Monogenic fields with odd class number Part II: even degree

Artane Siad

November 18, 2020

Abstract

In 1801, Gauss proved that there were infinitely many quadratic fields with odd class number. We generalise this result by showing that there are infinitely many $S_n$-fields of any given even degree and signature that have odd class number. Also, we prove that there are infinitely many fields of any even degree at least 4 and with at least one real embedding that have units of every signature.

To do so, we bound the average number of 2-torsion elements in the class group, narrow class group, and oriented class group of monogenised fields of even degree (and compute these averages precisely conditional on a tail estimate) using a parametrisation of Wood [35, 36]. These averages are the first $p$-torsion averages to be calculated for $p$ not coprime to the degree (in degree at least 3), shedding light on the question of Cohen–Lenstra–Martinet–Malle type heuristics for class groups and narrow class groups at “bad” primes.

Contents

1 Introduction 2

1.1 Class group heuristics ........................................... 3
1.2 Preliminary definitions ........................................... 4
1.3 Outline of the results ........................................... 5
1.4 Strategy ......................................................... 6
1.5 Organisation of the paper ....................................... 7
1.6 Acknowledgements .............................................. 7

2 The parametrisations 8

2.1 The parametrisation of monogenised $n$-ic rings ......... 8
2.2 Orbits of pairs of symmetric bilinear forms ................. 9
2.3 Rigid parametrisation of pairs of symmetric bilinear forms 9
2.4 SL$_n$($\mathbb{Z}$)-orbits and the oriented class group ....... 12
2.5 The counting problem ........................................... 12

3 Reduction theory 13

4 Averaging and cutting off the cusp 14

4.1 The case of $A$ anisotropic over $\mathbb{Q}$ ...................... 15
4.2 The case of $A$ isotropic over $\mathbb{Q}$ ....................... 15

5 Sieving to very large and acceptable collections 25

5.1 Sieving to projective elements .............................. 25
5.2 Sieving to acceptable sets conditional on a tail estimate 26
1 Introduction

In 1801, Gauss introduced class groups in his *Disquisitiones Arithmeticae* [20], and posed what is recorded as the first question concerning their behaviour over families: are there infinitely many quadratic fields with class number 1? This question, in the real quadratic case, is still open. Nevertheless, Gauss proved that there were infinitely many quadratic fields with odd class number.

That result has been generalised, first to cubic fields by Bhargava [4], and then to all odd degrees by Ho–Shankar–Varma [22].

**Theorem 1** (Bhargava [4], Ho–Shankar–Varma [22]). For any odd degree $n$ and signature $(r_1, r_2)$, there are infinitely many fields of degree $n$ and signature $(r_1, r_2)$ that have odd class number.

As a corollary of our main theorem, we generalise Gauss’s result to all fields of even degree.

**Theorem 2.** Let $n \geq 4$ be an even integer. For each choice of signature $(r_1, r_2)$, there are infinitely fields of degree $n$ and signature $(r_1, r_2)$ that have odd class number.

To obtain his result, Gauss calculated the size of the 2-part of the narrow class group of quadratic fields. Knowing the 2-part of the narrow class group gives information about unit signatures. As a corollary to our main theorem, we generalise to even degree the result of [9] and [22] that in each odd degree, there are infinitely many fields which have units of every possible signature.

**Theorem 3.** Let $n \geq 4$ be an even integer. For each choice of signature $(r_1, r_2)$, there are infinitely fields of degree $n$ and signature $(r_1, r_2)$ that have units of units of every signature.

These results come from bounding the average size of the 2-torsion part of the class group and narrow class group of monogenised fields of even degree. This means that we can add the adjectives monogenic and $S_n$ to Theorems [2] and [3].
1.1 Class group heuristics

The Cohen–Lenstra–Martinet–Malle heuristics which were developed in a series of ground-breaking works [13, 15, 16, 14, 28], constitute our best conjectural description of the distribution of the \( p^\infty \)-part of the class group, \( \text{Cl}(K)[p^\infty] \), over families of number fields \( K \) of fixed degree and signature ordered by discriminant for “good” primes \( p \). We say that a prime \( p \) is “good” if it is coprime to the degree of the field and “bad” otherwise.

Predictions arising from these heuristics have only been verified in two cases. Davenport and Heilbronn [18] calculated the average number of 3-torsion elements in the class group of quadratic fields, and Bhargava [4] calculated the average number of 2-torsion in the class group of cubic fields. The heuristics are expected to hold under any natural ordering on the family of fields, and not just when ordering by discriminant. In [22], Ho–Shankar–Varma found evidence to support this expectation by showing that the average number of 2-torsion elements in the class group of fields associated to binary \( n \)-ic forms, ordered either by naive height or by Julia invariant, coincided with the values predicted from the heuristics.

Remarkably, in all of the cases above (see also [9]), the averages remain the same when one imposes finitely many local conditions or even an acceptable family of local conditions. We call a set of local conditions acceptable if for large enough primes \( p \), it includes all fields with discriminant indivisible by \( p^2 \). It then becomes natural to ask about the effect of global conditions on the averages. Bhargava–Hanke–Shankar found in [7] that monogenicity had the effect of doubling the average number of non-trivial elements in the 2-torsion part of the class group of cubic fields! In Part I of this two-part series, we generalised this result to all odd degrees.

**Theorem 4** ([32]). Let \( n \geq 3 \) be an odd integers. Let \( \mathcal{R} \) be an acceptable family of monogenised fields ordered by naive height. The average number of 2-torsion elements in the class group of fields in \( \mathcal{R} \) satisfies the bound:

\[
\text{Avg}(\text{Cl}_2, \mathcal{R}) \leq 1 + \frac{2}{2^{r_1+r_2}-1}
\]

with equality conditional on a tail estimate.

Despite remarkable progress on refining, understanding and streamlining these heuristics (see [38, 31, 37, 2, 3, 27, 26]), nothing has been proposed so far to describe the distribution of \( p \)-torsion in the class group for “bad” primes \( p \). In particular, there is no prediction for the average number of the 2-torsion elements in the class group, narrow class group or oriented class group of number fields of even degree.

The most serious reason for this gap seems to be the presence of genus theory. Indeed, it is unclear how the \( 1/\text{Aut}(\cdot) \) count of Cohen–Lenstra mixes with the “deterministic” input from genus theory. Even in the quadratic case, Gerth conjectured [21] and Smith proved [33], that one needs to throw out the 2-part to recover a \( 1/\text{Aut}(\cdot) \) count. A less severe obstacle concerns the presence of 2-nd roots of unity in the base field. Malle showed that roots of unity in the base field affected Cohen–Lenstra averages and it is unknown to what extent this phenomenon intervenes when genus theory is involved.

We now clarify what we mean by genus theory. In *Disquisitiones Arithmeticae* [20], Gauss determined the structure of the 2-torsion part of the narrow class group of quadratic fields by relating it to binary quadratic forms with a composition law.

**Theorem 5** (Gauss’s genus theory [20]). Let \( K \) be a quadratic field, \( \Delta_{K/Q} \) its discriminant and \( \text{Cl}^+_2[K] \) the 2-torsion in its narrow class group. Let \( \omega(\Delta_{K/Q}) \) denote the number of distinct prime
factors of $\Delta_{K/Q}$. Then the 2-torsion in the narrow class group of $K$ is given by

$$\text{Cl}_2^+[K] \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\omega(\Delta_{K/Q})-1}.$$ 

The basic idea behind this theorem is that a ramified prime $q$ contributes a 2-torsion element to the narrow class group since it must split as $(q) = \mathfrak{a}^2$ for some prime ideal $\mathfrak{a}$. It is this feature that we call genus theory in the context of Cohen–Lenstra averages. More precisely, if $p$ is a “bad” prime, then primes $q$ which ramify as $(q) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ are a source of $p$-torsion elements in the class group.

In this paper, we bound the average number of 2-torsion elements in the class group, narrow class group and oriented class group of monogenised fields of even degree at least 4 (unramified at 2) (and compute it precisely conditional on a tail estimate). These averages are the first of their kind (in degree at least 3) to be calculated in a setting where genus theory, roots of unity, and global conditions all play a part.

1.2 Preliminary definitions

A number field $K$ of degree $n$ is said to be monogenic if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. The element $\alpha$ is called a monogeniser of the field $K$. A monogenised field is the data $(K, \alpha)$ of a monogenic field together with a choice of monogeniser. It is known that a monogenic field has finitely many monogenisers up to transformations of the form $\alpha \mapsto \pm \alpha + m$ for some $m \in \mathbb{Z}$. Furthermore, it is expected that 100% of monogenic fields possess a unique monogeniser up to transformations of the form $\alpha \mapsto \pm \alpha + m$ for some $m \in \mathbb{Z}$, see [8]. This motivates the following definition.

**Definition 6.** Two monogenised fields $(K, \alpha)$ and $(K', \alpha')$ are said to be isomorphic if there exists a field isomorphism from $K$ to $K'$ taking $\alpha$ to $\pm \alpha' + m$ for some $m \in \mathbb{Z}$.

Thus, we expect monogenised fields to be statistically equivalent to monogenic fields when computing averages. Nevertheless, suppose a statement holds for a “positive proportion” of monogenised fields. In that case, the same statement is true for “infinitely many” monogenic fields by using the arguments of [22] combined with the construction of strongly quasi-reduced elements of [8].

The height we choose for monogenised fields has a convenient interpretation. Each isomorphism class of monogenised field contains a unique element $(K, \alpha_0)$ with the property that $0 \leq \text{tr}(\alpha_0) < n$. If $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ is the minimal polynomial of $\alpha_0$, we define the naive height of the isomorphism class to be:

$$H\left([(K, \alpha_0)]\right) = \max_i \left\{|a_i|^{1/i}\right\}.$$ 

We denote by $\mathcal{R}^{r_1, r_2}$ the collection of isomorphism classes of monogenised $S_n$-fields of signature $(r_1, r_2)$ ordered by naive height. In Section 2 we will see that the set of monogenised fields is in natural bijection with the set of monic degree $n$ polynomials. This bijection equips the set of monogenised fields with a natural local measure, and we can speak of families of fields in $\mathcal{R}^{r_1, r_2}$ associated with sets of local specifications $(\Sigma_p)_p$ on monic polynomials.

We will also need the notion of oriented class groups to state our results. An oriented ideal is a pair $(I, \varepsilon)$ consisting of a fractional ideal $I$ together with an orientation $\varepsilon = \pm 1$. We say that an oriented ideal is a principal oriented ideal if it is of the form $((\alpha), \text{sgn}(N(\alpha)))$. 

4
**Definition 7.** The oriented class group, Cl\(^{*}\)(K), of a number field K consists of the set of oriented fractional ideals of K modulo the principal oriented fractional ideals. The operation is component-wise multiplication.

Recall that Cl\(^{*}\)(K) is isomorphic to the usual class group of K if K has a unit of negative norm and is a Z/2Z extension of the usual class group if K does not have a unit of negative norm, [6]. Notice that when K does not have a unit of negative norm, 2-torsion in the oriented class group is not always twice as big as 2-torsion in the usual class group. The reason is that some 4-torsion elements in the oriented class group could map to 2-torsion elements in the ordinary class group under the forgetful map.

1.3 Outline of the results

To quantify the contribution of genus theory in each of our averages, we introduce a local quantity that tracks the proportion of fields in the family which are evenly ramified at p, i.e. where \((p) = a^2\) for some ideal a.

**Definition 8.** Let \(R \subset R_{r_1, r_2}\) be a family of fields corresponding to an acceptable family of local specifications \(\Sigma = (\Sigma_p)_p\). We define \(r_p(R)\), the even ramification density of \(R\) at p, as the density in \(\Sigma_p\) of elements of \(\Sigma_p\) which are evenly ramified at p.

**Theorem 9** (Main theorem). Let \(R \subset R_{r_1, r_2}\) be a family of fields (unramified at 2 and with local conditions at 2 given modulo 2) corresponding to an acceptable family of local specifications \(\Sigma = (\Sigma_p)_p\) and let \(r_p(R)\) denotes its even ramification density at p.

If \(r_1 = 0\), the average number of 2-torsion elements in the class group, narrow class group, and oriented class group of fields in \(R\) satisfies the bound:

\[
\text{Avg}(\text{Cl}_2, R) = \text{Avg}(\text{Cl}_2^+, R) = \frac{1}{2} \text{Avg}(\text{Cl}_2^-, R) \leq \prod_{p \neq 2} (1 + r_p(R)) \left(1 + \frac{2}{2^{r_2}}\right) + \frac{1}{2^{r_2}}
\]

with equality conditional on tail estimate.

If \(r_1 > 0\), the average number of 2-torsion elements in the oriented class group of fields in \(R\) satisfies the bound:

\[
\text{Avg}(\text{Cl}_2^+, R) \leq \prod_{p \neq 2} (1 + r_p(R)) \left(1 + \frac{2}{2^{r_1+r_2-1}}\right) + \frac{1}{2^{r_1+r_2-1}}
\]

with equality conditional on tail estimate.

If \(r_1 > 0\), the average number of 2-torsion elements in the narrow class group of fields in \(R\) satisfies the bound:

\[
\text{Avg}(\text{Cl}_2^+, R) \leq \prod_{p \neq 2} (1 + r_p(R)) \left(1 + \frac{2}{2^{r_2}}\right) + \frac{1}{2^{r_2}}
\]

with equality conditional on tail estimate.

If \(r_1 > 0\), the average number of 2-torsion elements in the class group of fields in \(R\) satisfies the bound:

\[
\text{Avg}(\text{Cl}_2, R) \leq \frac{1}{2} \prod_{p \equiv 1 \mod 4} (1 + r_p(R)) \left(\prod_{p \equiv 3 \mod 4} (1 - r_p(R)) + \prod_{p \equiv 3 \mod 4} (1 + r_p(R))\right) + 1 + 2 \prod_{p \neq 2} (1 + r_p(R))\]

with equality conditional on tail estimate.
These averages have several interesting consequences, two of which were mentioned earlier. First, they generalise a theorem of Gauss stating that there are infinitely many quadratic fields with odd class number. For odd degree, Ho–Shankar–Varma proved in [22] that there are infinitely many fields of fixed odd degree and signature \((r_1, r_2)\) with odd class number. For even degree, the corresponding problem has remained open for degrees strictly larger than 4. In degree 4, the result is known for biquadratic fields (see Koymans–Pagano in [24]) but not for \(S_4\)-fields to the author’s knowledge.

**Corollary 10.** Let \(n \geq 4\) be an even integer. For each choice of signature \((r_1, r_2)\), there are infinitely many degree \(n\) monogenic \(S_n\)-fields with signature \((r_1, r_2)\) that have odd class number.

Second, the averages show that there are infinitely many even degree fields with units of every signature.

**Corollary 11.** Let \(n \geq 4\) be an even integer. For each choice of signature \((r_1, r_2)\), there are infinitely many degree \(n\) monogenic \(S_n\)-fields with signature \((r_1, r_2)\) that have units of units of every signature.

Third, conditional on a tail estimate, they show that genus theory is the only added complexity to consider for “bad” primes. Indeed, the formula for \(\text{Avg}(\text{Cl}_2, \mathcal{R})\) when all \(r_p(\mathcal{R}) = 0\) is only slightly different from the one for the average 2-torsion in the class group of monogenised fields of odd degree [32].

**Corollary 12.** Let \(n \geq 4\) be an even integers. Let \(\mathcal{R} \subset \mathcal{R}^{r_1, r_2}\) be a family of fields (unramified at 2 and with local conditions at 2 given modulo 2) corresponding to an acceptable family of local specifications \(\Sigma = (\Sigma_p)_p\) and such that the even ramification density at all primes is zero, \(r_p(\mathcal{R}) = 0\).

The average number of 2-torsion elements in the class group of fields in \(\mathcal{R}\) satisfies the bound:

\[
\text{Avg}(\text{Cl}_2, \mathcal{R}) \leq 1 + \frac{3}{2^{r_1+r_2}},
\]

with equality conditional on a tail estimate.

Lastly, they offer hints as to the “right answer” for Cohen–Lenstra averages for “bad” primes.

**Remark 13.** The assumption that the families considered are unramified at 2 and have local conditions at 2 given modulo 2 is an artefact of the particulars of the mass computation at 2 and does not change the validity of the “positive proportion” versions of the corollaries above. We expect to be able to remove it in the future and to be able to upgrade the theorems to compute the average value of \(|\text{Cl}_2(\mathcal{O})| - \frac{1}{2^{r_1+r_2}} |\mathcal{I}_2(\mathcal{O})|\) for orders which are not necessarily maximal.

### 1.4 Strategy

The strategy used to prove the main theorem is roughly the same as that used in [32]. We apply Wood’s parametrisation [35, 36] of 2-torsion ideal classes in rings associated to monic binary forms in terms of integral orbits for certain representations to reduce the question to an asymptotic counting problem in the geometry of numbers. The calculation reduces to counting integral orbits for a group acting on a variety. However, unlike in the odd degree case [32], a slight change in the choice of group and variety leads to a significant difference in the arithmetic information that is encoded. This feature is unique to the even degree case and arises because there are fields of even degree which don’t possess units of negative norm (in odd degree, the unit \(-1\) has norm \(-1\)).
We begin by describing the case of the oriented class group. When computing averages for 2-torsion in the oriented class group, the relevant space is the set of $\text{SL}_n(\mathbb{Z})$-orbits of pairs of integral symmetric matrices $(A, B)$ with the constraint $\det(A) = (-1)^{\frac{n}{2}}$. To apply the geometry of numbers, we borrow the idea of [7] and “linearise” the problem by noting that up to $\text{SL}_n(\mathbb{Z})$, there are only finitely many equivalence classes of symmetric integral matrices of determinant $(-1)^{\frac{n}{2}}$. We denote this finite collection by $\mathcal{L}_Z$. Counting $\text{SL}_n(\mathbb{Z})$ orbits on the space of pairs $(A, B)$ with the constraint $\det(A) = (-1)^{\frac{n}{2}}$ is thus reduced to counting $\text{SO}_{A_0}(\mathbb{Z})$ orbits on the space of pairs $(A_0, B)$. We handle this count in the usual way, and we get the inequality of the main theorem conditional on a tail estimate. A new feature unique to the even degree case appears when computing the local masses. There is extra local mass at primes which are evenly ramified!

Now, to compute the average 2-torsion in the class group, one cannot directly use the results for the oriented class group. Indeed, when $K$ does not have a unit of negative norm, some 4-torsion elements in the oriented class group map to 2-torsion elements in the usual class group under the forgetful map. These elements are captured by pairs $(A, B)$ where $\det(A) = -1 \cdot (-1)^{\frac{n}{2}}$. This means that we need to run the strategy above on $\text{SL}_n^\pm$-orbits on the space of pairs $(A, B)$ of bilinear forms with $\det(A) = \pm 1$. A new feature appears in the final calculation because the local masses for $\det(A) = (-1)^{\frac{n}{2}}$ and $\det(A) = -1 \cdot (-1)^{\frac{n}{2}}$ behave differently at primes congruent to 3 mod 4. This is why the averages for the class group look more complicated than those for the oriented and narrow class groups.

