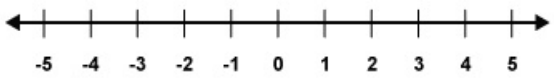
Chapter 1

Introduction

The main object of study in *number theory* is the ring of rational integers $\mathbb{Z}$.



The ring $\mathbb{Z}$ can be studied from several different perspectives. One of them is to study the distribution of prime numbers, the building blocks of its multiplicative structure, and functions theoreof. More precisely, given a sufficiently well-behaved sequence of complex numbers $\{a_n\}_n$ indexed by natural numbers $n \in \mathbb{N}$, one might ask for an estimate of the sum

$$\sum_{p \text{ prime}} a_p. \tag{1.1}$$

For instance, if the sequence $\{a_n\}_n$ is defined by

$$a_n = \begin{cases} 1 & \text{if } n \leq X \\ 0 & \text{otherwise,} \end{cases}$$

then the statement that

$$\left| \sum_{p \text{ prime}} a_p - \int_2^X \frac{dt}{\log t} \right| \leq \frac{X^{\frac{1}{2}} \log X}{8\pi}$$

for all sufficiently large real numbers X is equivalent to the famous Riemann Hypothesis [37, Corollary 1, p. 339].

Another way to study arithmetic of the ring $\mathbb{Z}$ is to study solutions of polynomial equations over the integers. One such equation is the *negative Pell equation*: given a positive integer d, one might ask when the equation

$$x^2 - dy^2 = -1 \tag{P$^-$}$$

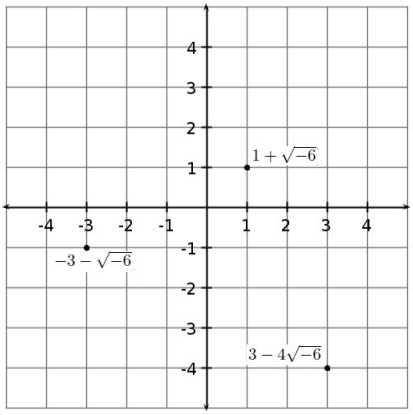
has solutions $x, y \in \mathbb{Z}$. For example, if $d = 2016$, then (P$^-$) has no solutions, while if $d = 2017$, then (P$^-$) has infinitely many solutions, the smallest of which is

$$(x, y) = (1065152991326031845038444444, 23716961153808075597914 81).$$

An area of number theory that naturally combines the above two perspectives of studying the integers is the study of *arithmetic statistics* of 2-parts of class groups of quadratic number fields.

1.1 Quadratic rings and arithmetic statistics

When solving polynomial equations over $\mathbb{Z}$, it is often useful to view these equations inside rings that are slightly larger than $\mathbb{Z}$. One natural generalization of $\mathbb{Z}$ that is particularly conducive to studying the negative Pell equation is a *quadratic ring*, i.e., a commutative ring with unity that is a free $\mathbb{Z}$-module of rank 2. An example of a quadratic ring is $\mathbb{Z}[\sqrt{-6}] = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{-6}$.



$$(1+\sqrt{-6}) \cdot (-3-\sqrt{-6}) = 3-4\sqrt{-6}$$

There are many quadratic rings. In fact, their isomorphism classes are in one-to-one correspondence with the set of integers congruent to 0 or 1 modulo 4, where a quadratic ring corresponds to its *discriminant* (see for instance [2, Theorem 8, p. 231]). In light of this, instead of studying a particular quadratic ring, one might study the *average* behavior of certain arithmetic invariants attached to quadratic rings in families parametrized by special types of discriminants. The subject dealing with these types of problems is called *arithmetic statistics*.

A quadratic ring whose discriminant is not a square is an integral domain and in fact an *order* in the quadratic number field that is its field of fractions. We will call such a ring a *quadratic domain*. If R is a quadratic domain of discriminant D, then there exists an isomorphism of rings

$$R \cong \mathbb{Z}[(D+\sqrt{D})/2].$$

Among quadratic domains, a special role is played by those that are maximal orders in quadratic number fields. The discriminant of a quadratic number field is defined to be the discriminant of the maximal order in the quadratic number field. Such a discriminant is called a *fundamental discriminant*. Fundamental discriminants are exactly the integers of the form

$$\begin{cases} d, & \text{where } d \neq 1 \text{ is squarefree and } d \equiv 1 \bmod 4, \text{ and} \\ 4d, & \text{where } d \text{ is squarefree and } d \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

We now introduce two arithmetic invariants of quadratic domains that are relevant to the negative Pell equation.

