points.

The idea now is to show that every ideal $\mathfrak{a}$ can be realized as a convex body in $\mathbb{R}^n$ containing a non-trivial integral point. Recall for a degree n number field K, there are n embeddings $\sigma_i \colon K \to \mathbb{C}$. Some of these embeddings will be *real*, i.e. $\sigma_i(K) \subseteq \mathbb{R}$, while others will be *complex*, $\sigma_i(K) \subseteq \mathbb{C}$. If r_1, r_2 denote the number of real and complex embeddings, respectively, then $r_1 + 2r_2 = n$, since complex embeddings come in conjugate pairs. We will index the σ_i to be such that the real embeddings are written first. Define

$$\sigma\colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad \alpha \mapsto (\sigma_i(\alpha)), \quad 1 \le i \le n.$$

For computational purposes, we will make the identification $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$. That is, if

$$\begin{aligned} \sigma_s(\alpha) &= x_s & 1 \le s \le r_1, \\ \sigma_{r_1+j}(\alpha) &= y_j + iz_j & 1 \le j \le r_2, \end{aligned}$$

we write

$$\sigma(\alpha) = (x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}).$$

It is clear that σ maps $\mathbb{Q}$-linearly independent elements of K to $\mathbb{R}$-linear independent elements of $\mathbb{R}^n$. Thus, the image of an ideal $\mathfrak{a}$ with $\mathbb{Z}$-basis $\{\theta_1, \ldots, \theta_n\}$ under σ is a lattice with generators $\{\sigma(\theta_1), \ldots, \sigma(\theta_n)\}$.

Proposition 2.9. *The volume of a fundamental domain for $\sigma(\mathfrak{a})$ is $2^{-r_2} N(\mathfrak{a}) \sqrt{|d_K|}$.*

Proof. Let $\{\theta_1, \ldots, \theta_n\}$ be a $\mathbb{Z}$-basis for $\mathfrak{a}$. Then the volume of a fundamental domain for $\sigma(\mathfrak{a})$ is given by the absolute value of the determinant of the matrix V whose rows are $\sigma(\theta_i)$, $1 \le i \le n$. It is clear that $|\det(V)| = 2^{-r_2} \Delta[\theta_1, \ldots, \theta_n]^{1/2}$. Using the relation from Fact 2.3 (6) we have

$$\operatorname{Vol}(\sigma(\mathfrak{a})) = |\det(V)| = 2^{-r_2} N(\mathfrak{a}) \sqrt{|d_K|}.$$

□

Lemma 2.10 (Minkowski)**.** *Let Ω be a convex body, and $\lambda_1, \ldots, \lambda_n \in \mathbb{R}^n$ be $\mathbb{R}$-linearly independent vectors. If* $\operatorname{Vol}(\Omega) > 2^n |\det(A)|$, *then there exist* $0 \neq P =$

$(x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $\sum_{i=1}^n x_i\lambda_i \in \Omega$. Here, A denotes the matrix with λ_i as its row vectors.

Proof. Let $\Omega' = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : \sum_{i=1}^n x_i\lambda_i \in \Omega\}$. It is clear that $\Omega' = A^{-1}\Omega$ so Ω' is a convex body. Thus by Lemma 2.7, if $\mathrm{Vol}(\Omega') > 2^n$ then we have the desired point. By linear algebra,

$$\mathrm{Vol}(\Omega') > 2^n \iff \mathrm{Vol}(\Omega)|\det(A)|^{-1} > 2^n \iff \mathrm{Vol}(\Omega) > 2^n|\det(A)|.$$

□

Lemma 2.11 (Minkowski's bound)**.** *Let K be a number field of degree n over $\mathbb{Q}$ with discriminant d_K, and let r_1, r_2 denote the number of real and complex embeddings $\sigma_i \colon K \to \mathbb{C}$, respectively. Then every ideal class in $\mathrm{CL}(K)$ contains an integral ideal $\mathfrak{a}$ that is equivalent to another integral ideal $\mathfrak{b}$ such that*

$$N(\mathfrak{b}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|d_K|^{1/2}.$$

Proof. First we show the existence of $\mathfrak{a}$. Let $\mathcal{A} = \frac{\mathfrak{m}}{\mathfrak{n}}$ be a fractional ideal of $\mathcal{O}_K$. By Fact 2.3 (1), we know there is some $0 \neq t \in \mathfrak{n} \cap \mathbb{Z}$. Then, $(t) = \mathfrak{n}\mathfrak{l}$, for some integral ideal $\mathfrak{l}$. And so, $(t)\mathcal{A} = \mathfrak{n}\mathfrak{l}\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right) = \mathfrak{l}\mathfrak{m} = \mathfrak{a}$, say. Thus $\mathcal{A} \sim \mathfrak{a}$.

To complete the proof, we will need Lemma 2.10. Let

$$\Omega_t := \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{r_1}|x_i| + \sum_{j=r_1+1}^{r_1+2r_2-1} 2\sqrt{x_j^2 + x_{j+1}^2} < t\right\}.$$

It can be easily verified that Ω_t is a convex body and a straightforward calculation shows that $\mathrm{Vol}(\Omega_t) = \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!}$ (see Exercises 6.5.9 and 6.5.10 in [13]). Let V be the matrix constructed in the proof of Proposition 2.9. If t is chosen so that $\mathrm{Vol}(\Omega_t) > 2^n|\det(V)|$, then by Lemma 2.10 we know Ω_t contains $\sum_{i=1}^n x_i\sigma(\theta_i)$, where the $x_i \in \mathbb{Z}$ are not all zero. Writing $0 \neq \alpha = \sum_{i=1}^n x_i\theta_i \in \mathfrak{a}$, we have by the arithmetic mean-geometric mean inequality,

$$|N(\alpha)|^{1/n} = \left(\prod_{i=1}^n |\sigma_i(\alpha)|\right)^{1/n} \leq \frac{\sum_{i=1}^n |\sigma_i(\alpha)|}{n} < \frac{t}{n} \Rightarrow |N(\alpha)| < \frac{t^n}{n^n}. \tag{2.12}$$

By Proposition 2.9 and the above remarks we have,

$$\frac{t^n}{n!} > \frac{2^n|\det(V)|}{2^{r_1-r_2}\pi^{r_2}} = \left(\frac{4}{\pi}\right)^{r_2} N(\mathfrak{a})\sqrt{|d_K|}.$$

Combining this with Equation (2.12) we have shown

$$|N(\alpha)| < \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} N(\mathfrak{a})\sqrt{|d_K|}.$$

Since $\alpha \in \mathfrak{a}$, $(\alpha) = \mathfrak{a}\mathfrak{b}$ for some integral ideal $\mathfrak{b}$, and so by Facts 2.3 (4) and (7) we are done. $\square$

With Lemmas 2.4 and 2.11, Theorem 2.1 is proved.