1.5 Organisation of the paper

In Section 2 we recall the parametrisation of 2-torsion ideal classes in the oriented class group in terms of $\text{SL}_n(\mathbb{Z})$-orbits on pairs integral symmetric matrices. This parametrisation already appears in [6], albeit with a small mistake which we correct. In Sections 3-6 we run the geometry of numbers arguments to obtain an asymptotic formula for the number of 2-torsion elements in the oriented class group of monogenised fields of height at most $X$ in terms of a product of local volumes dependent on $X$. Because we use a square-free sieve dependent on a conjectural tail estimate to bound the 2-torsion from below in terms of the product of local volumes, this equality is conditional. In Section 7 we compute the total local mass. It is there that we find genus theory at play in the guise of extra orbits at evenly ramified primes. In Sections 8 and Section 9 we see how the total local masses distribute among the $(A_0, B)$ slices by applying the equidistribution techniques of [32]. Lastly, we complete the proof of the main theorem for the oriented class group in Section 10 by summing the $A_0$ counts over all $A_0 \in \mathcal{L}_Z$. In Section 11 we repeat the steps above to prove the main theorem for class groups and narrow class groups. We can recycle most of the counting arguments, but the parametrisation and the final count are much more subtle.

1.6 Acknowledgements

It is a pleasure to thank Arul Shankar for suggesting the problem and for many helpful conversations. I am grateful to Manjul Bhargava, Jonathan Hanke, Ashvin Swaminathan, and Ila Varma for useful discussions and many helpful comments. Many thanks to Beñat Mencia Uranga and Simon Lieu of the Cavendish Laboratory for their hospitality during the summer of 2019. The author’s research was supported by a McCuaig–Throop Bursary and an Ontario Graduate Scholarship.
2 The parametrisations

2.1 The parametrisation of monogenised n-ic rings

In order to count the number of monogenised n-ic rings having bounded height, we will use the following parametrisation in terms of binary n-ic forms:

**Definition 14.** Let \( U = \text{Sym}_n(2) \) denote the space of binary n-ic forms. We denote by \( U_1 \subset U \) the space of all monic binary n-ic forms \( f(x, y) = x^n + a_{n-1}x^{n-1}y + \ldots + a_0y^n \). The group \( \text{GL}_2 \) acts on \( U \) via the twisted action \( \gamma \cdot f(x, y) := \det(\gamma)^{-1}f((x, y) \cdot \gamma) \) for \( \gamma \in \text{GL}_2 \) and \( f \in U \). Let \( F \subset \text{GL}_2 \) denote the group of lower triangular unipotent matrices. Then the action of \( F \) on \( U \) preserves \( U_1 \) and yields an action of \( F \) on \( U_1 \).

We say that a pair \((R, \alpha)\) is a monogenised n-ic ring if \( R \) is an n-ic ring and \( \alpha \) is an element of \( R \) such that \( R = \mathbb{Z}[\alpha] \). Two monogenised n-ic rings \((R, \alpha)\) and \((R, \alpha')\) are said to be isomorphic if \( R \) and \( R' \) are isomorphic via a ring isomorphism sending \( \alpha \) to \( \alpha' + m \) for some \( m \in \mathbb{Z} \). We then have the following explicit parametrisation of monogenised n-ic rings in terms of the orbit data introduced above:

**Theorem 15.** There is a natural bijection between isomorphism classes of monogenised n-ic rings and \( F(\mathbb{Z}) \)-orbits on \( U_1(\mathbb{Z}) \).

**Proof.** Consider the map sending a monic binary n-ic form \( f(x, y) \in U_1(\mathbb{Z}) \) to the monogenised n-ic ring \( R_f := \left( \frac{\mathbb{Z}[\theta]}{(f(\theta, 1)), \theta} \right) \). This map descends to a map from \( F(\mathbb{Z}) \setminus U_1(\mathbb{Z}) \) to isomorphism classes of monogenised n-ic rings which we denote by \( \Phi \). Indeed, if \( g = \gamma \cdot f \) for \( \gamma = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \in F(\mathbb{Z}) \), then \( g(\theta, 1) = f(\theta + m, 1) \) and the monogenised ring \( \left( \frac{\mathbb{Z}[\theta]}{(f(\theta + m, 1))}, \theta \right) \) is isomorphic to the monogenised ring \( \left( \frac{\mathbb{Z}[\theta]}{(f(\theta + m, 1))}, \theta \right) \) through \( \theta \mapsto \theta + m \). To verify that \( \Phi \) is surjective, note that it was already surjective as a map from monic binary n-ic forms to monogenised n-ic rings. To verify that \( \Phi \) is injective, suppose that \( \Phi(f) = \left( \frac{\mathbb{Z}[\theta]}{(f(\theta, 1))}, \theta \right) \) is isomorphic to \( \Phi(g) = \left( \frac{\mathbb{Z}[\omega]}{(g(\omega, 1))}, \omega \right) \). Then \( \theta \mapsto \omega + m \) for some \( m \in \mathbb{Z} \) under this isomorphism. Consequently, \( f(\theta, 1) = 0 \) in \( \Phi(f) \) means that \( f(\omega + m, 1) = 0 \) in \( \Phi(g) \). In other words, the polynomial \( g(\omega, 1) \) divides \( f(\omega + m, 1) \). But since both are monic, we must have \( g(\omega, 1) = f(\omega + m, 1) \). Thus, \( g = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \cdot f \) and \( g = f \in F(\mathbb{Z}) \setminus U_1(\mathbb{Z}) \).

2.2 Orbits of pairs of symmetric bilinear forms

We define the space of pairs of symmetric matrices as well as the resolvent map.

**Definition 16.** Let \( T \) be a base ring. Let

\[
V(T) = T^2 \otimes \text{Sym}^2(T^n)
\]

be the space of pairs of symmetric \( n \times n \) matrices with coefficients in \( T \). The group \( \text{GL}_n(T) \) acts on \( V(T) \) by change of basis. In other words, if \( \gamma \in \text{GL}_n(T) \) and \((A, B) \in V(T)\), we define

\[
\gamma(A, B) = (\gamma^t A \gamma, \gamma^t B \gamma),
\]

where \( \gamma^t \) denotes the transpose of \( \gamma \).

There is a natural map from this space of pairs of matrices, \( V(T) \), to the space of polynomials, \( U(T) \), called the resolvent map.
Definition 17 (The resolvent map $\pi$). Let $T$ be a base ring. We define the resolvent map $\pi: V(T) \to U(T)$ by
\[
(A, B) \mapsto \text{disc}(Ax - By) = (-1)^{\frac{n}{2}} \det(Ax - B).
\]
We say that a pair $(A, B) \in V(T)$ is non-degenerate if the associated binary form $f_{(A,B)}$ is non-degenerate (has non-zero discriminant).

Example 18. In contrast to the odd case, when the degree $n$ is even, there might not exist for every $f \in \mathbb{Z}[x, y]$ a pair $(A, B) \in V(\mathbb{Z})$ whose resolvent polynomial is $f$. For instance, the binary form $-x^2 - y^2$ is not resolvent polynomial of any element of $V(\mathbb{R})$. For monic $f$, however, the torsor is always non-empty! For example, $x^2 + y^2$ is the resolvent of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $x^2 - y^2$ is the resolvent of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

We now let $\text{SL}_n(\mathbb{Z})$ act on $V$ by change of basis. This action corresponds, at the level of equivalence classes of triples $(I, \mathcal{B}, \delta)$, to the action of $\text{SL}_n(\mathbb{Z})$ on the basis $\mathcal{B}$ of the fractional ideal $I$. This action only changes the basis and does not change $I$, $\delta$, nor the orientation of $\mathcal{B}$. In particular, it does not change the defining conditions:

1. $I^2 \subset \delta R_f^{n-3}$
2. $N(I)^2 = N(\delta)N(R_f^{n-3})$

The rigid parametrisation can be used to describe $\text{SL}_n(\mathbb{Z})$ orbits.

Theorem 19 (36). Take a non-degenerate binary $n$-ic form $f \in U(T)$ and let $R_f = \frac{T[x]}{(f(x))}$. Then the pairs symmetric bilinear forms $(A, B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples $(I, \mathcal{B}, \delta)$

where $I \subset K_f$ is a based fractional ideal of $R_f$ with basis $\mathcal{B}$ given by a $T$ module isomorphism $\mathcal{B}: I \to T^n$, $\delta \in K_f^\times$ such that $I^2 \subset \delta R_f^{n-3}$ as ideals and the norm equation holds $N(I)^2 = N(\delta)N(R_f^{n-3})$ (as based ideals). Two triples $(I, \mathcal{B}, \delta)$ and $(I', \mathcal{B}', \delta')$ are equivalent if there exists a $\kappa \in K_f^\times$ with the property that $I = \kappa I'$, $\mathcal{B} \circ (\times \kappa) = \mathcal{B}'$ and $\delta = \kappa^2 \delta$.

2.4 $\text{SL}_n(\mathbb{Z})$-orbits and the oriented class group

We now let $\text{SL}_n(\mathbb{Z})$ act on $V$ by change of basis. This action corresponds, at the level of equivalence classes of triples $(I, \mathcal{B}, \delta)$, to the action of $\text{SL}_n(\mathbb{Z})$ on the basis $\mathcal{B}$ of the fractional ideal $I$. This action only changes the basis and does not change $I$, $\delta$, nor the orientation of $\mathcal{B}$. In particular, it does not change the defining conditions:

1. $I^2 \subset \delta R_f^{n-3}$
2. $N(I)^2 = N(\delta)N(R_f^{n-3})$

The rigid parametrisation can be used to describe $\text{SL}_n(\mathbb{Z})$ orbits.

Theorem 20 (36). Let $f$ be a non-degenerate monic binary $n$-ic form $f \in U_1(\mathbb{Z})$, let $R_f = \frac{\mathbb{Z}[x]}{(f(x))}$ and $K_f = R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The $\text{SL}_n(\mathbb{Z})$ orbits on pairs symmetric bilinear forms $(A, B) \in V(\mathbb{Z})$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples $(I, \varepsilon, \delta)$

where $I \subset K_f$ is a fractional ideal of $R_f$, $\varepsilon = \pm 1$ indicates the orientation of $I$, and $\delta \in K_f^\times$ is such that $I^2 \subset \delta R_f$ as ideals and the norm equation $N(I)^2 = N(\delta)$ holds (as oriented ideals). Two triples $(I, \varepsilon, \delta)$ and $(I', \varepsilon', \delta')$ are equivalent if there exists a $\kappa \in K_f^\times$ with the property that $I = \kappa I'$, $\varepsilon = \text{sgn}(N(\kappa))\varepsilon'$ and $\delta = \kappa^2 \delta'$. 

9
We recall the definition of the oriented class group of an order in a number field.

**Definition 21.** The oriented class group, \( \text{Cl}^*(\mathcal{O}) \), of an order \( \mathcal{O} \) consists of the set of oriented fractional ideals of \( \mathcal{O} \) modulo the principal oriented fractional ideals of \( \mathcal{O} \). We recall that \( \text{Cl}^*(\mathcal{O}) \) is isomorphic to the usual class group of \( \mathcal{O} \) when \( \mathcal{O} \) has a unit of negative norm and is \( \mathbb{Z}/2\mathbb{Z} \) extension of the usual class group of \( \mathcal{O} \) otherwise.

We now describe the relation between SL\(_n(\mathbb{Z}) \) orbits and the 2-torsion part of the oriented class group of \( R_f \).

**Definition 22.** A triple pair \( (I, \varepsilon, \delta) \) is said to be projective if the ideal \( I \) is invertible. Equivalently, a triple \( (I, \varepsilon, \delta) \) is projective if \( I^2 = (\delta) \). For an \( S_n \) order \( \mathcal{O} \), we write \( H^*(\mathcal{O}) \) for the set of oriented projective ideals of \( \mathcal{O} \).

As the oriented class group is comprised of invertible oriented ideals, let us consider the restriction of the parametrisation above to the set \( H^*(\mathcal{O}) \). Consider the forgetful map:

\[
H^*(\mathcal{O}) \rightarrow \text{Cl}^*_2(\mathcal{O}).
\]

Elements \( (I_0, \varepsilon_0, \delta_0) \) in the kernel of this forgetful map have the property that \( I_0 = (\alpha) \) for some \( \alpha \) in \( K \) as oriented ideals. Thus, \( (I_0, \varepsilon_0, \delta_0) \sim ((\alpha), \varepsilon_0, \delta_0) \sim (\mathcal{O}, 1, \alpha^{-2} \delta_0) \). Now, \( \mathcal{O} \subset \alpha^{-2} \delta_0 \mathcal{O} \) and \( 1 = N(\alpha^{-2} \delta_0) \). This implies that \( (I_0, \varepsilon_0, \delta_0) \) is equivalent to \( (\mathcal{O}, 1, u) \) where \( u \) is norm 1 unit of \( \mathcal{O}^\times \).

We are allowed to mod out \( u \) by squares of units of \( K^\times \) which fix the oriented ideal \( (\mathcal{O}, 1) \). But those are precisely the norm 1 units of \( \mathcal{O} \). The sequence above can thus be completed to a short exact sequence:

\[
1 \rightarrow \frac{\mathcal{O}^\times_{N=1}}{(\mathcal{O}^\times_{N=1})^2} \rightarrow H^*(\mathcal{O}) \rightarrow \text{Cl}^*_2(\mathcal{O}) \rightarrow 1.
\]

Applying Dirichlet’s unit theorem allows us to compute that 100% of the time (since having a non-trivial torsion is rare):

\[
\left| \frac{\mathcal{O}^\times_{N=1}}{(\mathcal{O}^\times_{N=1})^2} \right| = \begin{cases} 
2^{r_1+r_2} & \text{if } \mathcal{O} \text{ has a unit of norm } -1 \\
2^{r_1+r_2} & \text{otherwise}
\end{cases}.
\]

We thus obtain the following formula for the number of elements in \( H^*(\mathcal{O}) \).

**Lemma 23.** Let \( \mathcal{O} \) be an order in an \( S_n \)-number field of degree \( n \) and signature \((r_1, r_2)\). Then:

\[
|H^*(\mathcal{O})| = 2^{r_1+r_2} |\text{Cl}^*_2(\mathcal{O})|.
\]

We now proceed to the description of the points in the cuspidal regions.

Here is the version of the reducibility criterion in Ho–Shankar–Varma which is valid in even degree. Roughly, for \((A, B)\) to be reducible, all we need is to have the two components of some \( \text{SL}_n(\mathbb{Q}) \) translate of \((A, B)\) contain a common subsquare which is zero except at possibly one entry on the diagonal.

**Lemma 24** (Even degree distinguished orbits lemma). \((A, B) \in V(\mathbb{Q})\) is distinguished if and only if there is an \( \text{SL}_n(\mathbb{Q}) \) translate of \((A, B)\) with the property that

\[
a_{i,j} = b_{i,j} = 0
\]

for all \( 1 \leq i, j \leq \frac{n}{2} \) except for \( i = j = \frac{n}{2} \) for which \( a_{\frac{n}{2}, \frac{n}{2}} \neq b_{\frac{n}{2}, \frac{n}{2}} \).
Proof. By [31], we know that a self adjoint operator in $V_f(\mathbb{Q})$ is distinguished if and only if there exists a $\mathbb{Q}$ rational $\frac{n-2}{2}$ plane $X$ such that $\text{Span}\{X, TX\}$ is an isotropic $\frac{n-2}{2} + 1$ plane. It thus suffices to translate this condition into the second condition in the statement of the lemma.

First, let’s suppose that $(A, B)$ are such that $a_{i,j} = b_{i,j} = 0$ for all $1 \leq i, j \leq \frac{n}{2} - 1$ except for $i = j = \frac{n}{2}$ for which $a_{\frac{n}{2}, \frac{n}{2}} = 0 \neq b_{\frac{n}{2}, \frac{n}{2}}$. Let $\{e_1, \ldots, e_{\frac{n}{2}}, f_1, \ldots, f_{\frac{n}{2}}\}$ be the standard basis and let $T = A^{-1}B$. Then, let us set $X = \{e_1, \ldots, e_{\frac{n}{2} - 1}\}$. We claim that $\text{Span}\{X, TX\}$ is an isotropic $\frac{n}{2}$ plane. Indeed, $B(e_i) \in \text{Span}\{f_1, \ldots, f_{\frac{n}{2}}\}$ for $1 \leq i \leq \frac{n}{2} - 1$ and thus $A^{-1}B(e_i) \in \text{Span}\{e_1, \ldots, e_{\frac{n}{2}}\}$. Therefore, $(A, B)$ is distinguished in that case.

The other direction is easy. For instance, it follows directly from the arguments of [31] or a direct calculation from Melanie Wood’s parametrisation.

Definition 25. Let $\mathcal{O}$ be an order. We denote by $\mathcal{I}_2^*(\mathcal{O})$ the 2-torsion subgroup of the oriented ideal group of $\mathcal{O}$.

Proposition 26. Let $\mathcal{O}_f$ be an order corresponding to the integral primitive irreducible non-degenerate monic binary form $f$. Then, $\mathcal{I}_2^*(\mathcal{O}_f)$ is in natural bijection with the set of projective reducible $\text{SL}_n(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$.

In particular, for maximal rings, there are always exactly 2 projective reducible orbits. This will come into play when we calculate the final averages in Section [10].

SL$_n$-orbits over fields and local rings

In this section, we compute the number orbits, and the size of the stabilisers for the action of $\text{SL}_n$ on the arithmetic rings $\mathbb{Z}_p$, $\mathbb{Q}$, and $\mathbb{R}$. Let $T$ be a principal ideal domain. We first restate the rigid parametrisation in this case.

Theorem 27 ([2]). Let $f$ be a non-degenerate monic binary $n$-ic form $f \in U_1(T)$, let $R_f = \frac{T[x]}{(f(x))}$ and $K_f = R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The $\text{SL}_n(T)$ orbits on pairs symmetric bilinear forms $(A, B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples

$$(I, s, \delta)$$

where $I \subset K_f$ is a fractional ideal of $R_f$, $s$ is in the fraction field of $T$ and is such that $N(I) = sT$, and $\delta \in K_f^\times$ such that $I^2 \subset \delta R_f$ as ideals and the norm equation $s^2 = N(\delta)$ holds. Two triples $(I, s, \delta)$ and $(I', s', \delta')$ are equivalent if there exists a $\kappa \in K_f^\times$ with the property that $I = \kappa I'$, $s = N(\kappa)s'$, and $\delta = \kappa^2\delta'$.

Then, we have the following theorem whose proof is straightforward.

Lemma 28. The stabiliser in $\text{SL}_n(T)$ corresponds to the 2-torsion of $R_f^\times$ which have norm 1:

$$R_f^2[2]_{N=1}.$$

Remark 29. It follows that the $\text{SL}_n(\mathbb{Q})$ stabiliser of any element $v$ whose resolvent is irreducible is equal to 2.