1.2 Class groups

The arithmetic of quadratic domains can be more complicated than that of the ring $\mathbb{Z}$. The *fundamental theorem of arithmetic* states that $\mathbb{Z}$ is a *unique factorization domain*, that is, a domain in which every non-zero element has a factorization into irreducible elements that is *unique* up to reordering and multiplication by units. In a quadratic domain, this need not be the case. For example, in $\mathbb{Z}[\sqrt{-6}]$,

$$2 \cdot 5 \quad \text{and} \quad (2+\sqrt{-6}) \cdot (2-\sqrt{-6})$$

are two distinct factorizations of the element 10 into irreducible elements. An integral domain which is not a unique factorization domain cannot be a principal ideal domain. Hence one obstruction to unique factorization in a quadratic domain is the failure of ideals to be principal. One way to measure this obstruction is via an algebraic invariant called the *class group*.

Let R be a quadratic domain, and let D and K denote its discriminant and its field of fractions, respectively. Then the (ordinary) class group Cl of R is defined as the quotient

$$\mathrm{Cl} = \mathcal{I}/\mathcal{P},$$

where $\mathcal{I}$ is the group of invertible fractional ideals of R and $\mathcal{P}$ is the subgroup of $\mathcal{I}$ consisting of principal invertible fractional ideals. Since a discriminant determines a quadratic ring up to isomorphism, we will sometimes denote the class group of R by $\mathrm{Cl}(D)$. A closely related group is the *narrow class group* Cl^+, defined as the quotient

$$\mathrm{Cl}^+ = \mathcal{I}/\mathcal{P}^+,$$

where now $\mathcal{P}^+$ is the subgroup of $\mathcal{I}$ consisting of principal invertible fractional ideals that can be generated by a totally positive element (i.e., an element $\alpha \in K$ such that $\sigma(\alpha) > 0$ for all real embeddings $\sigma : K \hookrightarrow \mathbb{R}$). The study of the narrow class group precedes that of the ordinary class group – the narrow class group was introduced by Gauss [21], albeit in the language of binary quadratic forms.

We recall that Cl is a finite abelian group. We also note that if a quadratic domain is the maximal order in a quadratic number field, then it is a unique factorization domain if and only if it is a principal ideal domain, and so the class group is in fact the *only* obstruction to unique factorization. For example, the ring $\mathbb{Z}[\sqrt{-6}]$ from above is the maximal order in the quadratic number field $\mathbb{Q}(\sqrt{-6})$, its class group $\mathrm{Cl}(-24)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and the ideal

generated by 2 and $\sqrt{-6}$ is not principal. A standard reference for these definitions and facts is [25].

As a fairly simple algebraic object that nonetheless carries very important information about the arithmetic of the corresponding quadratic domain, the class group is one of the most important and widely studied invariants in number theory.

1.3 What do class groups look like?

We already mentioned above that class groups are finite abelian groups. Given a finite abelian group G, a prime number ℓ, and a positive integer k, we define the ℓ^k-rank of G to be

$$\mathrm{rk}_{\ell^k} G = \dim_{\mathbb{F}_\ell} \left(\ell^{k-1} G / \ell^k G \right).$$

In other words, $\mathrm{rk}_\ell G$ is the number of cyclic ℓ-groups appearing in the decomposition of G as a direct sum of cyclic subgroups of prime-power order, and $\mathrm{rk}_{\ell^k} G$ is the number of these cyclic ℓ-groups that have an element of order ℓ^k. Hence the ℓ-rank measures the "width" of the ℓ-part, while the ℓ^k-rank as k increases measures the "depth" of the ℓ-part.

Knowing the ℓ^k-rank of G for every prime power ℓ^k is equivalent to knowing the isomorphism class of G. Therefore, as $\mathrm{Cl}(D)$ is a finite abelian group, we can study the average behavior of $\mathrm{Cl}(D)$ as D ranges over some family of discriminants by studying the distribution of $\mathrm{rk}_{\ell^k}\mathrm{Cl}(D)$ for various prime powers ℓ^k.

