



Universiteit
Leiden
The Netherlands

Enumerative arithmetic

Pagano, C.

Citation

Pagano, C. (2018, December 5). *Enumerative arithmetic*. Retrieved from <https://hdl.handle.net/1887/67539>

Version: Not Applicable (or Unknown)

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/67539>

Note: To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/67539> holds various files of this Leiden University dissertation.

Author: Pagano, C.

Title: Enumerative arithmetic

Issue Date: 2018-12-05

CHAPTER

2

4-Ranks and the general model for
statistics of ray class groups of imaginary
quadratic number fields

C. Pagano and E. Sofos

4-RANKS AND THE GENERAL MODEL FOR STATISTICS OF RAY CLASS GROUPS OF IMAGINARY QUADRATIC NUMBER FIELDS

C. PAGANO AND E. SOFOS

ABSTRACT. We use homological algebra to extend the Cohen–Lenstra heuristics to the setting of ray class groups of imaginary quadratic number fields, viewed as exact sequences of Galois modules. By asymptotically estimating the mixed moments governing the distribution of a cohomology map, we prove these conjectures in the case of 4-ranks.

CONTENTS

1. Introduction	25
2. Heuristics and conjectures for p odd	31
3. Heuristic and conjectures for $p = 2$	38
4. Special divisors and 4-rank	46
5. Main theorems on the 2-part of ray class sequences	50
6. Main theorems on special divisors	54
7. From the mixed moments to the distribution	63
References	65

1. INTRODUCTION

Let c be a positive odd square-free integer. Partition the set of its prime divisors, S , into $S_1 \cup S_3$, where if $l \in S_i$ then $l \equiv i \pmod{4}$. For an imaginary quadratic number field K , denote by $\text{Cl}(K, c)$ the ray class group of K of conductor c , and by $D(K)$ the discriminant of K . Let j_1 and j_2 be two non-negative integers. The following theorem will be shown to be a special case of the present work.

Theorem 1.1. *Consider all imaginary quadratic number fields K such that $D(K) \equiv 1 \pmod{4}$ and $\mathcal{O}_K/c \cong_{\text{ring}} \prod_{l \in S} \mathbb{F}_l^2$. When such K are ordered by the size of their discriminants the fraction of them that satisfy*

$$\text{rk}_4(\text{Cl}(K)) = j_1, \text{rk}_4(\text{Cl}(K, c)) = j_2$$

approaches

$$\frac{\eta_\infty(2)}{\eta_{j_1}(2)^{2^{j_1}}} \frac{\#\{\varphi \in \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \mathbb{F}_2^{\#S_3}) : \text{rk}(\varphi) = \#S - (j_2 - j_1)\}}{\#\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \mathbb{F}_2^{\#S_3})}.$$

For $M \in \mathbb{Z}_{\geq 1}$ and $s \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$, $\eta_s(M)$ denotes $\prod_{i=1}^s (1 - M^{-i})$. For the statement in full generality see Theorem 5.4.

Date: November 7, 2018.

2010 Mathematics Subject Classification. 11R65, 11R29, 11R11, 11R45.

The special case $c = 1$ of Theorem 1.1 recovers a result of Fouvry and Klüners [7, Cor. 1] (in the subfamily of imaginary quadratic number fields above). The theorem of Fouvry and Klüners on 4-ranks is one of the strongest pieces of evidence for the heuristic of Cohen–Lenstra and Gerth about the distribution of the p -Sylow subgroup of the class group of an imaginary quadratic number field.

Indeed, for odd primes p , Cohen and Lenstra [4] constructed a heuristic model to predict the outcome of any statistic on the p -Sylow of the class group of imaginary quadratic number fields. For every prime p they equipped the set of isomorphism classes of abelian p -groups, \mathcal{G}_p , with the only probability measure that gives to each abelian p -group G a weight inversely proportional to $\#\text{Aut}(G)$. This measure is now often called the Cohen–Lenstra measure on \mathcal{G}_p , and denoted by μ_{CL} . Their heuristic model, for odd primes p , consisted in predicting the equidistribution of $\text{Cl}(K)[p^\infty]$ in \mathcal{G}_p , as K ranges through natural families of imaginary quadratic number fields. Later, Gerth [9] adapted this heuristic model for $p = 2$. His idea was that the only obstruction for $\text{Cl}(K)[2^\infty]$ to behave like a random abelian 2-group in the sense of Cohen–Lenstra comes from $\text{Cl}(K)[2]$; therefore his heuristic model is that $2\text{Cl}(K)[2^\infty]$ behaves like a random abelian 2-group. The result of Fouvry and Klüners can then be formulated by saying that, consistently with Gerth’s conjecture, the 2-torsion of $2\text{Cl}(K)$ behaves like the 2-torsion of a random abelian 2-group in the sense of Cohen–Lenstra.

Before the present paper, no analogue of any of these heuristics has been proposed for ray class groups. Our second main achievement, aside from the proof of Theorem 1.1, is to provide an extension of the Cohen–Lenstra and Gerth heuristics for ray class groups. We obtain this by means of two innovations, one of a rather conceptual nature and one of a technical nature. Namely we first introduce the novel viewpoint of using homological algebra to weight the possible occurrences of ray class groups, as explained in §2. Secondly, to overcome the difficulties imposed by $p = 2$, we introduce in §3 the new notion of *embeddable extensions* (see Definition 3.2). This notion allows us to take care of the additional structure of this case, furnishing a natural way to define the adjusted weights for the 2-part of ray class groups. Theorem 1.1 will then be a strong evidence supporting our new heuristic for ray class groups and precisely in the case where our heuristic has the most demanding algebraic shape. The agreement of Theorem 1.1 and our heuristic at $p = 2$ is established in Proposition 3.5.

With our model we can provide the conjectural analogue of Theorem 1.1 for all odd primes p . Partition S into $S_1 \cup \dots \cup S_{p-1}$, where $l \in S_i$ if $l \equiv i \pmod{p}$.

Conjecture 1.2. *Let p be an odd prime. Consider all imaginary quadratic number fields K having the property $\mathcal{O}_K/c \cong_{\text{ring}} \prod_{l \in S} \mathbb{F}_{l^2}$. When such K are ordered by the size of their discriminants the fraction of them that satisfy*

$$\text{rk}_p(\text{Cl}(K)) = j_1, \text{rk}_p(\text{Cl}(K, c)) = j_2$$

approaches

$$\frac{\eta_\infty(p)}{\eta_{j_1}(p)^2 p^{j_1^2}} \frac{\#\{\varphi \in \text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{j_1}, \mathbb{F}_p^{\#S_{p-1}}) : \text{rk}(\varphi) = \#S_1 + \#S_{p-1} - (j_2 - j_1)\}}{\#\text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{j_1}, \mathbb{F}_p^{\#S_{p-1}})}.$$

For the statement in the general case see Conjecture 2.10, in particular, in the main body of the paper, we shall allow any admissible ring structure for \mathcal{O}_K/c . From our model in its full generality we shall derive conjectural formulas for the average size of the p -torsion of ray class groups of imaginary quadratic number fields.

Conjecture 1.3. *Let p be an odd prime. The average value of $\#\text{Cl}(K, c)[p]$ as K ranges over imaginary quadratic number fields with $\gcd(D(K), c) = 1$ and ordered by their discriminant is:*

(1)

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}} \left(1 + \left(\frac{p+1}{2} \right)^{\#\{l \text{ prime: } l|c, l \equiv 1 \text{ or } -1 \pmod{p}\}} \right)$$

if p^2 does not divide c ,

(2)

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}+1} \left(1 + p \left(\frac{p+1}{2} \right)^{\#\{l \text{ prime: } l|c, l \equiv 1 \text{ or } -1 \pmod{p}\}} \right)$$

if p^2 divides c .

For $p = 3$ this conjecture was recently proved by Varma [18] using geometry of numbers. In [18, §1] she asked whether one can formulate an extension of the Cohen–Lenstra heuristic that explains her result. Our model for ray class groups settles this for imaginary quadratic number fields (for the full comparison with Varma’s result see §2.2).

Our main theorems and conjectures are not merely about the group $\text{Cl}(K, c)$ but also about the entire exact sequence naturally attached to it:

$$1 \rightarrow \frac{(\mathcal{O}_K/c)^*}{\mathcal{O}_K^*} \rightarrow \text{Cl}(K, c) \rightarrow \text{Cl}(K) \rightarrow 1.$$

For simplicity, in this section we will continue to assume that all the primes in S are inert in K . Then one can show that there is a long exact sequence whose first terms are

$$1 \rightarrow \left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \right)^2 [2] \rightarrow (2\text{Cl}(K, c))[2] \rightarrow (2\text{Cl}(K))[2] \xrightarrow{\delta_2(K)} \prod_{l \in S_3} \frac{\mathbb{F}_l^{*2}}{\mathbb{F}_l^{*4}}.$$

To obtain the last map one chooses any identification between $\frac{\left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle}\right)^2}{\left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle}\right)^4}$ and $\prod_{l \in S} \frac{\mathbb{F}_l^{*2}}{\mathbb{F}_l^{*4}}$ via an identification of the rings \mathcal{O}_K/c and $\prod_{l \in S} \mathbb{F}_l$. The resulting set of maps is an orbit under $\text{Aut}_{\text{ring}}(\prod_{l \in S} \mathbb{F}_l)$, acting by post-composition. But $\text{Aut}_{\text{ring}}(\prod_{l \in S} \mathbb{F}_l)$ acts trivially on $\prod_{l \in S_3} \frac{\mathbb{F}_l^{*2}}{\mathbb{F}_l^{*4}}$, so one has a canonical identification.

Let Y be a subspace of $\prod_{l \in S_3} \frac{\mathbb{F}_l^{*2}}{\mathbb{F}_l^{*4}}$ and j a non-negative integer. In this setting we manage to control the statistical distribution of $(\#\text{Cl}(K)[2], \text{Im}(\delta_2(K)))$, thus providing a considerable refinement of Theorem 1.1. Our result is as follows.

Theorem 1.4. *Consider all imaginary quadratic number fields K such that $D(K) \equiv 1 \pmod{4}$ and $\mathcal{O}_K/c \cong_{\text{ring}} \prod_{l \in S} \mathbb{F}_l$. When such K are ordered by the size of their discriminants the fraction of them that satisfy*

$$(2\text{Cl}(K))[2] \cong \mathbb{F}_2^j, \text{Im}(\delta_2(K)) = Y$$

approaches

$$\frac{\eta_\infty(2)}{\eta_{j_1}(2)^2 2^{j_1^2}} \frac{\#\text{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j, Y)}{\#\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j, \prod_{l \in S_3} \frac{\mathbb{F}_l^{*2}}{\mathbb{F}_l^{*4}})}.$$

This means that $(\#(2\text{Cl}(K))[2], \text{Im}(\delta_2(K)))$ behaves like $(\#G[2], \text{Im}(\delta))$, where G is a random abelian 2-group in the Cohen–Lenstra sense, and $\delta : G[2] \rightarrow \mathbb{F}_2^{\#S_3}$ is a random map. For the statement in full generality see Theorem 5.2. We show in §3 that this result is also predicted by our heuristic model. Our model enables us to provide a conjectural analogue of Theorem 1.4 for all odd p . Its formulation is in Conjecture 2.8.

Theorem 1.4 determines the joint distribution of the pair $(\#(2\text{Cl}(K))[2], \text{Im}(\delta_2(K)))$. Theorem [7, Cor.1] of Fouvry and Klüners determines the distribution of the first component, $\#(2\text{Cl}(K))[2]$ via the use of another result of the two authors, [8, Theorem 3], where they obtained asymptotics for all moments of $\#(2\text{Cl}(K))[2]$. A surprising feature of our work is that we establish the joint distribution of the pair $(\#(2\text{Cl}(K))[2], \text{Im}(\delta_2(K)))$ by means of the moment-method, despite the fact that $\text{Im}(\delta_2(K))$ is not a number. *Although the general philosophy of using moments to study distributions is standard in the literature related to the Cohen–Lenstra heuristics (see, for example, [22]), we stress that no object like the image of the δ -map has been treated in the subject.* It is instructive to see how we incorporate the image-data into the Fouvry–Klüners method. We do this by introducing for every real character $\chi : \prod_{l \in S_3} \mathbb{F}_l^{*2} \rightarrow \mathbb{R}^*$, the random variable

$$m_\chi(\delta_2(K)) := \#\ker(\chi(\delta_2(K))).$$

To know the pair $(\#(2\text{Cl}(K))[2], \text{Im}(\delta_2(K)))$ is equivalent to knowing $(m_\chi(\delta_2(K)))_\chi$. However, the advantage is that the latter is a *numerical* vector and therefore one can hope to apply the method of moments to control its distribution. This is precisely what we achieve in Theorem 5.6. The expressions that appear during the proof of Theorem 5.6 are of the shape

$$\sum_{D < X} \prod_{\chi} m_\chi(\delta_2(\mathbb{Q}(\sqrt{-D})))^{k_\chi},$$

where D ranges over all positive square-free integers with $D \equiv 3 \pmod{4}$ and χ ranges over all real characters $\chi : \prod_{l \in S_3} \mathbb{F}_l^{*2} \rightarrow \mathbb{R}^*$. As explained in §6.1, the additional complexity of these expressions compared to the classical case settled by Fouvry and Klüners, is tempered by the fact that, with our heuristic model for ray class groups, we already have a candidate main term. In particular, the shape of its expression suggests a way to subdivide the sum, with the benefit of hindsight, in many smaller sub-sums. For each of these sub-sums it turns out that the techniques of Fouvry and Klüners are applicable with only minor modifications. After proving Theorem 5.6 we turn our attention to the distribution of $(\#(2\text{Cl}(K))[2], \text{Im}(\delta_2(K)))$, which we reconstruct from the mixed moments by following an argument of Heath-Brown [10].

We stress that Theorem 1.4 is stronger than Theorem 1.1. Here the finer information (which is the *image* of the δ -map), is obtained precisely owing to the fact that we use ring identifications rather than merely group identifications¹. Using the latter we could have studied only the *size* of $\text{Im}(\delta_2(K))$, which is precisely what occurs in Theorem 1.1. On the other hand, it is important to note that the techniques employed in the proof of Theorem 1.4 are not applicable in studying directly the moments of the isolated quantity $\#(2\text{Cl}(K, c))[2]$: we can access the distribution of the quantity $\#(2\text{Cl}(K, c))[2]$ only by the moments of a finer object, the δ -map. This contrast reflects the fact that the natural algebraic structure attached to the ray class group is the entire exact sequence naturally attached to it, rather than just the isolated group $\text{Cl}(K, c)$. It is precisely this phenomenon that leads us to

¹We thank Hendrik Lenstra for having suggested this.

formulate a general heuristic for ray class *sequences* of conductor c . In this framework, Theorem 1.4 gives compelling evidence that our heuristic model predicts correct answers also when it is challenged to produce the outcome of statistics about the *ray class sequence*, and not only when, less directly, one isolates the group $\text{Cl}(K, c)$.

Encouraged by this corroboration, we formulate our heuristic to predict the outcome of *any* statistical question about the p -part of the ray class sequence, viewed as an exact sequence of Galois modules. A positive side effect of this enhanced generality is the consequent logical simplification of our conjectural framework: our heuristic is based on a simple unifying principle, which, if true, implies at once all our conjectures. This heuristic principle is stated in §2 for an odd prime p , and in §3 for $p = 2$.

Let p be an odd prime and G a finite abelian p -group. The following is an attractive and easy example of the conjectural conclusions that are available in this new model:

Conjecture 1.5. *Consider all imaginary quadratic number fields K having the property that $\mathcal{O}_K/c \cong_{\text{ring}} \prod_{l \in S} \mathbb{F}_{l^2}$. When such K are ordered by the size of their discriminants, the fraction of them having the properties that the p -part of the ray class sequence of modulus c splits and*

$$\text{Cl}(K)[p^\infty] \cong_{\text{ab.gr.}} G,$$

approaches

$$\frac{\eta_\infty(p)}{\#\text{Aut}_{\text{ab.gr.}}(G)} \frac{1}{\#\text{Hom}_{\text{ab.gr.}}(G, \prod_{l \in S_{p-1}} \mathbb{F}_{l^2}^*)}.$$

1.1. Comparison with the literature. The present work sits in an active area of research focused on extending the classical Cohen–Lenstra heuristics to other interesting arithmetical objects and on establishing the correctness of these statistical models in cases where an ‘analytically-friendly’ description of the problem is available. Developments along this line of research can be found in the very recent work by Wood [21], which provides a heuristic for the average number of unramified G -extensions of a quadratic number field for any finite group G : the Cohen–Lenstra heuristics are recovered by taking G to be an abelian group. It would be interesting to reach the generality of both the present paper and [21], by considering G -extensions with prescribed ramification data. The evidence provided in [21] is over function fields, by means of the approach of Ellenberg, Venkatesh and Westerland [6]. In a recent preprint, Alberts and Klys [1] offered evidence for the heuristics in Wood’s work [21] over number fields using the approach of Fouvry and Klüners. It is interesting to note that in a previous work Klys [14] extended the work of Fouvry and Klüners to the p -torsion of cyclic degree p extensions. These last two examples, together with the present work, show the remarkable versatility of the method used in [8] and pioneered (in the context of Selmer groups) by Heath-Brown [10].

The case of narrow class groups was investigated by Bhargava and Varma [3] and by Dummit and Voight [5]. The latter work provides, among other things, a conjectural formula for the average size of the 2-torsion of narrow class groups among the family of S_n -number fields, for odd n . For $n = 3$, this was a theorem of Bhargava and Varma [3].

Very recently, Jordan, Klagsbrun, Poonen, Skinner and Zaytman [13] made a conjecture for the distribution of the p -torsion of K -groups of real and imaginary quadratic number fields. Building on the recent improvement of the work of Bhargava, Shankar and Tsimerman [2], they established their conjecture for the average size of the 3-torsion. Incidentally, the

work [2] is also employed by Varma [18] on the average 3-torsion of ray class groups, which is placed in a general conjectural framework by the present paper.

Despite this rich context of developments, the present paper is, to the best of our knowledge, the first one to propose a heuristic model for the ray class sequence of imaginary quadratic number fields and to prove its correctness for the pair $(\#(2\text{Cl}(K))[2], \text{Im}(\delta_2(K)))$, establishing, as a corollary, the joint distribution of the 4-ranks of $\text{Cl}(K)$ and $\text{Cl}(K, c)$.

1.2. Organization of the material. The remainder of this paper is organized as follows: In §2 we explain our heuristic model for the distribution of the p -part of ray class sequences of imaginary quadratic number fields, for odd primes p . We draw several conjectures from this heuristic principle and verify its consistency with the theorems of Varma [18] in the imaginary quadratic case.

In §3 we examine the case $p = 2$. This case requires some additional work to isolate the ‘random’ part of the 2-Sylow of the ray class sequences of imaginary quadratic number fields. This additional difficulty arises already for the ordinary class group as can be seen in the work of Gerth [9]. However, for ray class sequences overcoming such difficulties is much more intricate due to the more articulate underlying algebraic structures. This will allow us to formulate a number of predictions that will be proved in §§5-7. A key step in these proofs is the reformulation of the problem about 4-ranks into a purely analytic problem about mixed moments. For this we introduce the notion of special divisors in §4 and certain related statistical questions that will be subsequently answered. This statistic is a special case of a ray class group statistic, as subsequently established in §5. Therefore the material of §3 would implicitly provide a heuristic for it. Nevertheless, in §4 we present the problem and the heuristic in a direct way using the language of special divisors. This has the advantage that §4, Theorems 5.6-5.7, §6 and §7 are mostly analytic in nature and can be read independently of the algebraic considerations in §2 and §3.

In §5 we state the main theorems about the 2-part of the ray class sequences and reduce their proof so as to establish the predictions in §4. The section ends with the statement of the corresponding main theorems on special divisors. In §6 we prove the main theorem on mixed moments attached to the maps on special divisors introduced in §4. Finally, in §7 we reconstruct the distribution from the mixed moments, concluding the proof of all theorems stated in §5.