Just as in [22], we can compute the number of orbits with the caveat that we need to distinguish the case where $f$ has an odd degree factor, from the case where all of $f$’s factors are even.
Lemma 30. Let $T$ be a field or $\mathbb{Z}_p$. Let $f$ be a monic separable, non-degenerate binary form in $U_1(T)$. Then the projective $\text{SL}_n(T)$ orbits of $V(T)$ with resolvent $f$ are in bijection with elements of 

$$(R_f^\times/(R_f^\times)^2)_{N \equiv 1}.$$ 

if $f$ has an odd degree factor and have a 2 to 1 map to 

$$(R_f^\times/(R_f^\times)^2)_{N \equiv 1}$$ 

if $f$ only has even degree factors.

Remark 31. We can describe the real orbits. Suppose that $f$ is a non-degenerate monic polynomial of degree $n$ with $r_1$ real roots and $2r_2$ complex roots. If $r_1 = 0$, then there are 2 $\text{SL}_n(\mathbb{R})$ orbits in $V(\mathbb{R})$ with resolvent polynomial $f$. If $r_1 > 1$, there are $2^{r_1-1}$ $\text{SL}_n(\mathbb{R})$ orbits in $V(\mathbb{R})$ with resolvent polynomial $f$. Furthermore, for $r_1 = 0$, the stabiliser has size $2^{r_2}$ while for $r_1 > 0$ it has size $2^{r_1+r_2-1}$. The size of the stabilizer depends only on $r_2$ and we denote it by $\sigma(r_2)$.

2.5 The counting problem

We first count the average number of 2-torsion elements in the oriented class group of monogenised rings and fields of even degree. To make sense of this, we order monogenised fields using the naive height on the minimal polynomial of a generator of the ring of integers whose trace is contained in $[0, n)$. Take a monic integral polynomial $f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$. We define the naive height of $f$ by:

$$H(f) := \max\{|a_i|^{1/i}\} = \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}.$$ 

Note that $H$ has the property that

$$H(\lambda B) = \lambda H(f)$$ 

so that $H$ is homogeneous of degree 1. This will be needed when we apply arguments from the geometry of numbers. The goal of the paper is to determine the following averages:

$$\lim_{X \to \infty} \frac{\sum_{\mathcal{O} \in \mathfrak{R}} |\text{Cl}^+_2(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\mathcal{O} \in \mathfrak{R}} 1}_{H(\mathcal{O}) < X},$$

$$\lim_{X \to \infty} \frac{\sum_{\mathcal{O} \in \mathfrak{R}} |\text{Cl}_2(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\mathcal{O} \in \mathfrak{R}} 1}_{H(\mathcal{O}) < X},$$

and

$$\lim_{X \to \infty} \frac{\sum_{\mathcal{O} \in \mathfrak{R}} |\text{Cl}^+_2(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\mathcal{O} \in \mathfrak{R}} 1}_{H(\mathcal{O}) < X},$$

where $\mathfrak{R} \subset \mathfrak{R}^{r_1, r_2}$ is any acceptable family of monogenic rings (an acceptable family is one which includes all rings with squarefree discriminant). The asymptotic formula for the denominator is found in the work of Bhargava–Shankar–Wang, [8].
Theorem 32 (Bhargava–Shankar–Wang, [8]). Let $S = (S_p)$ be an acceptable collection of local specifications. If $0 \leq b < n$ is fixed and $U_{1,b}$ denotes the set of monic polynomial whose $x^{n-1}$ coefficient is $b$, then we have

$$\left| U_{1,\delta}^r(S)_{<X} \right| = \text{Vol}(U_{1,\delta}^r(\mathbb{R})_{<X}) \prod_p \text{Vol}(S_p) + o(X^{\frac{n(n+1)}{2}-1}).$$

Now $\text{Vol}(S_{\infty,H})_{<X}$ grows like $X^{\frac{n(n+1)}{2}-1}$. Thus, the main term dominates the error term.

3 Reduction theory

Fix an element $A \in \mathcal{L}_\mathbb{Z}$ and $\delta \in T(r_2)$. We build a finite cover of the fundamental domain for the action of $SO_A(\mathbb{Z})$ on $V_{A}^{r_2,\delta}(\mathbb{R})$.

Definition 33. The height of an element in $B \in V_{A}^{r_2,\delta}$ is defined to be the height of the associated resolvent polynomial. That is,

$$H(B) := H(\text{disc}(Ax - By)) = H \left( (-1)^\frac{d}{2} \det(Ax - B) \right).$$

The construction of [5] can be adapted to give a fundamental set $R_{A}^{r_2,\delta}$ for the action of $SO_A(\mathbb{R})$ on $V_{A}^{r_2,\delta}(\mathbb{R})$ (which could be empty) with the following properties:

1. The set $R_{A}^{r_2,\delta}$ is a semi-algebraic.
2. If $R_{A}^{r_2,\delta}(X)$ denotes the set of elements of height at most $X$, then the coefficients of elements $B \in R_{A}^{r_2,\delta}(X)$ are bounded by $O(X)$. The implied constant is independent of $B$.

We define an indicator function that records whether $V_{A}^{r_2,\delta}(\mathbb{R})$ is empty.

Definition 34. We define the indicator function

$$\chi_A(\delta) := \begin{cases} 1 & \text{if } V_{A}^{r_2,\delta}(\mathbb{R}) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}.$$ 

We can now build a cover of a fundamental domain for the action of $SO_A(\mathbb{Z})$ on $V_{A}^{r_2,\delta}(\mathbb{R})$. To do so, we pick a fundamental domain $\mathcal{F}_A$ for the action of $SO_A(\mathbb{Z})$ on $SO_A(\mathbb{R})$ and act on $R_{A}^{r_2,\delta}$. This gives a $\sigma(r_2)$ cover of a fundamental domain for the action of $SO_A(\mathbb{Z})$ where $\sigma(r_2)$ is the size of the stabiliser in $SO_A(\mathbb{R})$ of an element $v \in V_{A}^{r_2,\delta}(\mathbb{R})$.

Proposition 35. Let $\mathcal{F}_A$ be a fundamental domain for the action of $SO_A(\mathbb{Z})$ on $SO_A(\mathbb{R})$. Then

1. If $\chi_A(\delta) = 1$, $\mathcal{F}_A \cdot R_{A}^{r_2,\delta}$ is an $\frac{\sigma(r_2)}{2}$-fold cover of a fundamental domain for the action of $SO_A(\mathbb{Z})$ on $V_{A}^{r_2,\delta}(\mathbb{R})$, where we regard $\mathcal{F}_A \cdot R_{A}^{r_2,\delta}$ as a multiset.
2. If $\chi_A(\delta) = 0$, then $\emptyset$ is a fundamental domain.

Proof. The stabiliser in $SO_A(\mathbb{R})$ of an element $B \in V_{A}^{r_2,\delta}(\mathbb{R})$ coincides with the stabiliser in $SL_n(\mathbb{R})$ of $(A,B)$ which has size $\sigma(r_2)$. The factor of $\frac{1}{2}$ comes from the fact that $-1$ also always stabilises $(A,B)$. \qed

Remark 36. The characteristic functions will be used to define the archimedean mass and will make the final computation more transparent.
4 Averaging and cutting off the cusp

For the purpose of cutting off the cusp and averaging, it suffices to work with $\text{SO}_A$ instead of $\text{SO}_A^*$ since $\text{SO}_A(Z)\setminus\text{SO}_A(R)$ is in bijection with $\text{SO}_A(Z)\setminus\text{SO}_A(R)$.

There are now two different cases to consider: 1) the case where $A$ is anisotropic over $\mathbb{Q}$ and 2) the case where $A$ is isotropic over $\mathbb{Q}$. For each, we need to show that:

1. the number of absolutely irreducible integral points in the cuspidal region is negligible; and
2. the number of reducible integral points in the main body is negligible.

We define absolutely irreducible points and reducible points and set the notation for the remainder of this section.

**Definition 37.** An element $v \in V(Z)$ is said to be absolutely irreducible if $v$ does not correspond to the identity element in the class group and the resolvent of $v$ corresponds to an order in an $S_n$-field. An element which is not absolutely irreducible is said to be reducible.

We have the following theorem which gives conditions on reducibility.

**Theorem 38 (Reducibility criterion).** Let $(A, B) \in V(Z)$ be such that all the variables in one of the following sets vanish. Then $(A, B)$ is reducible.

1. **The modified squares:**
   \[
   \{a_{i,j}, b_{i,j}\}
   \]
   for all $1 \leq i, j \leq \frac{n}{2}$ except for $i = j = \frac{n}{2}$ where $a_{\frac{n}{2}, \frac{n}{2}} = 0$.
   These pairs correspond to the identity element in the class group.

2. **The rectangles:**
   \[
   \{a_{ij}, b_{ij}\} | 1 \leq i \leq k, 1 \leq j \leq n - k
   \]
   for some $1 \leq k \leq n - 1$.
   These pairs correspond to the resolvent having repeated roots.

We define the affine spaces $V_{A,b}$ just as we did in the odd degree case [32].

**Definition 39.** Let $A$ be a fixed quadratic form in $L_\mathbb{Z}$ and fix $0 \leq b < n$. We let $V_A \subset V$ denote the space of pairs $(A, B)$, where $B$ is arbitrary. Note that the resolvent map takes $V_A$ to $U$. Now, we let $V_{A,b}$ denote the inverse image under the resolvent map of the set $U_b$. It is easy to see that $V_{A,b}$ is an affine subspace of $V_A$ of dimension $\frac{n(n+1)}{2} - 1$.

**Definition 40.** Let $S \subset V^{r_2, \delta}_A(Z) := V^{r_2, \delta}_A(R) \cap V_{A,b}(Z)$ be an $\text{SO}_A(Z)$ invariant set. Denote by $N_H(S; X)$ the number of absolutely irreducible $\text{SO}_A(Z)$-orbits on $S$ that have height bounded by $X$. For any $L \subset V_A(Z)$, let $L^{\text{irr}}$ denote the set of absolutely irreducible elements. Note that any absolutely irreducible element has a resolvent form corresponding to an order $O$ in an $S_n$-number field and so $O^\times [2]$ has size 2. As a result, the stabiliser in $\text{SO}_A(Z)$ of absolutely irreducible elements has size 2.

Therefore, we have
\[
N_H(S; X) = \frac{2}{\sigma(r_2)} \# \{F_A \cdot R^{r_2, \delta}_A(X) \cap S^{\text{irr}}\}.
\]

The goal of this section is to obtain an asymptotic formula for $N_H(S; X)$.
4.1 The case of $A$ anisotropic over $\mathbb{Q}$

When $A$ is anisotropic, we can pick a compact fundamental domain $\mathcal{F}_A$ for the action of $\text{SO}_A(\mathbb{Z})$ on $\text{SO}_A(\mathbb{R})$. It then follows that $\mathcal{F}_A \cdot R^{r_2,\delta}_{A,b}$ is bounded. To estimate the number of absolutely irreducible integral points in the fundamental domain for the action of $\text{SO}_A(\mathbb{Z})$ on $V^{r_2,\delta}_{A,b}$, we apply results from the geometry of numbers directly. We use Davenport’s refinement of the Lipschitz method on $\mathcal{F}_A \cdot R^{r_2,\delta}_{A,b}(X)$ to obtain the desired asymptotic formula.

We will need the following version of Davenport’s lemma.

**Lemma 41 (Davenport’s Lemma).** Let $E \subset \mathbb{R}^n$ be a bounded semi-algebraic multiset with maximum multiplicity at most $m$ which is defined by $k$ algebraic inequalities of each having degree at most $l$. Let $E'$ be the image of $E$ under any upper/lower triangular unipotent transformation. Then the number of integral points in $E'$ counted with multiplicity is

$$\text{Vol}(E) + O_{m,k,l}(\max\{\text{Vol}(E), 1\})$$

where $\text{Vol}(E)$ denotes the greatest $d$-dimensional volume of a projection of $E$ onto a $d$-dimensional coordinate hyperplane for $1 \leq d \leq n-1$.

**Lemma 42.** The number of integral points in $\mathcal{F}_A \cdot R^{r_2,\delta}_{A,b}$ which are not absolutely irreducible is bounded by $o\left(X^{\frac{n(n+1)}{2} - 1}\right)$.

**Proof.** The proof is the same as in [32], and follows directly from adapting the results of Ho–Shankar–Varma [22].

We thus obtain the following asymptotic formula for $N_H(S; X)$.

**Theorem 43.** Let $A \in \mathcal{L}_\mathbb{Z}$ be anisotropic over $\mathbb{Q}$. We have

$$N(V^{r_2,\delta}_{A,b}(\mathbb{Z}); X) = \frac{1}{\sigma(r_2)} \text{Vol} \left( \mathcal{F}_A \cdot R^{r_2,\delta}_{A,b}(X) \right) + o(X^{\frac{n(n+1)}{2} - 1}).$$

4.2 The case of $A$ isotropic over $\mathbb{Q}$

The arguments are almost the same as in the odd degree case [32] except for the totally split case where the Iwasawa coordinates change slightly.

Suppose now that $A$ is isotropic over $\mathbb{Q}$. Then there exists an element $g_A \in \text{SL}_n(\mathbb{Q})$ such that $g_A^t A g_A = A_{F_0}$ where

$$A_{F_0} := \begin{pmatrix}
1 & & \\
& \ddots & 1 \\
& 1 & 1 \\
& & \ddots \\
& 1 & \ddots & 1 \\
\end{pmatrix},$$

where $F_0$ is a $\mathbb{Q}$ anisotropic form. We define $m = \frac{n-\dim(F_0)}{2}$. We note that $0 < m \leq \frac{n}{2}$.

Now for $K = \mathbb{Q}$ or $\mathbb{R}$, we consider the maps

$$\sigma_V : V^{r_2,\delta}_{A,b} \to V^{r_2,\delta}_{A_{F_0},b}$$
\[ \sigma_A : \text{SO}_A(K) \to \text{SO}_{Af_0}(K) \]
defined by \( \sigma_V(A, B) = (A_{F_0}, g_A^tB g_A) \) and \( \sigma_A(h) = g_A^t h (g_A^t)^{-1} \). We note that
\[
H(A, B) = H(\sigma_V(A, B))
\]
since \( \pi \circ \sigma_V = \pi \). Furthermore, \( \sigma_V(h \cdot v) = \sigma_A(h) \cdot \sigma_V(v) \).

Now, we denote by \( \mathcal{L} \subset V_{Af_0, 0}(\mathbb{R}) \) the lattice \( \sigma_V \left( V_{Af_0, 0}(\mathbb{Z}) \right) \). We denote by \( \Gamma \subset \text{SO}_{Af_0}(\mathbb{R}) \) the subgroup \( \sigma_A(\text{SO}_A(\mathbb{Z})) \). This subgroup is commensurable with \( \text{SO}_{Af_0}(\mathbb{Z}) \). Therefore, there exists a fundamental domain \( \mathcal{F} \) for the action of \( \Gamma \) on \( \text{SO}_{Af_0}(\mathbb{R}) \) which is contained in a finite union of \( \text{SO}_{Af_0}(\mathbb{Q}) \) translates of a Siegel domain, \( \bigcup_i g_i \mathcal{S} \) for \( g_i \in \text{SO}_{Af_0}(\mathbb{Q}) \). This is known from [11].

The choice of the standard \( Af_0 \) as above is convenient at this point. Indeed, we may now choose as our Siegel domain \( \mathcal{S} \) the product \( NTK \) where we choose \( K \) to be compact, \( N \) to be a subgroup of the group of lower triangular matrices with 1 on the diagonal and \( T \) to be
\[
T := \left\{ \begin{pmatrix} t_1^{-1} & \cdots & t_m^{-1} \\ \vdots & \ddots & \vdots \\ t_m^{-1} & \cdots & t_1^{-1} \end{pmatrix} \right\}_{t_1/t_2 > c, \ldots, t_{m-1}/t_m > c, t_m > c}
\]
for some constant \( c > 0 \) if \( \dim(F_0) > 0 \) and
\[
T_0 := \left\{ \begin{pmatrix} t_1^{-1} & \cdots & t_m^{-1} \\ \vdots & \ddots & \vdots \\ t_m^{-1} & \cdots & t_1^{-1} \end{pmatrix} \right\}_{t_1/t_2 > c, \ldots, t_{m-1}/t_m > c, t_{m-1}t_m > c}
\]
for some constant \( c > 0 \) if \( \dim(F_0) = 0 \). This can be found in many sources, see for instance [10], [30], or [29].

When \( m < \frac{n}{2} \), note that \( s_i = t_i/t_{i+1}, 0 \leq i \leq m-1 \) and \( s_m = t_m \) forms a set of simple roots.

When \( m = \frac{n}{2} \), note that \( s_i = t_i/t_{i+1}, 0 \leq i \leq m-1 \) and \( s_m = t_{m-1}t_m \) forms a set of simple roots.

Moreover, if we denote by \( e^\rho \) the exponential of the half sum of the positive roots counted with multiplicities, we have
\[
e^\rho = \prod_{i=1}^{m} \frac{t_i^{n/2-i}}{i!}.
\]

When \( m < \frac{n}{2} \), we find:
\[
e^\rho = \prod_{i=1}^{m} \frac{t_i^{n/2-i}}{i!}
\]
\[
\begin{align*}
&= \prod_{i=1}^{m} \left( \prod_{j=i}^{m} s_j \right)^{\frac{n-i}{2}} \\
&= \prod_{i=1}^{m} s_i^{\left( \sum_{j=1}^{i} \frac{n-j}{2} \right)} \\
&= \prod_{i=1}^{m} s_i^{i\left(\frac{a-i-1}{2}\right)}.
\end{align*}
\]

When \( m = \frac{n}{2} \), we find:

\[
\begin{align*}
\rho &= \prod_{i=1}^{m} t_i^{n-i} \\
&= \prod_{i=1}^{m-2} \left( (s_{m-1}s_m)^{-\frac{1}{2}} \prod_{j=i}^{m} s_j \right)^{\frac{n-i}{2}} (s_{m-1}s_m)^{\frac{1}{2}} \\
&= \prod_{i=1}^{m-2} s_i^{i\left(\frac{n-i-1}{2}\right)} (s_{m-1}s_m)^{\frac{1}{2}} (s_{m-1}s_m)^{\frac{1}{2}(m-2)\left(\frac{n}{2}-\frac{m-1}{2}\right)} \\
&= \prod_{i=1}^{m-2} s_i^{i\left(\frac{n-i-1}{2}\right)} (s_{m-1}s_m)^{\frac{n(n-2)}{8}}.
\end{align*}
\]

We now fix some notation for our choice of Haar measure on \( G = \text{SO}_{A_F} \). We let \( dg \) denote the Haar measure on \( G \), \( dn \) denote the Haar measure on the unipotent group \( N \), and \( dk \) denote the Haar measure on the compact group \( K \). For every \( 1 \leq i \leq m \) we write \( d^\times t_i = \frac{dt_i}{t_i} \) and \( d^\times s_i = \frac{ds_i}{s_i} \). Furthermore, we write \( dt = \prod_{i=1}^{m} dt_i \), \( d^\times t = \prod_{i=1}^{m} d^\times t_i \) and \( ds = \prod_{i=1}^{m} ds_i \), \( d^\times s = \prod_{i=1}^{m} d^\times s_i \).