Remark 2.13. Lemma 2.11 is very useful in computing $h(K)$ because, as we will see below, it means that $\mathrm{CL}(K)$ is generated by the prime ideals in $\mathcal{O}_K$ with norm less than Minkowski's bound M_K. Furthermore, if $M_K < 2$, then $\mathrm{CL}(K)$ is trivial and $h(K) = 1$. For real quadratic fields, $r_1 = 2$ and $r_2 = 0$ so if $|d_K| < 16$ then $h(K) = 1$. Similarly, for imaginary quadratic fields, if $|d_K| < \pi^2$ then $h(K) = 1$.

To utilize Minkowski's bound, we need to compute d_K, which requires an integral basis. In practice, it is often not easy to compute an integral basis for an arbitrary number field K. However, in the quadratic case there is a nice description:

Fact 2.14. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 0$ is square free. An integral basis $\{1, \theta\}$ for K can be classified as follows,

$$\theta = \begin{cases} \sqrt{d} & d \not\equiv 1 \mod 4, \\ \frac{1}{2}(1+\sqrt{d}) & d \equiv 1 \mod 4. \end{cases}$$

A general method for computing an integral basis of higher degree extensions can be found in [8].

For a given prime $p \in \mathbb{Z}$, it is often useful to be able to determine if, and how, (p) factors in $\mathcal{O}_K$. The next theorem gives a method for doing so under special conditions.

Theorem 2.15. *Let $p \in \mathbb{Z}$ be prime and $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$. If $f(x)$ is the minimal polynomial of θ, and*

$$f(x) \equiv \prod_{i=1}^{k} f_i(x)^{e_i} \mod p,$$

with f_i irreducible in $\mathbb{F}_p[x]$, then (p) factors as

$$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i},$$

where $\mathfrak{p}_i = (p, f_i(\theta))$ are prime ideals and $N(\mathfrak{p}_i) = p^{\deg f_i}$.

A proof of Theorem 2.15 can be found in [13].

Let $\mathfrak{a}$ be an integral representative of an ideal class such that $N(\mathfrak{a}) \leq M_K$. By unique factorization, $\mathfrak{a}$ can be written uniquely as $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, with each $\mathfrak{p}_i$ a prime ideal. So by Lemma 2.11 we have

$$\prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i} = N(\mathfrak{a}) \leq M_K,$$

and so $N(\mathfrak{p}_i) \leq M_K$ for all $1 \leq i \leq k$. By Fact 2.3 (5) $N(\mathfrak{p}_i)$ is a power of some prime p, which means $p \leq M_K$. Thus, to compute $\mathrm{CL}(K)$ we need only find the prime ideals of $\mathcal{O}_K$ lying above primes $p \leq M_K$.

Example 2.16. We compute the class number of $K = \mathbb{Q}(\sqrt{-5})$. By Fact 2.14, $\{1, \sqrt{-5}\}$ is an integral basis for K and so $d_K = -20$, $M_K = \frac{2}{\pi}\sqrt{20} < 2.85$. The only prime below M_K is 2, so by the above comments we need to determine if (2) is prime in $\mathcal{O}_K$. Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, we can use Theorem 2.15 to determine that $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. By taking norms, we see that neither of these prime factors are principal. Thus, any representative $\mathfrak{a}$ of an ideal class in $\mathrm{CL}(K)$ is either equivalent to a principal ideal or to $(2, 1 + \sqrt{-5})$, and so $h(K) = 2$.

Example 2.17. Consider $K = \mathbb{Q}(\sqrt{d})$. For $d = -1, -2, -3, -7$, we have $M_K < 2$ and so $h(K) = 1$.

(1) $d = -11$: $M_K < 2.12$ and following the notation of Theorem 2.15,

$$f(x) = x^2 - x + 3 \equiv x^2 - x + 1 \mod 2,$$

which is irreducible in $\mathbb{F}_2[x]$ so (2) remains prime in $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. Thus, $h(K) = 1$.

(2) $d = -19$: This case is identical to $d = -11$ since $M_K < 2.78$ and the minimal polynomial of $\theta = \frac{1+\sqrt{-19}}{2}$ is $f(x) = x^2 - x + 5$, which is irreducible in $\mathbb{F}_2[x]$.

(3) $d = -43$: $M_K < 4.18$ so we must check primes $p = 2, 3$. The minimal polynomial is $f(x) = x^2 - x + 11$ which is irreducible in $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$ by checking the possible roots, so once again $h(K) = 1$.

(4) $d = -63$: $M_K < 5.21$ and the list of primes to check are $p = 2, 3, 5$. We have $f(x) = x^2 - x + 17$, which is irreducible in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$ and $\mathbb{F}_5[x]$.

(5) $d = -163$: $M_K < 8.13$. The minimal polynomial $f(x) = x^2 - x + 41$ is irreducible in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$ and $\mathbb{F}_7[x]$.

We have thus checked that the list of $d < 0$ for which $\mathbb{Q}(\sqrt{d})$ has class number one given in the introduction is indeed accurate. However, the problem of showing these are the *only* admissible $d < 0$ is much more difficult.

2.1. **Elementary Diophantine conditions.**

Example 2.18. Let $g > 1$ be an integer. If $n > 1$ is odd and $n^g - 1 = d$ is square free, then $\mathrm{CL}(K)$ contains an element of order g.