Notation. The symbol $D(K)$ will always refer to the discriminant of a number field K . Let us furthermore denote

$$\mathcal{F} := \{K \text{ imaginary quadratic number field}\}.$$

Acknowledgements. We are very grateful to Hendrik Lenstra for several insightful discussions and for useful feedback during the course of this project. In particular, we thank him for suggesting to consider the first terms of the ray class sequences only up to *ring* automorphisms, which turned out to be a natural level of greater generality where we could prove our main theorems on 4-ranks. We thank Alex Bartel for many stimulating discussions about our work, as well as organizing an inspiring conference on the Cohen–Lenstra heuristics in Warwick in July 2016, where this project started. We also wish to thank Djordjo Milovic and Peter Koymans for useful discussions and Ila Varma and Peter Stevnhagen for profitable feedback. Furthermore, we thank Alex Bartel, Joseph Gunther and Peter Koymans for helpful remarks on earlier versions of this paper.

2. HEURISTICS AND CONJECTURES FOR p ODD

Let p be an odd prime number and c a positive integer. Denote by C_2 a group with 2 elements and denote by τ its generator. In this section we provide a heuristic model that predicts the statistical behavior of the exact sequence of $\mathbb{Z}_p[C_2]$ -modules attached to the ray class group of conductor c of an imaginary quadratic number field K . Denote it by

$$S_p(K) := \left(1 \rightarrow \frac{(\mathcal{O}_K/c)^*}{\mathcal{O}_K^*}[p^\infty] \rightarrow \text{Cl}(K, c)[p^\infty] \rightarrow \text{Cl}(K)[p^\infty] \rightarrow 1\right), \quad (2.1)$$

where the C_2 -action comes from the natural action of $\text{Gal}(K/\mathbb{Q})$ on each term of the sequence. The reader is referred to [15, §IV] for related background material. We shall call $S_p(K)$ the p -part of the *ray class sequence* of conductor c . We shall henceforth ignore the fields $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-3})$, to ensure that $\mathcal{O}_K^* = \langle -1 \rangle$. Owing to $p \neq 2$ we furthermore have $((\mathcal{O}_K/c)^*/\langle -1 \rangle)[p^\infty] = (\mathcal{O}_K/c)^*[p^\infty]$, thus allowing us to write

$$S_p(K) := (1 \rightarrow (\mathcal{O}_K/c)^*[p^\infty] \rightarrow \text{Cl}(K, c)[p^\infty] \rightarrow \text{Cl}(K)[p^\infty] \rightarrow 1).$$

Denote by \mathcal{G}_p a set of representatives of isomorphism classes of finite abelian p -groups, viewed as C_2 -modules under the action of $-\text{Id}$ and call $G_p(K)$ the unique representative of $\text{Cl}(K)[p^\infty]$ in \mathcal{G}_p . Any family of imaginary quadratic fields can be partitioned in finitely many subfamilies where the isomorphism class of the ring \mathcal{O}_K/c is fixed, by imposing finitely many congruence conditions on the discriminants. Therefore we can always assume that $(\mathcal{O}_K/c)^*$ has been fixed as the unit group of some ring that is independent of K .

Definition 2.1. Let K, c be as above and R a finite commutative ring. We shall say that K is of type R if $\mathcal{O}_K/\text{char}(R) \cong R$ as rings. With this definition in mind let us denote

$$\mathcal{F}(R) := \{K \text{ imaginary quadratic number field of type } R\}.$$

From now on we will assume that R is of the form $R := \mathcal{O}_{\mathcal{A}}/c$, where $\mathcal{O}_{\mathcal{A}}$ is the integral closure of $\prod_{l|c} \mathbb{Z}_l$ in $\mathcal{A} := \prod_{l|c} E_l$, with E_l being an étale \mathbb{Q}_l -algebra of degree 2. Under this assumption, a positive fraction of all discriminants lies in $\mathcal{F}(R)$.

Suppose K is of type R . Then $(\mathcal{O}_K/c)^*$ can be identified with R^* via any restriction of a ring isomorphism, that is via any element of $\text{Isom}_{\text{ring}}(\mathcal{O}_K/c, R)$. Furthermore, we can identify $\text{Cl}(K)[p^\infty]$ and $G_p(K)$ via any element of $\text{Isom}_{\text{ab.gr.}}(\text{Cl}(K)[p^\infty], G_p(K))$. Therefore applying $\text{Isom}_{\text{ring}}(\mathcal{O}_K/c, R) \times \text{Isom}_{\text{ab.gr.}}(\text{Cl}(K)[p^\infty], G_p(K))$ to $S_p(K)$, we obtain a unique orbit

$$\mathcal{O}_{c,p}(K) \in \text{Ext}_{\mathbb{Z}_p[C_2]}(G_p(K), R^*[p^\infty]) / (\text{Aut}_{\text{ring}}(R) \times \text{Aut}_{\text{ab.gr.}}(G_p(K))).$$

We refer the reader to [19, §3] for definition and properties of $\text{Ext}_S(A, B)$, where S is a ring and A, B are S -modules. For the remainder of the paper, given S -modules A, B, C, A', B' and C' , we call a *commutative diagram* of S -modules, a diagram of maps of S -modules

$$\begin{array}{ccccccc} 0 & \rightarrow & B_1 & \rightarrow & C_1 & \rightarrow & A_1 \rightarrow 0 \\ & & & & \downarrow f_1 & & \downarrow g_1 \\ & & & & \downarrow \psi_1 & & \downarrow \psi_2 \\ 0 & \rightarrow & B_2 & \rightarrow & C_2 & \rightarrow & A_2 \rightarrow 0, \\ & & & & \downarrow f_2 & & \downarrow g_2 \end{array}$$

with $\psi_2 \circ f_1 = f_2 \circ \psi_1$ and $\psi_3 \circ g_1 = g_2 \circ \psi_2$. Note that $\text{Cl}(K_1)[p^\infty] \cong_{\text{ab.gr}} \text{Cl}(K_2)[p^\infty]$ and $O_{c,p}(K_1) = O_{c,p}(K_2)$ if and only if there is a commutative diagram of $\mathbb{Z}_p[C_2]$ modules

$$\begin{array}{ccccccc} 0 & \rightarrow & (\mathcal{O}_{K_1}/c)^*[p^\infty] & \rightarrow & \text{Cl}(K_1, c)[p^\infty] & \rightarrow & \text{Cl}(K_1)[p^\infty] \rightarrow 0 \\ & & \downarrow \varphi_1 & & \downarrow \varphi_2 & & \downarrow \varphi_3 \\ 0 & \rightarrow & (\mathcal{O}_{K_2}/c)^*[p^\infty] & \rightarrow & \text{Cl}(K_2, c)[p^\infty] & \rightarrow & \text{Cl}(K_2)[p^\infty] \rightarrow 0, \end{array}$$

with φ_1 being the restriction of a ring isomorphism and φ_3 being an isomorphism of abelian groups.

Definition 2.2. Define $\mathcal{S}_p(R)$ as the set of equivalence classes of pairs (G, θ) , where

$$G \in \mathcal{G}_p, \theta \in \text{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty])$$

under the following equivalence relation: two pairs $(G_1, \theta_1), (G_2, \theta_2)$ are identified if $G_1 = G_2$ and θ_1 and θ_2 are in the same $\text{Aut}_{\text{ring}}(R) \times \text{Aut}_{\text{ab.gr.}}(G_1)$ -orbit.

Let us denote by $\widetilde{\mathcal{S}}_p(R)$ the set of pairs (G, θ) where $G \in \mathcal{G}_p$ and $\theta \in \text{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty])$, thus bringing into play the quotient map $\pi : \widetilde{\mathcal{S}}_p(R) \rightarrow \mathcal{S}_p(R)$. We are interested in studying the distribution of $S'_p(K)$ given by the pair

$$K \mapsto S'_p(K) := (G_p(K), O_{c,p}(K)) \in \mathcal{S}_p(R).$$

Definition 2.3. Let μ_{CL} be the unique probability measure on \mathcal{G}_p which gives to each abelian p -group G a weight inversely proportional to the size of the automorphism group of G .

This measure was introduced by Cohen and Lenstra in [4] to predict the distribution of $G_p(K)$, the first component of $S'_p(K)$. We shall introduce a measure on $\mathcal{S}_p(R)$ that enables us to predict the joint distribution of the vector $S'_p(K)$. Consider the discrete σ -algebra on both $\widetilde{\mathcal{S}}_p(R), \mathcal{S}_p(R)$ and equip $\widetilde{\mathcal{S}}_p(R)$ with the following measure,

$$\widetilde{\mu}_{\text{seq}}((G, \theta)) := \frac{\mu_{\text{CL}}(G)}{\#\text{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty])}.$$

Let $\mu_{\text{seq}} := \pi_*(\widetilde{\mu}_{\text{seq}})$ be the pushforward measure of $\widetilde{\mu}_{\text{seq}}$ on $\mathcal{S}_p(R)$ via π . It is evident that $\widetilde{\mu}_{\text{seq}}$ and μ_{seq} are probability measures. We now formulate a heuristic which roughly states that ray class sequences equidistribute within the set of isomorphism classes of exact sequences with respect to the measure μ_{seq} .

Heuristic assumption 2.4. For any ‘reasonable’ function $f : \mathcal{S}_p(R) \rightarrow \mathbb{R}$ we have

$$\lim_{X \rightarrow \infty} \#\{K \in \mathcal{F}(R) : |D(K)| \leq X\}^{-1} \sum_{\substack{K \in \mathcal{F}(R) \\ |D(K)| \leq X}} f(S'_p(K)) = \sum_{S \in \mathcal{S}_p(R)} f(S) \mu_{\text{seq}}(S).$$

Letting f be the indicator function of a singleton yields the following statement.

Conjecture 2.5. For any $S \in \mathcal{S}_p(R)$ we have

$$\lim_{X \rightarrow \infty} \frac{\#\{K \in \mathcal{F}(R) : |D(K)| \leq X, S'_p(K) = S\}}{\#\{K \in \mathcal{F}(R) : |D(K)| \leq X\}} = \mu_{\text{seq}}(S).$$

A special concrete example is the case of split sequences.

Conjecture 2.6. *The fraction of $K \in \mathcal{F}(R)$, ordered by the size of their discriminant, for which $\text{Cl}(K)[p^\infty] \cong_{\text{ab.gr.}} G$ and the p -part of the ray class sequence of modulus c splits, approaches*

$$\frac{\mu_{\text{CL}}(G)}{\#\text{Hom}_{\text{ab.gr.}}(G, R^*[p^\infty]^-)},$$

where $(R^*[p^\infty])^-$ denotes the minus part of $R^*[p^\infty]$ under the action of C_2 .

Indeed, $\text{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty]) = \text{Ext}_{\mathbb{Z}_p}(G, (R^*[p^\infty])^-)$ holds, hence Conjecture 2.6 is derived from Conjecture 2.5 by recalling that for two finite abelian p -groups A, B , there is a non-canonical isomorphism $\text{Ext}_{\mathbb{Z}_p}(A, B) \cong_{\text{ab.gr.}} \text{Hom}_{\mathbb{Z}_p}(A, B)$.

2.1. Conjectures on the p -torsion. We next state certain consequences of Heuristic assumption 2.4 regarding the p -torsion of the ray class sequences. Taking p -torsion in (2.1) provides us with a long exact sequence whose first four terms are given by

$$S(K)[p] := \left(1 \rightarrow (\mathcal{O}_K/c)^*[p] \rightarrow \text{Cl}(K, c)[p] \rightarrow \text{Cl}(K)[p] \xrightarrow{\delta_p(K)} \frac{(\mathcal{O}_K/c)^*}{((\mathcal{O}_K/c)^*)^p} \right),$$

where the map $\delta_p(K)$ is defined as follows: given a class $x \in \text{Cl}(K)[p]$ pick a representative ideal \mathcal{I} of x which is coprime to c , take a generator of \mathcal{I}^p and reduce it modulo c . The choice of another representative does not change it modulo p -th powers. More generally, taking p -torsion in any short exact sequence of $\mathbb{Z}_p[C_2]$ -modules

$$S := (0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0)$$

provides us with a long exact sequence whose first terms are

$$S[p] := \left(1 \rightarrow A[p] \rightarrow B[p] \rightarrow C[p] \xrightarrow{\delta_p(S)} \frac{A}{pA} \right),$$

where $\delta_p(S)$ is defined in the same way as explained above (in particular we have $\delta_p(S_p(K)) = \delta_p(K)$). Thus this provides a map sending an element θ of $\text{Ext}_{\mathbb{Z}_p[C_2]}(C, A)$ to a map $\delta_p(\theta) : C[p] \rightarrow A/pA$. We will make repeatedly use of the following fact.

Proposition 2.7. *The map sending θ to $\delta_p(\theta)$, from $\text{Ext}_{\mathbb{Z}_p[C_2]}(C, A)$ to $\text{Hom}_{\mathbb{Z}_p[C_2]}(C[p], A/pA)$, is a surjective group homomorphism.*

The reader interested in a proof of Proposition 2.7, can look at the proof of the analogous, but more complicated, Proposition 3.5: all the ingredients for the proof of Proposition 2.7 are contained in the proof of Proposition 3.5.

Next we shall define $j := \dim_{\mathbb{F}_p}(\text{Cl}(K)[p])$ and apply any pair of identifications from $\text{Isom}_{\mathbb{F}_p}(\text{Cl}(K)[p], \mathbb{F}_p^j) \times \text{Isom}_{\text{ring}}(\mathcal{O}_K/c, R)$. Therefore, we obtain a unique orbit of maps $\varphi \in \text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^j, (\frac{R^*}{R^{*p}})^-)$ under the action of $\text{GL}_j(\mathbb{F}_p) \times \text{Aut}_{\text{ring}}(R)$. This is tantamount to having a $\text{Aut}_{\text{ring}}(R)$ -orbit of images in $(\frac{R^*}{R^{*p}})^-$ of $\delta_p(K)$ via any of the previous identifications. We denote this orbit by $[\text{Im}(\delta_p(K))]$. The assignment $K \mapsto [\text{Im}(\delta_p(K))]$ attaches to each imaginary quadratic field $K \in \mathcal{F}_c(R)$ a well-defined $\text{Aut}_{\text{ring}}(R)$ -orbit of vector sub-spaces of $(\frac{R^*}{R^{*p}})^-$.

By Proposition 2.7, the map

$$\text{Ext}_{\mathbb{Z}_p}(G, R^*[p^\infty]^-) \rightarrow \text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$$

induces, by pushforward, the counting probability measure from $\text{Ext}_{\mathbb{Z}_p}(G, (R^*[p^\infty])^-)$ to $\text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$. Therefore, fixing a sub- \mathbb{F}_p -space Y of $(\frac{R^*}{R^{*p}})^-$ and a non-negative integer j , Heuristic assumption 2.4 supplies us with the following.

Conjecture 2.8. *The proportion of $K \in \mathcal{F}(R)$ ordered by the size of their discriminant, for which $\dim_{\mathbb{F}_p}(\text{Cl}(K)[p]) = j$ and $[\text{Im}(\delta_p(K))]$ is $O(Y)$, the $\text{Aut}_{\text{ring}}(R)$ -orbit of Y , approaches*

$$\mu_{\text{CL}}(G \in \mathcal{G}_p : \dim_{\mathbb{F}_p}(G[p]) = j) = \frac{\#\text{Epi}_{\mathbb{F}_p}(\mathbb{F}_p^j, Y) \cdot \#O(Y)}{\#\text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^j, (R^*/R^{*p})^-)}.$$

We will prove the analogous statement of this Conjecture 2.8 for $p = 2$ in Theorem 5.2. A concrete special case is given by the following

Conjecture 2.9. *The proportion of $K \in \mathcal{F}(R)$ ordered by the size of their discriminant, for which $\dim_{\mathbb{F}_p}(\text{Cl}(K)[p]) = j$ and $\text{Cl}(K, c)[p]$ splits as the direct sum of $\text{Cl}(K)[p]$ and $(\mathcal{O}_K/c)^*[p]$, approaches*

$$\frac{\mu_{\text{CL}}(G \in \mathcal{G}_p : \dim_{\mathbb{F}_p}(G[p]) = j)}{\#\text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^j, (R^*/R^{*p})^-)}.$$

More generally, as a cruder result, one derives a conjectural formula for the joint distribution of the p -rank of $\text{Cl}(K)$ and of $\text{Cl}(K, c)$, as follows. Fix j_1, j_2 two non-negative integers.

Conjecture 2.10. *As K varies among imaginary quadratic number fields of type R , the proportion of them for which $\dim_{\mathbb{F}_p}(\text{Cl}(K)[p]) = j_1$ and $\dim_{\mathbb{F}_p}(\text{Cl}(K, c)[p]) = j_2$ approaches*

$$\mu_{\text{CL}}(G \in \mathcal{G}_p : \dim_{\mathbb{F}_p}(G[p]) = j_1) = \frac{\#\{\varphi : \mathbb{F}_p^{j_1} \rightarrow (R^*/R^{*p})^- : \text{rk}(\varphi) = \text{rk}_p(R^*) - (j_2 - j_1)\}}{\#\text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{j_1}, (R^*/R^{*p})^-)}.$$

The statements analogous to Conjectures 2.8 and 2.10 for $p = 2$ will be proved in Theorem 5.3, with a more explicit version provided by Theorem 5.4.

2.2. Agreement with Varma's results. In this section we make a certain choice for f in Heuristic assumption 2.4 with the aim of stating conjectures for the average of p -torsion of ray class groups. These statements were previously proved for $p = 3$ by Varma [18]. In fact, the present paper partly began as an effort to fit her results into a general heuristic framework.

For an element $S \in \mathcal{S}_p(R)$, denote by $M(S)$ the isomorphism class of the middle term of the sequence corresponding to S . Similarly, for $\theta \in \text{Ext}_{\mathbb{Z}_p}[C_2]$ we denote by $M(\theta)$ the isomorphism class of the middle term of the equivalence class of sequences corresponding to θ . We will adopt the standard notation \hat{A} for the dual of a finite abelian group A .

Proposition 2.11. *We have*

$$\sum_{S \in \mathcal{S}_p(R)} \#M(S)[p] \mu_{\text{seq}}(S) = \# \left(\frac{R^*}{R^{*p}} \right)^+ \left(1 + \# \left(\frac{R^*}{R^{*p}} \right)^- \right).$$

Proof. By the definition of μ_{seq} we obtain equality of the sum in our proposition with

$$\sum_{G \in \mathcal{G}_p} \frac{\mu_{\text{CL}}(G)}{\#\text{Ext}_{\mathbb{Z}_p}[C_2](G, R^*[p^\infty])} \sum_{\theta \in \text{Ext}_{\mathbb{Z}_p}[C_2](G, R^*[p^\infty])} \#M(\theta)[p].$$

Again by Proposition 2.7 we know that the map $\theta \rightarrow \delta_p(\theta)$ is a surjective homomorphism

$$\text{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^{\infty}]) \rightarrow \text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$$

Thus we can rewrite the last sum as

$$\sum_{G \in \mathcal{G}_p} \frac{\mu_{\text{CL}}(G)}{\#\text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)} \sum_{\delta}^* \#R^*[p] \frac{\#G[p]}{\#\text{Im}(\delta)}, \quad (2.2)$$

where the sum \sum^* is taken over δ in $\text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$. For each χ in the dual of $(R^*/R^{*p})^-$ denote by $\mathbf{1}_{\chi}$ the indicator function of those δ for which χ vanishes on the image of δ . This allows us to recast (2.2) in the following manner,

$$\sum_{G \in \mathcal{G}_p} \frac{\mu_{\text{CL}}(G)}{\#\text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)} \sum_{\delta}^* \#(R^*/R^{*p})^+ \#G[p] \sum_{\chi \in (R^*/R^{*p})^-} \mathbf{1}_{\chi}(\delta),$$

where δ varies over all elements in $\text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$. Exchanging the order of summation yields

$$\sum_{G \in \mathcal{G}_p} \#(R^*/R^{*p})^+ \#G[p] \mu_{\text{CL}}(G) \sum_{\chi \in (R^*/R^{*p})^-} \frac{\sum_{\delta \in \text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)} \mathbf{1}_{\chi}(\delta)}{\#\text{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)}.$$

The χ -th summand in the last expression equals 1 if χ is the trivial character and equals $\frac{1}{\#G[p]}$ otherwise, thus obtaining

$$\sum_{G \in \mathcal{G}_p} \#(R^*/R^{*p})^+ \#G[p] \left(1 + \frac{\#(R^*/R^{*p})^- - 1}{\#G[p]}\right) \mu_{\text{CL}}(G).$$

Recalling the classical equality $\sum_{G \in \mathcal{G}_p} \#G[p] \mu_{\text{CL}}(G) = 2$ provides us with

$$\#(R^*/(R^{*p}))^+ (2 + \#(R^*/R^{*p})^- - 1) = \#(R^*/R^{*p})^+ \left(1 + \# \left(\frac{R^*}{R^{*p}}\right)^-\right),$$

which concludes our proof. \square

Combining Proposition 2.11 and Heuristic Assumption 2.4 offers the following.