Changing variables between the \( t \)-coordinates and the \( s \)-coordinates gives us

\[ d^\times t = d^\times s. \]

Therefore, if \( m < \frac{n}{2} \), the Haar measure is given in \( NTK \)-coordinates by

\[
\begin{align*}
dg &= e^{-2\rho} du d^\times t dk \\
&= \prod_{i=1}^{m} t_{i}^{2i-n} du d^\times t dk \\
&= \prod_{i=1}^{m} s_i^{i(i+1-n)} du d^\times s dk.
\end{align*}
\]

Therefore, if \( m = \frac{n}{2} \), the Haar measure is given in \( NTK \)-coordinates by

\[
\begin{align*}
dg &= e^{-2\rho} du d^\times t dk \\
&= \prod_{i=1}^{m} t_{i}^{2i-n} du d^\times t dk \\
&= \prod_{i=1}^{m-2} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} du d^\times s dk.
\end{align*}
\]

We define the main body and the cuspidal region of the multiset \( \mathcal{F}_A \cdot R_{A,b}^{r^2,\delta} \).
Definition 44 (Main body and cuspidal region). The main body consists of all the elements of $\mathcal{F}_A \cdot P_{A,b}^{T,\delta}$ for which $|b_{11}| \geq 1$. The cuspidal region consists of all the elements for which $|b_{11}| < 1$.

We are now ready to cut off the cuspidal region.

Construction 45 (Partial order on the coordinates of $V_A$). We construct a partial order on the $n(n+1)/2$ coefficients $\{b_{ij}\}$ for $i \leq j$. These define a set of coordinates on $B$ which we denote by $U$.

Definition 46. The weight $w(b_{ij})$ of an element $b_{ij} \in U$ is the factor by which $b_{ij}$ scales under the action of $(t_1^{-1}, \ldots, t_m^{-1}, 1, \ldots, 1, t_m, \ldots, t_1) \in T$.

We are now ready to define a partial order on $U$.

Definition 47 (A partial order on subsets of $U$). Let $b$ and $b'$ be two elements of the set of coordinates $U$. We say that $b \prec b'$ if in the expression for $w(b)$ in the $s$-coordinates, the exponents of the variables $s_1, \ldots, s_m$ are smaller than or equal to the corresponding exponents appearing in the expression for $w(b')$ in the $s$-coordinates. The relation $\prec$ defines a partial order on $U$.

Example 48. We have $b_{11} \prec b_{m+1,m+1}$ because $w(b_{11}) = s_1^{-2} \cdots s_m^{-2}$ while $w(b_{m+1,m+1}) = 1 = s_1^0 \cdots s_m^0$. On the other hand, $b_{1,n-2}$ and $b_{2,n-3}$ cannot be compared in $\prec$ because $w(b_{1,n-2}) = s_1^{-1} s_2^{-1}$ while $w(b_{2,n-3}) = s_2^{-1} s_3^{-1}$. The important thing to note about the partial order $(U, \prec)$ is that if $i \leq i'$ and $j \leq j'$ then $b_{ij} \prec b_{i'j'}$.

We now cut off the cusp in two specific cases which will serve as bases cases in the proof by induction of the general case.

Example 49 (Base case of cusp cutting induction for $\dim(F_0) = 0$). We now do the case $n = 4$, $m = 2$ before moving on to cutting off the cusp in the general case. We see that torus elements act as follows:

$$t \cdot v = \begin{pmatrix} t_1^{-2} & t_1^{-1} t_2^{-1} & t_1^{-1} t_2 & 1 \\ t_1^{-1} t_2^{-1} & t_2^{-1} & 1 & t_1 t_2^{-1} \\ t_1^{-1} t_2 & 1 & t_2 & t_1 t_2 \\ 1 & t_1 t_2^{-1} & t_1 t_2 & t_1^2 \end{pmatrix} O(X).$$

We can now easily read off the weights. The Haar measure takes the form

$$dg = du \frac{1}{t_1^2} d^X t dk = du \frac{1}{s_1 s_2} d^X s dk.$$

For any subset of $U$ containing $b_{11}$, we now want to estimate

$$\tilde{I}(U_1, X) = X^{9-\#U_1} \int_{t \in T_X} \prod_{b_{ij} \in U_1} w(b_{ij}) \frac{d^X s}{s_1 s_2}.$$

We only need to look at proper subsets of $U_0 = \{b_{11}\}$ which are left-closed and up-closed. Recall that we have the bound $s_1 < C X$ and $s_2 < C^2 X^2$. Let’s compute:

$$\tilde{I}(\{b_{11}\}, X) = \int_{s_1 = c}^{C X} \int_{s_2 = c}^{C^2 X^2} \frac{d^X s}{s_1 s_2} = X^8 \int_{s_1 = c}^{C X} \int_{s_2 = c}^{C^2 X^2} d^X s = O(e(X^{8+c})$$

The number of absolutely irreducible elements in the cusp which have height at most $X$ is thus $O_e(X^{9-1+c})$ and we just barely cut off the cusp! The induction argument given below shows that in all other cases, we have much more room!
We recall that we had

\[ N_H(S; X) = \frac{1}{\sigma(r_2)} \# \{ F_A \cdot R_{A^2}^{r_2, \delta}(X) \cap S_{\text{irr}} \} \]

Now, let \( G_0 \) be a bounded open \( K \)-invariant ball in \( \text{SO}_{A_0}(\mathbb{R}) \). We can average the above expression by the usual trick to obtain

\[ N_H(S; X) = \frac{1}{\sigma(r_2) \text{Vol}(G_0)} \int_{h \in F_A} \# \{ h G_0 R_{A^2}^{r_2, \delta}(X) \cap S_{\text{irr}} \} \, dh. \]

Now, again we may use classical arguments to see that the number of absolutely irreducible integral points in the cusp which have height at most \( X \) is

\[ O \left( \int_{t \in T} \# \{ t G_0 R_{A^2}^{r_2, \delta}(X) \cap S_{\text{irr}} \} \prod_{i=1}^m s_i^{i(i+1-n)} d^\times s \right) \]

when \( m < \frac{n}{2} \) and

\[ O \left( \int_{t \in T} \# \{ t G_0 R_{A^2}^{r_2, \delta}(X) \cap S_{\text{irr}} \} \prod_{i=1}^m s_i^{i(i+1-n)} (s_{m-1} s_m) \frac{n(n-2)}{s} d^\times s \right) \]

when \( m = \frac{n}{2} \).

**Definition 50.** Let \( U_1 \subset U \) be a subset of the set of coordinates. We define

\[ V_A(\mathbb{R})(U_1) = \{ B \in V_A(\mathbb{R}) : |b_{ij}(B)| < 1 \text{ if and only if } b_{ij} \in U_1 \} \]

and

\[ V_A(\mathbb{Z})(U_1) = V_A(\mathbb{Z}) \cap V_A(\mathbb{R})(U_1). \]

It thus suffices to show that

\[ N(V_A(\mathbb{Z})(U_1); X) = O_\epsilon \left( X^{\frac{1}{2} (n+1)} - 1 + \epsilon \right) \]

for all \( U_1 \subset U \) such that \( b_{11} \in U_1 \).

We get a priori bounds on the coordinates \( s_i \) from the reducibility criterion. Let \( C \) be an absolute constant such that \( C X \) bounds the absolute value of all the coordinates of elements \( B \in G_0 R_{A^2}^{r_2, \delta}(X) \).

If \( (s_1^{-1}, s_2^{-1}, 1, \ldots, 1, s_m, \ldots, s_1) \in T \) and \( C X w(b_{i_0 n-i_0}) < 1 \) for some \( i_0 \in \{1, \ldots, m\} \), then \( C X w(b_{ij}) < 1 \) for all \( i \leq i_0 \) and \( j \leq n - i_0 \). This comes from the **Rectangles** part of the criterion for reducibility. Therefore, we may assume that

\[ s_i < C X \]

for all \( i \in \{1, \ldots, m\} \) if \( m < \frac{n}{2} \) and that

\[ s_i < C X \]

for all \( i \in \{1, \ldots, m-1\} \) and \( s_m < C^2 X^2 \) if \( m = \frac{n}{2} \).

Let us write \( T_X \) to denote the set of \( t = (s_1, \ldots, s_m) \in T \) which satisfy this condition.
Now Davenport’s lemma gives us

\[ N(V(\mathbb{Z})(U_1); X) = O \left( \int_{t \in T_X} \text{Vol}(tG_0R^2_{A_\delta}(X) \cap V(\mathbb{R})(U_1)) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^s \right) \]

\[ = O \left( X^{\left( \frac{n(n+1)}{2} - 1 \right)} - \#U_1 \prod_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^s \right). \]

for \( m < \frac{n}{2} \) and

\[ N(V(\mathbb{Z})(U_1); X) = O \left( \int_{t \in T_X} \text{Vol}(tG_0R^2_{A_\delta}(X) \cap V(\mathbb{R})(U_1)) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^s \right) \]

\[ = O \left( X^{\left( \frac{n(n+1)}{2} - 1 \right)} - \#U_1 \prod_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} d^s \right). \]

for \( m = \frac{n}{2} \). So, we have reduced our problem to one of estimating the following integrals.

**Definition 51.** The active integral of \( U_1 \subset U \) is defined by

\[ \overline{I}(U_1, X) := X^{\left( \frac{n(n+1)}{2} - 1 \right)} - \#U_1 \prod_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} d^s \]

if \( m < \frac{n}{2} \) and

\[ \overline{I}(U_1, X) := X^{\left( \frac{n(n+1)}{2} - 1 \right)} - \#U_1 \prod_{t \in T_X} \prod_{b_{ij} \notin U_1} w(b_{ij}) \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{8}} d^s \]

if \( m = \frac{n}{2} \).

Recall, that \( b_{ij} \prec b_{i_0j_0} \) when \( i \leq i_0 \) and \( j \leq j_0 \). Therefore, if \( U_1 \subset U \) contains \( b_{i_0j_0} \) but not \( b_{ij} \), then

\[ \overline{I}(U_1 \setminus \{b_{i_0j_0}\} \cup \{b_{ij}\}, X) \geq \overline{I}(U_1, X). \]

As a result, in order to obtain an upper bound for \( \overline{I}(U_1, X) \) we may assume that if \( b_{i_0j_0} \in U_1 \), then \( b_{ij} \in U_1 \) for all \( i \leq i_0 \) and \( j \leq j_0 \). In other words, we may assume that \( U_1 \) is both left closed and up closed.

Furthermore, such a set \( U_1 \) cannot contain any element on, or on the right of, the off anti-diagonal within the first \( m \)-rows, since otherwise, we would be in the case of **Rectangles** in the reducibility criterion and so \( N(V(\mathbb{Z})(U_1); X) = 0 \).

**Definition 52.** We define the subset \( U_0 \subset U \) as the set of coordinates \( b_{ij} \) such that \( i \leq j, i \leq m, \) and \( i + j \leq n - 1 \).

Now, if \( m = \frac{n}{2} \), every element in \( V(\mathbb{Z})(U_0) \) is reducible and it suffices to consider \( \overline{I}(U_1, X) \) for all \( U_1 \subset U_0 \). On the other hand if \( m < \frac{n}{2} \) we need to consider all \( U_1 \subset U \).

Since the product of the weight over all the coordinates is 1, we make the following definition.
Definition 53. We define for a subset $U_1 \subseteq U$

$$I(U_1, X) = X^{\frac{n(n+1)}{2}} \tilde{I}(U_1, X) = X^{-\#U_1} \int_{t \in TX} \prod_{b_{ij} \in U_1} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^x s$$

if $m < \frac{n}{2}$ and

$$I(U_1, X) = X^{\frac{m(n+1)}{2}} \tilde{I}(U_1, X) = X^{-\#U_1} \int_{t \in TX} \prod_{b_{ij} \in U_1} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} (s_{m-1}s_m)^{-\frac{n(n-2)}{2}} d^x s$$

if $m = \frac{n}{2}$.

We are now ready to state and prove the main cusp cutting lemma.

Lemma 54 (Main cusp cutting estimate). Let $U_1$ be a non-empty proper subset of $U_0$. Then we have the estimate

$$I(U_1, X) = O_{\epsilon} \left( X^{-1+\epsilon} \right).$$

We also have $I(\emptyset) = O_{\epsilon} \left( X^{\frac{m(m+1)(2m-3n+4)}{2}} \right)$ and $I(U_0) = O_{\epsilon} \left( X^{m(2m+1-n)+\epsilon} \right)$.

Proof. We prove this lemma via a combinatorial argument using induction on $m$. Recall that $n = 2m + \dim(F_0)$. The cases $\dim(F_0) \geq 2$ and $\dim(F_0) = 0$ are slightly different and we handle them separately.

The case $\dim(F_0) = 0$ is actually the same as is [31] with a different normalization of the height. It thus suffices to consider the case $\dim(F_0) \geq 2$.

To start, let us assume that $\dim(F_0) > 0$. First, we compute $I(U_0, X)$

$$I(U_0, X) = X^{-\#U_0} \int_{t \in TX} \prod_{b_{ij} \in U_0} w(b_{ij})^{-1} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^x s.

= X^{-m(n-(m+1))} \int_{t \in TX} (t_1^{n-2+1}t_2^{n-4+2}t_3^{n-6+2} \cdots t_m^{n-2m+2}) \prod_{i=1}^{m} t_i^{2i-n} d^x t

= X^{-m(n-(m+1))} \int_{t \in TX} t_1 t_2^3 \cdots t_m d^x t

= X^{-m(n-(m+1))} \int_{s_1, \ldots, s_m = c}^{CX} s_1^3 s_2^5 \cdots s_m^{2m-1} d^x s

= O \left( X^{-m(n-(m+1)) + m^2} \right)

= O \left( X^{m(2m+1-n)} \right)

= O \left( X^{-m(\dim(F_0)-1)} \right).$$

We compute $I(\emptyset, X)$ directly

$$I(\emptyset, X) = \int_{s_1, \ldots, s_n = c}^{CX} \prod_{i=1}^{m} s_i^{i(i+1-n)} d^x s = O \left( X^{\frac{m(m+1)(2m-3n+4)}{2}} \right)

= O \left( X^{\frac{m(m+1)(-4m-3\dim(F_0)+4)}{2}} \right).$$
Now, let $U'_1$ denote $U_0 \setminus U_1$. Define $I'_m(U'_1, X) := I(U_1, X)$. Then we have:

$$I'_m(U'_1, X) = X^{|U'_1| - m(n-m+1)} \int_{t \in TX} \left( \prod_{b_{ij} \in U'_1} w(b_{ij}) \right) t_1 t_2 \cdots t_m d^x t.$$  

$$= X^{|U'_1| - m(n-m+1)} \int_{s_1, \ldots, s_m = c}^{XC} \left( \prod_{b_{ij} \in U'_1} w(b_{ij}) \right) s_1 s_2 \cdots s_m d^x s.$$

We now work out the base case of the induction. When $m = 1$, we have:

$$I_1(\emptyset, X) = O_\epsilon \left( X^{-\dim(F_0) + \epsilon} \right)$$

$$I_1(\{b_{11}\}) = O_\epsilon \left( X^{1 - \dim(F_0) + \epsilon} \right)$$

$$I_1(\{b_{11}, \ldots, b_{1k}\}) = O_\epsilon \left( X^{1 - \dim(F_0) + \epsilon} \right)$$

$$I_1(U_0, X) = O_\epsilon \left( X^{1 - \dim(F_0) + \epsilon} \right).$$

In particular, when $\dim(F_0) \geq 2$ we see that all these quantities are $O_\epsilon(X^{-1+\epsilon})$. This will come up in the induction step.

Now, suppose that $m \geq 2$.

Now, for any decomposition $k = k_1 + k_2$ we have:

$$\int_c^{CX} s^k d^x s \ll c \int_c^{CX} s^{k_1} d^x s \int_c^{CX} s^{k_2} d^x s.$$  

Consequently, we see that $I'_n(U'_1, X)$ is bounded by the product

$$I'_n(U'_1, X) \leq J_m(U'_2, X) K_m(U'_3, X),$$

where $U'_2$ consist of all the elements of $U'_1$ in the first row, $U'_3$ consists of the rest of the elements of $U'_1$, and

$$J_m(U'_2, X) = \left( X^{|U'_2| - (n-2)} \int_{s_1, \ldots, s_n = c}^{CX} \left( \prod_{b_{ij} \in U'_2} w(b_{ij}) \right) s_1 s_2 \cdots s_m d^x s \right)$$

$$K_m(U'_3, X) = \left( X^{|U'_3| - |U_0| + (n-2)} \int_{s_2, \ldots, s_n = c}^{CX} \left( \prod_{b_{ij} \in U'_3} w(b_{ij}) \right) s_2 s_3 \cdots s_m d^x s \right).$$

Note that $K_m(U'_3, X) = I_{m-1}(U'_2, X)$ and we can estimate it by induction. Now, $U_1$ is left-closed and non-empty and hence the subset $U'_3$ is either empty or of the form $\{b_{1k}, \ldots, b_{1n-2}\}$ for some $k \geq 2$.