Let D be a fundamental discriminant. The "width" of the 2-part of $\mathrm{Cl}(D)$ is given by *Gauss's genus theory* [21]. More precisely, we have

$$\mathrm{rk}_2 \mathrm{Cl}(D)^+ = \omega(D) - 1, \tag{1.2}$$

where $\omega(D)$ denotes the number of distinct primes dividing D.

Cohen and Lenstra [4] developed a heuristic model to predict the behavior of the *odd* parts of class groups of maximal orders in quadratic number fields. Roughly, *Cohen-Lenstra heuristics* stipulate that an odd abelian group G occurs as the odd part of a class group with probability proportional to the inverse of the size of the automorphism group of G. These heuristics can be used to make many precise conjectures about the distribution of ℓ^k-ranks for $\ell \neq 2$. Gerth [22] noticed that after accounting for Gauss's genus theory, the Cohen-Lenstra heuristics can be extended to the 2-parts of class groups, leading to precise conjectures about the distribution of 2^k-ranks for $k \geq 2$. Proving these conjectures is a principal goal of arithmetic statistics.

After more than 30 years, very few such conjectures have been proved. In fact, the only result for $\ell \neq 2$ giving a precise asymptotic formula is that of Davenport and Heilbronn [11], for the average value of $3^{\mathrm{rk}_3\mathrm{Cl}(D)}$ as D ranges over all positive (or negative) fundamental discriminants (their result actually predates the Cohen-Lenstra heuristics by more than 10 years; see also [3] and [43] for subsequent refinements). Their methods and results are still insufficient to produce a positive proportion of D with $\mathrm{rk}_3\mathrm{Cl}(D) = 1$.

Much more is known in the case that $\ell = 2$. Rédei [34] gave formulas for the 4-rank in terms of the individual primes dividing the discriminant (see also [28, Theorem 1.2.3, p. 20]), and his work was sufficient to deduce distribution results over discriminants with a fixed 2-rank (see [22]). Extending these distribution results to all discriminants was a much harder problem, resolved by Fouvry and Klüners [14]. They succeeded in proving that, for each integer $k \geq 0$, the set of fundamental discriminants D such that $\mathrm{rk}_4\mathrm{Cl}(D) = k$ has the positive density predicted by Cohen and Lenstra (see [14] and also [13]).

Fouvry and Klüners [16] proved certain distribution results about the 8-rank in a special family of positive discriminants, but under the constraint that the 4-rank is equal to 1. Perhaps the most general result concerning the 8-rank is due to Stevenhagen [40]. He proved that if $d \neq 0$ and $k \geq 0$ are integers, then the set of primes p such that $\mathrm{rk}_8\mathrm{Cl}(dp) = k$ and such that dp is a fundamental discriminant has a density which is a rational number.

Density results appear to be far more difficult to obtain for the 16-rank than for the lower 2-power ranks (see [41, p. 16-18]). Our main goal is to prove density results about the 16-rank, albeit in certain particularly simple families of quadratic number fields. Before we state our results, we first give further motivation coming from the study of the negative Pell equation.

1.4 Fundamental units and the negative Pell equation

Let R, D, K, $\mathcal{I}$, $\mathcal{P}$, and $\mathcal{P}^+$ be defined as in Section 1.2. We say that R is *imaginary* if there are no real embeddings $K \hookrightarrow \mathbb{R}$, or, equivalently, if its discriminant D is negative. In this case, the narrow class group clearly coincides with the ordinary class group. Otherwise, if $D > 0$, we say that R is *real*. In this case, the relationship between the ordinary and the narrow class groups is more interesting.

Let R be a real quadratic domain. The group $\mathcal{P}^+$ is an index-1 or -2 subgroup of $\mathcal{P}$, depending on whether or not R has a unit of norm -1. Indeed, the norm of a totally positive element is clearly positive, while the norm of

$\sqrt{D} \in R$ is negative, and so the principal ideal generated by $\sqrt{D}$ can be generated by a totally positive element if and only if R has a unit of norm -1.

The unit group of R is of the form

$$R^\times \cong \langle -1 \rangle \times \langle \varepsilon \rangle \,,$$

where ε is a unit of infinite order (see for instance [25, Theorem 11.19, p. 61]). We say that ε is a *fundamental unit*. The norm $\mathrm{Norm}(\varepsilon)$ does not depend on the choice of ε, and is thus an invariant of a real quadratic domain.