Conjecture 2.12. *The average value of $\#\text{Cl}(K, c)[p]$, as K ranges among imaginary quadratic number fields of type R ordered by their discriminant, is given by*

$$\# \left(\frac{R^*}{R^{*p}}\right)^+ \left(1 + \# \left(\frac{R^*}{R^{*p}}\right)^-\right).$$

In particular we can now derive conjectural formulas for the average size of $\text{Cl}(K, c)[p]$ with K varying in larger families.

We next consider here two cases: in §2.2.1 the case when all the primes dividing c are required to be unramified in K , and in §2.2.2 the case where K ranges through all discriminants. The letter l will refer to a prime until the end of §2.

2.2.1. *Collecting unramified discriminants.* Observe that if R correspond to a splitting type where all the primes dividing c are unramified in K , and if p^2 does not divide c (so there is no contribution to the p -part from p itself in case it divides c) then we have that

$$\# \left(\frac{R^*}{R^{*p}} \right)^+ \left(1 + \# \left(\frac{R^*}{R^{*p}} \right)^- \right) = p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}} (1 + p^{\omega_R(c)}),$$

where $\omega_R(c)$ is defined by

$$\#\{l \text{ prime: } l|c, (l \equiv 1 \pmod{p}) \text{ and } l \text{ is split in } R\} \text{ or } (l \equiv -1 \pmod{p}) \text{ and } l \text{ is inert in } R\}.$$

Therefore when we average over all $2^{\omega(c)}$ choices of R , using the binomial formula we get

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}} \left(1 + \left(\frac{p+1}{2} \right)^{\#\{l \text{ prime: } l|c, l \equiv 1 \text{ or } -1 \pmod{p}\}} \right)$$

as average value of the size of $\text{Cl}(K, c)[p]$ when K ranges over imaginary quadratic number fields unramified at all primes dividing c , as long as $p^2 \nmid c$. Instead, if $p^2 | c$ there is an additional contribution from the principal units modulo p^2 to $\# \left(\frac{R^*}{R^{*p}} \right)^+ \left(1 + \# \left(\frac{R^*}{R^{*p}} \right)^- \right)$, which gives

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}+1} \left(1 + p \left(\frac{p+1}{2} \right)^{\#\{l \text{ prime: } l|c, l \equiv 1 \text{ or } -1 \pmod{p}\}} \right).$$

This leads to the Conjecture 1.3 that we stated in the introduction. The special case $p = 3$ of Conjecture 1.3 was recently proved by Varma [18, Th.2.(b)].

Theorem 2.13 (Varma). *The average value of $\# \text{Cl}(K, c)[3]$ as K ranges over imaginary quadratic number fields with $\gcd(D(K), c) = 1$ is:*

(1)

$$3^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{3}\}} (1 + 2^{\#\{l \text{ prime: } l|c, l \not\equiv 3\}})$$

if 9 does not divide c .

(2)

$$3^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{3}\}+1} (1 + 3 \cdot 2^{\#\{l \text{ prime: } l|c, l \not\equiv 3\}})$$

if 9 divides c .

2.2.2. *Collecting all discriminants.* We now consider the case where K is allowed to ramify at the primes dividing c . Now we have to evaluate

$$\sum_R \# \left(\frac{R^*}{R^{*p}} \right)^+ \left(1 + \# \left(\frac{R^*}{R^{*p}} \right)^- \right) w(R),$$

where R varies between all the possible types of ring at c , and

$$w(R) := \lim_{X \rightarrow +\infty} \frac{\#\{K \in \mathcal{F}_c(R) : |D(K)| \leq X\}}{\#\{K \in \mathcal{F} : |D(K)| \leq X\}}.$$

First observe that if $p^2 \nmid c$ then

$$\# \left(\frac{R^*}{R^{*p}} \right)^+ = p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}},$$

while if $p^2 | c$ then

$$\# \left(\frac{R^*}{R^{*p}} \right)^+ = p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}+1}.$$

Therefore we are left with computing the average of $\# \left(\frac{R^*}{R^{*p}} \right)^-$, over all R . But this, as a function of c , is multiplicative, thus we only have to deal with prime powers, i.e. $c = l^n$ for

some prime l and some positive integer n . Clearly, the value of this average is 1 if l is such that $\gcd(p, l^3 - l) = 1$. Instead, if $p|l^2 - 1$ the value of the average is

$$\frac{1}{l+1} + \frac{\left(\frac{p+1}{2}\right)l}{l+1} = 1 + \left(\frac{p-1}{2}\right)\frac{l}{l+1},$$

where the first contribution comes from the R ramified at l , and the second from the R unramified at l .² Meanwhile, the value of the average for $p = c$ is

$$\frac{p}{p+1} + \frac{p}{p+1},$$

where the first contribution comes from R ramified at p and the second from R unramified at p . Lastly, we consider the case $p^2|c$. Remarkably enough, one observes that the case $p = 3$ acquires a special status in the computation of this average: indeed $\frac{1}{8}$ of the imaginary quadratics locally at 3 give the extension $\mathbb{Q}_3(\zeta_3)/\mathbb{Q}_3$, and the result for them will be different than for the $\frac{1}{8}$ totally ramified that locally at 3 become $\mathbb{Q}_3(\sqrt{3})$. Clearly for all $p > 3$ there is no p -th root of unity in a quadratic extension of \mathbb{Q}_p , so, as we will see, in that case the contribution from the two R ramified at p will be the same.

Assume $p = 3$. The contribution from powers of 3 starting from 9 is

$$\frac{9}{8} + \frac{3}{8} + \frac{9}{4} = \frac{15}{4},$$

where the first contribution is from $\mathbb{Q}_3(\zeta_3)$, the second from $\mathbb{Q}_3(\sqrt{3})$ and the third from unramified R . This gives a prediction that was previously verified by Varma [18, Th.1.(b)].

Theorem 2.14 (Varma). *The average value of $\#\text{Cl}(K, c)[3]$ as K ranges through imaginary quadratic number fields ordered by their discriminant is:*

(1)

$$3^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{3}\}} \left(1 + \prod_{l|c} \left(1 + \frac{l}{l+1}\right)\right)$$

if 3 does not divide c ,

(2)

$$3^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{3}\}} \left(1 + \frac{6}{7} \prod_{l|c} \left(1 + \frac{l}{l+1}\right)\right)$$

if 3 divides c but 9 does not divide c ,

(3)

$$3^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{3}\}+1} \left(1 + \frac{15}{7} \prod_{l|c} \left(1 + \frac{l}{l+1}\right)\right)$$

if 9 divides c .

Now assume that $p > 3$. Then we get

$$\frac{p}{p+1} + \frac{p^2}{p+1},$$

where the first contribution is from the R ramified at p and the second from R unramified at p . Collecting everything together we get the following prediction.

² R is said unramified at l if R/lR does not contain non-zero nilpotents. Otherwise R is said ramified at l .

Conjecture 2.15. *Suppose $p > 3$. Then the average value of $\#\text{Cl}(K, c)[p]$ as K ranges over imaginary quadratic number fields ordered by their discriminant is:*

(1)

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}} \left(1 + \prod_{l|c, p|l^2-1} \left(1 + \frac{p-1}{2} \frac{l}{l+1} \right) \right)$$

if p does not divide c ,

(2)

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}} \left(1 + \left(\frac{2p}{p+1} \right) \prod_{l|c, p|l^2-1} \left(1 + \frac{p-1}{2} \frac{l}{l+1} \right) \right)$$

if p divides c but p^2 does not divide c ,

(3)

$$p^{\#\{l \text{ prime: } l|c, l \equiv 1 \pmod{p}\}} \left(1 + \left(\frac{p+p^2}{p+1} \right) \prod_{l|c, p|l^2-1} \left(1 + \frac{p-1}{2} \frac{l}{l+1} \right) \right)$$

if p^2 divides c .

It would be desirable to extend Varma's arguments to prove Conjecture 2.12 for $p = 3$. In particular, it would be informative to see how the proof distinguishes between the cases $R/3^m = \mathcal{O}_{\mathbb{Q}_3(\zeta_3)}/3^m$ and $R/3^m = \mathcal{O}_{\mathbb{Q}_3(\sqrt{3})}/3^m$, for $m \geq 2$.

3. HEURISTIC AND CONJECTURES FOR $p = 2$

Let c be an odd positive integer. In this section we explain a heuristic model for the 2-part of ray class sequences of conductor c , in the case that no primes dividing c ramify in the fields. The additional difficulty with respect to the case of p odd, is that $\text{Cl}(K)[2^\infty]$ does not behave like a random 2-group (in the sense of Cohen and Lenstra), but instead (as conjectured by Gerth [9]), $2\text{Cl}(K)[2^\infty]$ is believed to behave like a random 2-group: the behavior of $\text{Cl}(K)[2]$ is governed instead by genus theory which trivially excludes any Cohen–Lenstra behavior for $\text{Cl}(K)[2^\infty]$, when K varies among usual families of imaginary quadratic number fields.

Our approach will be as follows: we will see that for ‘most’ discriminants of type R , $2\text{Cl}(K, c)$ is an extension of $2\text{Cl}(K)$ with a certain subgroup of $\frac{R^*}{\langle -1 \rangle}$, which we will call W_R . Nevertheless, one cannot completely ignore the presence of the class group, since it leaves an additional restriction on such extensions. Namely it forces them to belong to a certain subgroup of the Ext, that we will call $\widetilde{\text{Ext}}$. From there we will proceed in analogy with the previous section replacing Ext with $\widetilde{\text{Ext}}$. Using this heuristic we will offer several predictions which are proved in the subsequent sections.

Since we will only consider the case that no primes dividing c ramify in the imaginary number fields K , and since we assume that c is odd, we do not lose generality in assuming that c is also square-free: indeed, in our setting, the 2-part of $(\mathcal{O}_K/c)^*/\langle -1 \rangle$ is no different from the one of $(\mathcal{O}_K/c')^*/\langle -1 \rangle$, where c' is the square-free part of c . Therefore the choice of a ring type at c amounts to the choice of a partition of the set $S_c := \{l \text{ prime} : l|c\}$ in the disjoint union of two sets $S_c(\text{inert})$ and $S_c(\text{split})$. Then one takes $R := \left(\prod_{l \in S_c(\text{inert})} \mathbb{F}_{l^2} \right) \times \left(\prod_{l' \in S_c(\text{split})} (\mathbb{F}_{l'})^2 \right)$. For such an R , the C_2 -action is given by l -Frobenius on the non-split components, and by swapping on the split components. We will call such R , unramified at c . By a small abuse of notation, we denote by $\mathbb{Z}/c\mathbb{Z}$ the natural image of $\mathbb{Z}/c\mathbb{Z}$ in R .

For R unramified at c , we define

$$W_R := \frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1 \rangle} \left(\frac{R^*}{\langle -1 \rangle} \right)^2 \subseteq \frac{R^*}{\langle -1 \rangle}. \quad (3.1)$$

Now fix some R unramified at c . For the remainder of this section we will assume, for simplicity, the imaginary quadratic number field K to have an odd discriminant. We shall prove that one has an exact sequence

$$2S(K) := (0 \rightarrow W_R \rightarrow 2\text{Cl}(K, c) \rightarrow 2\text{Cl}(K) \rightarrow 0),$$

for all imaginary quadratic number fields of type R with the exception of $O(x(\log x)^{-1/\varphi(c)})$ discriminants up to x . Indeed, by the theory of ambiguous ideals, one has that

$$\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \cap 2\text{Cl}(K, c) = \langle \{q \text{ prime and } q \mid D(K)\} \rangle \left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \right)^2.$$

Therefore it is enough to show that the set of positive square-free $D \leq x$ such that

$$\{q \pmod{c} : q \text{ prime and } q \mid D\} \neq (\mathbb{Z}/c\mathbb{Z})^*$$

is $O(x(\log x)^{-1/\varphi(c)})$. This cardinality is

$$\leq \sum_{a \in (\mathbb{Z}/c\mathbb{Z})^*} \sum_{\substack{1 \leq D \leq X \\ p \mid D \Rightarrow p \neq a \pmod{c}}} \mu(D)^2 \ll \frac{x}{(\log x)^{1/\varphi(c)}},$$

where the last bound is easily derived by using [12, Eq.(1.85)] with f being the characteristic function of integers all of whose prime divisors are not $a \pmod{c}$. Identifying \mathcal{O}_K/c with R via a ring isomorphism gives an identification between W_R and

$$\frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1 \rangle} \left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \right)^2.$$

Definition 3.1. Among the imaginary quadratic number fields of type R , we call *strongly* of type R , those satisfying

$$\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \cap 2\text{Cl}(K, c) = \frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1 \rangle} \left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \right)^2.$$

Let $E(x)$ denote the cardinality of negative discriminants $1 \pmod{4}$ of absolute value at most x and which are of type R but not strongly of type R . The analysis above can be summarised by the bound

$$E(x) \ll \frac{x}{(\log x)^{1/\varphi(c)}}. \quad (3.2)$$

One could be tempted to think of the sequence $S_2(K) := 2S(K)[2^\infty]$ as a ‘random’ sequence, just as in the previous section. This would be incorrect, since the way the sequences $S_2(K)$ are produced naturally puts on them an additional restriction. Namely one has a commutative diagram of $\mathbb{Z}[C_2]$ -modules:

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} & \rightarrow & \text{Cl}(K, c) & \xrightarrow{\pi} & \text{Cl}(K) \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \rightarrow & \frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1 \rangle} \left(\frac{(\mathcal{O}_K/c)^*}{\langle -1 \rangle} \right)^2 & \rightarrow & 2\text{Cl}(K, c) & \rightarrow & 2\text{Cl}(K) \rightarrow 0 \end{array}$$

where i_1, i_2, i_3 are the natural inclusion maps, so i_2 and i_3 consist of isomorphisms between the source groups and the double of the target groups. The top sequence has two obvious properties that are automatically satisfied:

$$\pi(\mathrm{Cl}(K, c)[2^\infty]^-) = \mathrm{Cl}(K)[2^\infty] \text{ and } \pi(\mathrm{Cl}(K, c)[2^\infty]^+) = \mathrm{Cl}(K)[2].$$

The first property is equivalent to the sequence remaining exact after taking $(1 + \tau)$ -torsion, where τ is the generator of C_2 . Indeed, this is equivalent to the natural map

$$\mathrm{Cl}(K)[2^\infty] \rightarrow \frac{\frac{R^*}{\langle -1 \rangle}}{(\tau + 1)\frac{R^*}{\langle -1 \rangle}}$$

being the 0-map, which holds since the norm of an integral ideal is always an integer. The second property follows from the fact that we are looking at families of discriminants coprime to c . Therefore we are allowed to lift a prime ideal \mathfrak{q} lying above a prime q dividing $D(K)$, using the class of the ideal \mathfrak{q} in $\mathrm{Cl}(K, c)$: this class will still be a fixed point, since it is the class of a τ -invariant *ideal*. This motivates the following:

Definition 3.2. Let G be a finite abelian 2-group, viewed as a C_2 module with the $-$ id-action. We say that an element θ of $\mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$:

$$\theta : 1 \rightarrow W_R[2^\infty] \rightarrow B \rightarrow G \rightarrow 1$$

is *embeddable* if there is an exact sequence of $\mathbb{Z}_2[C_2]$ -modules

$$1 \rightarrow \frac{R^*}{\langle -1 \rangle}[2^\infty] \rightarrow \tilde{B} \rightarrow \tilde{G} \rightarrow 1$$

and a commutative diagram of $\mathbb{Z}_2[C_2]$ -modules

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \rightarrow & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \rightarrow & W_R[2^\infty] & \rightarrow & B & \rightarrow & G \rightarrow 0 \end{array}$$

where:

- The map $\pi : \tilde{B} \rightarrow \tilde{G} \rightarrow 1$ satisfies

$$\pi(\tilde{B}^-) = \tilde{G} \text{ and } \pi(\tilde{B}^+) = \tilde{G}[2].$$

- The maps i_2 and i_3 are isomorphisms between the source groups and the double of the target groups. The map i_1 is the natural inclusion.

We denote the set of embeddable extensions by $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$. It will be clear by Proposition 3.5, that the two following sets do not always coincide:

$$\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty]), \mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty]).$$

On the other hand, the set of embeddable extensions has the algebraic structure that allows us to proceed in perfect parallel with the previous section.

Proposition 3.3. *One has that $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is a subgroup of $\mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ stable under the action of $\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G)$.*

Proof. Let

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \rightarrow & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \rightarrow & W_R[2^\infty] & \rightarrow & B & \xrightarrow{f} & G \rightarrow 0 \end{array}$$

and

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \rightarrow & \tilde{B}' & \xrightarrow{\pi'} & \tilde{G}' \rightarrow 0 \\ & & \uparrow i'_1 & & \uparrow i'_2 & & \uparrow i'_3 \\ 0 & \rightarrow & W_R[2^\infty] & \rightarrow & B' & \xrightarrow{f'} & G \rightarrow 0 \end{array}$$

be two embeddable extensions equipped with their respective diagrams. We now consider the following commutative diagram of $\mathbb{Z}_2[C_2]$ -modules,

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \rightarrow & (\tilde{B} \times_G \tilde{B}')/Y' & \xrightarrow{\pi \times \pi'} & \tilde{G} \times_G \tilde{G}' \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 \times i'_2 & & \uparrow i_3 \times i'_3 \\ 0 & \rightarrow & W_R[2^\infty] & \rightarrow & (B \times_G B')/Y & \xrightarrow{f \times f'} & G \rightarrow 0 \end{array}$$

where $\tilde{B} \times_G \tilde{B}' := \{(b_1, b_2) \in \tilde{B} \times \tilde{B}' : 2\pi(b_1) = 2\pi'(b_2)\}$, while Y' denotes the anti-diagonal embedding of $\frac{(R)^*}{\langle -1 \rangle}[2^\infty]$ in $\tilde{B} \times_G \tilde{B}'$. Similarly $B \times_G B' := \{(b_1, b_2) \in B \times B' : f(g_1) = f'(g_2)\}$, with Y denoting the anti-diagonal embedding of $W_R[2^\infty]$, and

$$\tilde{G} \times_G \tilde{G}' := \{(g_1, g_2) \in \tilde{G} \times \tilde{G}' : 2g_1 = 2g_2\}.$$

There is an obviously induced compatible C_2 action on each terms and one can deduce that

$$(\pi \times \pi')(((\tilde{B} \times_G \tilde{B}')/Y')^-) = \tilde{G} \times_G \tilde{G}' \text{ and } (\pi \times \pi')(((\tilde{B} \times_G \tilde{B}')/Y')^+) = (\tilde{G} \times_G \tilde{G}') [2]$$

using the fact that individually π and π' satisfy the respective property.