Now, if $U'_2 = \emptyset$:

$$J_m(U'_2, X) = O_\epsilon \left( X^{2m-1-n+2} \right) = O_\epsilon \left( X^{1 - \dim(F_0) + \epsilon} \right) = O_\epsilon \left( X^{-1+\epsilon} \right).$$
Now, if $k = 2$, then:

$$J_m(U_2', X) = X^{-1} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{2-n} t_2^{1} s_1^2 s_2^2 \cdots s_m^2 d^x s$$

$$= O_\epsilon \left( X^{-1+4m(3-n)-(m-1)+(2m-1)+\epsilon} \right)$$

$$= O_\epsilon \left( X^{-1+3m-m(2m+\dim(F_0))+m+\epsilon} \right)$$

$$= O_\epsilon \left( X^{-1+4m-2m^2-m\dim(F_0)+\epsilon} \right)$$

$$= O_\epsilon \left( X^{-1+\epsilon} \right).$$

Now, if $k = 3$, then:

$$J_m(U_2', X) = X^{-2} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{4-n} s_1^2 s_2^2 \cdots s_m^2 d^x s$$

$$= O_\epsilon \left( X^{-2+6m-(4-n)+2m-1+\epsilon} \right)$$

$$= O_\epsilon \left( X^{-3+6m-2m^2-m\dim(F_0)+\epsilon} \right)$$

$$= O_\epsilon \left( X^{-1+\epsilon} \right).$$

If $4 \leq k \leq m$, then:

$$J_m(U_2', X) = X^{1-k} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{-(n-2)-(k+1)} t_k^{1} t_{m}^{1} \cdots t_{m}^{1} s_1^2 s_2^2 \cdots s_m^2 d^x s$$

$$= X^{1-k} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{-(n-2)-(k+1)} t_{k-1} \cdots t_{k-1} s_1^2 s_2^2 \cdots s_m^2 d^x s$$

$$= X^{1-k} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{-(n-2)-(k+1)} s_1^2 s_2^2 \cdots s_{k-1}^2 s_1^2 s_2^2 \cdots s_{m}^2 d^x s$$

$$= O_\epsilon \left( X^{1-k+\frac{(k-1)(k-2)}{2}+2m-1+m(k+1-2m-\dim(F_0))+\epsilon} \right)$$

$$= O_\epsilon \left( X^{-1+\epsilon} \right).$$

If $m+1 \leq k \leq m + \dim(F_0)$, then:

$$J_m(U_2', X) = X^{1-k} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{-(n-2)-(k+1)} t_{m}^{1} \cdots t_{m}^{1} s_1^2 s_2^2 \cdots s_m^2 d^x s$$

$$= X^{1-k} \int_{s_1, \ldots, s_n = c}^{CX} t_1^{-(n-2)-(k+1)} t_{m}^{1} \cdots t_{m}^{1} s_1^2 s_2^2 \cdots s_m^2 d^x s$$

23
\[= X^{1-k} \int_{s_1, \ldots, s_n = \epsilon}^{CX} t_1^{-(n-2)-k+1} s_3 s_4^2 \cdots s_{m-1} s_1 s_2^2 \cdots s_m d^X s\]
\[= O_\epsilon \left( X^{1-k + \frac{(m-3)(m-2)}{2} + 2m-1+m(k+1-2m-\dim(F_0))+\epsilon} \right) \]
\[= O_\epsilon (X^{1+\epsilon}). \]

If \( m + \dim(F_0) + 1 \leq k \leq n - 2 \), then:
\[J_m(U'_2, X) = X^{1-k} \int_{s_1, \ldots, s_n = \epsilon}^{CX} t_1^{-(n-2)-k+1} t_{n-2-k+1} \cdots t_3 s_1 s_2^2 \cdots s_m d^X s\]
\[= X^{1-k} \int_{s_1, \ldots, s_n = \epsilon}^{CX} t_1^{-(n-2)-k+1} t_3 \cdots t_{n-k-1} s_2 s_3^2 \cdots s_m d^X s\]
\[= X^{1-k} \int_{s_1, \ldots, s_n = \epsilon}^{CX} t_1^{-(n-2)-k+1} s_3 s_4^2 \cdots s_{n-k-1} s_1 s_2 \cdots s_m d^X s\]
\[= O_\epsilon \left( X^{1-k + \frac{(n-k-1)(n-k)}{2} + 2m-1+m(k+1-2m-\dim(F_0))+\epsilon} \right) \]
\[= O_\epsilon (X^{1+\epsilon}). \]

Therefore, in all cases we find
\[J_m(U'_2, X) = O_\epsilon (X^{1+\epsilon}). \]

The lemma now follows by induction on \( m \) used to bound \( I'_m(U'_3, X) \) by \( O_\epsilon (X^{1+\epsilon}) \).

**Proposition 55.** The number of absolutely irreducible elements in the cusp which have height at most \( X \) is \( O_\epsilon \left( X^{\frac{n(n+1)}{2} - 1+\epsilon} \right) \).

We also find that the number of reducible elements in the main body is negligible.

**Lemma 56.** The number of integral points in the main body of \( \mathcal{F}_A \cdot R^{r_2, \delta}_{A, b} \) which are not absolutely irreducible is bounded by \( o \left( X^{\frac{n(n+1)}{2} - 1} \right) \).

**Proof.** The proof is identical to the anisotropic case.

Therefore, we find the following asymptotic formula.

**Theorem 57.** Let \( A \in \mathcal{L}_\mathbb{Z} \) be isotropic over \( \mathbb{Q} \). We have

\[N(V^{r_2, \delta}_{A, b}(\mathbb{Z}); X) = \frac{1}{\sigma(r_2)} \text{Vol} \left( \mathcal{F}_A \cdot R^{r_2, \delta}_{A, b}(X) \right) + o \left( X^{\frac{n(n+1)}{2} - 1} \right). \]

**Remark 58.** We can upgrade the results of this section to deal with \( A \) not having the property that the \( \mathbb{Q} \) degree of \( \text{SO}_A \) is equal to its \( \mathbb{R} \) degree. To do so, it suffices to push through the arguments with generalised Siegel sets instead of the usual Siegel sets. We can deal with the compact parts of \( M^0 \) which appear by using the o-minimal version of Davenport’s lemma (see [1]).
5 Sieving to very large and acceptable collections

In this section, we determine the desired asymptotic formulas. The results and proof contained in this section are adaptations of those of \[22\] to the case at hand and are repeated from Part I \[32\] for the reader’s convenience. We begin with the definition of a family of local specifications.

**Definition 59** (Collection of local specifications and the associated set). We say that a family \(\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu\) of subsets \(\Lambda_{A,b,\nu} \subset V_{A,b}(O_\nu)\) indexed by the places \(\nu\) of \(\mathbb{Q}\) is a **collection of local specifications** if: 1) for each finite prime \(p\) the set \(\Lambda_{A,b,p} \subset V_{A,b}(\mathbb{Z}_p)\) \(\setminus \{\Delta = 0\}\) is an open subset which is non-empty and whose boundary has measure 0; and 2) at \(\nu = \infty\), we have \(\Lambda_{A,b,\infty} = V_{A,b}^{r_2,\delta}(\mathbb{R})\) for some integer \(r_2\) with \(0 \leq r_2 \leq \frac{a-1}{2}\) and \(\delta \in \mathcal{T}(r_2)\). We associate the set \(\mathcal{V}(\Lambda_{A,b}) := \{v \in V_{A,b}(\mathbb{Z}) : \forall \nu (v \in \Lambda_{A,b,\nu})\}\) to the collection of local specifications \(\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu\).

5.1 Sieving to projective elements

**Definition 60.** For a prime \(p\), we denote by \(V_{A,b}(\mathbb{Z}_p)^{\text{proj}}\) the set of elements \(v \in V_{A,b}(\mathbb{Z}_p)\) which correspond to a projective pair \((I, \delta)\) (i.e. with the property that \(I^2 = (\delta)\)) under the parametrisation.

We have

\[
V_{A,b}^{r_2,\text{proj}}(\mathbb{Z}) = V_{A,b}^{r_2}(\mathbb{Z}) \cap \left(\bigcap_p V_{A,b}^{\text{proj}}(\mathbb{Z})\right).
\]

**Definition 61.** We denote by \(W_{A,b,p}\) the set of elements in \(V_{A,b}(\mathbb{Z})\) that do not belong to \(V_{A,b}^{\text{proj}}(\mathbb{Z}_p)\).

As in Part I \[32\], we have the following estimate on the number of element of \(W_{A,b,p}\) for large \(p\).

**Theorem 62.** We have

\[
N(\cup_{p \geq M} W_{A,b,p}, X) = O\left(\frac{X^{\frac{n(n+1)}{2}}}{M^{1-\epsilon}}\right) + o\left(\frac{X^{\frac{n(n+1)}{2}}}{M^{1-\epsilon}}\right)
\]

where the implied constant is independent of \(X\) and \(M\).

We now define the concept of **very large collections of local specifications** and state the asymptotic formula. Roughly, a collection of local specifications is very large if for large enough primes \(p\), it includes all elements of \(V\) which are projective at \(p\).

**Definition 63** (Very large collection of local specifications). Let \(\Lambda_{A,b} = (\Lambda_{A,b,\nu})_\nu\) be a collection of local specifications. We say that \(\Lambda_{A,b}\) is **very large** if for all but finitely many primes, the sets \(\Lambda_{A,b,p}\) contains all projective elements of \(V_{A,b}(\mathbb{Z}_p)\). If \(\Lambda_{A,b}\) is very large, we also say that the associated set \(\mathcal{V}(\Lambda_{A,b})\) is very large.

**Theorem 64.** Let \(r_2\) be an integer such that \(0 \leq r_2 \leq \frac{n-1}{2}\) and let \(\delta \in \mathcal{T}(r_2)\). Then for a very large collection of local specifications \(\Lambda_{A,b}\) such that \(\Lambda_{A,b,\infty} = V_{A,b}^{r_2,\delta}(\mathbb{R})\), we have

\[
N(\mathcal{V}(\Lambda_{A,b}^\delta), X) = \frac{1}{\sigma(r_2)} \text{Vol}(F_A \cdot R_{A,b}^{r_2,\delta}(X)) \prod_p \text{Vol}(\Lambda_{A,b,p}) + o\left(\frac{X^{\frac{n(n-1)}{2} - 1}}{M^{1-\epsilon}}\right),
\]

where the volume of subsets of \(V_{A,b}(\mathbb{R})\) are computed with respect to the Euclidean measure normalized so that \(V_{A,b}(\mathbb{Z})\) has covolume 1 and the volumes of subsets of \(V_{A,b}(\mathbb{Z}_p)\) are computed with respect to the Euclidean measure normalized so that \(V_{A,b}(\mathbb{Z}_p)\) has measure 1.

25
5.2 Sieving to acceptable sets conditional on a tail estimate

We now define the concept of *acceptable collections of local specifications* and state the asymptotic formula. Roughly, a collection of local specifications is acceptable if for large enough primes $p$, it includes all fields with discriminant indivisible by $p^2$.

**Definition 65** (Acceptable collection of local specifications). Let $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_{\nu}$ be a collection of local specifications. We say that $\Lambda_{A,b}$ is acceptable if for all but finitely many primes, the set $\Lambda_{A,b,p}$ contains all elements of $V_{A,b}(\mathbb{Z}_p)$ whose discriminant is not divisible by $p^2$. If $\Lambda_{A,b}$ is acceptable, we also say that the associated set $V(\Lambda_{A,b})$ is acceptable.

We have the following unconditional asymptotic inequality.

**Theorem 66.** Let $\Lambda_{A,b} = (\Lambda_{A,b,\nu})_{\nu}$ be an acceptable collection of local specifications.

$$N(V(\Lambda_{A,b}), X) \leq \frac{1}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A \cdot R_{A,b,\delta}^{r_2}(X)) \prod_p \text{Vol}(\Lambda_{A,b,p}) + o\left(X^{\frac{n(n+1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.

The following tail estimates are known for $n = 4$ as will be shown in a forthcoming work with Arul Shankar and likely to be true for $n \geq 6$. Indeed they follow from a suitable version of the $abc$ conjecture by work of Granville.

**Definition 67.** Let $p$ be a prime. We denote by $W_{A,b,p}$ the set of elements $v \in V_{A,b}(\mathbb{Z})$ such that $p^2 | \Delta(v)$.

**Conjecture 68** (Conjectural tail estimates). We have

$$N(\cup_{p \geq M} W_{A,b,p}, X) = O\left(X^{\frac{n(n+1)}{2}-1} \frac{M^{1-\epsilon}}{M^{1-\epsilon}} \right) + o\left(X^{\frac{n(n+1)}{2}-1}\right)$$

where the implied constant is independent of $X$ and $M$.

We have the following asymptotic formula conditional on the preceding tail estimates.

**Theorem 69.** Suppose that the preceding tail estimates hold. Let $r_2$ be an integer such that $0 \leq r_2 \leq \frac{n-1}{2}$ and let $\delta \in T(r_2)$. Then for an acceptable collection of local specifications $\Lambda_{A,b}$ such that $\Lambda_{A,b}(\infty) = V_{A,b}^{r_2,\delta}(\mathbb{R})$ we have

$$N(V(\Lambda_{A,b}^{\delta}), X) = \frac{1}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A \cdot R_{A,b,\delta}^{r_2}(X)) \prod_p \text{Vol}(\Lambda_{A,b,p}) + o\left(X^{\frac{n(n+1)}{2}-1}\right),$$

where the volume of subsets of $V_{A,b}(\mathbb{R})$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z})$ has covolume 1 and the volumes of subsets of $V_{A,b}(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V_{A,b}(\mathbb{Z}_p)$ has measure 1.
6 Change of measure formula

To compute the volumes of sets and multi-sets in \( V_{A,b}(\mathbb{R}) \) and \( V_{A,b}(\mathbb{Z}_p) \), we have the following version of the change of variable formula. Let \( dv \) and \( df \) denote the Euclidean measure on \( V_{A,b} \) and \( U_{A,b} \) respectively normalized so that \( V_{A,b}(\mathbb{Z}) \) and \( U_{A,b}(\mathbb{Z}) \) have co-volume 1. Furthermore, let \( \omega \) be an algebraic differential form generating the rank 1 module of top degree left-invariant differential forms on \( SO_A \) over \( \mathbb{Z} \).

Proposition 70 (Change of measure formula). Let \( K = \mathbb{Z}_p, \mathbb{R} \) or \( \mathbb{C} \). Let \( | \cdot | \) denote the usual absolute value on \( K \) and let \( s: U_{1,b}(K) \to V_{A,b}(K) \) be a continuous map such that \( \pi(f) = \) for each \( f \in U_{1,b} \). Then there exists a rational non-zero constant \( J_A \), independent of \( K \) and \( s \), such that for any measurable function \( \phi \) on \( V_{A,b}(K) \), we have:

\[
\int_{SO_A(K) \cdot s(U_{1,b}(K))} \phi(v) \, dv = |J_A| \int_{f \in U_{1,b}(K)} \int_{g \in SO_A(K)} \phi(g \cdot s(f)) \omega(g) \, df
\]

Proposition 72. We have

\[
\text{Vol} \left( F_A \cdot R_{A,b}^{\nu,\delta}(X) \right) = \chi_A(\delta) |J_A| \text{Vol}(F_A^\nu) \text{Vol}(U(\mathbb{R})_{H < \chi})
\]

Let \( S_p \subset U_{1,b}(\mathbb{Z}_p) \) be a non-empty open set whose boundary has measure 0. Consider the set \( \Lambda_{A,b,p} = V_{A,b}(\mathbb{Z}_p) \cap \pi^{-1}(S_p) \). Then we have

\[
\text{Vol}(\Lambda_{A,b,p}) = |J_A|_p \text{Vol}(SO_A(\mathbb{Z}_p)) \int_{f \in S_p} m_p(f, A) \, df
\]

7 The product of local volumes and the local mass

The calculation of the total mass is slightly more delicate here, and we divide it into a couple of lemmas.
Lemma 73 (Total quantity). Let \( R \) be a non-degenerate ring of degree \( n \) over \( \mathbb{Z}_p \). The quantity

\[
\frac{|R^\times/(R^\times)^2|}{|R^\times[2]|}
\]

is equal to 1 if \( p \neq 2 \) and to \( 2^n \) if \( p = 2 \).

Proof. The following sequence is exact:

\[
0 \rightarrow R^\times[2] \rightarrow R^\times \xrightarrow{\cdot 2} R^\times \rightarrow R^\times/(R^\times)^2 \rightarrow 0.
\]

Let us note that \( R^\times \) is the direct product of a finite abelian subgroup \( F \) and \( \mathbb{Z}_p^n \) (written additively). The exact sequence above is thus the direct sum of the corresponding exact sequence on \( F \) and on \( \mathbb{Z}_p^n \). Computing the Euler characteristic on \( F \) we find:

\[
|F/F^2| = 1.
\]

The exact sequence on the free part takes the form:

\[
0 \rightarrow \mathbb{Z}_p^n \xrightarrow{\times 2} \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^n/(2\mathbb{Z}_p)^n \rightarrow 0.
\]

In order to extract information from this part, we need to treat the cases \( p \neq 2 \) and \( p = 2 \) separately. For \( p \neq 2 \), the map \( \times 2 \) is surjective so the free part contributes a factor of 1. For \( p = 2 \), the module \( (2\mathbb{Z}_2)^n \) has index \( 2^n \) in \( \mathbb{Z}_2^n \) and so the free part contributes a factor of \( 2^n \). This completes the proof of the lemma.

Lemma 74 (Norm isolation). Let \( R \) be a non-degenerate ring of degree \( n \) over \( \mathbb{Z}_p \). Let \( N \) denote the norm map from \( N: R^\times/(R^\times)^2 \rightarrow \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \). The quantity

\[
\frac{|N(R^\times/(R^\times)^2)|_{N=1}}{|R^\times[2]|}
\]

is equal to \( \frac{1}{|N(R^\times)|} \) if \( p \neq 2 \) and to \( \frac{2^n}{|N(R^\times)|} \) if \( p = 2 \).

Proof. The first isomorphism theorem gives us \( N(R^\times) \cong \frac{(R^\times/(R^\times)^2)}{N(R^\times)^2}_{N=1} \). Since everything is finite we get:

\[
|R^\times/(R^\times)^2|_{N=1} = \frac{|R^\times/(R^\times)^2|}{|N(R^\times)|}
\]

and the result follows from the previous lemma.

In particular, we get the following statement concerning the total local masses for maximal rings which are not evenly ramified at \( 2 \). It follows from the previous lemma and the fact that if \( \mathcal{O}^\times \) is the ring of integers of a finite extension of \( \mathbb{Q}_p \), the norm map \( N: \mathcal{O}^\times/(\mathcal{O}^\times)^2 \rightarrow \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \) is surjective when the extension has odd ramification degree and not surjective when \( p \neq 2 \) and the extension has even ramification degree.

Lemma 75. The total local mass for \( f \in \mathbb{Z}_p[x] \) maximal and not evenly ramified at \( p \) is given by:

\[
m_p(f) = \begin{cases} 
2^{n-1} & \text{if } p = 2 \\
1 & \text{if } p \neq 2
\end{cases}
\]

The total local mass for \( f \in \mathbb{Z}_p[x], p \neq 2, \) maximal and evenly ramified is given by:

\[
m_p(f) = 2.
\]
Remark 76. Thus, even ramification has a doubling effect on the total local mass. Heuristically, this is because if $f$ has even ramification at the prime $p$, then the ideal $(p)$ splits into a product of prime ideals $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_m^{e_m}$ each appearing to an even power $e_i$, and thus we can write $(p) = I^2$. So we have constructed a 2-torsion ideal in the oriented ideal class group. The fact that the total mass is twice as large means that on average, these ideals contribute one extra generator to the 2-torsion in the oriented ideal class group.

7.1 Computing the local masses

We now define the infinite mass and compute $m_p(f, A)$ for all $p \neq 2, \infty$.

Definition 77 (The infinite mass). Let $A \in \mathcal{L}_Z$ and $r_2$ be an integer such that $0 \leq r_2 \leq \frac{n-1}{2}$. The infinite mass of $A$ with respect to $r_2$ is defined to be

$$m_\infty(r_2, A) = \sum_{\delta \in T(r_2)} \chi_A(\delta).$$

The following lemma isolates the main properties of the local masses for all $p$, including the Archimedean place.

Lemma 78 (Main properties of the local masses). The local masses $m_p(f, A)$ and $m_\infty(A)$ have the following properties.