As the norm function is multiplicative, the real quadratic domain R has a unit of norm -1 if and only if $\mathrm{Norm}(\varepsilon) = -1$. Hence the invariant $\mathrm{Norm}(\varepsilon)$ simply detects if the ordinary and the narrow class groups differ.

We now link the invariant $\mathrm{Norm}(\varepsilon)$ to a negative Pell equation. Let

$$d = \begin{cases} D & \text{if } D \equiv 1 \bmod 4 \\ D/4 & \text{if } D \equiv 0 \bmod 4. \end{cases}$$

One can check that the unit group $\mathbb{Z}[\sqrt{d}]^\times$ is a subgroup of index 1 or 3 of the unit group $R^\times$. Hence $\mathrm{Norm}(\varepsilon) = -1$ if and only if $\mathbb{Z}[\sqrt{d}]$ has a unit of norm -1, and this happens if and only if (P^-) is solvable. Hence

$$x^2 - dy^2 = -1 \text{ is solvable over } \mathbb{Z} \iff \mathrm{Cl}(D) = \mathrm{Cl}(D)^+. \tag{1.3}$$

The odd parts of Cl and Cl^+ coincide, so the study of the 2-parts of the ordinary and the narrow class groups is closely related to the study of solutions of the negative Pell equation. In fact, the equation $x^2 - dy^2 = -1$ is solvable over $\mathbb{Z}$ if and only if

$$\mathrm{rk}_{2^k}\mathrm{Cl}(D) = \mathrm{rk}_{2^k}\mathrm{Cl}(D)^+ \tag{1.4}$$

for all integers $k \geq 1$.

It follows from (1.3) that comparing the ordinary and the narrow class groups of *quadratic number fields* corresponds exactly to solving (P^-) for *squarefree* integers d. If d is divisible by a prime number $p \equiv 3 \bmod 4$, then (P^-) clearly has no solutions. Let $\mathbb{D}$ be the set of positive squarefree integers not divisible by a prime $p \equiv 3 \bmod 4$. Stevenhagen [42] made the remarkable conjecture that the set of squarefree d for which (P^-) is solvable has a positive density inside the set $\mathbb{D}$, given in terms of an explicit infinite product (see [42, Conjecture 1.2, p. 122]). Using the criterion (1.4), Fouvry and Klüners made significant progress on Stevenhagen's conjecture; they proved strong upper and lower bounds for the proportion of squarefree d in $\mathbb{D}$ for which (P^-) is solvable (see [15] and [16]).

1.5 The equation $x^2 - 2py^2 = -1$

To demonstrate the difficulty of improving the upper and lower bounds of Fouvry and Klüners, we now restrict our attention to a certain subset of $\mathbb{D}$, namely the set of integers of the form $2p$, where p is a prime number congruent to 1 mod 4. The associated quadratic number fields are the fields $\mathbb{Q}(\sqrt{2p})$ of discriminant $8p$. The reason this family is relatively simple is given by Gauss's genus theory.

From (1.2), we see that the 2-part of $\mathrm{Cl}(D)^+$ (and so also $\mathrm{Cl}(D)$) is relatively simpler to study when D has fewer prime divisors. If D has only one prime divisor, however, then the 2-part of the narrow class group is trivial and there is nothing to be done. Therefore, if we wish to study how the 2-part of the class group varies in some family of quadratic number fields, the simplest non-trivial types of families to consider are those parametrized by fundamental discriminants of the form qp, where $\pm q$ is an odd prime, 4, or 8, and where p varies over the set of prime numbers in some fixed congruence classes modulo 4. For instance, if we take $q = 8$ and allow p to vary over the set of prime numbers congruent to 1 modulo 4, we recover the family $\{\mathbb{Q}(\sqrt{2p})\}_{p \equiv 1 \bmod 4}$ that we mentioned above.