Proof. Since $d \equiv 2 \mod 4$, by Fact 2.14 we know $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. So we have the ideal factorization

$$(n^g) = (n)^g = (1 + \sqrt{-d})(1 - \sqrt{-d}).$$

If $(1+\sqrt{-d})$ and $(1-\sqrt{-d})$ are not co-prime then $2 \in (n^g)$ which is a contradiction since n is odd. Therefore

$$(1 + \sqrt{-d}) = \mathfrak{a}^g$$

$$(1 - \sqrt{-d}) = \mathfrak{b}^g,$$

for some ideals $\mathfrak{a}, \mathfrak{b}$. Hence $\mathfrak{a}$ has order dividing g in $\mathrm{CL}(K)$. Now suppose $\mathfrak{a}^m = (u + v\sqrt{-d})$. If $v = 0$ then $\mathfrak{a}^m = (u)$, which implies $\mathfrak{b}^m = (u)$ by the relation $\mathfrak{a}\mathfrak{b} = (n)$. But this means $\gcd(\mathfrak{a}^m, \mathfrak{b}^m) \neq 1$, a contradiction. Now if we take norms, we get

$$n^m = u^2 + dv^2 \geq d = n^g - 1.$$

Since $n^{g-1} \geq n^g - 1 \iff 1 \geq n^{g-1}(n-1) > 2$ we see that m cannot be less than g. Thus $\mathfrak{a}$ must have order g in $\mathrm{CL}(K)$. $\square$

Example 2.19. Let $g > 1$ be odd. If $d = 3^g - x^2$ is square free with x odd and satisfying $x^2 < 3^g/2$, then $\mathrm{CL}(K)$ has an element of order g.

Proof. It is clear that $d \equiv 2 \mod 4$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. The ideals $(x + \sqrt{-d})$ and $(x - \sqrt{-d})$ are co-prime, so 3 splits in $\mathcal{O}_K$, meaning we have

$$(3) = \mathfrak{p}_1 \mathfrak{p}_2.$$

And so, $(x + \sqrt{-d}) = \mathfrak{p}_1^g$. If $\mathfrak{p}_1^m = (u + v\sqrt{-d})$, for some $m|g$, then $3^m = u^2 + dv^2$. If $v \neq 0$, then $3^m \geq d > 3^g/2$, which is a contradiction for all $m \leq g-1$. But if $v = 0$, then $3^m = u^2$, which is another contradiction since m is odd. So it must be that $m = g$. $\square$

Example 2.20. Let g be odd and N denote the number of square free integers of the form $3^g - x^2$, where $0 < x^2 < 3^g/2$ and x is odd. For g sufficiently large, we have $N \gg 3^{g/2}$, and thus there are infinitely many imaginary quadratic fields K for which $g|h(K)$.

Proof. For a fixed g, the number of integers of the form $3^g - x^2$, where $0 < x^2 < 3^g/2$ and x is odd is $\frac{1}{2\sqrt{2}} 3^{g/2} + O(1)$. We now remove any numbers that are divisible by the square of a prime. Since g is odd, we know $4 \nmid 3^g - x^2$ as otherwise $x^2 \equiv -1 \mod 4$ has a solution. If x is a multiple of three, then $9|3^g - x^2$, so we remove $\frac{1}{6\sqrt{2}} 3^{g/2} + O(1)$ of such numbers. If $p > 3$ is prime, then the number of $3^g - x^2$

divisible by p^2 is at most $\frac{1}{p^2\sqrt{2}}3^{g/2} + O(1)$, so we have

$$N \geq \frac{3^{g/2}}{\sqrt{2}} \left(\frac{1}{2} - \frac{1}{6} - \sum_{\substack{p^2 < 3^g \\ p \geq 5}} \frac{1}{p^2} \right) + O\left(\frac{3^{g/2}}{g} \right).$$

The error term is an upper bound for $\pi(3^{g/2})$, where $\pi(x)$ is the usual prime counting function (see problem 1.1.26 in [13]). Since

$$\begin{aligned} \sum_{p \geq 5} \frac{1}{p^2} \leq \sum_{n=5}^{\infty} \frac{1}{n(n-1)} &= \left(\frac{1}{4} - \frac{1}{5} \right) + \left(\frac{1}{5} - \frac{1}{6} \right) + \cdots \\ &= \frac{1}{4}, \end{aligned}$$

we obtain $N \gg 3^{g/2}$. By Example 2.19, each integer counted in N gives rise to a quadratic field K for which $g|h(K)$. Applying the same argument to powers of g, we deduce that there are infinitely many imaginary quadratic fields K whose class number is divisible by g. □

Examples 2.18, 2.19 and 2.20 were taken from Chapter 6 of [13]. These are simple illustrations of how solutions to Diophantine equations can guarantee the existence of torsion subgroups of $\mathrm{CL}(K)$. A sophisticated amplification of these ideas is the basis for Theorem 1.3.

3. Proof of Theorem 1.3

To begin the proof of Theorem 1.3, we state a Diophantine condition analogous to Example 2.18.

Proposition 3.1. *Let $g_1 \geq 3$ be an integer and suppose $d \geq 63$ is a square free integer such that $m^{g_1} - n^2 = t^2 d$, where $t, m, n \in \mathbb{Z}_{>0}$, $(m, 2n) = 1$ and $m^{g_1} < (d+1)^2$. Then $\mathrm{CL}(K)$ contains an element of order g_1.*

Proof. We have the ideal factorization

$$(m^{g_1}) = (m)^{g_1} = (n + t\sqrt{-d})(n - t\sqrt{-d}).$$

Let $\mathfrak{d} = \gcd((n+t\sqrt{-d}), (n-t\sqrt{-d})) = (n+t\sqrt{-d})+(n-t\sqrt{-d})$. Then $2n, m^{g_1} \in \mathfrak{d}$, but since $(m^{g_1}, 2n) = 1$ we have $\mathfrak{d} = \mathcal{O}_K$. Thus the ideals on the right hand side are co-prime, and are each g_1-th powers.

Let $\mathfrak{a}^{g_1} = (n + t\sqrt{-d})$. If $\mathfrak{a}^r = (u + v\sqrt{-d})$, for some $u, v \in \mathbb{Z}$ or $\frac{1}{2} + \mathbb{Z}$, and r strictly divides g_1 then $r \leq \frac{g_1}{2} \Rightarrow \frac{g_1}{r} \geq 2$. Now, $(n + t\sqrt{-d}) = (\mathfrak{a}^r)^{g_1/r} = (u+v\sqrt{-d})^{g_1/r}$ so $n+t\sqrt{-d} = \pm(u+v\sqrt{-d})^{g_1/r}$, as the units in $\mathcal{O}_K$ are ± 1. Note that u and v are non-zero since n and t are not. If $\frac{g_1}{r} = 2$, then $t = 2uv$ which means both $u, v \in \mathbb{Z}$ so $|u|, |v| \geq 1$. Otherwise, $|u|, |v| \geq \frac{1}{2}$. Taking norms we obtain

$$m^{g_1} = n^2 + dt^2 = (u^2 + dv^2)^{g_1/r} \geq \begin{cases} (d+1)^2 & \text{if} \quad \frac{g_1}{r} = 2, \\ \\ \left(\frac{d+1}{4}\right)^3 & \text{if} \quad \frac{g_1}{r} > 2. \end{cases}$$

In both cases we have a contradiction of our assumption that $m^{g_1} < (d+1)^2$, since if $d \geq 63$, then $(d+1)^2 \leq \left(\frac{d+1}{4}\right)^3$. Thus, $\mathfrak{a}$ must have order g_1 in $\mathrm{CL}(K)$. $\square$

Remark 3.2. By Gauss' genus theory and the above proposition, if d has at least two odd prime factors and g_1 is odd then $\mathrm{CL}(K)$ will contain an element of order $g = 2g_1$.