1. If $\gamma \in \text{SL}_n(\mathbb{Z}_p)$, we have

$$m_p(f, \gamma^t A \gamma) = m_p(f, A).$$

2. If $\gamma \in \text{SL}_n(\mathbb{R})$, we have

$$m_\infty(r_2, \gamma^t A \gamma) = m_\infty(r_2, A).$$

3. In particular, if $A_1$ and $A_2$ are unimodular integral matrices lying in the same genus, we have

$$m_p(f, A_1) = m_p(f, A_2)$$

for all primes $p$ and

$$m_\infty(r_2, A_1) = m_\infty(r_2, A_2).$$

4. The sum of $m_2(f, A)$ over a set of representatives for the unimodular orbits of the action of $\text{SL}_n(\mathbb{Z}_2)$ on $\text{Sym}_n(\mathbb{Z}_2)$ is

$$\sum_{A \in \text{Sym}_n(\mathbb{Z}_2) \atop \text{det}(A) = 1 \in \mathbb{Z}_2} m_2(f, A) = m_2(f).$$

5. The sum of $m_p(f, A)$ over a set of representatives for the unimodular orbits of the action of $\text{SL}_n(\mathbb{Z}_p)$ on $\text{Sym}_n(\mathbb{Z}_p)$ is

$$\sum_{A \in \text{Sym}_n(\mathbb{Z}_p) \atop \text{det}(A) = 1 \in \mathbb{Z}_p} m_p(f, A) = m_p(f).$$
6. The sum of \( m_\infty(r_2, A) \) over a set of representatives for unimodular the orbits of the action of \( SL_n(\mathbb{R}) \) on \( Sym_n(\mathbb{R}) \) is

\[
\sum_{A \in \frac{Sym_n(\mathbb{R})}{SL_n(\mathbb{R})}, \det(A) = 1} m_\infty(r_2, A) = 2^{r_1 - 1}
\]

if \( r_1 > 0 \) and

\[
\sum_{A \in \frac{Sym_n(\mathbb{R})}{SL_n(\mathbb{R})}, \det(A) = 1} m_\infty(r_2, A) = 2
\]

if \( r_1 = 0 \).

We can now compute the local masses for all \( p \neq 2, \infty \) by noting that there is a unique \( SL_n(\mathbb{Z}_p) \) equivalence class of bilinear forms with determinant 1.

**Corollary 79** (Local masses for \( p \neq 2, \infty \)). For \( A \in \mathcal{L}_c \) and \( p \neq 2, \infty \) we have

\[
m_p(f, A) = \begin{cases} 
2 & \text{if } f \text{ is evenly ramified at } p \\
1 & \text{otherwise}
\end{cases}
\]

The computation of the local masses at \( p = 2, \infty \) is more delicate and is the object of the following sections.

8 Point count and the 2-adic mass

We compute the 2-adic mass for polynomials which are not evenly ramified at the prime 2. We begin by showing that this restriction allows us to exclude type II genera from our considerations.

**Theorem 80** (Type II genera and over-ramification at 2). Let \( A \) be the hyperbolic unimodular symmetric bilinear form over \( \mathbb{F}_2 \). Then the image under the resolvent map of \( V_A(\mathbb{F}_2) \) lies in

\[ \mathbb{F}_2[x^2] = \left( \mathbb{F}_2[x] \right)^2. \]

Therefore, pairs whose first component is hyperbolic modulo 2 correspond to ideal classes of monogenic orders which are “over-ramified” at 2 in the sense that (2) splits as a product of even powers of primes ideals. In particular, the discriminant of the resolvent polynomials of such pairs is not squarefree at 2. Furthermore, the statement of the theorem holds if \( \mathbb{F}_2 \) is replaced by any ring of characteristic 2.

**Proof.** Without loss of generality we can let \( A \) be the matrix with 1s on the anti-diagonal and \( B \) be any symmetric matrix. We proceed by examining the resolvent polynomial from the perspective of universal algebra. Let us introduce the multivariate polynomial

\[
\Phi(X_1, \ldots, X_\frac{\infty}{2}, Y_\frac{\infty}{2}, \ldots, Y_1) \in \mathbb{F}_2[X_1, \ldots, X_\frac{\infty}{2}, Y_\frac{\infty}{2}, \ldots, Y_1]
\]

which we define as the determinant:
We have chosen the subscripts above to match the Hasse–Witt symbol of the respective bilinear forms.

### Remark 81.
We have chosen the subscripts above to match the Hasse–Witt symbol of the respective bilinear forms.
We now state the constraint imposed on the total mass by the local mass.

**Lemma 82.** For any $f \in U_{1,b}(\mathbb{Z}_2)$, we have

$$m_2(f, M_1) + m_2(f, M_{-1}) = 2^{n-1}.$$ 

We give names to the integral of the 2-adic masses over $S_2$.

**Definition 83.** Define

$$c_2(n, M_1) = \int_{f \in S_2} m_2(f, M_1) \, df$$

$$c_2(n, M_{-1}) = \int_{f \in S_2} m_2(f, M_{-1}) \, df.$$ 

**Lemma 84** (Point count). Let $S_2 \subset U_{1,b}(\mathbb{Z}_2)$ be a local condition on the space of non-over-ramified monic polynomials at the prime 2 defined modulo 2. Denote by $\Lambda_{M_1}(2)$ and $\Lambda_{M_{-1}}(2)$ the pre-images in $V_{M_1,b}(\mathbb{Z}_2)$ and $V_{M_{-1},b}(\mathbb{Z}_2)$ respectively of $S_2$ under the resolvent map $\pi$. Then the volumes of these two sets are equal

$$\text{Vol}(\Lambda_{M_1}(2)) = \text{Vol}(\Lambda_{M_{-1}}(2)).$$

**Proof.** The canonical representatives $M_1$ and $M_{-1}$ are equal modulo 2. Since $\Lambda_{M_1}(2)$ and $\Lambda_{M_{-1}}(2)$ are defined by imposing congruence conditions modulo 2 on $V_{M_1,b}(\mathbb{Z}_2)$ and $V_{M_{-1},b}(\mathbb{Z}_2)$, the result follows. □

As in [32] we find.

**Lemma 85.** The rational numbers giving the Jacobian change of variables for $M_1$ and $M_{-1}$ are equal when the volume forms on the associated special orthogonal groups are those associated to point counting modulo increasing powers of $p$:

$$J_{M_1} = J_{M_{-1}}.$$ 

In particular, their 2-adic valuations are the same

$$|J_{M_1}|_2 = |J_{M_{-1}}|_2.$$ 

Finally, we compute the ratio of the 2-adic masses by finding the ratio between the volumes of the 2-adic points of the special orthogonal groups $SO_{M_1}$ and $SO_{M_{-1}}$.

**Proposition 86** (Volume ratio for Type I genera). We have

$$\frac{c_2(n, M_1)}{c_2(n, M_{-1})} = \frac{\text{Vol}(\Lambda_{M_1}(2)) \left( |J_{M_{-1}}|_2 \text{Vol}(SO_{M_{-1}}(\mathbb{Z}_2)) \right)}{\text{Vol}(\Lambda_{M_{-1}}(2)) \left( |J_{M_1}|_2 \text{Vol}(SO_{M_1}(\mathbb{Z}_2)) \right)} = \frac{\text{Vol}(SO_{M_{-1}}(\mathbb{Z}_2))}{\text{Vol}(SO_{M_1}(\mathbb{Z}_2))}$$

$$= 2^{n-2} \pm_8 2^{\frac{n-2}{2}},$$

where $\pm_8$ is + if $n$ is congruent to 0 or 2 mod 8 and – otherwise.
Proof. This calculation is the same as in [32]. Care is needed to keep track of the octane values of $M_1$ and $M_{-1}$ for different congruence classes of $n$ modulo 8 resulting in the cases for $\pm 8$. We find that $M_1$ has octane value $0 \pmod{8}$ if $n \equiv 0 \pmod{8}$, $4 \pmod{8}$ if $n \equiv 4 \pmod{8}$, $0 \pmod{8}$ if $n \equiv 2 \pmod{8}$, and $4 \pmod{8}$ if $n \equiv 6 \pmod{8}$. On the other hand, we find that $M_{-1}$ has octane value $4 \pmod{8}$ if $n \equiv 0 \pmod{8}$, $0 \pmod{8}$ if $n \equiv 4 \pmod{8}$, $4 \pmod{8}$ if $n \equiv 2 \pmod{8}$, and $0 \pmod{8}$ if $n \equiv 6 \pmod{8}$.

We thus obtain the values for the 2-adic mass.

Corollary 87. The 2-adic masses satisfy the following identities:

$$c_2(n, M_1) + c_2(n, M_{-1}) = 2^{n-1} \text{Vol}(S_2)$$

$$c_2(n, M_1) - c_2(n, M_{-1}) = \pm 2^{\frac{n-2}{2}+1} \text{Vol}(S_2).$$

In particular:

$$c_2(n, M_1) = \left(2^{n-2} \pm 8 \cdot 2^{\frac{n-2}{2}}\right) \text{Vol}(S_2)$$

$$c_2(n, M_{-1}) = \left(2^{n-2} \mp 8 \cdot 2^{\frac{n-2}{2}}\right) \text{Vol}(S_2)$$

where $\pm 8$ is + if $n$ is congruent to 0 or 2 mod 8 and – otherwise.

9 The infinite mass

In this section, we calculate the infinite masses. We begin by describing the distribution of $\delta$ among the different $A$ slices as in [32].

Definition 88. Let $\delta \in T(r_2)$. Define $\Omega_-(\delta)$ to be the number of negative eigenvalues of the first component of the orbit associated to $\delta$.

Theorem 89 (Signature distribution of first components of $T(r_2)$). If $r_1 > 0$, the number of $\delta$ in $T(r_2)$ such that $\Omega_-(\delta) = q$ is

$$\left(\frac{r_1}{q-r_2}\right).$$

In particular, if $q < r_2$, there are no $\delta \in T(r_2)$ which land in any $V_A$ for which $A$ has signature $(n-q,q)$. If $r_1 = 0$, there are 2 orbits which both land on the split slice.

Proof. The proof is the same as in [32].

To make the final calculation more transparent, we state the relation between the value of $\Omega_-(\cdot)$ and the Hasse–Witt symbol. We also obtain a couple of useful combinatorial identities.

If $n \equiv 0 \pmod{4}$, we are considering real bilinear forms with determinant 1. Among those, the ones which satisfy $\Omega(\delta) \equiv 0 \pmod{4}$ have Hasse–Witt symbol 1, while those which satisfy $\Omega(\delta) \equiv 2 \pmod{4}$ have Hasse–Witt symbol $-1$.

If $n \equiv 2 \pmod{4}$, we are considering real bilinear forms with determinant $-1$. Among those, the ones which satisfy $\Omega(\delta) \equiv 1 \pmod{4}$ have Hasse–Witt symbol 1, while those which satisfy $\Omega(\delta) \equiv 3 \pmod{4}$ have Hasse–Witt symbol $-1$.

We now define the infinite mass of an integral quadratic form $A \in \mathcal{L}_Z$ to be the number of $\delta \in T(r_2)$ whose associated orbit in $V$ intersects $V_A$ non-trivially.
Definition 90 (The infinite mass). Let \( A \in \mathcal{L}_\mathbb{Z} \) and \( r_2 \) be an integer such that \( 0 \leq r_2 \leq \frac{n-1}{2} \). The infinite mass of \( A \) with respect to \( r_2 \) is defined to be

\[
m_\infty(r_2, A) = \sum_{\delta \in T(r_2)} \chi_A(\delta).
\]

Above, we found that these infinite masses were equal to specific binomial coefficients. We now compute closed forms for certain total infinite masses arising when summing infinite masses over genera having the same 2-adic reduction.

Definition 91 (The total infinite mass). Let \( \mathcal{G}_2 \) be set of equivalence classes of unimodular bilinear forms over \( \mathbb{Z}_2 \) of dimension \( n \). Then \( \mathcal{G}_2 = \{ \mathcal{M}_{-1}, \mathcal{M}_1, \mathcal{M}_{\text{Type II}} \} \) where \( \mathcal{M}_{-1} \) and \( \mathcal{M}_1 \) are the odd unimodular forms with Hasse–Witt symbol \(-1\) and \(1\) respectively (canonical representative were described in the last section) and \( \mathcal{M}_{\text{Type II}} \) is simply the bilinear form with \(1\) on the anti-diagonal. Note that \( \mathcal{M}_{\text{Type II}} \) has Hasse–Witt symbol \(1\) if \( n \equiv 0, 2 \) (mod 8) and \(-1\) if \( n \equiv 4, 6 \) (mod 8). The total infinite mass, \( c_\infty(r_1, M) \), associated to an element \( M \in \mathcal{G}_2 \) is defined to be the sum of the infinite masses over all genera whose \( \mathbb{Z}_2 \) reduction coincides with \( M \).

Calculating the total infinite mass now becomes a question of evaluating sums of binomial coefficients in arithmetic progression.

Corollary 92. The infinite masses are as follows:

\[
c_\infty(r_1, \mathcal{M}_1) = 2^{r_1-2} \pm 8 2^{\frac{r_1-2}{2}}
\]

\[
c_\infty(r_1, \mathcal{M}_{-1}) = 2^{r_1-2} \mp 8 2^{\frac{r_1-2}{2}}.
\]

where \( \pm 8 \) is + if \( n \) is congruent to 0 or 2 (mod 8) and − otherwise. Furthermore, \( c_\infty(r_1, \mathcal{M}_{\text{Type II}}) = c_\infty(r_1, \mathcal{M}_1) \) if \( n \equiv 0, 2 \) (mod 8) and \( c_\infty(r_1, \mathcal{M}_{\text{Type II}}) = c_\infty(r_1, \mathcal{M}_{-1}) \) if \( n \equiv 4, 6 \) (mod 8).

10 Statistical consequences

We now pool together the elements assembled in the previous sections to compute the averages. We treat the cases \( r_1 = 0 \) and \( r_1 > 0 \) separately starting with totally imaginary orders. For simplicity, we present the computation for fields which are non-evenly ramified at all primes \( p \). We state the general theorem in the last subsection.

10.1 Oriented class group averages for non-evenly ramified totally imaginary fields

\[
\sum_{0 \leq b < n} \frac{2^{r_2} |\text{Cl}_2^+(\mathcal{O})| - |\mathcal{I}_2^+(\mathcal{O})|}{\left( \sum_{0 \leq b < n} \text{Vol}(U_{1, b}^+(\mathbb{R})) \right) \prod_p \text{Vol}(S_p)} + o(1).
\]

Now, by the preceding sections, we know that this sum is equal to:

\[
\sum_{0 \leq b < n} \sum_{\delta \in T(r_2)} \sum_{A \in \mathcal{L}_\mathbb{Z}} N_H(\mathcal{V}(A^\delta_{A, b}), X)
\]

\[
= \left( \sum_{0 \leq b < n} \text{Vol}(U_{1, b}^+(\mathbb{R})) \right) \prod_p \text{Vol}(S_p).
\]
Expanding, we find:

\[
\sum_{\delta \in T(r_2)} \sum_{A \in L_2} \frac{2}{\sigma(r_2)} \chi_A(\delta) \text{Vol}(\mathcal{F}_A) \prod_{p} \text{Vol}(SO_A(\mathbb{Z}_p)) \prod_{p \neq 2} m_p(A) \frac{\int_{f \in S_2} m_2(f, A) df}{\text{Vol}(S_2)}.
\]

The indicator functions come into play at this point.

\[
= \sum_{\delta \in T(r_2)} \sum_{A \in L_2} \frac{2}{\sigma(r_2)} \chi_A(\delta) \text{Vol}(\mathcal{F}_A) \prod_{p} \text{Vol}(SO_A(\mathbb{Z}_p)) \frac{\int_{f \in S_2} m_2(f, A) df}{\text{Vol}(S_2)}
\]

We now break up the collection $L_2$ into genera and sum over the forms in each genus separately before summing over the distinct genera. Since, both the characteristic function and the $p$-adic masses are constant over the forms in a single genus, they factor out of the inner sum.

\[
= \sum_{\delta \in T(r_2)} \sum_{\mathcal{G} \in L_2} \sum_{A \in G} \frac{2}{\sigma(r_2)} \chi_A(\delta) \text{Vol}(\mathcal{F}_A) \prod_{p} \text{Vol}(SO_A(\mathbb{Z}_p)) \frac{\int_{f \in S_2} m_2(f, A) df}{\text{Vol}(S_2)}
\]

Now, the inner sum gives the Tamagawa number of the special orthogonal group of an integral form in a genus. It is known to always be equal 2, see for instance [25] and [19]. We denote it by $\tau(SO)$.

\[
= \tau(SO) \sum_{\delta \in T(r_2)} \sum_{\mathcal{G} \in L_2} \frac{2}{\sigma(r_2)} \chi_{\mathcal{G}}(\delta) \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\text{Vol}(S_2)}
\]

At this point, we simplify the sum using the fact that $\sigma(r_2) = \frac{1}{2^{r_2-1}}$, the value of the 2-adic mass, the value of the infinite mass, and the classification of genera of unimodular integral quadratic forms as it appears in [12] or [17].

\[
= \frac{\tau(SO)}{2^{r_2-1}} \sum_{\delta \in T(r_2)} \sum_{\mathcal{G} \in L_2} \chi_{\mathcal{G}}(\delta) \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\text{Vol}(S_2)}
\]

\[
= \frac{\tau(SO)}{2^{r_2-1}} \sum_{\mathcal{G} \in L_2} \left( \frac{\int_{f \in S_2} m_2(f, \mathcal{G}) df}{\text{Vol}(S_2)} \sum_{\delta \in T(r_2)} \chi_{\mathcal{G}}(\delta) \right)
\]

\[
= \frac{\tau(SO)}{2^{r_2-1}} \left( c_2(M_1) \sum_{k \geq 0} \left( \frac{n}{4k} \right) + c_2(M_{-1}) \sum_{k \geq 0} \left( \frac{n}{4k + 2} \right) \right)
\]

\[
= \frac{\tau(SO)}{2^{r_2-1}} \left( c_2(M_1)c_{\infty,0} + c_2(M_{-1})c_{\infty,2} \right)
\]

Now, these values being known from previous sections, we substitute them and simplify.

\[
= \frac{1}{2^{r_2-1}} \cdot 4 \left( 2^{n-2} + \frac{2n^2}{4} \right)
\]
Therefore, since there are no units of negative norm for totally imaginary fields, the 2 torsion in the oriented class group is twice as large as the 2 torsion in the class group, we find that the average number of 2 torsion elements in the class group of totally imaginary fields of even degree at least 4 is:

\[
\text{Avg}(\text{Cl}_2, \text{totally imaginary}) = 1 + \frac{3}{2^{r_2}}.
\]

### 10.2 Oriented class group averages for non-evenly ramified not totally imaginary fields

The computation for \( r_1 > 0 \) proceeds in a similar way.

\[
\sum_{\mathcal{O} \in \mathfrak{B}_1} |\mathcal{H}^*(\mathcal{O})| - |\mathcal{I}^*_2(\mathcal{O})| \left( \sum_{0 \leq b < n} \text{Vol}(U_{1,b}^2(\mathbb{R}))_{<X} \right) \prod_p \text{Vol}(S_p) + o(1).
\]

Now, by the preceding sections, we know that this sum is equal to:

\[
\sum_{0 \leq b < n} \sum_{\delta \in \mathcal{T}(r_2)} \sum_{A \in \mathcal{Z}_2} N_H(\mathcal{V}(A^b_{A,b}), X) \left( \sum_{0 \leq b < n} \text{Vol}(U_{1,b}^2(\mathbb{R}))_{<X} \right) \prod_p \text{Vol}(S_p).
\]