For details of the following discussion, see [42]. Given a real number $X > 5$, let $\rho(X)$ denote the proportion of primes $p \equiv 1 \bmod 4$ less than X for which the negative Pell equation $x^2 - 2py^2 = -1$ is solvable. Stevenhagen's conjectural framework predicts that $\rho(X) \to \frac{2}{3}$ as $X \to \infty$. However, the best known bounds are

$$\frac{5}{8} \leq \liminf_{X \to \infty} \rho(X) \leq \limsup_{X \to \infty} \rho(X) \leq \frac{3}{4}. \tag{1.5}$$

These bounds are obtained in the following way. Gauss's genus theory implies that the 2-part of $\mathrm{Cl}(8p)^+$ is cyclic, so that the 2-part of $\mathrm{Cl}(8p)^+$ is completely determined by the largest integer k such that $\mathrm{rk}_{2^k}\mathrm{Cl}(8p)^+ = 1$. As $\mathrm{Cl}(8p)$ is a quotient of $\mathrm{Cl}(8p)^+$ by a subgroup of order 1 or 2, we deduce that

$$\mathrm{rk}_{2^k}\mathrm{Cl}(8p)^+ - 1 \leq \mathrm{rk}_{2^k}\mathrm{Cl}(8p) \leq \mathrm{rk}_{2^k}\mathrm{Cl}(8p)^+ \tag{1.6}$$

for all integers $k \geq 1$. The condition $p \equiv 1 \bmod 4$ ensures that

$$\mathrm{rk}_2\mathrm{Cl}(8p) = \mathrm{rk}_2\mathrm{Cl}(8p)^+ = 1.$$

By (1.6) and (1.3), we have the implications

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = 0 \Longrightarrow \mathrm{Cl}(8p) = \mathrm{Cl}(8p)^+ \Longrightarrow x^2 - 2py^2 = -1 \text{ is solvable.}$$

It turns out that for a prime $p \equiv 1 \bmod 4$,

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = 1 \Longleftrightarrow p \equiv 1 \bmod 8,$$

which gives a lower bound of

$$\frac{1}{2} \leq \liminf_{X \to \infty} \rho(X). \tag{1.7}$$

Now, again by (1.6) and (1.3), we have the implication

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = 1 \text{ and } \mathrm{rk}_4\mathrm{Cl}(8p) = 0 \Longrightarrow x^2 - 2py^2 = -1 \text{ is not solvable.}$$

The 4-rank of the ordinary class group and the 8-rank of the narrow class group are determined by variants of fourth-power residue symbols. More precisely, for a prime $p \equiv 1 \bmod 8$, let $[2,p]_4 = 1$ if 2 is a fourth power modulo p and let $[2,p]_4 = -1$ otherwise. Similarly, for a prime $p \equiv 1 \bmod 8$, let $[p,2]_4 = 1$ if $p \equiv 1 \bmod 16$ and let $[p,2]_4 = -1$ otherwise. Then, for a prime $p \equiv 1 \bmod 8$,

$$\mathrm{rk}_4\mathrm{Cl}(8p) = 1 \Longleftrightarrow [2,p]_4 = [p,2]_4. \tag{1.8}$$

Passing to Gaussian integers and using the Čebotarev Density Theorem, it is not too hard to see that the condition above is satisfied for one-half of primes $p \equiv 1 \bmod 8$. This gives the upper bound in (1.5). Next, to improve the lower bound in (1.7), we use the implication

$$\mathrm{rk}_4\mathrm{Cl}(8p)^+ = \mathrm{rk}_4\mathrm{Cl}(8p) = 1 \text{ and } \mathrm{rk}_8\mathrm{Cl}(8p)^+ = 0 \Longrightarrow x^2 - 2py^2 = -1 \text{ is solvable}$$

and the criterion, valid for primes $p \equiv 1 \bmod 8$,

$$\mathrm{rk}_8\mathrm{Cl}(8p)^+ = 1 \Longleftrightarrow [2,p]_4 = [p,2]_4 = 1. \tag{1.9}$$

Again, one can show that this holds for one-fourth of primes $p \equiv 1 \bmod 8$, which gives the lower bound in (1.5).

At this point, we emphasize the the best known bounds (1.5), although first explicitly stated in [42, p. 127], can be readily deduced from algebraic criteria (1.8) and (1.9) that were already known to Rédei [35] and Scholz [38] in the 1930's. In other words, there has been no tangible progress on the bounds (1.5) in over 80 years.

If we wish to improve the bounds in (1.5) using the same general strategy that we employed above, we would have to be able to compute the density of primes $p \equiv 1 \bmod 4$ satisfying either (for an improvement of the upper bound)

$$\mathrm{rk}_8\mathrm{Cl}(8p)^+ = 1 \text{ and } \mathrm{rk}_8\mathrm{Cl}(8p) = 0$$

or (for an improvement of the lower bound)

$$\mathrm{rk}_8\mathrm{Cl}(8p)^+ = \mathrm{rk}_8\mathrm{Cl}(8p) = 1 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(8p) = 0.$$

As we will soon see, these two problems are of a similar difficulty. We focus on the second problem, namely the 16-rank of $\mathrm{Cl}(8p)^+$.