The next proposition gives a condition for the existence of even order elements.

Proposition 3.3. *If $g_1 \geq 2$ is an even integer, and $d = 2m^{g_1/2} - t^2$ is square free, where $(m, 2t) = 1$ and $m^{g_1/2} < (d+1)$, then $\mathrm{CL}(K)$ contains an element of order g_1.*

Proof. Apply Proposition 3.1 with $n = m^{g_1/2} - t^2$. □

3.1. **Outline of ideas.** Now that we have sufficient conditions to determine when a square free d gives rise to elements of order g_1, we define $g := 2g_1$ and count the frequency with which the admissible d occur. We apply Proposition 3.3, when g_1 is even, and Proposition 3.1, when g_1 is odd. It is clear that the different cases of Theorem 1.3 correspond to the parity of g_1.

For even g_1, let $\mathscr{S}_{e,g}(X)$ denote the number of square free $d \leq X$ with at least one solution in m and t to

$$d = 2m^{g_1} - t^2 \quad \text{where } 0 < m < d^{1/g_1},\ 0 < t \text{ and } m \text{ is odd.} \tag{3.4}$$

By Proposition 3.3, we have $\mathscr{N}_g(X) \geq \mathscr{S}_{e,g}(X)$. If $\mathscr{R}_e(d)$ denotes the number of solutions to (3.4) for some fixed square free $d \leq X$, then we expect

$$\sum_{d \leq X} \mathscr{R}_e(d) \gg X^{1/2+1/g_1}, \tag{3.5}$$

since roughly speaking, m takes values at most X^{1/g_1} and $t \leq X^{1/2}$.

It should be noted that the special case of $g = 2g_1 = 2$ is missed by this approach. However, the below proposition gives a concise description of this scenario.

Proposition 3.6. *Let d be an odd square free integer and let $\mathscr{R}_2(d)$ denote the number of solutions to (3.4) with $g_1 = 2$. Then $\mathscr{R}_2(d) = 0$ unless $d \equiv 1 \mod 8$ is composed entirely of primes congruent to $\pm 1 \mod 8$. In this case, $\mathscr{R}_2(d) = \tau(d)/2$ and $\mathrm{CL}(K)$ has at least $\tau(d)$ elements of order 4, where $\tau(n)$ is the divisor counting function. This gives $\mathscr{N}_4(X) \gg X/\sqrt{\log(X)}$.*

Proof. For $g_1 = 2$, we wish to count the number of representations of d by quadratic forms of discriminant 8. There are exactly two classes of such forms; namely $\pm(2x^2-$

y^2). Hence, by a classical result (see Sections 11.4 and 12.4 of [12]), the number of solutions to $\pm d = 2x^2 - y^2$ with $0 < x < \sqrt{d}$ and $0 < y$ is given by

$$\sum_{l|d} \left(\frac{8}{l}\right) = \begin{cases} \tau(d) & \text{if } p|d \Rightarrow p \equiv \pm 1 \mod 8 \\ \\ 0 & \text{otherwise.} \end{cases}$$

If $d = 2x^2 - y^2$ then $-d = 2(x-y)^2 - (2x-y)^2$, so $\mathscr{R}_2(d)$ is either $\tau(d)/2$ or 0 depending on the prime factorization of d. The condition $d = 2x^2 - y^2 \equiv \pm 1 \mod 8$ corresponds to odd and even x, respectively. To show that $\mathrm{CL}(K)$ has at least $\tau(d)$ elements of order four, we note that by Proposition 3.1 each solution to $d = 2m^2 - t^2$ produces *two* elements of order four (counting inverses). Thus it is sufficient to show that distinct solutions counted in $\mathscr{R}_2(d)$ produce distinct order four elements in $\mathrm{CL}(K)$. Let (m,t) and (u,v) be two such solutions, and $\mathfrak{a}$, $\mathfrak{b}$ be the corresponding elements of order four in $\mathrm{CL}(K)$. Substituting $n_1 = m^2 - t^2$, $n_2 = u^2 - v^2$ in the proof of Proposition 3.1, we have

$$\mathfrak{a}^4 = (m^2 - t^2 + t\sqrt{-d}),$$

$$\mathfrak{b}^4 = (u^2 - v^2 + v\sqrt{-d}).$$

To reach a contradiction, we suppose $\mathfrak{a} \sim \mathfrak{b}$. Then $\mathfrak{a}\mathfrak{b}^{-1} = (a + b\sqrt{-d})$ is a principal ideal. Taking norms, we have $d > mu = N(\mathfrak{a}\mathfrak{b}^{-1}) = a^2 + b^2 d$, so $b = 0$. Therefore

$$(a)^4 = (\mathfrak{a}\mathfrak{b}^{-1})^4 = (m^2 - t^2 + t\sqrt{-d})(u^2 - v^2 - v\sqrt{-d}).$$

Comparing the $\sqrt{-d}$ term on both sides, we have $t(u^2 - v^2) = v(m^2 - t^2)$. Since d is square free, it must be the case that $\gcd(m,t) = \gcd(u,v) = 1$ which implies $t = v$ and $m = u$. This contradicts our assumption that (m,t) and (u,v) are distinct.