Expanding, we find:

\[
= \sum_{\delta \in \mathcal{T}(r_2)} \sum_{A \in \mathcal{Z}_2} \frac{2}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(\mathbb{Z}_p)) \prod_{p \neq 2} m_p(A) \frac{\int_{f \in S_2} m_2(f, A) df}{\text{Vol}(S_2)}.
\]

The indicator functions come into play at this point.

\[
= \sum_{\delta \in \mathcal{T}(r_2)} \sum_{A \in \mathcal{Z}_2} \frac{2}{\sigma(r_2)} \chi_A(\delta) \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(\mathbb{Z}_p)) \frac{\int_{f \in S_2} m_2(f, A) df}{\text{Vol}(S_2)}
\]

We now break up the collection \( \mathcal{Z}_2 \) into genera and sum over the forms in each genus separately before summing over the distinct genera. Since, both the characteristic function and the \( p \)-adic masses are constant over the forms in a single genus, they factor out of the inner sum.

\[
= \sum_{\delta \in \mathcal{T}(r_2)} \sum_{G \in \mathcal{G}} \sum_{A \in G \cap \mathcal{Z}_2} \frac{2}{\sigma(r_2)} \chi_A(\delta) \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(\mathbb{Z}_p)) \frac{\int_{f \in S_2} m_2(f, A) df}{\text{Vol}(S_2)} \left( \sum_{A \in G \cap \mathcal{Z}_2} \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(\mathbb{Z}_p)) \right)
\]

\[
= \frac{1}{2^{r_2-1}} \cdot 4 \left( 2^{2r_2-2} + 2^{r_2-1} \right) = 2(2^{r_2} + 2)
\]
Now, the inner sum gives the Tamagawa number of the special orthogonal group of an integral form in a genus. It is known to always be equal 2, see for instance \cite{25} and \cite{17}. We denote it by $\tau(\text{SO})$.

$$
= \tau(\text{SO}) \sum_{\delta \in \mathcal{T}(r_2)} \sum_{G \in \mathbb{G}_2} \chi_{G}(\delta) \frac{\int_{f \in S_2} m_2(f, G) df}{\text{Vol}(S_2)}
$$

At this point, we simplify the sum using the fact that $\sigma(r_2) = \frac{1}{2^{r_1+r_2}-1}$, the value of the 2-adic mass, the value of the infinite mass, and the classification of genera of unimodular integral quadratic forms as it appears in \cite{12} or \cite{17}.

$$
= \frac{2\tau(\text{SO})}{2^{r_1+r_2-1}} \sum_{\delta \in \mathcal{T}(r_2)} \sum_{G \in \mathbb{G}_2} \chi_{G}(\delta) \frac{\int_{f \in S_2} m_2(f, G) df}{\text{Vol}(S_2)}
$$

$$
= \tau(\text{SO}) \frac{2^{r_1+r_2-2}}{2^{r_1+r_2-2}} \sum_{G \in \mathbb{G}_2} \left( \sum_{\delta \in \mathcal{T}(r_2)} \chi_{G}(\delta) \frac{\int_{f \in S_2} m_2(f, G) df}{\text{Vol}(S_2)} \right)
$$

$$
= \tau(\text{SO}) \frac{2^{r_1+r_2-2}}{2^{r_1+r_2-2}} \left( c_2(\mathcal{M}_1) \sum_{k \geq 0} \left( \frac{n}{4k} \right) + c_2(\mathcal{M}_1-1) \sum_{k \geq 0} \left( \frac{n}{4k+2} \right) \right)
$$

$$
= \tau(\text{SO}) \frac{2^{r_1+r_2-2}}{2^{r_1+r_2-2}} \left( c_2(\mathcal{M}_1)c_{\infty,0} + c_2(\mathcal{M}_1-1)c_{\infty,2} \right)
$$

Now, these values being known from previous sections, we substitute them and simplify.

$$
= \frac{1}{2^{r_1+r_2-2}} \cdot 2 \left( (2^{n-2} \pm_8 2^{n-2})(2^{r_1-2} \pm_8 2^{r_1-2}) + (2^{n-2} \mp_8 2^{n-2})(2^{r_1-2} \mp_8 2^{r_1-2}) \right)
$$

$$
= \frac{1}{2^{r_1+r_2-2}} \cdot 2 \cdot 2 \left( 2^{n+r_1-4} + 2^{n+r_1-4} \right)
$$

$$
= 8 \left( 2^{r_1+r_2-3} + 2^{-1} \right)
$$

$$
= 2^{r_1+r_2} + 4
$$

Therefore, this leads to the following formula for average 2-torsion in the oriented class group of non-evenly ramified fields with at least one real embedding:

$$
\text{Avg}(\text{Cl}_2) = 1 + \frac{3}{2^{r_1+r_2-1}}
$$

10.3 General oriented class group averages

For simplicity, we carried out the calculations of the previous subsections under the assumption that there was no even ramification. In general, even ramification increases the mass at $p \neq 2$ from 1 to 2. If we take this into account, the computations of the previous section carry through with an additional term which captures this increase in total mass.

**Definition 93.** Let $\mathcal{R} \subset \mathcal{R}^{r_1 \cdot r_2}$ be a family of rings (unramified at 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$. We define the even ramification density at $p$, $r_p(\mathcal{R})$, as the density in $\Sigma_p$ of elements of $\Sigma_p$ which are evenly ramified at $p$. 37
We obtain the following averages by calculating as above.

**Theorem 94** (General Averages for the oriented class group). Let $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}$ be a family of rings (unramified at 2) corresponding to an acceptable family of local specifications $\Sigma = (\Sigma_p)_p$ and let $r_p(\mathfrak{R})$ denotes its even ramification density at $p$.

If $r_1 = 0$, the average number of 2-torsion elements in the oriented class group over $\mathfrak{R}$ is given by:

$$
\text{Avg}(\text{Cl}^2_\mathfrak{R}) = 2 \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \left( 1 + \frac{2}{2^{r_1}} + \frac{2}{2^{r_2}} \right).
$$

If $r_1 > 0$, the average number of 2-torsion elements in the oriented class group over $\mathfrak{R}$ is given by:

$$
\text{Avg}(\text{Cl}^2_\mathfrak{R}) = \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \left( 1 + \frac{2}{2^{r_1+r_2-1}} + \frac{1}{2^{r_1+r_2-1}} \right).
$$

**Remark 95.** A priori, we have to be careful about summing over the $b$ because the even ramification densities at different values of $b$ might be different. However, this occurs only at primes $p$ which divide $n$. For those finitely many primes, the quantity $\sum_{0 \leq b \leq n-1} \prod_{p|n} (1 + r_{p,b}(\mathfrak{R}))$ when expanded is a finite sum of densities, which can then be factored again to give $\prod_{p|n} (1 + r_p(\mathfrak{R}))$. The same considerations apply to the final calculations in the next section. (Thanks to Ashvin Swaminathan and Arul Shankar for pointing out this issue and telling me how to fix it).

## 11 Averages for the class group and narrow class group

We can handle the question of computing the average number of 2-torsion elements in the usual class group by looking at $\text{SL}_n^\pm$-orbits. The catch is that to get a torsor of the full class group, we must capture ideals with the property that $I^2 = (\alpha)$ with $\alpha \in K^\times$ and $N(\alpha) < 0$ in the rigid parametrisation. But those occur when we consider $-f$ instead of our monic $f$. Of course, this now introduces potential double-counting for rings that have a unit of negative norm. But this is offset by the fact that the fibre space $((R_f^r)_{N=\pm 1})/((R_f^r)^2)$ is half as large when $R_f$ has a unit of negative norm as opposed to when it does not. We therefore recover the result of [36] that the set of pairs $(A, B)$ with resolvent polynomial equal to $\pm f$ is an extension by $R_f^r/(R_f^r)^2$ of a torsor of the 2-torsion in the class group of $R_f$.

We explain the parametrisation in more detail.

### 11.1 Rigid parametrisation by pairs of symmetric bilinear forms

Let $T$ be a principal ideal domain. Recall once again the rigid parametrisation of the pairs of bilinear forms $(A, B) \in V(T)$ with resolvent polynomial equal to $f$ in terms of the based fractional ideal data for $R_f$.

**Theorem 96** ([36]). Take a non-degenerate binary $n$-ic form $f \in U(T)$ and let $R_f = \frac{T[x]}{(j(2x))}$. Then the pairs symmetric bilinear forms $(A, B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples

$$(I, B, \delta)$$

where $I \subset K_f$ is a based fractional ideal of $R_f$ with basis $B$ given by a $T$ module isomorphism $B: I \to T^n$, $\delta \in K_f^\times$ such that $I^2 \subset \delta R_f^{n-3}$ as ideals and the norm equation holds $N(I)^2 = N(\delta)N(R_f^{n-3})$
(as based ideals). Two triples \((I, B, \delta)\) and \((I', B', \delta')\) are equivalent if there exists a \(\kappa \in K_f^*\) with the property that \(I = \kappa I', B \circ (\times \kappa) = B'\) and \(\delta = \kappa^2 \delta\).

11.2 \(SL_n^\pm(\mathbb{Z})\)-orbits and the class group

We now let \(SL_n^\pm(\mathbb{T})\) act on \(V\) by change of basis. This action corresponds, at the level of equivalence classes of triples \((I, B, \delta)\), to the action of \(SL_n^\pm(\mathbb{T})\) on the basis \(B\) of the fractional ideal \(I\). This action only changes the basis and does not change \(I\) nor \(\delta\). In particular, it does not change the defining conditions:

1. \(I^2 \subset \delta R_f^{n-3}\)
2. \(N(I)^2 = N(\delta)N(R_f^{n-3})\)

Indeed, acting by an element of \(SL_n^\pm(\mathbb{T})\) with negative determinant reverses the orientation of the ideal \(I\), but since the second condition only depends on \(N(I)^2\), this is immaterial.

The rigid parametrisation can be reformulated to describe \(SL_n^\pm(\mathbb{Z})\) orbits.

**Theorem 97.** Let \(f\) be a non-degenerate monic binary \(n\)-ic form \(f \in U_1(\mathbb{Z})\), let \(R_f = \mathbb{Z}[x]/(f)\) and \(K_f = R_f \otimes \mathbb{Q}\). The \(SL_n^\pm(\mathbb{Z})\) orbits on pairs symmetric bilinear forms \((A, B) \in V(\mathbb{Z})\) with \(f_{(A,B)} = f\) are in bijection with equivalence classes of pairs

\[
(I, \delta)
\]

where \(I \subset K_f\) is a fractional ideal of \(R_f\), and \(\delta \in K_f^*\) is such that \(I^2 \subset \delta R_f\) as ideals and the norm equation \(N(I)^2 = N(\delta)\) holds (this is the norm of \(\delta\) as an ideal). Two pairs \((I, \delta)\) and \((I', \delta')\) are equivalent if there exists a \(\kappa \in K_f^*\) with the property that \(I = \kappa I'\) and \(\delta = \kappa^2 \delta'\).

We now describe the relation between \(SL_n^\pm(\mathbb{Z})\) orbits on \(\pi^{-1}(\pm f) \subset V(\mathbb{Z})\) and the 2-torsion part of the class group of \(R_f\).

**Definition 98.** A pair \((I, \delta)\) is said to be projective if the ideal \(I\) is invertible. Equivalently, a pair \((I, \delta)\) is projective if \(I^2 = (\delta)\). For an \(S_n\) order \(\mathcal{O}\), we write \(H(\mathcal{O})\) for the set of oriented projective pairs on \(\pi^{-1}(\pm f) \subset V(\mathbb{Z})\).

As the oriented class group is comprised of invertible oriented ideals, let us consider the restriction of the parametrisation above to the set \(H(\mathcal{O})\). Consider the forgetful map:

\[H(\mathcal{O}) \rightarrow Cl_2(\mathcal{O}).\]

Elements \((I_0, \delta_0)\) in the kernel of this forgetful map are such that \(I_0^2 = (\delta)\) and \(N(\delta_0) = \pm N(I_0)^2\) and have the property that \(I_0 = (\alpha)\) for some \(\alpha \in K\) as ideals. Thus, \((I_0, \delta_0) \sim (\langle \alpha \rangle, \delta_0) \sim (\mathcal{O}, \alpha^{-2} \delta_0)\).

Now, \(\mathcal{O} \subset \alpha^{-2} \delta_0 \mathcal{O}\) and \(\pm 1 = N(\alpha^{-2} \delta_0)\). This implies that \((I_0, \delta_0)\) is equivalent to \((\mathcal{O}, u)\) where \(u\) is norm \(\pm 1\) unit of \(\mathcal{O}^*\). We are allowed to mod out \(u\) by squares of elements of \(K^*\) which fix the ideal \(\mathcal{O}\). But those are precisely the units of \(\mathcal{O}\). The sequence above can thus be completed to a short exact sequence:

\[
1 \rightarrow \frac{\mathcal{O}^*}{(\mathcal{O}^*)^2} \rightarrow H(\mathcal{O}) \rightarrow Cl_2(\mathcal{O}) \rightarrow 1.
\]
Applying Dirichlet’s unit theorem allows us to compute that 100% of the time (since having non-trivial torsion is rare):

\[
\left| \frac{O^\times}{(O^\times)^2} \right| = 2^{r_1+r_2}.
\]

We thus obtain the following formula for the number of elements in \(H(O)\).

**Lemma 99.** Let \(O\) be an order in an \(S_n\)-number field of degree \(n\) and signature \((r_1, r_2)\). Then:

\[
|H(O)| = 2^{r_1+r_2} |\text{Cl}_2(O)|.
\]

We can also say something about the narrow class group in this context. The proof that the fibres have the right size is exactly the same as in [22].

**Lemma 100.** if \(H^+(O)\) denotes the subgroup of \(H(O)\) consisting of pairs \((I, \delta)\) such that \(\delta\) is positive under every real embedding of the fraction field of \(O\), then

\[
|H^+(O)| = 2^{r_2} |\text{Cl}_2^+(O)|.
\]

We now proceed to the description of the points in the cuspidal regions.

**Lemma 101** (Even degree distinguished orbits lemma). \((A, B) \in V(Q)\) is distinguished if and only if there is an \(\text{SL}_n^\pm(Q)\) translate of \((A, B)\) with the property that

\[
a_{i,j} = b_{i,j} = 0
\]

for all \(1 \leq i, j \leq \frac{n}{2}\) except for \(i = j = \frac{n}{2}\) for which \(a_{\frac{n}{2}, \frac{n}{2}} = 0 \neq b_{\frac{n}{2}, \frac{n}{2}}\).

**Definition 102.** Let \(O\) be an order. We denote by \(I_2(O)\) the 2-torsion subgroup of the ideal group of \(O\).

**Proposition 103.** Let \(O_f\) be an order corresponding to the integral primitive irreducible non-degenerate monic binary form \(f\). Then, \(I_2(O_f)\) is in natural bijection with the set of projective reducible \(\text{SL}_n^\pm(Z)\)-orbits on \(V(Z) \cap \pi^{-1}(f)\).

**SL\(_n\)**-orbits over fields and local rings

In this section, we compute the number orbits, and the size of the stabilisers for the action of \(\text{SL}_n\) on the arithmetic rings \(Z_p, Q,\) and \(R\). Let \(T\) be a principal ideal domain. We first restate the rigid parametrisation in this case.

**Theorem 104** ([6]). Let \(f\) be a non-degenerate monic binary \(n\)-ic form \(f \in U_1(T)\), let \(R_f = \frac{T[x]}{(f(x))}\) and \(K_f = R_f \otimes Z Q\). The \(\text{SL}_n^\pm(T)\) orbits on pairs symmetric bilinear forms \((A, B) \in V(T)\) with \(f_{(A, B)} = f\) are in bijection with equivalence classes of pairs

\[
(I, \delta)
\]

where \(I \subset K_f\) is a fractional ideal of \(R_f\) and \(\delta \in K_f^\times\) such that \(I^2 \subset \delta R_f\) as ideals and the norm equation \(N(I)^2 = N(\delta)\) holds. Two pairs \((I, \delta)\) and \((I', \delta')\) are equivalent if there exists a \(\kappa \in K_f^\times\) with the property that \(I = \kappa I'\) and \(\delta = \kappa^2 \delta'\).

Then, we have the following theorem whose proof is straightforward.
Lemma 105. The stabiliser in $\text{SL}_n^\pm(T)$ corresponds to the 2-torsion of $R_f^\times$: 

$$R_f^\times[2].$$

Remark 106. It follows that the $\text{SL}_n^\pm(\mathbb{Q})$ stabiliser of any element $v$ whose resolvent is irreducible is equal to 2.

Just as in [22], we can compute the number of orbits with the caveat that we need to distinguish the case where $f$ has an odd degree factor from the case where all the factors of $f$ are even.

Lemma 107. Let $T$ be a field or $\mathbb{Z}_p$. Let $f$ be a monic separable, non-degenerate binary form in $U_1(T)$. Then the projective $\text{SL}_n(T)$ orbits of $V(T)$ with resolvent $\pm f$ are in bijection with elements of

$$(R_f^\times/(R_f^\times)^2)_{N\equiv\pm1}.$$

Remark 108. We now describe the real orbits in the case where the leading coefficient of $f$ is 1 and in the case where the leading coefficient is $-1$. Suppose that $f$ is a non-degenerate polynomial of degree $n$ with $r_1$ real roots and $2r_2$ complex roots. First, suppose that the leading coefficient of $f$ is $-1$. If $r_1 = 0$ there are no real orbits while if $r_1 > 0$, there are $2^{r_1-1}$ orbits and the stabiliser has size $2^{r_1+r_2}$. Now, suppose that the leading coefficient of $f$ is 1. If $r_1 = 0$, there is 1 real orbit while if $r_1 > 0$, there are $2^{r_1-1}$ real orbits. In both cases, the stabiliser has size $2^{r_1+r_2}$.

Now, instead of considering $\text{SO}_A$ orbits, we think $\text{O}_A$ orbits. Then the reduction theory, the cusp cutoff, the sieve, as well as the change of variable formula carry through precisely as above. We, therefore, obtain the following proposition.

Proposition 109. We have

$$\text{Vol}(\mathcal{F}_A \cdot R_A^{R_2,\delta}(X)) = \chi_A(\delta) |\mathcal{J}_A| \text{Vol}(\mathcal{F}_A) \text{Vol}(U(\mathbb{R})^2_{n<\infty}).$$

Let $S_p \subset U_{1,b}(\mathbb{Z}_p)$ be a closed subset whose boundary has measure 0. Consider the set $\Lambda(A)_p = V_{A,b}(\mathbb{Z}_p) \cap \pi^{-1}(S_p)$. Then we have

$$\text{Vol}(\Lambda(A)(p)) = |\mathcal{J}_A| \text{Vol}(O_A(\mathbb{Z}_p)) \int_{f \in S_p} m_p(f, A) \, df$$

where

$$m_p(f, A) := \frac{1}{\#\text{Stab}_{O_A(\mathbb{Z}_p)}(v)} \sum_{v \in V_{A,b}(\mathbb{Z}_p) \cap \pi^{-1}(f)} \frac{1}{O_A(\mathbb{Z}_p)}.$$

The computation of the total local mass could be slightly more delicate since we need to differentiate the case of $f$ having leading coefficient $\pm 1$. We treat this in detail in the next subsection.