The fields $\mathbb{Q}(\sqrt{2p})$ are real quadratic fields, so at first sight there seems to be no relation to studying imaginary quadratic fields. Generally, studying class groups of real quadratic fields is much more difficult than studying class groups of imaginary quadratic fields, primarily because real quadratic domains have units of infinite order. However, in this particular case, Stevenhagen established a connection between the 16-rank of $\mathrm{Cl}(8p)$ and the 16-ranks of $\mathrm{Cl}(-4p)$ and $\mathrm{Cl}(-8p)$ for primes $p \equiv 1 \bmod 4$ (see [41, Theorem 3, p. 3]). One consequence of Stevenhagen's result (already known to Oriat [33]) that can be stated simply is

$$\mathrm{rk}_{16}\mathrm{Cl}(8p)^{+} = 1 \Longrightarrow \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1.$$

Hence we could improve the lower bound in (1.5) by showing that

$$\mathrm{rk}_{8}\mathrm{Cl}(8p)^{+} = \mathrm{rk}_{8}\mathrm{Cl}(-8p) = 1 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 0$$

occurs for a positive density of primes $p \equiv 1 \bmod 4$. Similar improvements on the lower bound in (1.5) could be achieved by proving density results about the 16-rank of $\mathrm{Cl}(-4p)$ for primes $p \equiv 1 \bmod 4$.

Limitations in certain analytic tools prevented us from proving density results about the 16-rank for either of the families $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$ and $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv 1 \bmod 4}$. Instead, we proved results about the 16-rank for a subfamily of $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$ and for the family $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv -1 \bmod 4}$.

1.6 Statements of main results

The two main results of this thesis come from the articles [32] and [31], which will comprise Chapter 2 and Chapter 3, respectively. In the following, p always denotes a prime number. The first result concerns a subfamily of $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$.

Theorem A. *We have*

$$\lim_{X\to\infty} \frac{\#\{p \le X : p = a^2 + c^4 \text{ with } c \text{ even and } \mathrm{rk}_{16}\mathrm{Cl}(-4p) = 1\}}{\#\{p \le X : p = a^2 + c^4 \text{ with } c \text{ even}\}} = \frac{1}{4}.$$

The second result concerns the family $\{\mathbb{Q}(\sqrt{-2p})\}_{p\equiv -1 \bmod 4}$.

Theorem B. *We have*

$$\lim_{X\to\infty} \frac{\#\{p \le X : p \equiv -1 \bmod 4 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1\}}{\#\{p \le X : p \equiv -1 \bmod 4\}} = \frac{1}{8}.$$

Theorem A and Theorem B are the first non-trivial density results about the 16-rank in families of quadratic number fields. Both of these theorems

follow from new criteria for the 16-rank and estimates of sums of type (1.1), namely the sums

$$\sum_{p \leq X} a_p \tag{1.10}$$

where $\{a_n\}_n$ is a reasonably nice sequence of complex numbers indexed by natural numbers n and X is a positive real number tending to infinity. For Theorem A, the relevant sequence is given by

$$a_n = \begin{cases} 1 & \text{if } n = a^2 + c^2 \text{ with } a \equiv \alpha \bmod 16 \text{ and } c \equiv \gamma \bmod 4 \\ 0 & \text{otherwise,} \end{cases}$$

where α and γ are specified congruence classes modulo 16 and modulo 4, respectively. Proving an asymptotic formula for the sum (1.10) with a_n defined as above is a very difficult problem, and its solution by Friedlander and Iwaniec [19] in the 1990's is still considered a major achievement in analytic number theory.