The above arguments show that $\mathscr{N}_4(X)$ exceeds the number of square free $d \equiv 1 \mod 8$, where $d \leq X$, that are composed entirely of primes $p \equiv \pm 1 \mod 8$. An application of Theorem 2.10 in [9] shows that there are $\gg X/\sqrt{\log(X)}$ such d. $\square$

As a consequence of this proposition, we have $\mathscr{R}_e(d) \leq \tau(d)/2 \ll d^{\epsilon}$, and so $\mathscr{S}_{e,g}(X) = \sum_{\substack{d \leq X \\ \mathscr{R}_e(d) \neq 0}} 1$ is not too different from $\sum_{d \leq X} \mathscr{R}_e(d)$. Along with Equation (3.5), this implies the case of $g \equiv 0 \mod 4$ in Theorem 1.3.

For odd g_1, we define $T = X^{(g_1-2)/(g_1+1)}$, $M = T^{2/g_1} X^{1/g_1}/2$, and $N = T\sqrt{X}/2^{g_1+1}$. These are parameters to be optimized later in the counting arguments to produce the bounds in Theorem 1.3. Denote by $\mathscr{S}_{o,g}(X)$ the number of square free $d \leq X$ with at least one solution to

$$m^{g_1} - n^2 = t^2 d,\ (m, nt) = (t, 6) = 1,\ m \equiv 1 \bmod 18,\ n \equiv 2 \bmod 18, \tag{3.7}$$

where $T \leq t \leq 2T$, $M \leq m \leq 2M$, $N \leq n \leq 2N$. With a straight forward calculation to show $m^{g_1} \leq (d+1)^2$, we can apply Proposition 3.1 to conclude that $\mathrm{CL}(K)$ has an element of order g_1 for each d counted in $\mathscr{S}_{o,g}(X)$. Since $m^{g_1} \equiv n^2 \equiv 1 \mod 3$ and $(t, 3) = 1$, we know $3|d$. And since d is square free and large, we know d has at least two odd prime factors, which implies $\mathscr{N}_g(X) \geq \mathscr{S}_{o,g}(X)$. Finally, by a counting argument involving quadratic residues, we obtain a bound analogous to Equation (3.5) for the case of odd g_1, which implies the $g \equiv 2 \mod 4$ case of Theorem 1.3.

3.2. **Counting arguments.** The subsequent discussion makes use of *Dirichlet characters*, which are arithmetic functions arising from completely multiplicative characters on $(\mathbb{Z}/k\mathbb{Z})^{\times}$. The relevant background on periodic arithmetic functions and their Fourier expansions can be found in [17].

Lemma 3.8 (Pólya-Vinogradov inequality)**.** *If* χ *is any primitive character* mod k *then for all* $x \geq 1$ *we have*

$$\left| \sum_{m \leq x} \chi(m) \right| < \sqrt{k} \log(k).$$

Proof. Since $\chi(m)$ is periodic $\mod k$ and primitive, it has the finite Fourier expansion

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \bar{\chi}(n) e^{-2\pi i m n/k}.$$

Summing over m we have

$$\sum_{m \leq x} \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k-1} \bar{\chi}(n) \sum_{m \leq x} e^{-2\pi i m n/k}, \tag{3.9}$$

since $\chi(k) = 0$. Define the function

$$f(n) = \sum_{m \leq x} e^{-2\pi i m n/k}.$$

It is true that

$$f(k-n) = \sum_{m \leq x} e^{-2\pi i m(k-n)/k} = \sum_{m \leq x} e^{2\pi i m n/k} = \overline{f(n)}.$$

This shows $|f(k-n)| = |f(n)|$, so taking absolute values in Equation (3.9) and multiplying by $\sqrt{k}$ we obtain

$$\sqrt{k} \left| \sum_{m \leq x} \chi(m) \right| \leq \sum_{n=1}^{k-1} \left| \sum_{m \leq x} e^{-2\pi i m n/k} \right| = \sum_{n=1}^{k-1} |f(n)| = 2 \sum_{n \leq k/2} |f(n)|. \tag{3.10}$$

Writing $y = e^{-2\pi i n/k}$, and $z = e^{-\pi i n/k}$ we see that $y = z^2 \neq 1$ since $1 \leq n \leq k-1$. Furthermore, we have that $f(n) = \sum_{m=1}^{r} y^m$ is a geometric series in y so we can write

$$f(n) = y \frac{y^r - 1}{y - 1} = z^2 \frac{z^{2r} - 1}{z^2 - 1} = z^{r+1} \frac{z^r - z^{-r}}{z - z^{-1}},$$

where $r = \lfloor x \rfloor$. Again, taking absolute values we have

$$|f(n)| = \left| \frac{z^r - z^{-r}}{z - z^{-1}} \right| = \frac{\left|\sin(\frac{\pi r n}{k})\right|}{\left|\sin(\frac{\pi n}{k})\right|} \le \frac{1}{\sin(\frac{\pi n}{k})}.$$

Notice that in the interval $0 \le t \le \pi/2$, we have $\sin(t) \ge 2t/\pi$ and in the last sum in Equation (3.10), $n \le k/2$, which means $t = \pi n/k \le \pi/2$. So substituting t for $\pi n/k$, we see that

$$|f(n)| \le \frac{1}{\frac{2}{\pi}\frac{\pi n}{k}} = \frac{k}{2n}.$$

Finally, applying this to Equation (3.10) we get

$$\sqrt{k}\left|\sum_{m \le x} \chi(m)\right| \le k \sum_{n \le k/2} \frac{1}{n} < k\log(k),$$

which completes the proof. □

Lemma 3.11. *Let $t \in \mathbb{Z}$ be such that $(t, 6) = 1$, and $d > 1$ be a square free divisor of t. Then*

$$\sum_{\substack{M \le m \le 2M \\ m \equiv 1 \bmod 18 \\ (m,t)=1}} \left(\frac{m}{d}\right) \ll \tau(t)\sqrt{d}\log(d). \tag{3.12}$$

Additionally, for any odd m that is not a square and $R \ge 2$,

$$\sum_{\substack{r \le R \\ (r,6m)=1}} \mu(r)^2 \left(\frac{m}{r}\right) \ll R^{1/2} m^{1/4} \sqrt{\log(m)}. \tag{3.13}$$

Proof. Let χ be a character mod 18. We have

$$\begin{aligned}
\sum_{\substack{M \le m \le 2M \\ m \equiv 1 \bmod 18 \\ (m,t)=1}} \left(\frac{m}{d}\right) &= \frac{1}{\varphi(18)} \sum_{\chi \bmod 18} \sum_{\substack{M \le m \le 2M \\ (m,t)=1}} \chi(m)\left(\frac{m}{d}\right) \\
&= \frac{1}{\varphi(18)} \sum_{\chi \bmod 18} \sum_{M \le m \le 2M} \sum_{l \mid (t,m)} \mu(l)\chi(m)\left(\frac{m}{d}\right) \\
&\le \frac{1}{\varphi(18)} \sum_{\chi \bmod 18} \sum_{l \mid t} \left| \sum_{M/l \le s \le 2M/l} \chi(s)\left(\frac{s}{d}\right) \right|,
\end{aligned}$$

where we write $m = ls$ in the last line. Since $\chi(s)\left(\frac{s}{d}\right)$ is a non-principal character with conductor at most $18d$, by the Pólya-Vinogradov inequality, the above sum in s is $\ll \sqrt{d}\log(d)$, which implies Equation (3.12).