On the other hand, by construction one has that $i_2 \times i'_2$ and $i_3 \times i'_3$ are isomorphisms between the source groups and the double of the targets. This shows that $\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is closed under addition because the sequence $0 \rightarrow W_R[2^\infty] \rightarrow (B \times_G B')/Y \rightarrow G \rightarrow 0$ represents the class of the Baer sum of the two embeddable sequences in $\text{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$. Since $\text{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is finite, in order to conclude that $\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is a subgroup, one is only left to show that $\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is non-empty. To this end we refer the reader to Proposition 3.5, which in particular implies that $\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is non-empty (alternatively one could also directly prove that the split sequence is embeddable, which one can indeed show using the same steps of the proof of Proposition 3.5). Finally, given an embeddable sequence

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \xrightarrow{g} & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \rightarrow & W_R[2^\infty] & \xrightarrow{h} & B & \xrightarrow{f} & G \rightarrow 0 \end{array}$$

and a pair $(\varphi_1, \varphi_2) \in \text{Aut}_{\text{ring}}(R) \times \text{Aut}_{\text{ab.gr.}}(G)$, we can consider

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \xrightarrow{g\varphi_1} & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3\varphi_2^{-1} \\ 0 & \rightarrow & W_R[2^\infty] & \xrightarrow{h\varphi_1} & B & \xrightarrow{\varphi_2 f} & G \rightarrow 0 \end{array}$$

which gives an embeddability diagram for the sequence

$$(\varphi_1, \varphi_2)(0 \rightarrow W_R[2^\infty] \rightarrow B \rightarrow G \rightarrow 0)$$

showing that $\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is stable under the action of $\text{Aut}_{\text{ring}}(R) \times \text{Aut}_{\text{ab.gr.}}(G)$. \square

Denote by \mathcal{G}_2 a set of representatives of isomorphism classes of finite abelian 2-groups, viewed as C_2 -modules under the action of $-\text{Id}$. For an imaginary quadratic number field K , denote by $G_2(K)$ the unique representative of $2\text{Cl}(K)[2^\infty]$ in \mathcal{G}_2 . Suppose K is strongly of type R . Then $(\mathcal{O}_K/c)^*/\langle -1 \rangle$ can be identified with $R^*/\langle -1 \rangle$ via any restriction of a ring isomorphism, that is via any element of $\text{Isom}_{\text{ring}}(\mathcal{O}_K/c, R)$. Furthermore, we can identify $2\text{Cl}(K)[2^\infty]$ and $G_2(K)$ via any element of $\text{Isom}_{\text{ab.gr.}}(\text{Cl}(K)[2^\infty], G)$. Therefore applying $\text{Isom}_{\text{ring}}(\mathcal{O}_K/c, R) \times \text{Isom}_{\text{ab.gr.}}(2\text{Cl}(K)[2^\infty], G_2(K))$ to $S_2(K)$, we obtain a unique orbit

$$O_{c,2}(K) \in \widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G_2(K), W_R[2^\infty]) / (\text{Aut}_{\text{ring}}(R) \times \text{Aut}_{\text{ab.gr.}}(G)).$$

For K strongly of type R we use the notation

$$S'_2(K) := (G_2(K), O_{c,2}(K)).$$

If K is not strongly of type R , we set $S'_2(K)$ to be the symbol \bullet . We now proceed by offering a heuristic model for $S'_2(K)$ as K varies among imaginary quadratic number fields of type R . Let R be an unramified ring at c and denote by \mathcal{G}_2 a set of representatives of isomorphism classes of finite abelian 2-groups, viewed as C_2 -modules under the action of $-\text{Id}$. Denote by $\mathcal{S}_2(R)$ the union of the singleton $\{\bullet\}$ and of the set of equivalence classes of pairs (G, θ) , where $G \in \mathcal{G}_2$, $\theta \in \widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ and the equivalence is defined as follows: two pairs $(G_1, \theta_1), (G_2, \theta_2)$ are identified if $G_1 = G_2$ and θ_1, θ_2 are in the same $\text{Aut}_{\text{ring}}(R) \times \text{Aut}_{\text{ab.gr.}}(G)$ -orbit. Denote by $\widetilde{\mathcal{S}}_2(R)$ the union of the singleton $\{\bullet\}$ and the set of pairs (G, θ) , where $G \in \mathcal{G}_2$ and $\theta \in \widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$, thus bringing into play the quotient map

$$\pi : \widetilde{\mathcal{S}}_2(R) \rightarrow \mathcal{S}_2(R).$$

Consider the sigma algebra generated by all subsets on $\widetilde{\mathcal{S}}_2(R)$, as well as on $\mathcal{S}_2(R)$, and equip $\widetilde{\mathcal{S}}_2(R)$ with the measure

$$\tilde{\mu}_{\text{seq}}((G, \theta)) := \frac{\mu_{\text{CL}}(G)}{\#\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])}, \tilde{\mu}_{\text{seq}}(\{\bullet\}) = 0,$$

where μ_{CL} denotes, as usual, the Cohen–Lenstra probability measure on \mathcal{G}_2 that gives to each abelian 2-group G weight inversely proportional to the size of the automorphism group of G . Push forward, via π , the measure $\tilde{\mu}_{\text{seq}}$ to a measure μ_{seq} on $\mathcal{S}_2(R)$. It is clear by construction that $\tilde{\mu}_{\text{seq}}$ and μ_{seq} are probability measures.

The heuristic assumption that we propose for the 2-part of ray class sequences of conductor c of imaginary quadratic fields of type R is as follows.

Heuristic assumption 3.4. *For any ‘reasonable’ function $f : \mathcal{S}_2(R) \rightarrow \mathbb{R}$ one has that, as K varies among imaginary quadratic number fields of type R , the following equality of averages takes place*

$$\lim_{X \rightarrow \infty} \frac{\sum_{-D(K) \leq X} f(S'_2(K))}{\#\{-D(K) \leq X\}} = \sum_{S \in \mathcal{S}_2(R)} f(S) \mu_{\text{seq}}(S).$$

As a consistency check, observe that the above identity of average takes place if one chooses as f the indicator function of $\{\bullet\}$: indeed, since the number of K with $D(K) \leq X$ that are not strongly of type R is at most $\ll_c X(\log X)^{-1/\varphi(c)}$, we see that we obtain 0 in the left side, while in the right side we obtain 0 by definition. Clearly one can readily formulate the analogues of Conjectures 2.5 and 2.6. We shall instead opt to devote the rest of the section to the analogues of Conjectures 2.8-2.10.

If $\alpha \in R^*/\langle -1 \rangle$ then $\alpha^2 N(\alpha) \in W_R$, where $N(\cdot)$ is the norm-function with respect to the C_2 -action prescribed to $R^*/\langle -1 \rangle$: indeed both α^2 and $N(\alpha)$ are in W_R . We define the map $g_R : R^*/\langle -1 \rangle \rightarrow W_R$ given by $\alpha \mapsto \alpha^2 N(\alpha)$. With a small abuse of notation, we use the same notation for the induced map $g_R : \frac{R^*/\langle -1 \rangle}{(R^*/\langle -1 \rangle)^2} \rightarrow W_R/2W_R$ and we denote by $\text{Im}(g_R)$ the image of g_R in $W_R/2W_R$.

Proposition 3.5. *The image of the natural map*

$$\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R) \rightarrow \text{Hom}_{\mathbb{F}_2[C_2]}(G[2], W_R/2W_R)$$

is

$$\text{Hom}_{\mathbb{F}_2[C_2]}(G[2], \text{Im}(g_R)) \quad (= \text{Hom}_{\mathbb{F}_2}(G[2], \text{Im}(g_R))).$$

Proof. Consider θ an embeddable sequence

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \rightarrow & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \rightarrow & W_R[2^\infty] & \rightarrow & B & \xrightarrow{f} & G \rightarrow 0 \end{array}$$

and pick $b \in G[2]$. By definition of embeddability there exist \mathfrak{b} in \tilde{B}^+ such that $\pi(\mathfrak{b}) = i_3(b)$. On the other hand we can find $x \in \tilde{B}$ such that $\pi(2x) = i_3(b)$. Therefore there exists an element $\alpha \in \frac{(R)^*}{\langle -1 \rangle}[2^\infty]$ such that $\mathfrak{b}\alpha^{-1} = x^2$, which implies that $\mathfrak{b}^2 N(\alpha)^{-1} = N(x)^2$. Furthermore, $2x$ is in B , hence we have that $\delta_2(\theta)(b) = \mathfrak{b}^2 \alpha^{-2}$ as an element of $W_R/2W_R$. However note that $N(x)^2 \in 2W_R$: indeed, by definition of embeddability, we can always write $x = x^- \beta$ with x^- an anti-fixed point and $\beta \in \frac{R^*}{\langle -1 \rangle}$, so that $N(x)^2 = N(\beta)^2 \in W_R$. Therefore we find that $\delta_2(\theta)(b) = N(\alpha)\alpha^2$, i.e. $\delta_2(\theta)(b) \in \text{Im}(g_R)$.

Conversely, we prove that given a C_2 -map $\delta_0 : G[2] \rightarrow \text{Im}(g_R)$, there exists a $\theta \in \widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}$ such that $\delta_2(\theta) = \delta_0$. Firstly observe that $\text{Hom}_{\mathbb{F}_2[C_2]}(G[2], \text{Im}(g_R)) = \text{Hom}_{\mathbb{F}_2}(G[2], \text{Im}(g_R))$, since τ clearly fixes $N(\alpha)$ for any α in R and $\alpha^2 \tau(\alpha^2) = N(\alpha)^2 \in 2W_R$, therefore τ acts trivially on $\text{Im}(g_R)$ (see Lemma 3.6 for a more general fact). Thus pick $\delta_0 \in \text{Hom}_{\mathbb{F}_2}(G[2], \text{Im}(g_R))$. We divide the construction of θ and its embedding in four steps:

Step 1: Observe that $\alpha^2 N(\alpha) = \frac{\alpha^2}{N(\alpha)} N(\alpha)^2 = \frac{\alpha}{\tau(\alpha)} N(\alpha)^2$. Since $N(\alpha)^2 \in 2W_R[2^\infty]$, we conclude that any element of $\text{Im}(g_R)$ can be represented as $\frac{\alpha}{\tau(\alpha)}$ for some $\alpha \in \frac{R^*}{\langle -1 \rangle}[2^\infty]$.

Step 2: Write $G = \langle e_1 \rangle \oplus \dots \oplus \langle e_j \rangle$, with the order of e_i being 2^{m_i} for a positive integer m_i , for each $i \in \{1, \dots, j\}$. Therefore $G[2] = \langle 2^{m_1-1} e_1 \rangle \oplus \dots \oplus \langle 2^{m_j-1} e_j \rangle$ and now, use Step 1 for each $i \in \{1, \dots, j\}$ to construct $\alpha_i \in \frac{R^*}{\langle -1 \rangle}[2^\infty]$ such that $\delta_0(2^{m_i-1} e_i) = \frac{\alpha_i}{\tau(\alpha_i)}$.

Step 3: Embed G in a group $\tilde{G} = \langle \tilde{e}_1 \rangle \oplus \dots \oplus \langle \tilde{e}_j \rangle \oplus \langle d_1 \rangle \oplus \dots \oplus \langle d_h \rangle$, with the rules $2\tilde{e}_i = e_i$ for every i in $\{1, \dots, j\}$, $2d_s = 0$ for every $s \in \{1, \dots, h\}$ and $h \geq \text{rk}_2((\mathbb{Z}/c\mathbb{Z})^*) - 1$. Take an extension $\theta \in \text{Ext}_{\mathbb{Z}_2}(\tilde{G}, \frac{R^*}{\langle -1 \rangle})$ such that for every $i \in \{1, \dots, j\}$ one has that $\delta_{2^{m_i+1}}(\theta)(\tilde{e}_i) = \frac{\alpha_i}{\tau(\alpha_i)}$ and such that $\langle \{\delta_2(\theta)(d_1), \dots, \delta_2(\theta)(d_h)\} \rangle = \text{Im}((\mathbb{Z}/c\mathbb{Z})^* \rightarrow W_R/2W_R)$. Call \tilde{B} the middle term of this extension. Pick $\tilde{e}'_1, \dots, \tilde{e}'_j$ liftings of e_1, \dots, e_j with the property that $2^{m_i+1} \tilde{e}'_i = \frac{\alpha_i}{\tau(\alpha_i)}$

for all i in $\{1, \dots, j\}$. Choose also d'_1, \dots, d'_h liftings of d_1, \dots, d_h in \tilde{B} and put $2\tilde{B} = B$. Observe that by construction the kernel of $B \rightarrow G$ is $W_R[2^\infty]$. This gives a commutative diagram of \mathbb{Z}_2 -modules,

$$\begin{array}{ccccccc} 0 & \rightarrow & \frac{(R)^*}{\langle -1 \rangle}[2^\infty] & \rightarrow & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \rightarrow 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \rightarrow & W_R[2^\infty] & \rightarrow & B & \xrightarrow{f} & G \rightarrow 0. \end{array}$$

By construction i_2 and i_3 are isomorphisms between the source groups and the double of the target groups.

Step 4: Define $A_1 := \langle \{e'_1, \dots, e'_j\} \rangle$, $A_2 := \langle \{d'_1, \dots, d'_h\} \rangle$ and $A := \langle A_1, A_2 \rangle$. Consider A_1 as a C_2 -module with the $-\text{Id}$ -action and A_2 with the Id -action. Observe that, by construction, the C_2 -action on A_1 and A_2 restrict to the same C_2 -action on $A_1 \cap A_2$. Therefore the C_2 -action extend to an action on A . Observe that, by construction, the C_2 -action on A and $\frac{R^*}{\langle -1 \rangle}[2^\infty]$ restricts to the same C_2 -action on $A \cap \frac{R^*}{\langle -1 \rangle}[2^\infty]$. It is also clear that $\langle A, \frac{R^*}{\langle -1 \rangle}[2^\infty] \rangle = \tilde{B}$. Therefore one can put on \tilde{B} a C_2 -action which restricted to A is $-\text{Id}$ and restricted to $\frac{R^*}{\langle -1 \rangle}$ is the usual action. This turns the above diagram into a diagram of C_2 -modules, and we want to prove that the top sequence remains exact when we take $(1 + \tau)$ -torsion and when we take $(1 - \tau)$ -torsion. But by construction

$$\begin{aligned} (1 + \tau)(\tilde{B}) &= (1 + \tau)\left(\langle A_1, A_2, R^*/\langle -1 \rangle \rangle\right) = (1 + \tau)\left(\langle A_2, R^*/\langle -1 \rangle \rangle\right) \\ &= \langle 2A_2, (1 + \tau)(R^*/\langle -1 \rangle) \rangle \subseteq \langle (1 + \tau)(R^*/\langle -1 \rangle) \rangle \end{aligned}$$

and

$$\begin{aligned} (1 - \tau)(\pi^{-1}(\tilde{G}[2])) &= (1 - \tau)(\langle A_1 \cap \ker(2\pi), R^*/\langle -1 \rangle \rangle) \\ &= \langle 2(A_1 \cap \ker(2\pi)), (1 - \tau)(R^*/\langle -1 \rangle) \rangle \\ &\subseteq (1 - \tau)(R^*/\langle -1 \rangle), \end{aligned}$$

where the last two inclusions follow from Step 3. This shows that δ_0 can be realized as $\delta_2(\theta)$ for some θ in $\widetilde{\text{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ (i.e. $0 \rightarrow W_R[2^\infty] \rightarrow B \xrightarrow{f} G \rightarrow 0$). \square

If K is strongly of type R , we denote by $\delta_2(K)$ the map $\delta_2(S_2(K))$. By choosing any ring identification in $\text{Isom}_{\text{ring}}(\mathcal{O}_K/c, R)$ and any identification in $\text{Isom}_{\text{ab.gr.}}(2\text{Cl}(K), G_2(K))$ we obtain an $\text{Aut}_{\text{ring}}(R)$ -orbit of subspaces of $W_R/2W_R$. On the other hand this orbit is composed of a single element due to the following fact:

Lemma 3.6. *The action of $\text{Aut}_{\text{ring}}(R)$ on $\text{Im}(g_R)$ is trivial.*

Proof. Consider the ring decomposition $R = \prod_{l|c} R_l/lR$. It is clear that the following holds, $\text{Aut}_{\text{ring}}(R) = \prod_{l|c} \text{Aut}_{\text{ring}}(R_l/lR)$. On the other hand, this decomposition is compatible with g_R , i.e. $g_R = \prod_{l|c} g_{R_l/lR}$, where \prod of maps is to be thought of as the map obtained by applying the maps coordinatewise. This reduces the claim to $c = l$ a prime number. In that case one has that $\alpha^2\tau(\alpha)^2 = N(\alpha)^2$, but $N(\alpha)^2$ is in $2W_R$, therefore, modulo $2W_R$, one has that $\alpha^2N(\alpha)$ is fixed by τ . \square

Hence we see that $\text{Im}(\delta_2(K))$ can be identified with a well-defined subgroup of $\text{Im}(g_R)$. We will keep denoting this subgroup as $\text{Im}(\delta_2(K))$. Moreover, thanks to Proposition 3.5 and the fact that the pushforward, via an epimorphism, of the counting probability measure induces

the counting probability measure on the target group, we readily obtain the prediction of the distribution of the pair $(\#(2 \text{Cl}(K))[2], \text{Im}(\delta_2(K)))$.

Fix a subspace $Y \subseteq \text{Im}(g_R)$ and a non-negative integer j .

Prediction 3.7. *As K varies among imaginary quadratic number fields of type R , we have the following equality*

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\#\{K : -D(K) \leq X, \#(2 \text{Cl}(K))[2] = 2^j \text{ and } \text{Im}(\delta_2(K)) = Y\}}{\#\{K : -D(K) \leq X\}} \\ &= \mu_{\text{CL}}(G \in \mathcal{G}_2 : \#G[2] = 2^j) \frac{\# \text{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j, Y)}{\# \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j, \text{Im}(g_R))}. \end{aligned}$$

This will be proved in Theorem 5.2, but see also Theorem 5.4 for a more explicit statement. A crucial step is to deduce it from a statement about *mixed moments*. Indeed, observe that to know the pair

$$(\#G[2], \text{Im}(\delta : G[2] \rightarrow \text{Im}(g_R)))$$

is equivalent to knowing for each χ in the dual group $\widehat{\text{Im}(g_R)}$, the value of

$$m_\chi(\delta) := \#\ker(\chi(\delta)).$$

For each $\chi \in \widehat{\text{Im}(g_R)}$, fix a non-negative integer k_χ .

Notation. For any function $\widehat{\text{Im}(g_R)} \rightarrow \mathbb{Z}_{\geq 0}$, $\chi \mapsto k_\chi$, we will use the notation

$$|\mathbf{k}|_1 := \sum_{\chi \in \widehat{\text{Im}(g_R)}} k_\chi.$$

Pick a random subset of $\widehat{\text{Im}(g_R)}$ by choosing each character χ independently at random with the rule that χ is not in the set with probability $\frac{1}{2^{k_\chi}}$ and that χ is in the set with probability $\frac{2^{k_\chi}-1}{2^{k_\chi}}$. For a subspace $Y \subseteq \widehat{\text{Im}(g_R)}$ denote by $\mathbb{P}_{(k_\chi)}(Y)$ the probability that such a random subset generates Y . Observe that if $\dim(Y) > |\mathbf{k}|_1$ then $\mathbb{P}_{(k_\chi)}(Y) = 0$: indeed, in that case we select with probability 1 less characters than $\dim_{\mathbb{F}_2}(Y)$, so they they generate Y with zero probability. Denote by $\mathcal{A}_2(j)$ the number of vector subspaces of \mathbb{F}_2^j . If $j < 0$, we shall make sense of the expression $0 \cdot \mathcal{A}_2(j)$ by setting it equal to 0.

The following proposition reveals the value predicted by the heuristic model for the $(k_\chi)_{\chi \in \widehat{\text{Im}(g_R)}}$ -mixed moment. In what follows we use the convention $m_\chi(\delta_S) = 0$ if we have $S = \bullet \in \mathcal{S}_2(R)$.

Proposition 3.8. *One has that*

$$\sum_{S \in \mathcal{S}_2(R)} \mu_{\text{seq}}(S) \prod_{\chi \in \widehat{\text{Im}(g_R)}} m_\chi(\delta_S)^{k_\chi} = \sum_{Y \subseteq \widehat{\text{Im}(g_R)}} \mathbb{P}_{(k_\chi)}(Y) \mathcal{A}_2(|\mathbf{k}|_1 - \dim(Y)).$$

We do not spell out the proof of Proposition 3.8 because it is identical to the proof of Proposition 4.8 which we will provide in §4.

Proposition 3.8 leads to the following prediction.