For Theorem B, the relevant sequence $\{a_n\}_n$ is much more difficult to define for general n. At prime indices p, the sequence is given by

$$a_p = \begin{cases} 1 & \text{if } p \equiv -1 \bmod 4 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = 1 \\ -1 & \text{if } p \equiv -1 \bmod 4 \text{ and } \mathrm{rk}_{16}\mathrm{Cl}(-8p) = \mathrm{rk}_8\mathrm{Cl}(-8p) - 1 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

As such, proving Theorem B consists of proving a density result for the 8-rank, which is classical, and proving that a_p oscillates as p varies. In fact, with a_p defined as above, we prove that there exists $\delta > 0$ such that

$$\sum_{p \leq X} a_p \ll X^{1-\delta}$$

as X tends to infinity. The power-saving in X in the estimate above has additional implications about the 16-rank which we discuss in the introduction to Chapter 3. The method we use to prove that a_p oscillates can be traced back to the work of Vinogradov [44] from the 1930's, but our application of this method is reminiscent of its use by Friedlander and Iwaniec, coincidentally again in [19].

1.7 Strategies for the 16-rank

We now describe one reason that density results about the 16-rank are difficult to prove, and we present our strategies to circumvent these difficulties in case of the families from Theorem A and Theorem B. Before we can do so, we have to introduce some algebraic objects that allow us to interpret class groups as Galois groups.

1.7.1 Class groups as Galois groups

The following definitions and facts can be found in [25]. Let E/F be a finite abelian extension of number fields. Let $\mathcal{I}_F$ denote the free abelian group generated by prime ideals of F that are unramified in E. The *Artin map* is the group homomorphism

$$\left(\frac{\cdot}{E/F}\right) : \mathcal{I}_F \to \mathrm{Gal}(E/F)$$

defined as follows. Let $\mathfrak{p}$ be a prime ideal of F which is unramified in E and let $\mathfrak{P}$ be any prime ideal of E lying above $\mathfrak{p}$. Let $\mathrm{Norm}(\mathfrak{p})$ be the cardinality of the residue field at $\mathfrak{p}$. Then the *Artin symbol*

$$\left(\frac{\mathfrak{p}}{E/F}\right)$$

is the unique element of $\mathrm{Gal}(E/F)$ such that

$$\left(\frac{\mathfrak{p}}{E/F}\right)(\alpha) \equiv \alpha^{\mathrm{Norm}(\mathfrak{p})} \bmod \mathfrak{P}$$

for all α in the maximal order of E. We then extend $\left(\frac{\cdot}{E/F}\right)$ multiplicatively to $\mathcal{I}_F$.

The *Hilbert class field* H of F is the maximal unramified abelian extension of F. The Artin symbol induces a canonical isomorphism of groups

$$\left(\frac{\cdot}{H/F}\right) : \mathrm{Cl} \xrightarrow{\sim} \mathrm{Gal}(H/F), \tag{1.11}$$

where Cl is the ordinary class group of F. Similarly, the Artin symbol induces a canonical isomorphism between the narrow class group Cl^+ and the Galois group $\mathrm{Gal}(H^+/F)$, where H^+ denotes the *narrow Hilbert class field* of F, i.e., the maximal unramified at all finite primes abelian extension of F.

The isomorphism (1.11) shows that information about the class group of F is encoded in the Galois theory of unramified abelian extensions of F. Whenever we can construct such an extension E/F, it must hold true that $E \subset H$, and so $\mathrm{Gal}(E/F)$ is canonically isomorphic to a quotient of Cl.

1.7.2 2^n-Hilbert class fields

Let qp be a fundamental discriminant divisible by exactly two primes, as in the beginning of Section 1.5. Then Gauss's genus theory (see (1.2)) implies that the 2-part of the narrow class group $\mathrm{Cl}(qp)^+$ is cyclic. Let K denote the quadratic field $\mathbb{Q}(\sqrt{qp})$, and let $\mathrm{Cl}^+ = \mathrm{Cl}(qp)^+$. Suppose for the moment

that $\mathrm{rk}_{2^n}\mathrm{Cl}^+ = 1$. Then $(\mathrm{Cl}^+)^{2^n}$ is a subgroup of Cl^+ of index 2^n. We define the 2^n-*Hilbert class field* H_{2^n} to be the subfield of H fixed by the the image of $(\mathrm{Cl}^+)^{2^n}$ under the isomorphism (1.11). Since the 2-primary part of Cl is cyclic, it follows immediately that H_{2^n} is the *unique* unramified at all finite primes, cyclic, degree-2^n extension of K. Moreover, (1.11) induces a canonical isomorphism of cyclic groups of order 2^n

$$\left(\frac{\cdot}{H_{2^n}/K}\right) : \mathrm{Cl}^+/(\mathrm{Cl}^+)^{2^n} \longrightarrow \mathrm{Gal}(H_{2^n}/K). \tag{1.12}$$