Next, note that

$$\sum_{\substack{r\le R\\(r,6m)=1}} \mu(r)^2\left(\frac{m}{r}\right) = \sum_{r\le R}\mu(r)^2\left(\frac{36m}{r}\right) = \sum_{r\le R}\sum_{l^2|r}\mu(l)\left(\frac{36m}{r}\right)$$
$$\le \sum_{l\le\sqrt{R}}\left|\sum_{s\le R/l^2}\left(\frac{36m}{s}\right)\right|,$$

where we write $r = sl^2$ in the last line. Again, by the Pólya-Vinogradov inequality, the above sum over s is $\ll \sqrt{m}\log(m)$. Thus

$$\sum_{\substack{r\le R\\(r,6m)=1}} \mu(r)^2\left(\frac{m}{r}\right) \ll \sum_{l\le\sqrt{R}} \min\left(\frac{R}{l^2}, \sqrt{m}\log(m)\right) \ll R^{1/2}m^{1/4}\sqrt{\log(m)},$$

since $\left|\sum_{s\le R/l^2}\left(\frac{36m}{s}\right)\right| \le R/l^2$ trivially. This proves Equation (3.13). $\square$

Lemma 3.14. *Let*

$$\rho_m(l) = \#\{n \mod l : n^2 \equiv m^{g_1} \mod l\},$$

and t be as in Lemma 3.11, then

$$\sum_{\substack{M\le m\le 2M\\ m\equiv 1 \mod 18}}\sum_{\substack{T\le t\le 2T\\(t,6m)=1}} \rho_m(t^2) = \sum_{\substack{M\le m\le 2M\\ m\equiv 1 \mod 18}}\sum_{\substack{T\le t\le 2T\\(t,6m)=1}} 1 + O(TM^{5/8}\log(X)^3) \asymp MT.$$

Proof. Note that $\rho_m(l)$ is a multiplicative function in l, so for a prime $p \nmid 2m$ and odd g_1 we have

$$\rho_m(p^\alpha) = \rho_m(p) = 1 + \left(\frac{m^{g_1}}{p}\right) = 1 + \left(\frac{m}{p}\right), \tag{3.15}$$

for all $\alpha \geq 1$. Note that the first equality follows from Hensel's lemma. If we write $t = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then since t is odd,

$$\rho_m(t^2) = \prod_i \rho_m(p_i^{2\alpha_i}) = \prod_i \left(1 + \left(\frac{m}{p_i}\right)\right) = \sum_{d|t} \mu(d)^2 \left(\frac{m}{d}\right).$$

The $d = 1$ term contributes the main term

$$\sum_{\substack{M \leq m \leq 2M \\ m \equiv 1 \bmod 18}} \sum_{\substack{T \leq t \leq 2T \\ (t,6m)=1}} 1 = \sum_{\substack{M \leq m \leq 2M \\ m \equiv 1 \bmod 18}} \left(T\frac{\varphi(6m)}{6m} + O(\tau(6m))\right)$$

$$\asymp MT + O((M+T)\log(M)).$$

It remains to show that the contribution by $\sum_{d|t,\ d>1} \mu(d)^2 \left(\frac{m}{d}\right)$ is negligible. Let D be a parameter to be fixed later, we will split the divisors d of t into two regions, $1 \leq d \leq D$ and $d > D$. Define

$$S_1 := \sum_{\substack{M \leq m \leq 2M \\ m \equiv 1 \bmod 18}} \sum_{\substack{T \leq t \leq 2T \\ (t,6m)=1}} \sum_{\substack{d|t \\ 1 \leq d \leq D}} \mu(d)^2 \left(\frac{m}{d}\right),$$

$$S_2 := \sum_{\substack{M \leq m \leq 2M \\ m \equiv 1 \bmod 18}} \sum_{\substack{T \leq t \leq 2T \\ (t,6m)=1}} \sum_{\substack{d|t \\ d \leq t/D}} \mu(t/d)^2 \left(\frac{m}{t/d}\right).$$

The contribution we want to bound is $S_1 + S_2$. Expanding S_1 over the sum in m we have

$$S_1 = \sum_{\substack{T \leq t \leq 2T \\ (t,6)=1}} \sum_{\substack{d|t \\ 1 \leq d \leq D}} \mu(d)^2 \sum_{\substack{M \leq m \leq 2M \\ m \equiv 1 \bmod 18 \\ (m,t)=1}} \left(\frac{m}{d}\right),$$

so if we apply Equation (3.12) we obtain

$$S_1 \ll \sqrt{D}\log(D) \sum_{T \leq t \leq 2T} \tau(t)^2 \leq T\sqrt{D}\log(X)^4.$$

Now we estimate

$$S_2 = \sum_{\substack{M \le m \le 2M \\ m \equiv 1 \mod 18}} \sum_{\substack{d \le 2T/D \\ (d,6m)=1}} \sum_{\substack{\max(T/d,D) \le r \le 2T/d \\ (r,6m)=1}} \mu(r)^2 \left(\frac{m}{r}\right),$$

where we write $t = dr$. Using (3.13) we have

$$\begin{aligned} S_2 &\ll \sum_{\substack{M \le m \le 2M \\ m \ne \square}} \sum_{d \le 2T/D} \left(\frac{T}{d}\right)^{1/2} M^{1/4} \sqrt{\log(X)} + \sum_{\substack{M \le m \le 2M \\ m = \square}} \sum_{d \le 2T/D} \frac{T}{d} \\ &\ll \frac{TM^{5/4}}{\sqrt{D}} \sqrt{\log(X)} + T\sqrt{M} \log(X). \end{aligned}$$