Prediction 3.9. *As K varies among imaginary quadratic number fields of type R , the following equality of averages takes place*

$$\lim_{X \rightarrow \infty} \frac{\sum_{-D(K) \leq X} \prod m_\chi(\delta_2(K))^{k_\chi}}{\#\{K : -D(K) \leq X\}} = \sum_{V \subseteq \text{Im}(g_R)} \mathbb{P}_{(k_\chi)}(V) \mathcal{A}_2(|\mathbf{k}|_1 - \dim(V)).$$

A stronger statement will be proved in Theorem 5.1.

As a cruder result, one derives a prediction for the joint-distribution of the 4-ranks of the class group and the ray class group. Let j_1, j_2 be two non-negative integers. Then we have the following prediction.

Prediction 3.10. *As K varies among imaginary quadratic number fields of type R , we have the following equality*

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\#\{K : -D(K) \leq X, \text{rk}_4(\text{Cl}(K)) = j_1, \text{rk}_4(\text{Cl}(K, c)) = j_2\}}{\#\{K : -D(K) \leq X\}} \\ &= \mu_{\text{CL}}(G \in \mathcal{G}_2 : \dim_{\mathbb{F}_2}(G[2]) = j_1) \frac{\#\{\varphi \in \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \text{Im}(g_R)) : \text{rk}(\varphi) = \text{rk}_2(W_R) - (j_2 - j_1)\}}{\#\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \text{Im}(g_R))}. \end{aligned}$$

This will be proved in Theorem 5.3, but see also Theorem 5.4 for a more explicit law. Similarly, the heuristic of the present section can be used to conjecturally predict the distribution of the pair $(\text{rk}_{2^m}(\text{Cl}(K)), \text{rk}_{2^m}(\text{Cl}(K, c)))$ among imaginary quadratic number fields K with $\gcd(D(K), c) = 1$. For reasons of space we do not explicitly state such a conjecture but it is implicitly given in the present section; such a conjecture might be within reach given the recent work of Smith [16].

4. SPECIAL DIVISORS AND 4-RANK

Let D be a square-free odd positive integer. In this section we introduce the notion of *special divisors* of D , which will be instrumental in our proof of Theorems 5.1, 5.2, 5.3, and 5.4. We call a positive divisor d of D *special* if d is a square modulo D/d and D/d is a square modulo d . We denote by $S(D)$ the set of special divisors of D , and by $T(D)$ the set of all divisors of D . The set $T(D)$ has naturally the structure of a vector space over \mathbb{F}_2 under the operation

$$d_1 \odot d_2 := \frac{d_1 d_2}{\gcd(d_1, d_2)^2}.$$

Lemma 4.1. *The set $S(D)$ is a subspace of $T(D)$ over \mathbb{F}_2 .*

Proof. We need to show that if d_1, d_2 are special then $d_1 \odot d_2$ is special as well. This amounts to showing firstly that if a prime q divides D but $q \nmid d_1 \odot d_2$ then $d_1 \odot d_2$ is a square (mod q) and secondly that if a prime q divides $d_1 \odot d_2$ then $D/d_1 \odot d_2$ is a square (mod q).

For the proof of the first claim, suppose that $q|D$ but $q \nmid d_1 \odot d_2$. Then either $\gcd(d_1 d_2, q) = 1$ or $q|\gcd(d_1, d_2)$. In the first case we know that, since both d_1 and d_2 are special, d_1 and d_2 are both squares (mod q), thus showing that $d_1 \odot d_2$ is a square (mod q). In the second case we know that, since both d_1 and d_2 are special, D/d_1 and D/d_2 are both squares (mod q). This shows that

$$\frac{D}{d_1} \frac{D}{d_2} = (d_1 \odot d_2) \left(\frac{D}{\frac{d_1 d_2}{\gcd(d_1, d_2)^2}} \right)^2$$

is a square (mod q), hence $d_1 \odot d_2$ is a square (mod q).

Next, suppose that $q \mid d_1 \odot d_2$. Then, either $q \mid d_1$ and $q \nmid d_2$, or $q \mid d_2$ and $q \nmid d_1$: by symmetry we are allowed to focus on the former case. Then, since both d_1 and d_2 are special, we have that both D/d_1 and d_2 are squares (mod q). Therefore

$$\frac{D}{d_1} \frac{1}{d_2} \gcd(d_1, d_2)^2 = \frac{D}{(d_1 \odot d_2)}$$

is a square (mod q), thus concluding our proof. \square

Let n be another square-free odd positive integer with $\gcd(n, D) = 1$ and consider the group $G_n := (\mathbb{Z}/n\mathbb{Z})^*/(\mathbb{Z}/n\mathbb{Z})^{*2}$. One has a natural map $\varphi_{n,D} : S(D) \rightarrow G_n$ by reducing (mod n) and then modulo squares.

Lemma 4.2. *The map $\varphi_{n,D}$ is a homomorphism of \mathbb{F}_2 -vector spaces.*

Proof. By definition we have $d_1 \odot d_2 = \frac{d_1 d_2}{\gcd(d_1, d_2)^2}$ and reducing this equality (mod n) and then modulo squares, the right side yields $d_1 d_2$. Thus $\varphi_{n,D}(d_1 \odot d_2) = \varphi_{n,D}(d_1) \varphi_{n,D}(d_2)$. \square

Observe that $S(D)$ always contains the subgroup $\{1, D\}$. It is then a consequence of the work of Fouvry and Klüners [8] that $S(D)/\{1, D\}$ behaves like the 2-torsion of a random abelian 2-group, in the sense of Cohen and Lenstra. In other words, for every positive integer j we have

$$\lim_{X \rightarrow \infty} \frac{\#\{1 \leq D \leq X, D \text{ square-free} : S(D)/\{1, D\} \cong \mathbb{F}_2^j\}}{\#\{1 \leq D \leq X, D \text{ square-free}\}} = \mu_{\text{CL}}(A \in \mathcal{G}_2 : A[2] \cong \mathbb{F}_2^j),$$

where \mathcal{G}_2 is a set of representatives of isomorphism classes of finite abelian 2-groups. The present section in addition to Theorems 5.6-5.7, §6 and §7 are devoted to the determination of the distribution of the pair

$$(\#S(D), \text{Im}(\varphi_{n,D})).$$

The general heuristic constructed in §3 specializes to a heuristic model for this pair, thanks to the commutative diagram after Lemma 5.5. However, we choose to give here a direct presentation of this heuristic avoiding ray class groups. Therefore the present section, Theorems 5.6-5.7, §6 and §7 are completely self-contained.

Before proceeding we introduce a modification of $\varphi_{n,D}$ which will be required in the ray class group applications in §5. Denote by L_n the subgroup of G_n generated by an integer which is a quadratic non-residue modulo every prime dividing n and write $\tilde{G}_n := G_n/L_n$. Now let n_1, n_2 be two integers such that $2Dn_1n_2$ is square-free and assume that D is a square modulo n_1 and generates $L_{n_2} \pmod{n_2}$. Denote by $\varphi_{n_1, n_2, D}$ the natural map

$$\varphi_{n_1, n_2, D} : S(D)/\{1, D\} \rightarrow G_{n_1} \times \tilde{G}_{n_2}.$$

Our goal is to understand the statistical behavior of the pair

$$(\#S(D), \text{Im}(\varphi_{n_1, n_2, D})),$$

as D varies through positive square-free integers coprime to $n_1 n_2$, which are squares (mod n_1) and non-squares modulo every prime dividing n_2 . There is an obvious guess: namely that, once $\dim_{\mathbb{F}_2}(S(D)/\{1, D\}) = j$ is fixed, then $\text{Im}(\varphi_{n_1, n_2, D})$ should distribute as the image of a random map $\varphi : \mathbb{F}_2^j \rightarrow G_{n_1} \times \tilde{G}_{n_2}$. We formalize this guess in a more general heuristic principle.

Definition 4.3. Consider the set \mathcal{M}_{n_1, n_2} consisting of equivalence classes of pairs (A, V) , where A is a vector space over \mathbb{F}_2 and V is a vector subspace of $G_{n_1} \times \tilde{G}_{n_2}$: declare $(A_1, V_1), (A_2, V_2)$ identified, if A_1 and A_2 have the same \mathbb{F}_2 -dimension and $V_1 = V_2$. Denote this equivalence relation by \sim . Each representative pair (\mathbb{F}_2^j, V) is equipped with the following mass,

$$\mu((\mathbb{F}_2^j, V)) := \mu_{\text{CL}}(A \in \mathcal{G}_2 : A[2] \cong \mathbb{F}_2^j) \frac{\# \text{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j, V)}{\# \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j, G_{n_1} \times \tilde{G}_{n_2})}.$$

By construction, this is a probability measure on \mathcal{M}_{n_1, n_2} .

Now we formulate the following.

Heuristic assumption 4.4. For any ‘reasonable’ function $f : \mathcal{M}_{n_1, n_2} \rightarrow \mathbb{R}$ one has

$$\lim_{X \rightarrow \infty} \frac{\sum_{D \leq X} f((S(D)/\{1, D\}, \text{Im}(\varphi_{n_1, n_2, D})))}{\sum_{D \leq X} 1} = \sum_{T \in \mathcal{M}_{n_1, n_2}} f(T) \mu(T),$$

where in both sums D varies among square-free positive integers which are squares (mod n_1) and non-squares modulo any prime divisor of n_2 . Furthermore, for any positive integers a, r with $\gcd(r, an_1n_2) = 1$ the same holds if we have the additional restriction $D \equiv a \pmod{r}$.

The simple case where f is the indicator function of an element $(\mathbb{F}_2^j, V) \in \mathcal{M}_{n_1, n_2}$ yields the following prediction.

Prediction 4.5. We have

$$\lim_{X \rightarrow \infty} \frac{\#\{D \leq X, (S(D)/\{1, D\}, \varphi_{n_1, n_2, D}) \sim T\}}{\#\{D \leq X\}} = \mu(T),$$

where D varies among square-free positive integers which are squares (mod n_1) and non-squares modulo every prime divisor of n_2 .

This prediction will be confirmed in Theorem 5.7.

Despite the fact that the ‘random variable’ $(S(D), \text{Im}(\varphi_{n_1, n_2, D}))$ does not consist of two numbers, we achieve its distribution by means of the moment-method. For this we shall replace the pair $(S(D), \text{Im}(\varphi_{n_1, n_2, D}))$ by a higher-dimensional numerical ‘random variable’, which we proceed to define. For each character χ in the dual of $G_{n_1} \times \tilde{G}_{n_2}$ define

$$m_\chi(D) := \#\{d \in S(D) : \chi(\varphi_{n_1, n_2, D}(d)) = 1\} \tag{4.1}$$

and recall that $\text{Im}(\varphi_{n_1, n_2, D})^\perp$ is the set of all character χ with $\chi \circ \varphi_{n_1, n_2, D}$ being trivial. Clearly for each $\chi \in \text{Im}(\varphi_{n_1, n_2, D})^\perp$ we have $m_\chi(D) = m_1(D) = \#S(D)$, while for the remaining characters we have $m_\chi(D) = \#S(D)/2$. Therefore the knowledge of the pair

$$(\#S(D), \text{Im}(\varphi_{n_1, n_2, D}))$$

is equivalent to the knowledge of

$$(m_\chi(D))_{\chi \in \hat{G}_{n_1} \times \hat{G}_{n_2}}.$$

It will transpire that this shift in focus will be advantageous since it will allow us to study the asymptotic behaviour of the latter vector by the method of moments.

We conclude this section by providing a prediction regarding the mixed moments of $(m_\chi(D))$. This will be later used in the proof of Theorem 5.6.

Notation 4.6. For any function $\widehat{G}_{n_1} \times \widehat{G}_{n_2} \rightarrow \mathbb{Z}_{\geq 0}$, $\chi \mapsto k_\chi$, we will use the notation

$$\mathbf{k} := (k_\chi)_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \quad \text{and} \quad |\mathbf{k}|_1 := \sum_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} k_\chi.$$

Definition 4.7. For any subspace $Y \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}$, denote by $\mathbb{P}_{(k_\chi)}(Y)$ the probability that a random subset of $\widehat{G}_{n_1} \times \widehat{G}_{n_2}$ generates Y , where the characters χ are chosen independently and with probability $1 - 2^{-k_\chi}$.

For any pair (\mathbb{F}_2^j, Y) in \mathcal{M}_{n_1, n_2} , define $m_\chi((\mathbb{F}_2^j, Y))$ to be 2^j if $\chi(Y) = 1$, and 2^{j-1} otherwise. Observe that if $\dim(Y) > |\mathbf{k}|_1$ then $\mathbb{P}_{(k_\chi)}(Y) = 0$. Denote by $\mathcal{N}_2(j)$ the number of vector subspaces of \mathbb{F}_2^j . If $j < 0$ we define $\mathcal{N}_2(j) := 1$. It is important to note that every time $\mathcal{N}_2(j)$ appears for some negative j then it will always appear multiplied by zero.

Proposition 4.8. *One has that*

$$\sum_{T \in \mathcal{M}_{n_1, n_2}} \left(\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(T)^{k_\chi} \right) \mu(T) = \sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathcal{N}_2(|\mathbf{k}|_1 - \dim(W)).$$

Proof. We want to compute

$$\sum_{(\mathbb{F}_2^j, \delta)} \left(\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi((\mathbb{F}_2^j, \delta)^{k_\chi}) \right) \mu((\mathbb{F}_2^j, \delta)),$$

where j ranges over non-negative integers, δ ranges over $\text{Hom}(\mathbb{F}_2^j, G_{n_1} \times \widetilde{G}_{n_2})$ and

$$\mu((\mathbb{F}_2^j, \delta)) = \frac{\mu_{\text{CL}}(A \in \mathcal{G}_2 : \#A[2] = 2^j)}{\#\text{Hom}(\mathbb{F}_2^j, G_{n_1} \times \widetilde{G}_{n_2})}.$$

Therefore the sum becomes

$$\sum_{V \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \sum_{j \geq 0} \frac{2^{j|\mathbf{k}|_1}}{2^{\sum_{\chi \in V} k_\chi}} \frac{\#\text{Epi}(\mathbb{F}_2^j, V^\perp)}{\#\text{Hom}(\mathbb{F}_2^j, G_{n_1} \times \widetilde{G}_{n_2})} \mu_{\text{CL}}(A \in \mathcal{G}_2 : \#A[2] = 2^j).$$

We assume familiarity of the reader with Möbius inversion in posets, see [17, Chapter 3], for example. Writing $\text{Epi}(\mathbb{F}_2^j, V^\perp)$ via inclusion-exclusion on the poset of vector subspaces of $G_{n_1} \times \widetilde{G}_{n_2}$ and exchanging the order of summation we obtain

$$\sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \left(\sum_{V \subseteq W} \frac{\mu(V, W)}{2^{\sum_{\chi \in V} k_\chi}} \right) \left(\sum_{G \in \mathcal{G}_2} \#G[2]^{|\mathbf{k}|_1 - \dim(W)} \mu_{\text{CL}}(G) \right).$$

By applying Möbius inversion with respect to the poset of vector subspaces, to the obvious relation

$$2^{-\sum_{\chi \in W} k_\chi} = \mathbb{P}_{(k_\chi)}(V \subseteq W) = \sum_{V \subseteq W} \mathbb{P}_{(k_\chi)}(V)$$

we obtain

$$\mathbb{P}_{(k_\chi)}(W) = \sum_{V \subseteq W} \frac{\mu(V, W)}{2^{\sum_{\chi \in V} k_\chi}}.$$

On the other hand, one has that whenever $|\mathbf{k}|_1 - \dim(W) \geq 0$, then

$$\sum_{G \in \mathcal{G}_2} \#G[2]^{|\mathbf{k}|_1 - \dim(W)} \mu_{\text{CL}}(G) = \mathcal{N}_2(|\mathbf{k}|_1 - \dim(W)).$$

Instead, when $|\mathbf{k}|_1 - \dim(W) < 0$, we have that $\mathbb{P}_{(k_\chi)}(W) = 0$. In conclusion we get that the total sum equals

$$\sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathcal{N}_2(|\mathbf{k}|_1 - \dim(W)). \quad \square$$

Choosing $f(T) = \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(T)^{k_\chi}$ in Heuristic assumption 4.4 suggests the following prediction by means of Proposition 4.8.

Prediction 4.9. *We have*

$$\lim_{X \rightarrow \infty} \frac{\sum_{D \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi}}{\sum_{D \leq X} 1} = 2^{|\mathbf{k}|_1} \sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathcal{N}_2(|\mathbf{k}|_1 - \dim(W)),$$

where in both sums D varies among square-free positive integers which are squares (mod n_1) and non-squares modulo every prime divisors of n_2 .

A version of Prediction 4.9 with an explicit error term is proved in Theorem 5.6. This prediction has a noteworthy feature: it realizes the (k_χ) -mixed moments of $(m_\chi(D))$ as an average over all subspaces of $\widehat{G}_{n_1} \times \widehat{G}_{n_2}$ of ordinary moments of $\#S(D)$ and in doing so, it suggests the first step of the proof of Theorem 5.6, see (6.2).

5. MAIN THEOREMS ON THE 2-PART OF RAY CLASS SEQUENCES

Throughout the section we keep the notation used in §3. We begin by stating Theorems 5.1, 5.2 and 5.3 that corroborate Predictions 3.7, 3.9 and 3.10 when $D(K) \equiv 1 \pmod{4}$. We restrict our attention to the cases with $D(K) \equiv 1 \pmod{4}$ only for the sake of brevity, the remaining case being amenable to a similar analysis. Our main task in this section will then be to reduce Theorems 5.1, 5.2, 5.3 and 5.4 that are about ray class groups to Theorems 5.6 and 5.7 which regard only special divisors.

Theorem 5.1. *For any $\beta \in \mathbb{R}$ satisfying $0 < \beta < \min\{2^{-|\mathbf{k}|_1}, \varphi(c)^{-1}\}$ we have*

$$\frac{\sum_{-D(K) \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(\delta_2(K))^{k_\chi}}{\sum_{-D(K) \leq X} 1} = \sum_{V \subseteq \widehat{\text{Im}}(g_R)} \mathbb{P}_{(k_\chi)}(V) \mathcal{N}_2(|\mathbf{k}|_1 - \dim(V)) + O((\log X)^{-\beta}),$$

where in both sums K varies among imaginary quadratic number fields of type R , having $D(K) \equiv 1 \pmod{4}$ and the implied constant depends at most on c and $(k_\chi)_\chi$.

Theorem 5.2. *We have*

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\#\{K : -D(K) \leq X, \#(2\text{Cl}(K))[2] = 2^j \text{ and } \text{Im}(\delta_2(K)) = Y\}}{\#\{K : -D(K) \leq X\}} \\ &= \mu_{\text{CL}}(G \in \mathcal{G}_2 : \#G[2] = 2^j) \frac{\#\text{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j, Y)}{\#\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j, \text{Im}(g_R))}, \end{aligned}$$

where K varies among imaginary quadratic number fields with $D(K) \equiv 1 \pmod{4}$ and of type R .

Recall the definition of W_R in (3.1) and the definition of the map g_R before the statement of Proposition 3.5.

Theorem 5.3. *We have*

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\#\{K : -D(K) \leq X, \text{rk}_4(\text{Cl}(K)) = j_1, \text{rk}_4(\text{Cl}(K, c)) = j_2\}}{\#\{K : -D(K) \leq X\}} \\ &= \mu_{\text{CL}}(G \in \mathcal{G}_2 : \dim_{\mathbb{F}_2}(G[2]) = j_1) \frac{\#\{\varphi \in \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \text{Im}(g_R)) : \text{rk}(\varphi) = \text{rk}_2(W_R) - (j_2 - j_1)\}}{\#\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \text{Im}(g_R))}, \end{aligned}$$

where K varies among imaginary quadratic number fields with $D(K) \equiv 1 \pmod{4}$ and of type R .

We will prove a stronger version of Theorems 5.1, 5.2 and 5.3. Namely, the fact that we deal with progressions $a \pmod{q}$ in Theorems 5.6 and 5.7 yields results analogous to the ones in Theorems 5.1, 5.2 and 5.3 when one imposes finitely many unramified local conditions at primes independent of c on the discriminants $D(K)$. This supports the point of view in Wood's recent work [20] that local conditions on the quadratic field do not affect the distribution of class groups, with the obvious modification that for ray class groups such conditions must be taken independently of the primes dividing c .