1.7.3 General strategy

The general strategy to prove density statements about 2^n-ranks of class groups $\mathrm{Cl}(qp)$ with q fixed and p varying is to find a criterion, in terms of p, for the existence of the 2^n-Hilbert class field of $K = \mathbb{Q}(\sqrt{qp})$. We then use the criterion to encode some information about the 2^n-rank of $\mathrm{Cl}(dp)$ via a complex number a_p and study the sum

$$\sum_{p \leq X} a_p.$$

To prove something interesting about the sum above, our criterion must be sufficiently conducive to the available analytic techniques. In practice, we often have to extend the definition of a_n to all natural numbers n in some structured way. If the function $n \mapsto a_n$ is multiplicative, we can usually apply the classical theory of L-functions to deduce interesting results about the sum over primes. Otherwise, if the function $n \mapsto a_n$ is *not* multiplicative, in special cases we may be able to apply more advanced sieving techniques.

If we have an ideal of K, explicitly defined in terms of p, that generates the class of order 2 in $\mathrm{Cl}(qp)^+$, then we might be able to deduce a criterion for $\mathrm{rk}_{2^n}\mathrm{Cl}(qp)^+$ once we have found the 2^{n-1}-Hilbert class field of K, again explicitly in terms of p. Indeed, we see from (1.12) and the definition of the Artin symbol that $\mathrm{rk}_{2^n}\mathrm{Cl}(qp)^+ = 1$ if and only if the ideal generating the class of order 2 splits in the 2^{n-1}-Hilbert class field.

The main difficulty in proving density results about 16-ranks of the narrow class groups $\mathrm{Cl}(qp)^+$ with q fixed and p varying is that there is *no known* way to generate the 8-Hilbert class field H_8 explicitly enough in terms of p so that one could apply analytic techniques. This is also the reason that density results about 8-ranks of the ordinary class groups $\mathrm{Cl}(8p)$ and 16-ranks of the narrow class groups $\mathrm{Cl}(8p)^+$ are both difficult – if $\mathrm{rk}_8\mathrm{Cl}(8p)^+ = 1$, then $\mathrm{rk}_8\mathrm{Cl}(8p) = 1$ if and only if H_8 is totally real.

In the two cases $q = -4$ and $q = -8$, we manage to overcome the difficulty of explicitly generating the 8-Hilbert class field as follows. In the case $q = -4$,

instead of finding H_8 for *all* prime numbers $p \equiv 1 \bmod 4$, we are able to write down H_8 explicitly when p is a prime of the form $a^2 + c^4$ with c even. Thus, we trade the generality of working with the full family $\{\mathbb{Q}(\sqrt{-p})\}_{p\equiv 1 \bmod 4}$ in exchange for an explicit understanding of the 8-Hilbert class field of $\mathbb{Q}(\sqrt{-p})$.

If $p \equiv -1 \bmod 4$, then $\mathrm{rk}_4\mathrm{Cl}(-8p) = 1$ if and only if $p \equiv -1 \bmod 8$. In the case $q = -8$, the idea is to write down, for $p \equiv -1 \bmod 8$, *both*

- the 4-Hilbert class field H_4 of $\mathbb{Q}(\sqrt{-2p})$, *and*
- an ideal $\mathfrak{u}$ generating a class of order 4 in $\mathrm{Cl}(-8p)$

in terms of integers u and v satisfying $p = u^2 - 2v^2$, and then to characterize those p such that

$$\left(\frac{\mathfrak{u}}{H_4/\mathbb{Q}(\sqrt{-2p})}\right) = 1. \tag{1.13}$$

The isomorphism (1.12) for $n = 2$ and the equality (1.13) then imply that the class of order 4 in Cl in fact belongs to Cl^4, which proves that Cl has an element of order 16.

Without further ado, we now move to the main body of this thesis, which consists of two chapters. Chapter 2 is based on [32] and deals with Theorem A and related results. Since we deal with a family of quadratic number fields whose class groups have cyclic 2-parts, the 16-rank is 1 or 0 according to whether or not 16 divides the *class number*, i.e., the order of the class group. We adopt this terminology in Chapter 2.

Chapter 3, dedicated to Theorem B and related results, is based on [31].