Now if we fix $D = M^{5/4}/(\log(X))^{7/2}$ we have $S_1, S_2 \ll TM^{5/8}(\log(X))^3$, and we're done. $\square$

Proposition 3.16. *For a fixed square free $d \le X$, let $\mathscr{R}_o(d)$ denote the number of solutions to (3.7). Then*

$$\begin{aligned} \sum_{d \le X} \mathscr{R}_o(d) &\asymp \frac{MN}{T} + o(MT^{2/3}X^{1/3}) \\ &\asymp X^{1/2+1/g_1} T^{2/g_1} + o(X^{1/3+1/g_1} T^{2/3+2/g_1}). \end{aligned} \tag{3.17}$$

Proof. We adopt the following notation: N_1 is the number of of (m,n,t) satisfying Equation (3.7) such that $p^2 \nmid (m^{g_1} - n^2)/t^2 = d$ for all primes $p \le \log(X)$; N_2 is the number of (m,n,t) such that $p^2 | d$ for some prime $\log(X) < p \le Z := X^{1/3}T^{-1/3}(\log(X))^{2/3}$; N_3 is the number of (m,n,t) with $p^2 | d$ for some prime $p > Z$. The goal is to show

$$\begin{aligned} N_1 &\asymp \frac{MN}{T} + o(MT^{2/3}X^{1/3}), \\ N_2 &\ll \frac{MN}{T\log(X)} + o(MT^{2/3}X^{1/3}), \\ N_3 &= o(MT^{2/3}X^{1/3}). \end{aligned}$$

The congruence conditions on m and n from (3.7) imply that $4, 9 \nmid (m^{g_1} - n^2)/t^2$. Let $P := \prod_{5 \le p \le \log(X)} p$. For some fixed $M \le m \le 2M$ and $T \le t \le 2T$, with $m \equiv 1 \mod 18$ and $(t, 6m) = 1$, we now count the number of $N \le n \le 2N$ producing tuples (m, n, t) counted by N_1:

$$\sum_{\substack{N \le n \le 2N,\, (n,m)=1 \\ n \equiv 2 \mod 18 \\ n^2 \equiv m^{g_1} \mod t^2}} \sum_{l^2 | ((m^{g_1} - n^2)/t^2, P^2)} \mu(l) = \sum_{\substack{l | P \\ (l,m)=1}} \mu(l) \sum_{\substack{N \le n \le 2N \\ n \equiv 2 \mod 18 \\ n^2 \equiv m^{g_1} \mod l^2 t^2}} 1.$$

If we split the above sum in n into intervals of length $18 l^2 t^2$, we see that it is $N \rho_m(l^2 t^2)/(18 l^2 t^2) + O(\rho_m(l^2 t^2)) = N\rho_m(l^2t^2)/(18l^2t^2) + O(X^\epsilon)$, since $\rho_m(l^2t^2) \le \tau(lt) \ll X^\epsilon$. Using the fact that ρ_m is a multiplicative function and Equation (3.15), we have

$$\begin{aligned}
\sum_{\substack{l|P \\ (l,m)=1}} \mu(l) \left(\frac{N}{18} \frac{\rho_m(l^2t^2)}{l^2t^2} + O(X^\epsilon) \right) &= \frac{N\rho_m(t^2)}{18t^2} \sum_{\substack{l|P \\ (l,m)=1}} \frac{\mu(l)}{l^2} \rho_m \left(\frac{l}{(t,l)} \right) + O(X^\epsilon \tau(P)) \\
&= \frac{N\rho_m(t^2)}{18t^2} \prod_{\substack{p|P \\ p \nmid m}} \left(1 - \frac{\rho_m(p/(t,p))}{p^2} \right) + O(X^\epsilon) \\
&\asymp \frac{N}{T^2} \rho_m(t^2) + O(X^\epsilon).
\end{aligned}$$

Now, using Lemma 3.14 and summing over all admissible m and t we obtain the desired bound

$$N_1 \asymp \frac{MN}{T} + O(MTX^\epsilon) \asymp \frac{MN}{T} + o(MT^{2/3}X^{1/3}),$$

as $T \ll \sqrt{X} = o(X^{1-\epsilon})$.

We now estimate N_2 using the same arguments as above. For a fixed m and t with the appropriate constraints,

$$\begin{aligned}\sum_{\log(X)\le p\le Z}\ \sum_{\substack{N\le n\le 2N\\ n\equiv 2 \bmod 18\\ n^2\equiv m^{g_1} \bmod p^2t^2}} 1 &\ll \sum_{\log(X)\le p\le Z}\left(\frac{N}{t^2p^2}\rho_m(t^2p^2)+O(\rho_m(t^2))\right)\\ &\ll \frac{N}{T^2}\frac{\rho_m(t^2)}{\log(X)}+o(X^{1/3}T^{-1/3}\rho_m(t^2)).\end{aligned}$$

Now if we once again use Lemma 3.14 and sum over all m and t, we have $N_2 \ll MN/(T\log(X))+o(MT^{2/3}X^{1/3})$. Finally, it remains to estimate N_3. If (m,n,t) is a tuple counted by N_3, then by definition we have $m^{g_1}-n^2=\alpha t^2p^2$ for some $p>Z$, so $\alpha \ll X/Z^2 = X^{1/3}T^{2/3}(\log(X))^{-4/3}$. For a fixed $m\in[M,2M]$ satisfying the usual conditions and $\alpha \ll X^{1/3}T^{2/3}(\log(X))^{-4/3}$, the number of choices for n and t is bounded above by the number of solutions to $m^{g_1}=x^2+\alpha y^2$, where $(x,y)=1$. In $\mathbb{Q}(\sqrt{-\alpha})$ we have the ideal factorization $(m)^{g_1}=(x+y\sqrt{-\alpha})(x-y\sqrt{-\alpha})$. Since m is odd and $(m,x)=1$, the two ideals on the right hand side must be co-prime as otherwise $2x\in(m)^{g_1}$, a contradiction. Hence $(x+y\sqrt{-\alpha})=\mathfrak{a}^{g_1}$ and $(x-y\sqrt{-\alpha})=\mathfrak{b}^{g_1}$, for some ideals $\mathfrak{a},\mathfrak{b}$. Thus the number of choices for n and t is bounded by the number of factorizations $(m)=\mathfrak{a}\mathfrak{b}$, which is $\ll \tau(m)$. Hence

$$N_3 \ll \frac{X}{Z^2}\sum_{M\le m\le 2M}\tau(m) \ll \frac{X}{Z^2}M\log(X)=o(MT^{2/3}X^{1/3}).$$