We proceed to restate Theorem 5.3 in a more explicit way. Recalling that c is square-free we let $n_1(R)$ be the product of the prime divisors of c which are either $3 \pmod{4}$ and inert in R , or $1 \pmod{4}$ and split. Furthermore, let $n_2(R)$ be the product of the prime divisors of c that are $3 \pmod{4}$ and split in R . Recall that

$$\frac{\eta_{\infty}(2)}{\eta_{j_1}(2)^2 2^{j_1^2}} = \mu_{\text{CL}}(G \in \mathcal{G}_2 : \dim_{\mathbb{F}_2}(G[2]) = j_1).$$

Theorem 5.4. *We have*

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\#\{K : -D(K) \leq X, \text{rk}_4(\text{Cl}(K)) = j_1, \text{rk}_4(\text{Cl}(K, c)) = j_2\}}{\#\{K : -D(K) \leq X\}} \\ &= \frac{\eta_{\infty}(2)}{\eta_{j_1}(2)^2 2^{j_1^2}} \frac{\#\{\varphi \in \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, G_{n_1(R)} \times \tilde{G}_{n_2(R)}) : \text{rk}(\varphi) = \text{rk}_2(W_R) - (j_2 - j_1)\}}{\#\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, G_{n_1(R)} \times G_{n_2(R)})}, \end{aligned}$$

where K varies among imaginary quadratic number fields with $D(K) \equiv 1 \pmod{4}$ and of type R .

The congruence conditions $\pmod{4}$ related to the definition of $n_1(R)$ and $n_2(R)$ in Theorem 5.4 are analogous to the congruences $\pmod{3}$ for the primes l appearing in the first part of Varma's Theorem 2.13.

Our next goal is to realise the δ_2 -map

$$\delta_2(\mathbb{Q}(\sqrt{-D})) : (2 \text{Cl}(\mathbb{Q}(\sqrt{-D}))) [2] \rightarrow \text{Im}(g_R)$$

with the map on special divisors introduced in §4,

$$\varphi_{n_1(R), n_2(R), D} : \frac{S(D)}{\{1, D\}} \rightarrow G_{n_1(R)} \times \tilde{G}_{n_2(R)}.$$

5.1. **Realizing** $\delta_2(\mathbb{Q}(\sqrt{-D}))$ as $\varphi_{n_1(R), n_2(R), D}$. Let D be a square-free positive integer with $D \equiv 3 \pmod{4}$. and denote its prime factorization by $D = p_1 \cdots p_j$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_j$ be the corresponding prime ideals in $\mathbb{Q}(\sqrt{-D})$, i.e. $\mathfrak{p}_i^2 = (p_i)$. Recall that $\text{Cl}(\mathbb{Q}(\sqrt{-D}))[2]$ is generated by $\mathfrak{p}_1, \dots, \mathfrak{p}_j$ subject only to the relation $\mathfrak{p}_1 \cdots \mathfrak{p}_j = (\sqrt{-D})$. For any b positive divisor of D , denote by \mathfrak{b} the ideal of $\mathbb{Q}(\sqrt{-D})$ with $\mathfrak{b}^2 = (b)$. Let us now recall from [8, Lem.16] that given a positive divisor b of D , we have $\mathfrak{b} \in 2\text{Cl}(\mathbb{Q}(\sqrt{-D}))$ if and only if $b \in S(D)$. The assignment $\mathfrak{b} \mapsto b$ gives an isomorphism

$$(2\text{Cl}(\mathbb{Q}(\sqrt{-D}))) [2] \cong S(D) / \{1, D\}.$$

Indeed, from the proof of [8, Lem.16], we know that $b \in S(D)$ if and only if there exists a primitive element (i.e. not divisible by any $m \in \mathbb{Z}_{\geq 2}$) $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ and $w \in \mathbb{Z}_{\neq 0}$ such that

$$bw^2 = N_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(\alpha). \tag{5.1}$$

In that case the factorization of (α) gives an integral ideal $h(\mathfrak{b})$ such that $(\alpha) = h(\mathfrak{b})^2 \mathfrak{b}$. We rewrite this as $\mathfrak{b}(\alpha/b) = h(\mathfrak{b})^2$ and observe that this shows in particular that $\mathfrak{b} \in 2\text{Cl}(\mathbb{Q}(\sqrt{-D}))$.

By weak approximation for conics, one has that such an α can be found with $(\alpha, c) = 1$, i.e. a primitive point on (5.1) such that $\gcd(w, c) = 1$. Therefore both $(\alpha), h(\mathfrak{b})$ are coprime to (c) . Therefore the fractional ideal $\mathfrak{b}(\frac{\alpha}{c})$ can be employed as a lifting of \mathfrak{b} to $2\text{Cl}(\mathbb{Q}(\sqrt{-D}), c)$. Therefore the definition of the δ_2 -map gives us that

$$\delta_2(\mathbb{Q}(\sqrt{-D}))(\mathfrak{b}) = b \frac{\alpha^2}{b^2}.$$

However squares of integers in $W_R/2W_R$ give rise to the trivial element, therefore by (5.1) we obtain that $\delta(\mathfrak{b}) = g_R(\alpha)$. Recalling that $N(\cdot)$ is the norm-function with respect to the C_2 -action prescribed to $R^*/\langle -1 \rangle$ we see that $g_R(\alpha) = \alpha^2 N(\alpha)$. Next, we provide a more concrete description of $\text{Im}(g_R)$. The proof of the following result is straightforward and therefore omitted.

Lemma 5.5. *There is an isomorphism $\varphi_R : \text{Im}(g_R) \rightarrow G_{n_1(R)} \times G_{n_2(R)}$ such that*

$$\varphi_R(g_R(x)) = N(x)$$

for every $x \in \frac{R^*}{\langle -1 \rangle} [2^\infty]$.

Since $N(\alpha) = bw^2$ and w^2 is trivial in $W_R/2W_R$, we get a commutative diagram

$$\begin{array}{ccc} (2\text{Cl}(\mathbb{Q}(\sqrt{-D}))) [2] & \xrightarrow{\delta} & \text{Im}(g_R) \\ \downarrow \frac{S(D)}{\{1, D\}} & & \downarrow \varphi_R \\ & \xrightarrow{\varphi_{n_1, n_2, D}} & G_{n_1(R)} \times \tilde{G}_{n_2(R)} \end{array}$$

where the vertical rows are isomorphisms. This gives us precisely the realization of the δ_2 -map in terms of special divisors that we were looking for.

5.2. **Reduction to special divisors.** Our next result holds for integers a, q, n_1, n_2 satisfying

$$4n_1n_2 \text{ divides } q, a \equiv 3 \pmod{4}, \gcd(a, q) = 1, \tag{5.2}$$

$$a \text{ is a square } \pmod{n_1} \tag{5.3}$$

and

$$p \text{ prime, } p \mid n_2 \Rightarrow a \text{ is a non-square } \pmod{p}. \tag{5.4}$$

Theorem 5.6. *Let a, q, n_1, n_2 be positive integers satisfying (5.2), (5.3) and (5.4). Then for every $\delta \in (0, 2^{-|\mathbf{k}_1|})$ we have*

$$\frac{\sum_{D \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi}}{\sum_{D \leq X} 1} - 2^{|\mathbf{k}_1|} \left(\sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathcal{N}_2(|\mathbf{k}_1| - \dim(W)) \right) \ll (\log X)^{-\delta},$$

where in both sums D varies among square-free positive integers which are congruent to $a \pmod{q}$ and the implied constant depends at most on a, q, n_1, n_2, δ and $(k_\chi)_\chi$.

This proves Prediction 4.9 with an explicit error term.

Recall Definition 4.3. We shall use Theorem 5.6 in §7 to deduce the following.

Theorem 5.7. *Let a, q, n_1, n_2 be positive integers satisfying (5.2), (5.3) and (5.4). Then*

$$\lim_{X \rightarrow \infty} \frac{\#\{D \leq X, (S(D)/\{1, D\}, \varphi_{n_1, n_2, D}) \sim T\}}{\#\{D \leq X\}} = \mu(T),$$

where D varies among positive square-free integers satisfying $D \equiv a \pmod{q}$.

This confirms the Prediction 4.5.

We are finally in place to explain why Theorems 5.6 and 5.7 imply Theorems 5.1, 5.2, 5.3 and 5.4. Owing to the final diagram of the previous subsection, we have the following implications. Theorems 5.2, 5.3 and 5.4 follow immediately from Theorem 5.7 because the family of fields K that are strongly of type R has zero proportion.

To deduce Theorem 5.1 from Theorem 5.6 recall the definition of $E(X)$ given prior to (3.2) and that $m_\chi(\delta_2(K))$ coincides with $m_\chi(-D(K))$ if $D(K) \notin E(X)$ and that it vanishes otherwise. We thus obtain

$$\sum_{-D(K) \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(\delta_2(K))^{k_\chi} - \sum_{D \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi} = - \sum_{D \in E(X)} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi}. \quad (5.5)$$

Fixing any $\gamma \in (0, 1/\varphi(c))$ we can pick a positive integer p' which satisfies $\gamma\varphi(c) < 1 - 1/p' < 1$ and define q' via $1/p' + 1/q' = 1$. Using Hölder's inequality we see that the quantity in (5.5) has modulus

$$\begin{aligned} \sum_{D \in E(X)} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi} &= \sum_{D \leq X} \mathbf{1}_{E(X)}(D) \left(\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi} \right) \\ &\leq \left(\sum_{D \leq X} \mathbf{1}_{E(X)}(D)^{q'} \right)^{1/q'} \left(\sum_{D \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{p'k_\chi} \right)^{1/p'} \\ &= E(X)^{1/q'} \left(\sum_{D \leq X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{p'k_\chi} \right)^{1/p'}. \end{aligned}$$

Observe that the obvious bound $m_\chi(D) \leq \#S(D)$ shows that the second sum is

$$\leq \sum_{D \leq X} \#S(D)^{p'|\mathbf{k}_1|}$$

hence by [8, Th.9] it is $O_{p',k}(X)$. Using (3.2) we conclude that the quantity in (5.5) is

$$\ll \left(\frac{X}{(\log X)^{1/\varphi(c)}} \right)^{1/q'} X^{1/p'} = \frac{X}{(\log X)^{1/(q'\varphi(c))}} \ll \frac{X}{(\log X)^\gamma},$$

This concludes our argument that shows that Theorem 5.6 implies Theorem 5.1.

6. MAIN THEOREMS ON SPECIAL DIVISORS

This section is devoted to the proof of Theorem 5.6.

6.1. Pre-indexing trick. In the present subsection we reduce Theorem 5.6 into a statement that can be proved with the method of Fouvry and Klüners. Recall the definition of the set of special divisors $S(D)$ given in the beginning of §4. For a character $\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}$ we bring into play the sum

$$A_\chi(D) := \sum_{a'b'=D} \chi(a') \left(\sum_{c'|b'} \left(\frac{a'}{c'} \right) \right) \left(\sum_{d'|a'} \left(\frac{b'}{d'} \right) \right) \quad (6.1)$$

and let $A(D) := A_1(D)$. By definition (4.1) we see that $m_\chi(D)$ is the cardinality of elements $a' \in S(D)$ such that $\chi(a') = 1$. Detecting the latter condition via $(1 + \chi(a'))/2$ we obtain

$$m_\chi(D) = 2^{-\omega(D)} \frac{(A(D) + A_\chi(D))}{2}.$$

Recalling Notation 4.6 we obtain

$$\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} m_\chi(D)^{k_\chi} = 2^{-|\mathbf{k}_1| \omega(D)} \frac{\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} (A(D) + A_\chi(D))^{k_\chi}}{2^{|\mathbf{k}_1|}}. \quad (6.2)$$

Letting $|(i_\chi)|_1$ be the ℓ^1 -norm of the vector $(i_\chi)_\chi$ we see that the right side equals

$$2^{-|\mathbf{k}_1| \omega(D)} \sum_{\substack{(i_\chi)_\chi \\ 0 \leq i_\chi \leq k_\chi}} \frac{\lambda_{(i_\chi)}}{2^{|\mathbf{k}_1|}} A(D)^{|\mathbf{k}_1| - |(i_\chi)|_1} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{G}_{n_2}} A_\chi(D)^{i_\chi}$$

for some integers $\lambda_{(i_\chi)}$. To each vector (i_χ) we attach the space

$$Y_{(i_\chi)} := \langle \{\chi : i_\chi \neq 0\} \rangle \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}$$

and recalling Definition 4.7 we see that for a fixed subspace $Y \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2}$ we have

$$\sum_{\substack{(i_\chi): Y_{(i_\chi)} = Y \\ 0 \leq i_\chi \leq k_\chi}} \frac{\lambda_{(i_\chi)}}{2^{|\mathbf{k}_1|}} = \mathbb{P}_{(k_\chi)}(Y).$$

Hence Theorem 5.6 would follow from proving that for any $\varepsilon > 0$, any integers a, q, n_1, n_2 satisfying (5.2), (5.3) and (5.4), any $B \subseteq \widehat{G}_{n_1} \times \widehat{G}_{n_2} - \{1\}$ and any choice of a function $i : B \rightarrow \mathbb{Z}_{>0}$ with $i_\chi \leq k_\chi$, one has that

$$\begin{aligned} & \sum_{D \leq X} 2^{-|\mathbf{k}_1| \omega(D)} A(D)^{|\mathbf{k}_1| - \sum_{\chi \in B} i_\chi} \prod_{\chi \in B} A_\chi(D)^{i_\chi} \\ &= 2^{|\mathbf{k}_1|} \mathcal{N}_2(|\mathbf{k}_1| - \dim(Y_{(i_\chi)})) \left(\sum_{D \leq X} 1 \right) + O(X(\log X)^{\varepsilon - 2^{-|\mathbf{k}_1|}}), \end{aligned} \quad (6.3)$$

where in both sums D varies among positive square-free integers which are congruent to $a \pmod{q}$. Here $\mathcal{N}_2(h)$ denotes as usual the number of vector subspaces of \mathbb{F}_2^h . To prove (6.3) we will use the approach in the proof of [8, Th.6]. In the present notation their result corresponds to the case $B = \emptyset$ in (6.3).

6.2. Indexing trick. We begin by performing the following change of variables in (6.1),

$$a' = D_{10}D_{11}, b' = D_{00}D_{01}, c' = D_{00}, d' = D_{11}.$$

Letting $\Phi_1(\mathbf{u}, \mathbf{v}) := (\mathbf{u}_1 + \mathbf{v}_1)(\mathbf{u}_1 + \mathbf{v}_2)$ and $\Psi(\mathbf{u}) := \mathbf{u}_1$ we can thus conclude that

$$A_\chi(D) = \sum_{D=D_{10}D_{11}D_{00}D_{01}} \prod_{(\mathbf{u}, \mathbf{v}) \in (\mathbb{F}_2^2)^2} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right)^{\Phi_1(\mathbf{u}, \mathbf{v})} \prod_{\mathbf{u} \in \mathbb{F}_2^2} \chi(D_{\mathbf{u}})^{\Psi(\mathbf{u})}.$$

Next, if $\langle B \rangle$ is not the zero subspace we choose a basis $T \subset B$ of $\langle B \rangle$. Now suppose we choose in each factor of

$$A(D)^{|\mathbf{k}|_1 - \sum_{\chi \in B} i_\chi} \prod_{\chi \in B} A_\chi(D)^{i_\chi}$$

a decomposition of D as follows,

$$D = \prod_{\mathbf{u}^{(1)} \in \mathbb{F}_2^2} D_{\mathbf{u}^{(1)}}^{(1)} = \dots = \prod_{\mathbf{u}^{(|\mathbf{k}|_1)} \in \mathbb{F}_2^2} D_{\mathbf{u}^{(|\mathbf{k}|_1)}}^{(|\mathbf{k}|_1)}.$$

We change variables and write $D_{\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(|\mathbf{k}|_1)}} := \gcd(D_{\mathbf{u}^{(1)}}, \dots, D_{\mathbf{u}^{(|\mathbf{k}|_1)}})$, where one can reconstruct the old variables with the help of

$$D_{\mathbf{u}^{(\ell)}}^{(\ell)} = \prod_{\substack{1 \leq n \leq |\mathbf{k}|_1 \\ n \neq \ell}} \prod_{\mathbf{u}^{(n)} \in \mathbb{F}_2^2} D_{\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(\ell)}, \dots, \mathbf{u}^{(|\mathbf{k}|_1)}}$$

as in [8, Eq.(23)]. Thus we can write

$$A(D)^{|\mathbf{k}|_1 - \sum_{\chi \in B} i_\chi} \prod_{\chi \in B} A_\chi(D)^{i_\chi} = \sum_{\prod_{\mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} D_{\mathbf{u}} = D} \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \right) \left(\prod_{\mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})} \right),$$

where

$$\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v}) := \sum_{j=1}^{|\mathbf{k}|_1} \Phi_1(\mathbf{u}^{(j)}, \mathbf{v}^{(j)})$$

and Ψ_χ are linear maps from $\mathbb{F}_2^{2|\mathbf{k}|_1}$ to \mathbb{F}_2 , which we next describe. Decompose

$$\mathbb{F}_2^{2|\mathbf{k}|_1} = \mathbb{F}_2^{2|\mathbf{k}|_1 - 2 \sum_{\chi \in B} i_\chi} \times \prod_{\chi \in B} \mathbb{F}_2^{2i_\chi}$$

and we denote a vector in this space as $\mathbf{u} := (\mathbf{u}_0, (\mathbf{u}^{(\chi)})_{\chi \in B})$, where $\mathbf{u}^{(\chi)} := (\mathbf{u}_1^{(\chi)}, \dots, \mathbf{u}_{i_\chi}^{(\chi)})$ and for every j we have $\mathbf{u}_j^{(\chi)} \in \mathbb{F}_2^2$. Next, write

$$\Psi'_\chi(\mathbf{u}) = \sum_{j=1}^{i_\chi} \Psi(\mathbf{u}_j^{(\chi)})$$

and note that we have

$$\Psi_\chi(\mathbf{u}) = \sum_{\chi' \in B_\chi} \Psi'_{\chi'}(\mathbf{u}), \tag{6.4}$$

where B_χ denotes the set of characters $\chi' \in B$, such that χ is used in writing χ' in the basis T . In particular, this implies that $\chi \in B_\chi$. The construction of Ψ_χ depends on T and (i_χ) , but we suppress this dependency to simplify the notation.

Let us observe that there are $\#T = \dim(\langle B \rangle)$ many linear maps Ψ_χ and that they are independent. Indeed, given $\chi \in T$, all maps $\Psi_{\chi'}$ with $\chi' \in T - \{\chi\}$ vanish on the vectors \mathbf{u} with $\mathbf{u}^{(\tilde{\chi})} = \mathbf{0}$ for each $\tilde{\chi} \neq \chi$, while Ψ_χ evaluated in such \mathbf{u} equals $\Psi'_\chi(\mathbf{u}^{(\chi)})$, which does not vanish identically.

We can therefore rewrite the first sum over D in (6.3) as

$$\begin{aligned} & \sum_{D \leq X} 2^{-|\mathbf{k}|_1 \omega(D)} A(D)^{|\mathbf{k}|_1 - \sum_{\chi \in B} i_\chi} \prod_{\chi \in B} A_\chi(D)^{i_\chi} \\ &= \sum_{(D_{\mathbf{u}})} \left(\prod_{\mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \right) \left(\prod_{\mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})} \right), \end{aligned} \quad (6.5)$$

where the second sum is over positive integers $D_{\mathbf{u}}$ such that $\prod_{\mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}} D_{\mathbf{u}}$ varies among positive square-free integers which are congruent to $a \pmod{q}$ and at most X .