11.3 The product of local volumes and the local mass

The total mass for the case where $f$ has leading coefficient 1 is the following.

Lemma 110 (+1 total mass). Let $R$ be a non-degenerate ring of degree $n$ over $\mathbb{Z}_p$. Let $N$ denote the norm map from $N: R^\times/(R^\times)^2 \to \mathbb{Z}_p^\times/(\mathbb{Z}_p)^2$. Then the quantity

$$\frac{|(R^\times/(R^\times)^2)_{N\equiv1}|}{|R^\times|^{2n}}$$

is equal to $\frac{1}{|N(R^\times)|}$ if $p \neq 2$ and to $\frac{2^n}{|N(R^\times)|}$ if $p = 2$. 

41
The total mass for the case where \( f \) has leading coefficient \(-1\) is the following.

**Lemma 111** \((-1\) total mass\). Let \( R \) be a non-degenerate ring of degree \( n \) over \( \mathbb{Z}_p \). Let \( N \) denote the norm map from \( N: R^\times/(R^\times)^2 \to \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \). The quantity

\[
\frac{|(R^\times/(R^\times)^2)_{N \equiv -1}|}{|R^\times|^2}
\]

is equal to 0 if \(-1\) is not in the image of \( N \). Otherwise, it is equal to \( \frac{1}{|N(R^\times)|} \) if \( p \neq 2 \) and to \( \frac{2^n}{|N(R^\times)|} \) if \( p = 2 \).

**Proof.** The fibres of a group homomorphism are either empty or are of the same size as the kernel. The size of the kernel was calculated in the previous lemma.

In particular, we get the following statement concerning the total local masses for maximal rings which not evenly ramified at 2.

**Lemma 112.** The total local mass for \( f \in \mathbb{Z}_p[x] \) maximal and not evenly ramified is given by:

\[
m_p^\pm(f) = \begin{cases} 
2^{n-2} & \text{if } p = 2 \\
\frac{1}{2} & \text{if } p \neq 2
\end{cases}
\]

The total local mass for \( f \in \mathbb{Z}_p[x], p \neq 2 \), maximal and evenly ramified is given by:

\[
m_p^+(f) = 1
\]

\[
m_p^-(f) = \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4 \\
0 & \text{if } p \equiv 3 \mod 4
\end{cases}
\]

**Proof.** \(-1\) is not in the image of the norm map when \( f \) is maximal and evenly ramified at \( p \equiv 3 \mod 4 \).

\[\square\]

### 11.4 Distribution of total local masses among genera

The distribution techniques work well here. As soon as the total mass is known, knowing the local mass for each genus is straightforward easy. We note the results here.

Let \( p \neq 2 \). Then, up to \( \text{SL}_n^\pm(\mathbb{Z}_p) \) equivalence, there is a unique bilinear form of determinant 1 and a unique bilinear form of determinant \(-1\). Both have Hasse-Witt symbol equal to 1. Therefore, the local masses are the same as before.

The computation of the local masses at \( p = 2, \infty \) is more delicate and is treated in the next to subsections.

### 11.5 Point count and the 2-adic masses

For \( p = 2 \), up to \( \text{SL}_n^\pm(\mathbb{Z}_2) \) equivalence, there are 3 quadratic forms of determinant 1 and 2 quadratic forms of determinant \(-1\). By restricting to rings which are not evenly ramified at 2, we eliminate one of the forms of determinant 1.
For \( n \equiv 0 \mod 4 \) we can take:

\[
\mathcal{M}_1^+ = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix},
\mathcal{M}_1^- = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix}.
\]

\[
\mathcal{M}_1 = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix},
\mathcal{M}_1^- = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix}.
\]

For \( n \equiv 2 \mod 4 \) we can take:

\[
\mathcal{M}_1^+ = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix},
\mathcal{M}_1^- = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix}.
\]

\[
\mathcal{M}_1 = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix},
\mathcal{M}_1^- = \begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix}.
\]

The superscripts indicate the sign of \((-1)_{2^n} \det(\cdot)\) and the subscripts indicate the Hasse-Witt symbol.

Now, the argument proceeds just as before except that now the octane values of \( \mathcal{M}_1^- \) and \( \mathcal{M}_1^- \) are now \( \pm 2 \mod 8 \). This means that the volumes of the respective orthogonal groups are equal and thus that the masses at 2 are equal! We summarise the numbers in the following lemma.

**Corollary 113.** The 2-adic masses are:

\[
c_2(n, \mathcal{M}_1^+) = \frac{1}{2} \left( 2^{n-2} \pm 8 \frac{2^{n-2}}{2} \right) \text{Vol}(S_2)
\]

\[
c_2(n, \mathcal{M}_1^-) = \frac{1}{2} \left( 2^{n-2} \mp 8 \frac{2^{n-2}}{2} \right) \text{Vol}(S_2)
\]

\[
c_2(n, \mathcal{M}_1) = \frac{1}{2} (2^{n-2}) \text{Vol}(S_2)
\]

\[
c_2(n, \mathcal{M}_1^-) = \frac{1}{2} (2^{n-2}) \text{Vol}(S_2)
\]

where \( \pm 8 \) is + if \( n \) is congruent to 0 or 2 mod 8 and − otherwise.
11.6 The infinite masses

We assume that \( r_1 > 0 \) since the totally imaginary case was already covered. Since the 2-adic masses for leading coefficient \(-1\) are equal across genera, we will only need to know the total infinite mass, which is \( 2^{r_1 - 1} \).

11.7 Statistical consequences

We now pool together the elements assembled in the previous subsections to compute the averages.

The computation basically carries through as above. In order to deal with the Tamagawa number and the half-integral local masses (which at first might seem to multiply to 0), one needs to use the following facts. If \( G \) denotes a genus, then we have the following identity of local volumes:

\[
\text{Vol}(O_A(\mathbb{Z})) = 2\text{Vol}(SO_A(\mathbb{Z})),
\]

\[
\sum_{A \in G} \text{Vol}(O_A(\mathbb{Z}) \setminus O_A(\mathbb{R})) \prod_p \text{Vol}(SO_A(\mathbb{Z})) = 2,
\]

where the sum is over all \( \text{SL}_n^\pm(\mathbb{Z}) \) equivalence classes of integral representatives in \( G \).

We now proceed with the computation.

**Definition 114.** Let \( \mathcal{R} \subset \mathcal{R}^{r_1,r_2} \) be a family of rings (unramified at 2) corresponding to an acceptable family of local specifications \( \Sigma = (\Sigma_p)_p \). We define the even ramification density at \( p \), \( r_p(\mathcal{R}) \), as the density in \( \Sigma_p \) of elements of \( \Sigma_p \) which are evenly ramified at \( p \).

Let \( \mathcal{L}_Z^+ \) denote a set of representatives of integral bilinear forms of determinant 1 under the action of \( \text{SL}_n^\pm(\mathbb{Z}) \) and let \( \mathcal{L}_Z^- \) denote a set of representatives of integral bilinear forms of determinant \(-1\) under the action of \( \text{SL}_n^\pm(\mathbb{Z}) \). Denote by \( G_Z^+ \) the set of genera of quadratic \( n \)-ary forms containing an integral element of determinant 1 and denote by \( G_Z^- \) the set of genera of quadratic \( n \)-ary forms containing an integral element of determinant \(-1\). Notice that \( G_Z^+ \) partitions \( \mathcal{L}_Z^+ \) and that \( G_Z^- \) partitions \( \mathcal{L}_Z^- \).

Now, by the preceding sections, we know that this sum is equal to:

\[
\sum_{0 \leq b < n} \sum_{\delta \in \mathcal{T}(r_2)} N_H(V(\Lambda_{A,b}^\delta), X) = \left( \sum_{0 \leq b < n} \text{Vol}(U_{1,b}^\sigma(\mathbb{R})) \right) \prod_p \text{Vol}(S_p).
\]

Expanding, we find that the first sum is equal to:

\[
\sum_{\delta \in \mathcal{T}(r_2)} \sum_{A \in \mathcal{L}_Z^-} \frac{2}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A^\delta) \prod_p \text{Vol}(SO_A(\mathbb{Z}_p)) \prod_{p=1 \mod 4} (1+r_p(\mathcal{R})) \prod_{p=3 \mod 4} (1-r_p(\mathcal{R})) \int_{f \in S_2} 2m_2(f,A) df \frac{\text{Vol}(S_2)}{\text{Vol}(S_2)}.
\]
Expanding, we find that the second sum is equal to:

\[
\sum_{\delta \in T} \sum_{A \in \mathcal{L}_Z^-} \frac{2}{\sigma(r_2)} \text{Vol}(F_{A}) \prod_p \text{Vol}(	ext{SO}_A(Z_p)) \prod_{p \neq 2} (1 + r_p(\mathcal{R})) \frac{\int_{f \in S_2} 2|m_2(f, A)|df}{\text{Vol}(S_2)}.
\]

We can now process both of these sums separately just as we did before by breaking up \( \mathcal{L}_Z^- \) and \( \mathcal{L}_Z^+ \) into genera and then first summing within each genus and then across the different genera.

After this is done, the \( \mathcal{L}_Z^- \) sum becomes:

\[
\frac{2\tau(\text{SO})}{2^{r_1+r_2}} \left( 2c_2(n, \mathcal{M}^-_{1})c_{\infty,0} + 2c_2(n, \mathcal{M}^-_{-1})c_{\infty,2} \right) \left( \prod_{p \equiv 1 \mod 4} (1 + r_p(\mathcal{R})) \prod_{p \equiv 3 \mod 4} (1 - r_p(\mathcal{R})) \right)
\]

\[
= \frac{1}{2^{r_1+r_2-1}} \cdot 2 \cdot 2^{n-2} \cdot 2^{r_1-1} \cdot \left( \prod_{p \equiv 1 \mod 4} (1 + r_p(\mathcal{R})) \prod_{p \equiv 3 \mod 4} (1 - r_p(\mathcal{R})) \right)
\]

\[
= 2^{r_1+r_2-1} \left( \prod_{p \equiv 1 \mod 4} (1 + r_p(\mathcal{R})) \prod_{p \equiv 3 \mod 4} (1 - r_p(\mathcal{R})) \right)
\]

And the \( \mathcal{L}_Z^+ \) sum becomes:

\[
\frac{2\tau(\text{SO})}{2^{r_1+r_2}} \left( 2c_2(n, \mathcal{M}^+_{1})c_{\infty,0} + 2c_2(n, \mathcal{M}^+_{-1})c_{\infty,2} \right) \left( \prod_{p \neq 2} (1 + r_p(\mathcal{R})) \right)
\]

\[
= \frac{1}{2^{r_1+r_2-1}} \cdot 2 \cdot 2^{n-r_1-4} \cdot 2^{n+r_2-4} \cdot \left( \prod_{p \neq 2} (1 + r_p(\mathcal{R})) \right)
\]

\[
= (2^{r_1+r_2-1} + 2) \left( \prod_{p \neq 2} (1 + r_p(\mathcal{R})) \right)
\]

Therefore, we find the following formula for average 2-torsion in the class group of fields square-free at 2 with at least one real embedding:

\[
\text{Avg}(\text{Cl}_2, \mathcal{R}) = \frac{1}{2} \prod_{p \equiv 1 \mod 4} (1 + r_p(\mathcal{R})) \prod_{p \equiv 3 \mod 4} (1 - r_p(\mathcal{R})) + \prod_{p \equiv 3 \mod 4} (1 + r_p(\mathcal{R}))
\]

\[
+ \frac{1 + 2 \prod_{p \neq 2} (1 + r_p(\mathcal{R}))}{2^{r_1+r_2}}
\]

As a sanity check, note that \( \left( \prod_{p \equiv 3 \mod 4} (1 - r_p(\mathcal{R})) + \prod_{p \equiv 3 \mod 4} (1 + r_p(\mathcal{R})) \right) \geq 2 \), so the quantity above is always greater than 1.
The computation for the narrow class group is similar and gives us:

\[
\frac{\sum_{\mathcal{O} \in \mathcal{H}} 2^{r_2} |\text{Cl}_{2}^+(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\left( \sum_{0 \leq b < n} \text{Vol}(\mathcal{U}_{1,b}^+(\mathbb{R})) < \chi \right) \prod_p \text{Vol}(S_p)} + o(1)
\]

\[
= \frac{\sum_{0 \leq b < n} \sum_{G \in G_{\pm}} N_H(V(\Lambda_{A,b}^{\delta > 0}), X)}{\left( \sum_{0 \leq b < n} \text{Vol}(\mathcal{U}_{1,b}^+(\mathbb{R})) < \chi \right) \prod_p \text{Vol}(S_p)}
\]

\[
= \sum_{A \in \mathcal{A}_{\pm}^+} \frac{2}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(Z_p)) \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right) \frac{\int_{f \in S_2} 2m_2(f, A) df}{\text{Vol}(S_2)}
\]

\[
= \sum_{A \in \mathcal{A}_{\pm}^+} \frac{2}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(Z_p)) \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right) \frac{\int_{f \in S_2} 2m_2(f, A) df}{\text{Vol}(S_2)} \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right)
\]

\[
= \tau(\text{SO}) \sum_{G \in \mathcal{G}_G} \frac{2}{\sigma(r_2)} \text{Vol}(\mathcal{F}_A) \prod_p \text{Vol}(\text{SO}_A(Z_p)) \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right)
\]

\[
= \frac{2\tau(\text{SO})}{2^{r_1+r_2}} \sum_{G \in \mathcal{G}_G} \chi_G(\delta > 0) \frac{\int_{f \in S_2} 2m_2(f, G) df}{\text{Vol}(S_2)} \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right)
\]

\[
= \frac{1}{2^{r_1+r_2}} \cdot 2^{n-2} \left( 2^{n-2} + 2^{\frac{n-2}{2}} \right) \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right)
\]

\[
= \left( 2^{r_2} + 2^{r_2} \frac{2^{n-2}}{2^{n-2}} \right) \left( \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \right).
\]

Therefore, we find the following formula for average 2-torsion in the narrow class group of fields unramified at 2:

\[
\text{Avg}(\text{Cl}_{2}^+, \mathfrak{R}) = \prod_{p \neq 2} (1 + r_p(\mathfrak{R})) \left( 1 + \frac{2}{2^2} \right) + \frac{1}{2^{r_2}}.
\]

Note that for totally imaginary fields, the narrow class group is the same as the class group and that the formulas do agree in that case!
References

[1] Fabrizio Barroero and Martin Widmer. Counting lattice points and \( \mathcal{O} \)-minimal structures. *Int. Math. Res. Not. IMRN*, (18):4932–4957, 2014.

[2] Alex Bartel, Henri Johnston, and Hendrik W. Lenstra Jr. Galois module structure of oriented arakelov class groups, 2020.

[3] Alex Bartel and Hendrik W. Lenstra, Jr. On class groups of random number fields. *Proc. Lond. Math. Soc. (3)*, 121(4):927–953, 2020.

[4] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[5] Manjul Bhargava. Most hyperelliptic curves over \( \mathbb{Q} \) have no rational points, 2013.

[6] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits. In *Representations of reductive groups*, volume 312 of *Progr. Math.*, pages 139–171. Birkhäuser/Springer, Cham, 2015.

[7] Manjul Bhargava, Jonathan Hanke, and Arul Shankar. The mean number of 2-torsion elements in the class groups of \( n \)-monogenized cubic fields, 2020.

[8] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Squarefree values of polynomial discriminants i, 2016.

[9] Manjul Bhargava and Ila Varma. On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. *Duke Math. J.*, 164(10):1911–1933, 2015.

[10] Armand Borel. Ensembles fondamentaux pour les groupes arithmétiques. In *Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962)*, pages 23–40. Librairie Universitaire, Louvain; GauthierVillars, Paris, 1962.

[11] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[12] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[13] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[14] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[15] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.

[16] Henri Cohen and Jacques Martinet. Heuristics on class groups: some good primes are not too good. *Math. Comp.*, 63(207):329–334, 1994.
[17] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, second edition, 1993. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[18] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[19] Alex Eskin, Ze’ev Rudnick, and Peter Sarnak. A proof of Siegel’s weight formula. *Internat. Math. Res. Notices*, (5):65–69, 1991.

[20] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.

[21] Frank Gerth, III. The 4-class ranks of quadratic fields. *Invent. Math.*, 77(3):489–515, 1984.

[22] Wei Ho, Arul Shankar, and Ila Varma. Odd degree number fields with odd class number. *Duke Math. J.*, 167(5):995–1047, 2018.

[23] Burton W. Jones. A canonical quadratic form for the ring of 2-adic integers. *Duke Math. J.*, 11:715–727, 1944.

[24] Peter Koymans and Carlo Pagano. Higher genus theory. *International Mathematics Research Notices*, August 2020.

[25] R. P. Langlands. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 143–148. Amer. Math. Soc., Providence, R.I., 1966.

[26] Michael Lipnowski, Will Sawin, and Jacob Tsimerman. Cohen-Lenstra heuristics and bilinear pairings in the presence of roots of unity, 2020.

[27] Michael Lipnowski and Jacob Tsimerman. Cohen-Lenstra heuristics for étale group schemes and symplectic pairings. *Compos. Math.*, 155(4):758–775, 2019.

[28] Gunter Malle. On the distribution of class groups of number fields. *Experiment. Math.*, 19(4):465–474, 2010.

[29] P. Sawyer. Spherical functions on $\text{SO}_0(p,q)/\text{SO}(p)\times\text{SO}(q)$. *Canad. Math. Bull.*, 42(4):486–498, 1999.

[30] P. Sawyer. Computing the Iwasawa decomposition of the classical Lie groups of noncompact type using the $QR$ decomposition. *Linear Algebra Appl.*, 493:573–579, 2016.

[31] Arul Shankar and Xiaoheng Wang. Average size of the 2-selmer group of jacobians of monic even hyperelliptic curves. 2013.

[32] Artane Siad. Monogenic fields with odd class number part i: odd degree, in preparation.

[33] Alexander Smith. Governing fields and statistics for 4-selmer groups and 8-class groups, 2016.

[34] Weitong Wang and Melanie Matchett Wood. Moments and interpretations of the cohen-lenstra-martinet heuristics, 2019.
[35] Melanie Matchett Wood. Rings and ideals parameterized by binary \( n \)-ic forms. *J. Lond. Math. Soc. (2)*, 83(1):208–231, 2011.

[36] Melanie Matchett Wood. Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.*, 689:169–199, 2014.

[37] Melanie Matchett Wood. Cohen-Lenstra heuristics and local conditions. *Res. Number Theory*, 4(4):Paper No. 41, 22, 2018.

[38] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. *Amer. J. Math.*, 141(2):383–398, 2019.