□

Proposition 3.18. *Let $\mathscr{R}_o(d)$ be as in Proposition 3.16. Then*

$$\sum_{d\le X}\mathscr{R}_o(d)(\mathscr{R}_o(d)-1)\ll T^{2+4/g_1}X^{2/g_1+\epsilon}. \tag{3.19}$$

Proof. Clearly,

$$\mathscr{R}_o(d) \ll \# \left\{ m \in [M, 2M], n \in [N, 2N], t \in [T, 2T] : \frac{m^{g_1} - n^2}{t^2} \in \mathbb{Z} \right\}.$$

Then the desired sum is bounded by the number of $(m_1, m_2, n_1, n_2, t_1, t_2)$ where $(m_1, n_1, t_1) \neq (m_2, n_2, t_2)$, $(m_i, t_i) = 1$ and $t_2^2(m_1^{g_1} - n_1^2) = t_1^2(m_2^{g_1} - n_2^2)$. If we fix m_1, m_2, t_1, t_2, then since $(t_1n_2 - t_2n_1)(t_1n_2 + t_2n_1) = t_1^2 m_2^{g_1} - t_2^2 m_1^{g_1}$ we conclude that n_1 and n_2 are fixed in $\ll X^\epsilon$ ways, as long as $t_1^2 m_2^{g_1} \neq t_2^2 m_1^{g_1}$. Now if this is the case, we must have $m_1 = m_2$ and $t_1 = t_2$ since $(m_i, t_i) = 1$. Hence $n_1 = n_2$, contradicting our assumption that $(m_1, n_1, t_1) \neq (m_2, n_2, t_2)$. Finally, we have

$$\sum_{d \leq X} \mathscr{R}_o(d)(\mathscr{R}_o(d) - 1) \ll X^\epsilon \sum_{M \leq m_1, m_2 \leq 2M} \sum_{T \leq t_1, t_2 \leq 2T} 1 \ll T^2 M^2 X^\epsilon.$$

Substituting for M, we obtain Equation (3.19). □

Sketch of proof of Equation (3.5). The proof of Equation (3.5) is very similar in principle to that of the previous proposition. Since $\sum_{d \leq X} \mathscr{R}_e(d)$ exceeds the number of (m, t) with $X^{1/g_1}/4 \leq m \leq X^{1/g_1}/2$ and odd, and $\sqrt{X}/2^{g_1+1} \leq t \leq \sqrt{X}/2^{g_1}$ such that $d = 2m^{g_1} - t^2$ is square free, we consider two regions. Let M_1 denote the number of such pairs such that $2m^{g_1} - t^2$ is not divisible by any prime $p \leq \log(X)$, and M_2 denote the number of pairs for which this difference is divisible by the square of a prime $p > \log(X)$. Using the same arguments as before, we have $M_1 \asymp X^{1/2+1/g_1}$ and $M_2 \ll X^{1/2+1/g_1} / \log(X)$. This gives Equation (3.5). □

We now complete the proof of Theorem 1.3. By the Cauchy-Schwarz inequality, we have

$$\left(\sum_{d \leq X} \mathscr{R}_o(d)^2 \right) \mathscr{S}_{o,g}(X) \geq \left(\sum_{d \leq X} \mathscr{R}_o(d) \right)^2,$$

since $\mathscr{S}_{o,g}(X) = \sum_{\substack{d \le X \\ \mathscr{R}_o(d) \neq 0}} 1$. The above expression gives that

$$\mathscr{S}_{o,g}(X) \geq \frac{(3.17)^2}{(3.17) + (3.19)},$$

which completes the $g \equiv 2 \mod 4$ case of Theorem 1.3.

References

[1] A. Baker, 'Linear forms in logarithms of algebraic numbers', *Mathematika* (1966), 204-216.

[2] B. Gross and D. B. Zagier, 'Heegner points and derivatives of L-series', *Invent. Math.* 84 (1986), 225-320.

[3] D. Goldfeld, 'The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer', *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) 3 (1976), 624-663.

[4] D. Goldfeld, 'Gauss class number problem for imaginary quadratic fields', *Bull. Amer. Math. Soc.* 13 (1985), 23-37.

[5] H. Davenport and H. Heilbronn, 'On the density of discriminants of cubic fields II', *Proc. Roy. Soc. London Ser.* A 322 (1971), 405-420.

[6] H. M. Stark, 'A complete determination of the complex quadratic fields of class number one', *Michigan Mathematics Journal* (1967), 1-27.

[7] I. Stewart and D. Tall, 'Algebraic Number Theory and Fermat's Last Theorem, 3rd edition', (A. K. Peters, 2002) 42-51.

[8] J. P. Cook, 'Computing Integral Bases', Lecture Notes (2010), 3-9.

[9] J. P. Serre, 'Oeuvres - Collected Papers: Volume 3: 1972 - 1984', (Springer Science & Business Media, 2003) 235.

[10] K. Heegner, 'Diophantische analysis und modulfunktionen', *Math. Zeit.* (1952), 227-253.

[11] K. Soundararajan, 'Divisibility of class numbers of imaginary quadratic fields', *J. London Math. Soc.* (2) 61 (2000), no. 3, 681-690.

[12] L. K. Hua, 'Introduction to Number Theory' (Springer, Berlin, 1982) 278-283, 307-309.

[13] M. R. Murty and J. Esmonde, 'Problems in Algebraic Number Theory, 2nd edition', (Springer-Verlag, 2005) 49-59, 248-250.

[14] M. Watkins, 'Class numbers of imaginary quadratic fields', *Math. Comp.* 73 (2004), 907-938.

[15] P. L. Clark, 'Geometry of Numbers with Applications to Number Theory', Lecture Notes (2012), 15-16.

[16] P. L. Clark, 'A Theorem of Minkowski; the Four Squares Theorem', Lecture Notes 3-4.

[17] T. M. Apostol, 'Introduction to Analytic Number Theory' (Springer-Verlag, 1976) 133-141, 157-173.

[18] W. Kohnen and K. Ono, 'Indivisibility of class numbers of imaginary quadratic number fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication', *Invent. Math.* 135 (1999), 387-398.