Our goal in §§6.3-6.5 is to prove an asymptotic for the sum over $D_{\mathbf{u}}$ in (6.5) under the assumptions on the integers a, q, n_1, n_2 in Theorem 5.6. For a real number $X > 1$ we bring into play the following subset of $\mathbb{N}^{4|\mathbf{k}|_1}$,

$$\mathcal{D}(X, |\mathbf{k}|_1; q, a) := \left\{ (D_{\mathbf{u}})_{\mathbf{u}} \in \mathbb{N}^{4|\mathbf{k}|_1}, \mathbf{u} = (\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(|\mathbf{k}|_1)}) \in (\mathbb{F}_2^2)^{|\mathbf{k}|_1} : \begin{array}{l} \prod_{\mathbf{u}} D_{\mathbf{u}} \text{ is square-free,} \\ \text{bounded by } X \text{ and} \\ \text{congruent to } a \pmod{q} \end{array} \right\}.$$

We are interested in asymptotically evaluating the succeeding average,

$$S_\chi(X, |\mathbf{k}|_1; q, a) := \sum_{(D_{\mathbf{u}}) \in \mathcal{D}(X, |\mathbf{k}|_1; q, a)} 2^{-|\mathbf{k}|_1 \omega(D)} \left(\prod_{\mathbf{u}, \mathbf{v} \in (\mathbb{F}_2^2)^{|\mathbf{k}|_1}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \right) \left(\prod_{\mathbf{u} \in (\mathbb{F}_2^2)^{|\mathbf{k}|_1}} \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})} \right)$$

and in doing so we shall not keep track of the dependence of the implied constants on $T, (i_\chi), \mathbf{k}, \chi, a, q, n_1, n_2$. The sum S_χ also depends on (i_χ) and the choice of T but we suppress this in the notation. The function S_χ should be compared with [8, Eq.(26)]; we will verify in §6.3 that the presence of the characters χ does not affect the analysis of Fouvry–Klüners [8] in the error term and we shall see in §§6.4-6.5 how their presence influences the main term.

6.3. The four families of sums of Fouvry and Klüners. We begin by restricting the summation in $S_\chi(X, |\mathbf{k}|_1; q, a)$ to variables having a suitably small number of prime factors as in [8, §5.3]. Letting $\Omega := 2^{|\mathbf{k}|_1+1} |\mathbf{k}|_1^{-1} \log \log X$ we shall study the contribution, say Σ_1 , towards $S_\chi(X, |\mathbf{k}|_1; q, a)$ of elements not fulfilling

$$\omega(D_{\mathbf{u}}) \leq \Omega, \text{ for all } \mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}.$$

Writing $m = \prod_{\mathbf{u}} D_{\mathbf{u}}$ and bounding each character by 1 provides us with

$$\Sigma_1 \ll \sum_{m \leq X} \frac{\mu(m)^2}{\tau(m)^{|\mathbf{k}|_1}} \sum_{\substack{m_1 \cdots m_{4|\mathbf{k}|_1} = m \\ \omega(m_1) > \Omega}} 1 \leq 4^{-|\mathbf{k}|_1 \Omega} \sum_{m \leq X} \frac{\mu(m)^2}{\tau(m)^{|\mathbf{k}|_1}} \sum_{m_1 \cdots m_{4|\mathbf{k}|_1} = m} 4^{|\mathbf{k}|_1 \omega(m_1)}.$$

Invoking [12, Eq.(1.82)] to bound the sum over m makes the following estimate available,

$$\Sigma_1 \ll X(\log X)^{-1-2^{|\mathbf{k}_1|+1} \log(4/e)-2^{|\mathbf{k}_1|}}. \quad (6.6)$$

We continue in the footsteps laid out in [8, §5.4], where four families of elements in $\mathbb{N}^{4^{|\mathbf{k}_1|}}$ are shown to make a negligible contribution towards a quantity that resembles $S_{\chi}(X, |\mathbf{k}_1; q, a)$. Using the trivial bound

$$\left| \prod_{\mathbf{u} \in (\mathbb{F}_2^{|\mathbf{k}_1|})} \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})} \right| \leq 1 \quad (6.7)$$

allows us to adopt in a straightforward manner the arguments leading to [8, Eq.(34),(39)] and we proceed to briefly explain how. Let

$$\Delta := 1 + (\log X)^{-2^{|\mathbf{k}_1|}}$$

and let $A_{\mathbf{u}}$ denote numbers of the form Δ^m where $m \in \mathbb{Z}_{\geq 0}$. For $\mathbf{A} = (A_{\mathbf{u}})_{\mathbf{u} \in (\mathbb{F}_2^{|\mathbf{k}_1|})}$ we let

$$S_{\chi}(X, |\mathbf{k}_1; q, a; \mathbf{A}) := \sum_{\substack{(D_{\mathbf{u}}) \in \mathcal{D}(X, |\mathbf{k}_1; q, a) \\ \forall \mathbf{u} (A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}}) \\ \forall \mathbf{u} (\omega(D_{\mathbf{u}}) \leq \Omega)}} 2^{-|\mathbf{k}_1| \omega(D)} \left(\prod_{\mathbf{u}, \mathbf{v} \in (\mathbb{F}_2^{|\mathbf{k}_1|})} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right)^{\Phi_{|\mathbf{k}_1|}(\mathbf{u}, \mathbf{v})} \right) \prod_{\mathbf{u} \in (\mathbb{F}_2^{|\mathbf{k}_1|})} \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})}$$

and note that, in light of (6.6), we can deduce as in [8, Eq.(32)] that

$$S_{\chi}(X, |\mathbf{k}_1; q, a) = \sum_{\mathbf{A}: \prod_{\mathbf{u}} A_{\mathbf{u}} \leq X} S_{\chi}(X, |\mathbf{k}_1; q, a; \mathbf{A}) + O(X(\log X)^{-1}). \quad (6.8)$$

The contribution towards (6.8) of the first family, defined through

$$\prod_{\mathbf{u}} A_{\mathbf{u}} \geq \Delta^{-4^{|\mathbf{k}_1|}} X,$$

can be proved to be $\ll X(\log X)^{-1}$ with a similar argument as the one leading to [8, Eq.(34)]. We now let

$$X^{\ddagger} := \min \{ \Delta^{\ell} \geq \exp((\log X)^{\varepsilon 2^{-|\mathbf{k}_1|}}) \}.$$

The contribution towards (6.8) of those \mathbf{A} fulfilling that

$$\text{at most } 2^{|\mathbf{k}_1|} - 1 \text{ of the } A_{\mathbf{u}} \text{ are larger than } X^{\ddagger} \quad (6.9)$$

can be shown to be $\ll X(\log X)^{\varepsilon - 2^{-|\mathbf{k}_1|}}$ as in [8, Eq.(39)].

We next pass to arguments related to cancellation due to oscillation of characters, in this case (6.7) is not enough. The exponents $\Phi_k(\mathbf{u}, \mathbf{v})$ will now play a rôle. Following Fouvry and Klüners we call two indices \mathbf{u}, \mathbf{v} *linked* if $\Phi_{|\mathbf{k}_1|}(\mathbf{u}, \mathbf{v}) + \Phi_{|\mathbf{k}_1|}(\mathbf{v}, \mathbf{u}) = 1$. We next define

$$X^{\dagger} := (\log X)^{3[1+4^{|\mathbf{k}_1|}(1+2^{|\mathbf{k}_1|})]}$$

and consider the contribution of \mathbf{A} with

$$\prod_{\mathbf{u}} A_{\mathbf{u}} < \Delta^{-4^{|\mathbf{k}_1|}} X \text{ and for two linked } \mathbf{u} \text{ and } \mathbf{v} \text{ we have } \min\{A_{\mathbf{u}}, A_{\mathbf{v}}\} \geq X^{\dagger}. \quad (6.10)$$

Fouvry and Klüners treat this case by drawing upon the important work of Heath-Brown [11] in the form stated in [8, Lem.12]. Specifically for \mathbf{A} as in (6.10) we have

$$|S_{\chi}(X, |\mathbf{k}|_1; q, a; \mathbf{A})| \leq \sum_{(D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}}} \left(\prod_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{w}})} \right) \sum_{\substack{a_1, a_2 \in (\mathbb{Z} \cap (0, q])^2 \\ a_1 a_2 \prod_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}} D_{\mathbf{w}} \equiv a \pmod{q}}} |M((D_{\mathbf{w}}))|,$$

where

$$M((D_{\mathbf{w}})) := \sum_{D_{\mathbf{u}}, D_{\mathbf{v}}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right) g(D_{\mathbf{u}}, (D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}}) g(D_{\mathbf{v}}, (D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}}),$$

$$g(D_{\mathbf{u}}, (D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}}) := \frac{\mathbf{1}_{a_1, q}(D_{\mathbf{u}})}{2^{|\mathbf{k}|_1 \omega(D_{\mathbf{u}})}} \prod_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{w}}} \right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{w})} \prod_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}} \left(\frac{D_{\mathbf{w}}}{D_{\mathbf{u}}} \right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{w}, \mathbf{u})} \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})},$$

$\mathbf{1}_{\alpha, \beta}$ denotes the indicator function of the set $\{m \in \mathbb{Z} : m \equiv \alpha \pmod{\beta}\}$ and similarly for $g(D_{\mathbf{v}}, (D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}})$. Since $|g(D_{\mathbf{u}}, (D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}})|, |g(D_{\mathbf{v}}, (D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}})| \leq 1$ the argument in [8, p.476] that validates [8, Eq.(42)] can be adopted in the obvious way to yield

$$\sum_{\mathbf{A} \text{ fulfils (6.10)}} |S_{\chi}(X, |\mathbf{k}|_1; q, a; \mathbf{A})| \ll X(\log X)^{-1}.$$

Note that we have used [8, Lem.15] for sequences satisfying $|a_m|, |b_n| \leq 1$ rather than $|a_m|, |b_n| < 1$, however using [8, Lem.15] for $a_m/2, b_n/2$ in place of a_m, b_n proves a version of [8, Lem.15] under the more general assumption $|a_m|, |b_n| < 2$ and with the same conclusion.

The fourth family consists of \mathbf{A} fulfilling $\prod_{\mathbf{u}} A_{\mathbf{u}} < \Delta^{-4|\mathbf{k}|_1} X$, any linked \mathbf{u}, \mathbf{v} satisfy the inequality $\min\{A_{\mathbf{u}}, A_{\mathbf{v}}\} < X^{\dagger}$ and there exist linked \mathbf{u}, \mathbf{v} with $2 \leq A_{\mathbf{v}}$ and $A_{\mathbf{u}} \geq X^{\ddagger}$. Their contribution towards $S_{\chi}(X, |\mathbf{k}|_1; q, a; \mathbf{A})$ is

$$\ll \max_{\substack{\sigma \pmod{q} \\ \gcd(\sigma, q) = 1}} \sum_{\substack{(D_{\mathbf{w}})_{\mathbf{w} \notin \{\mathbf{u}, \mathbf{v}\}} \\ A_{\mathbf{w}} \leq D_{\mathbf{w}} < \Delta A_{\mathbf{w}}}} \sum_{\substack{D_{\mathbf{v}} \\ A_{\mathbf{v}} \leq D_{\mathbf{v}} < \Delta A_{\mathbf{v}}}} |M_{\sigma}|, \quad (6.11)$$

where M_{σ} is defined through

$$\sum_{\substack{D_{\mathbf{u}} \equiv \sigma \pmod{q} \\ A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}}}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right) \prod_{\chi \in T} \chi(D_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})} = \left(\prod_{\chi \in T} \chi(\sigma)^{\Psi_{\chi}(\mathbf{u})} \right) \sum_{\substack{D_{\mathbf{u}} \equiv \sigma \pmod{q} \\ A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}}}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}} \right).$$

Letting $P^+(m)$ denote the largest prime factor of a positive integer $m > 1$ and setting $P^+(1) := 1, m := D_{\mathbf{u}}/P^+(D_{\mathbf{u}})$ we obtain

$$M_{\sigma} \ll \sum_{\substack{m P^+(m) < \Delta A_{\mathbf{u}} \\ (m, q) = 1}} \frac{\mu(m)^2}{2^{|\mathbf{k}|_1 \omega(m)}} \left| \sum_{m p \equiv \sigma \pmod{q}} \mu(pm) \prod_{\mathbf{w} \neq \mathbf{u}} D_{\mathbf{w}} \right|^2 \left(\frac{p}{D_{\mathbf{v}}} \right),$$

where the inner sum is over primes p with $\max\{A_{\mathbf{u}}/m, P^+(m)\} \leq p < \Delta A_{\mathbf{u}}/m$. We may now use Dirichlet characters to modulus q to detect the congruence condition on p . We will subsequently be faced with $\varphi(q)$ new sums over p , each one of which can be bounded via [8, Lem.13]. This furnishes

$$\sum_{m p \equiv \sigma \pmod{q}} \mu(pm) \prod_{\mathbf{w} \neq \mathbf{u}} D_{\mathbf{w}} \left(\frac{p}{D_{\mathbf{v}}} \right) \ll \frac{A_{\mathbf{v}}^{1/2} A_{\mathbf{u}}}{m} (\log X)^{-N \varepsilon 2^{-|\mathbf{k}|_1 + 1}} + \Omega,$$

valid for each large enough positive N that is independent of \mathbf{A} and m . The term Ω accounts for the presence of the μ^2 -terms. Indeed, by (6.6) the number of distinct prime divisors of m and each $D_{\mathbf{w}}$ is at most Ω . A moment's thought now reveals that once the last bound is injected into (6.11) and N is suitably increased in comparison to $|\mathbf{k}|_1$, the contribution of \mathbf{A} in the fourth case is $\ll X(\log X)^{-1}$, as in [8, Eq.(47)].

Let us now introduce the conditions

$$\left\{ \begin{array}{l} \prod_{\mathbf{u} \in (\mathbb{F}_2^k)^k} A_{\mathbf{u}} < \Delta^{-4|\mathbf{k}|_1} X, \\ \text{at least } 2^{|\mathbf{k}|_1} \text{ indices satisfy } A_{\mathbf{u}} > X^{\ddagger}, \\ \text{two indices } \mathbf{u} \text{ and } \mathbf{v} \text{ with } A_{\mathbf{u}}, A_{\mathbf{v}} > X^{\ddagger} \text{ are always linked,} \\ \text{if } A_{\mathbf{u}} \text{ and } A_{\mathbf{v}} \text{ with } A_{\mathbf{v}} \leq A_{\mathbf{u}} \text{ are linked, then either} \\ A_{\mathbf{v}} = 1 \text{ or } (2 \leq A_{\mathbf{v}} < X^{\ddagger} \text{ and } A_{\mathbf{v}} \leq A_{\mathbf{u}} < X^{\ddagger}). \end{array} \right. \quad (6.12)$$

Increasing the value of A in comparison to $|\mathbf{k}|_1$ and assorting all estimates so far yields

$$S_{\mathcal{X}}(X, |\mathbf{k}|_1; q, a) = \sum_{\mathbf{A} \text{ satisfies (6.12)}} S_{\mathcal{X}}(X, |\mathbf{k}|_1; q, a; \mathbf{A}) + O(X(\log X)^{\varepsilon-2^{-|\mathbf{k}|_1}}), \quad (6.13)$$

which is in analogy with [8, Prop.2].

6.4. The main term. We can now obtain the following as in [8, Prop.3],

$$S_{\mathcal{X}}(X, |\mathbf{k}|_1; q, a) = \sum_{\mathbf{A} \text{ satisfies (6.15)}} S_{\mathcal{X}}(X, |\mathbf{k}|_1; q, a; \mathbf{A}) + O(X(\log X)^{\varepsilon-2^{-|\mathbf{k}|_1}}), \quad (6.14)$$

where

$$\left\{ \begin{array}{l} \mathcal{U} := \{\mathbf{u} : A_{\mathbf{u}} > X^{\ddagger}\} \text{ is a maximal subset of unlinked indices,} \\ \prod_{\mathbf{u} \in (\mathbb{F}_2^k)^{|\mathbf{k}|_1}} A_{\mathbf{u}} \leq \Delta^{-4|\mathbf{k}|_1} X \text{ and } A_{\mathbf{u}} = 1 \text{ for } \mathbf{u} \notin \mathcal{U}. \end{array} \right. \quad (6.15)$$

Similarly to [8, Eq.(50)] we will say that \mathbf{A} is *admissible* for \mathcal{U} if $A_{\mathbf{u}} > X^{\ddagger} \Leftrightarrow \mathbf{u} \in \mathcal{U}$, $A_{\mathbf{u}} = 1 \Leftrightarrow \mathbf{u} \notin \mathcal{U}$ and $\prod_{\mathbf{u} \in (\mathbb{F}_2^k)^{|\mathbf{k}|_1}} A_{\mathbf{u}} \leq \Delta^{-4|\mathbf{k}|_1} X$. Assume that \mathbf{A} is admissible for \mathcal{U} and note that $\#\mathcal{U} = 2^{|\mathbf{k}|_1}$. By quadratic reciprocity we obtain that $S_{\mathcal{X}}(X, |\mathbf{k}|_1; q, a; \mathbf{A})$ equals

$$\begin{aligned} & \sum_{(h_{\mathbf{u}}) \in (\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}}, \prod_{\mathbf{u} \in \mathcal{U}} h_{\mathbf{u}} \equiv 3 \pmod{4}} \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathcal{U}} (-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v}) \frac{h_{\mathbf{u}}-1}{2} \frac{h_{\mathbf{v}}-1}{2}} \right) \times \\ & \sum_{\substack{(g_{\mathbf{u}}) \in (\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}}, \prod_{\mathbf{u} \in \mathcal{U}} g_{\mathbf{u}} \equiv a \pmod{q} \\ \forall \mathbf{u} \in \mathcal{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{4})}} \left(\prod_{\mathbf{u} \in \mathcal{U}} \prod_{\chi \in T} \chi(g_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})} \right) \times \\ & \sum_{\substack{(D_{\mathbf{u}}) \in \mathbb{N}^{2^{|\mathbf{k}|_1}}, \forall \mathbf{u} (\omega(D_{\mathbf{u}}) \leq \Omega) \\ \forall \mathbf{u} (D_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{q}), A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}}}} \left(\prod_{\mathbf{u} \in \mathcal{U}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \mu^2 \left(\prod_{\mathbf{u} \in \mathcal{U}} D_{\mathbf{u}} \right). \end{aligned}$$

We can evaluate the sum over $D_{\mathbf{u}}$ via the estimate,

$$\sum_{\substack{m \in \mathbb{N} \cap [y, Y] \\ \omega(m) = \ell \\ m \equiv g \pmod{q}}} \mu(n_0 m)^2 = \frac{1}{\varphi(q)} \sum_{\substack{m \in \mathbb{N} \cap [y, Y] \\ \omega(m) = \ell \\ \gcd(m, q) = 1}} \mu(n_0 m)^2 + O_A \left(\frac{(\ell+1)^A}{Y^{-1}(\log 2Y)^A} + \frac{\omega(n_0)}{Y^{-1+\frac{1}{\ell}}} \right), \quad (6.16)$$

valid for each square-free integer n_0 that is coprime to q , $A > 0, Y \geq y \geq 1, \ell \in \mathbb{Z}_{\geq 0}$, where the implied constant depends at most on A . This can be proved in a similar way as [8,

Lem.19] by replacing the congruence condition to modulus 4 on p_ℓ in [8, Eq.(53)] by one to modulus q . Applying (6.16) repeatedly as in [8, p.g.481-482] to estimate the sums over $D_{\mathbf{u}}$ leads us to

$$\begin{aligned} & \sum_{\substack{(D_{\mathbf{u}}) \in \mathbb{N}^{2|\mathbf{k}|_1}, \forall \mathbf{u} (\omega(D_{\mathbf{u}}) \leq \Omega) \\ \forall \mathbf{u} (D_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{q}, A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}})}} \left(\prod_{\mathbf{u} \in \mathscr{U}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \mu^2 \left(\prod_{\mathbf{u} \in \mathscr{U}} D_{\mathbf{u}} \right) \\ = & \varphi(q)^{-2|\mathbf{k}|_1} \sum_{\substack{(D_{\mathbf{u}}) \in \mathbb{N}^{2|\mathbf{k}|_1}, \forall \mathbf{u} (\omega(D_{\mathbf{u}}) \leq \Omega) \\ \forall \mathbf{u} (A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}})}} \left(\prod_{\mathbf{u} \in \mathscr{U}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \mu^2 \left(q \prod_{\mathbf{u} \in \mathscr{U}} D_{\mathbf{u}} \right) + O(X(\log X)^{-1-4^{|\mathbf{k}|_1}(1+2^{|\mathbf{k}|_1})}). \end{aligned}$$

Using this we obtain as in [8, Eq.(55)] that for any fixed admissible \mathscr{U} we have

$$\begin{aligned} \sum_{\mathbf{A} \text{ admissible for } \mathscr{U}} S_{\chi}(X, |\mathbf{k}|_1; q, a; \mathbf{A}) &= 2^{-|\mathbf{k}|_1} \varphi(q)^{-2|\mathbf{k}|_1} \sum_{\substack{(h_{\mathbf{u}}) \in (\mathbb{Z}/4\mathbb{Z})^{2|\mathbf{k}|_1} \\ \prod_{\mathbf{u} \in \mathscr{U}} h_{\mathbf{u}} \equiv 3 \pmod{4}}} \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathscr{U}} (-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \frac{h_{\mathbf{u}}-1}{2} \frac{h_{\mathbf{v}}-1}{2} \right) \times \\ & \sum_{\substack{(g_{\mathbf{u}}) \in (\mathbb{Z}/q\mathbb{Z})^{2|\mathbf{k}|_1}, \prod_{\mathbf{u} \in \mathscr{U}} g_{\mathbf{u}} \equiv a \pmod{q} \\ \forall \mathbf{u} \in \mathscr{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{4})}} \left(\prod_{\mathbf{u} \in \mathscr{U}} \prod_{\chi \in T} \chi(g_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})} \right) \times \\ & \sum_{\substack{(D_{\mathbf{u}}) \in \mathbb{N}^{2|\mathbf{k}|_1}, \forall \mathbf{u} (\omega(D_{\mathbf{u}}) \leq \Omega) \\ \forall \mathbf{u} (A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}})}} \left(\prod_{\mathbf{u} \in \mathscr{U}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \mu^2 \left(\text{rad}(q) \prod_{\mathbf{u} \in \mathscr{U}} D_{\mathbf{u}} \right) + O\left(\frac{X}{\log X}\right), \end{aligned}$$

where the radical $\text{rad}(m)$ stands for the product of the distinct prime divisors of an integer $m > 1$. We can now see that the condition $\omega(D_{\mathbf{u}}) \leq \Omega$ can be ignored at the cost of an error term of size $\ll X(\log X)^{-1}$ as in the beginning of §6.3. We can furthermore show as in [8, p.g.482] that

$$\sum_{\substack{(D_{\mathbf{u}}) \in \mathbb{N}^{2|\mathbf{k}|_1} \\ \forall \mathbf{u} (A_{\mathbf{u}} \leq D_{\mathbf{u}} < \Delta A_{\mathbf{u}})}} \left(\prod_{\mathbf{u} \in \mathscr{U}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \mu^2 \left(\text{rad}(q) \prod_{\mathbf{u} \in \mathscr{U}} D_{\mathbf{u}} \right) = \sum_{m \leq X} \mu(\text{rad}(q)m)^2 + O\left(X(\log X)^{\varepsilon-2^{|\mathbf{k}|_1}}\right).$$

It is easily proved via Möbius inversion that for fixed $a, q > 0$ with $\text{gcd}(a, q) = 1$ we have

$$\sum_{m \leq X} \mu(\text{rad}(q)m)^2 = \frac{\varphi(q)}{q} \left(\prod_{p|q} (1-p^{-2}) \right) X + O\left(\sqrt{X}\right)$$

and

$$\sum_{\substack{m \leq X \\ m \equiv a \pmod{q}}} \mu(m)^2 = \frac{1}{q} \left(\prod_{p|q} (1-p^{-2}) \right) X + O\left(\sqrt{X}\right).$$

Combining these yields

$$\sum_{m \leq X} \mu(\text{rad}(q)m)^2 = \varphi(q) \sum_{\substack{m \leq X \\ m \equiv a \pmod{q}}} \mu(m)^2 + O\left(\sqrt{X}\right).$$

We thus obtain the following for every maximal unlinked subset \mathcal{U} ,

$$\sum_{\mathbf{A} \text{ admissible for } \mathcal{U}} S_{\chi}(X, |\mathbf{k}|_1; q, a; \mathbf{A}) = \frac{\gamma_{\psi}(\mathcal{U})}{2^{|\mathbf{k}|_1} \varphi(q)^{2^{|\mathbf{k}|_1} - 1}} \left(\sum_{\substack{m \leq X \\ m \equiv a \pmod{q}}} \mu(m)^2 \right) + O\left(X(\log X)^{\varepsilon - 2^{|\mathbf{k}|_1}}\right),$$

where

$$\gamma_{\psi}(\mathcal{U}) := \sum_{\substack{(h_{\mathbf{u}}) \in (\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}} \\ \prod_{\mathbf{u} \in \mathcal{U}} h_{\mathbf{u}} \equiv 3 \pmod{4}}} \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathcal{U}} (-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \frac{h_{\mathbf{u}} - 1}{2} \frac{h_{\mathbf{v}} - 1}{2} \right) \sum_{\substack{(g_{\mathbf{u}}) \in (\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}} \\ \prod_{\mathbf{u} \in \mathcal{U}} g_{\mathbf{u}} \equiv a \pmod{q} \\ \forall \mathbf{u} \in \mathcal{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{4})}} \left(\prod_{\mathbf{u} \in \mathcal{U}} \prod_{\chi \in T} \chi(g_{\mathbf{u}})^{\Psi_{\chi}(\mathbf{u})} \right).$$

We can now infer via (6.14) that the last equation proves

$$\frac{S_{\chi}(X, |\mathbf{k}|_1; q, a)}{\#\{m \in [1, X] : q \mid m - a, \mu(m)^2 = 1\}} = \left(\sum_{\mathcal{U}} \gamma_{\psi}(\mathcal{U}) \right) \frac{\varphi(q)^{1 - 2^{|\mathbf{k}|_1}}}{2^{|\mathbf{k}|_1}} + O((\log X)^{\varepsilon - 2^{|\mathbf{k}|_1}}),$$

where \mathcal{U} ranges over maximal unlinked subsets of $\mathbb{F}_2^{2^{|\mathbf{k}|_1}}$.

6.5. Simplifying $\gamma_{\psi}(\mathcal{U})$. Introduce the following Dirichlet character (mod $n_1 n_2$),

$$\rho_{\mathbf{u}} := \prod_{\chi \in T} \chi^{\Psi_{\chi}(\mathbf{u})}.$$

We will call a maximal set of unlinked indices \mathcal{U} *stable* if

$$\forall \chi \in T, \forall \mathbf{u} \in \mathcal{U} (\Psi_{\chi}(\mathbf{u}) = 0) \text{ or } \forall \chi \in T, \forall \mathbf{u} \in \mathcal{U} (\Psi_{\chi}(\mathbf{u}) = 1).$$

Let us now prove that

$$\sum_{\substack{(g_{\mathbf{u}}) \in (\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}} \\ \prod_{\mathbf{u} \in \mathcal{U}} g_{\mathbf{u}} \equiv a \pmod{q} \\ \forall \mathbf{u} \in \mathcal{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{4})}} \prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}}(g_{\mathbf{u}}) = \mathbf{1}_{\mathcal{U} \text{ stable}(\mathcal{U})} \left(\frac{\varphi(q)}{2} \right)^{2^{|\mathbf{k}|_1} - 1}.$$

Write $q = 2^b n_0 m$, where $b := \nu_2(q)$, $\gcd(n_0, n_1 n_2) = 1$ and n_0 has radical equal to $n_1 n_2$. Define

$$U_1(n_0) := \{u \in \mathbb{Z}/n_0\mathbb{Z} : u \equiv 1 \pmod{n_1 n_2}\} \text{ and } U_1(2^b) := \{u \in \mathbb{Z}/2^b\mathbb{Z} : u \equiv 1 \pmod{4}\}.$$

Recalling the identification of groups $(\mathbb{Z}/q\mathbb{Z})^* = U_1(2^b) \times (\mathbb{Z}/4\mathbb{Z})^* \times U_1(n_0) \times (\mathbb{Z}/n_1 n_2\mathbb{Z})^*$, we see that

$$\sum_{\substack{(g_{\mathbf{u}}) \in (\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}} \\ \prod_{\mathbf{u} \in \mathcal{U}} g_{\mathbf{u}} \equiv a \pmod{q} \\ \forall \mathbf{u} \in \mathcal{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{4})}} \prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}}(g_{\mathbf{u}}) = (\#U_1(2^b) \#U_1(n_0) \varphi(m))^{2^{|\mathbf{k}|_1} - 1} \sum_{\substack{(m_{\mathbf{u}}) \in (\mathbb{Z}/n_1 n_2\mathbb{Z})^{2^{|\mathbf{k}|_1}} \\ \prod_{\mathbf{u} \in \mathcal{U}} m_{\mathbf{u}} \equiv a \pmod{n_1 n_2}}} \prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}}(m_{\mathbf{u}}).$$

Note that we have $\prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}_0}(m_{\mathbf{u}}) = \rho_{\mathbf{u}_0}(a) = 1$ owing to (5.2)-(5.4). Therefore, fixing $\mathbf{u}_0 \in \mathcal{U}$, we have the following equality for any choice of $m_{\mathbf{u}}$ in the above sum

$$\prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}}(m_{\mathbf{u}}) = \rho_{\mathbf{u}_0}(\mathbf{u}_0) \prod_{\mathbf{u} \in \mathcal{U} - \{\mathbf{u}_0\}} \rho_{\mathbf{u}}(\mathbf{u}) = \prod_{\mathbf{u} \in \mathcal{U} - \{\mathbf{u}_0\}} \left(\frac{\rho_{\mathbf{u}}(m_{\mathbf{u}})}{\rho_{\mathbf{u}_0}(m_{\mathbf{u}})} \right).$$

Therefore

$$\sum_{\substack{(m_{\mathbf{u}}) \in (\mathbb{Z}/n_1 n_2 \mathbb{Z})^{2|\mathbf{k}|_1} \\ \prod_{\mathbf{u} \in \mathcal{U}} m_{\mathbf{u}} \equiv a \pmod{n_1 n_2}}} \prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}}(m_{\mathbf{u}}) = \sum_{(m_{\mathbf{u}}) \in ((\mathbb{Z}/n_1 n_2 \mathbb{Z})^*)^{2|\mathbf{k}|_1 - 1}} \prod_{\mathbf{u} \in \mathcal{U} - \{\mathbf{u}_0\}} \frac{\rho_{\mathbf{u}}(m_{\mathbf{u}})}{\rho_{\mathbf{u}_0}(m_{\mathbf{u}})}.$$

But the last clearly splits as

$$\prod_{\mathbf{u} \in \mathcal{U} - \{\mathbf{u}_0\}} \left(\sum_{(m_{\mathbf{u}}) \in (\mathbb{Z}/n_1 n_2 \mathbb{Z})^*} \frac{\rho_{\mathbf{u}}(m_{\mathbf{u}})}{\rho_{\mathbf{u}_0}(m_{\mathbf{u}})} \right) = \prod_{\mathbf{u} \in \mathcal{U} - \{\mathbf{u}_0\}} \left(\sum_{(m_{\mathbf{u}}) \in (\mathbb{Z}/n_1 n_2 \mathbb{Z})^*} \prod_{\chi \in T} \chi^{\psi_{\chi}(\mathbf{u}) - \psi_{\chi}(\mathbf{u}_0)}(m_{\mathbf{u}}) \right).$$

Using that the set of χ in T consists of a set of linearly independent characters, we obtain that each factor of the last product vanishes if and only if ψ_{χ} is not constant on \mathcal{U} , i.e. if and only if \mathcal{U} is not stable. In the stable case its value is $\varphi(n_1 n_2)^{2|\mathbf{k}|_1 - 1}$. Therefore we have proved that

$$\begin{aligned} \sum_{\substack{(g_{\mathbf{u}}) \in (\mathbb{Z}/q\mathbb{Z})^{2|\mathbf{k}|_1} \\ \prod_{\mathbf{u} \in \mathcal{U}} g_{\mathbf{u}} \equiv a \pmod{q} \\ \forall \mathbf{u} \in \mathcal{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} \pmod{4})}} \prod_{\mathbf{u} \in \mathcal{U}} \rho_{\mathbf{u}}(g_{\mathbf{u}}) &= (\#U_1(2^b) \#U_1(n_0) \varphi(m) \varphi(n_1 n_2))^{2|\mathbf{k}|_1 - 1} \mathbf{1}_{\mathcal{U} \text{ stable}}(\mathcal{U}) \\ &= \left(\frac{\varphi(q)}{2} \right)^{2|\mathbf{k}|_1 - 1} \mathbf{1}_{\mathcal{U} \text{ stable}}(\mathcal{U}), \end{aligned}$$

from which we deduce that

$$\sum_{\mathcal{U}} \gamma_{\psi}(\mathcal{U}) = \left(\frac{\varphi(q)}{2} \right)^{2|\mathbf{k}|_1 - 1} \sum_{\substack{\mathcal{U} \text{ stable} \\ (h_{\mathbf{u}})_{\mathbf{u} \in \mathcal{U}} \in (\mathbb{Z}/4\mathbb{Z})^{2|\mathbf{k}|_1} \\ \prod_{\mathbf{u} \in \mathcal{U}} h_{\mathbf{u}} \equiv 3 \pmod{4}}} \sum_{\mathbf{u}, \mathbf{v} \in \mathcal{U}} \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathcal{U}} (-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \frac{h_{\mathbf{u}} - 1}{2} \frac{h_{\mathbf{v}} - 1}{2} \right),$$

where the pairs \mathbf{u}, \mathbf{v} are unordered. The inner sum is identical to the one appearing in the work of Fouvry and Klüners, however the outer sum does not appear in their work. Define

$$\gamma(\mathcal{U}) := \sum_{\substack{(h_{\mathbf{u}})_{\mathbf{u} \in \mathcal{U}} \in (\mathbb{Z}/4\mathbb{Z})^{2|\mathbf{k}|_1} \\ \prod_{\mathbf{u} \in \mathcal{U}} h_{\mathbf{u}} \equiv 3 \pmod{4}}} \left(\prod_{\mathbf{u}, \mathbf{v} \in \mathcal{U}} (-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u}, \mathbf{v})} \frac{h_{\mathbf{u}} - 1}{2} \frac{h_{\mathbf{v}} - 1}{2} \right).$$

We are left with proving

$$\sum_{\mathcal{U} \text{ stable}} \gamma(\mathcal{U}) = 2^{2|\mathbf{k}|_1 + |\mathbf{k}|_1 - 1} \mathcal{N}_2(|\mathbf{k}|_1 - \#T) \quad (6.17)$$

and this will be our aim in §6.6.

6.6. Combinatorics. From [8, Lem.18] we know that the maximal unlinked sets of indices \mathcal{U} consist precisely of cosets of $|\mathbf{k}|_1$ -dimensional subspaces of $\mathbb{F}_2^{2|\mathbf{k}|_1}$. Therefore stable \mathcal{U} are cosets of $|\mathbf{k}|_1$ -dimensional subspace of $\mathbb{F}_2^{2|\mathbf{k}|_1}$, where all the Ψ_{χ} vanish.

Next, introduce the bilinear form on $\mathbb{F}_2^{2|\mathbf{k}|_1}$ via

$$L(\mathbf{u}, \mathbf{v}) := \sum_{j=0}^{|\mathbf{k}|_1} \mathbf{u}_{2j+1} (\mathbf{v}_{2j+1} + \mathbf{v}_{2j+2}).$$

Using the terminology from [8], we say that a $|\mathbf{k}|_1$ -dimensional subspace, \mathcal{U}_0 , of $\mathbb{F}_2^{2^{|\mathbf{k}|_1}}$ is *good* if

$$L|_{\mathcal{U}_0 \times \mathcal{U}_0} \equiv 0.$$

Recall that the upshot of [8, Lem.22-25] is that γ vanishes on all cosets of non-good subspaces, meanwhile the total contribution from the set of cosets of a fixed good subspace is $2^{2^{|\mathbf{k}|_1} + |\mathbf{k}|_1 - 1}$. This provides us with

$$\sum_{\mathcal{U} \text{ stable}} \gamma(\mathcal{U}) = 2^{2^{|\mathbf{k}|_1} + |\mathbf{k}|_1 - 1} \#\{\mathcal{U}_0 \text{ good} : \Psi_\chi(\mathcal{U}_0) = 0 \text{ for each } \chi \in T\}.$$

Now, following the proof of [8, Lem.26], if $\{e_1, \dots, e_{2^{|\mathbf{k}|_1}}\}$ denotes the standard basis of $\mathbb{F}_2^{2^{|\mathbf{k}|_1}}$, choose a new basis via

$$\{b_1, \dots, b_{2^{|\mathbf{k}|_1}}\} = \{e_1 + e_2, e_2, \dots, e_{2^{j-1}} + e_{2^j}, e_{2^j}, \dots, e_{2^{|\mathbf{k}|_1-1}} + e_{2^{|\mathbf{k}|_1}}, e_{2^{|\mathbf{k}|_1}}\}.$$

Then, with respect to the new basis, L assumes the form

$$L(\mathbf{x}, \mathbf{y}) = \sum_{j=0}^{j-1} \mathbf{x}_{2^{j+1}} \mathbf{y}_{2^{j+2}}.$$

In the proof of part (i) of [8, Lem.25] it is verified that, if X consists of the subspace generated by $\{b_i : i \text{ odd}\}$ and Y consists of the subspace generated by $\{b_i : i \text{ even}\}$, the map sending $\mathcal{U}_0 \mapsto \pi_X(\mathcal{U}_0)$ where π_X is the projection map $\mathbb{F}_2^{2^{|\mathbf{k}|_1}} = X \oplus Y \rightarrow X$ gives a bijection between good subspaces of $\mathbb{F}_2^{2^{|\mathbf{k}|_1}}$ and vector subspaces of $\mathbb{F}_2^{|\mathbf{k}|_1}$. On the other hand, we are counting only good subspaces where Ψ_χ vanishes for each $\chi \in T$. Observe that owing to (6.4) we have that Ψ_χ are all constantly 0 on Y , hence they define $\#T$ linearly independent linear functions from X to \mathbb{F}_2 which we will denote by the same letters. Therefore $\mathcal{U}_0 \rightarrow \pi_X(\mathcal{U}_0)$ provides a bijection between good subspaces where all Ψ_χ vanish and subspaces of X where all Ψ_χ vanish. Given that $\Psi_\chi : X \rightarrow \mathbb{F}_2$ are independent we find that the cardinality of such subspaces is precisely $\mathcal{N}_2(|\mathbf{k}|_1 - \#T)$. This substantiates (6.17), which concludes the proof of Theorem 5.6.

7. FROM THE MIXED MOMENTS TO THE DISTRIBUTION

This section is devoted to deduce Theorem 5.7 from Theorem 5.6. We will follow an adaptation of a method used by Heath-Brown in [10]. As explained in §4, Theorem 5.7 can be equivalently rephrased as a theorem about the distribution of the vector

$$D \mapsto (m_\chi(D))_{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}.$$

Namely consider for any positive integer j and subspace $Y \subseteq \widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}$, the vector

$$\mathbf{v}^{(j,Y)} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}},$$

defined as $\mathbf{v}_\chi^{(j,Y)} = j$ if $\chi \in Y$ and $\mathbf{v}_\chi^{(j,Y)} = j - 1$ if $\chi \notin Y$. Assign to $\mathbf{v}^{(j,Y)}$ mass

$$\mu(\mathbf{v}^{(j,Y)}) = \mu_{\text{CL}}(A \in \mathcal{G}_2 : \#A[2] = 2^{j-1}) \frac{\#\text{Epi}(\mathbb{F}_2^{j-1}, Y)}{\#\text{Hom}(\mathbb{F}_2^{j-1}, \widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2})}.$$

On the other hand, assign to all other vectors $\mathbf{v} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ mass equal to 0. In Proposition 4.8 it is shown that this equips $\mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ with a probability measure satisfying the following *moment equations*:

$$\sum_{\mathbf{v} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}} 2^{\mathbf{v} \cdot \mathbf{k}} \mu(\mathbf{v}) = C_{\mathbf{k}},$$

where for any $\mathbf{k} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ we define

$$C_{\mathbf{k}} := 2^{|\mathbf{k}|_1} \sum_{Y \subseteq \widehat{G}_{n_1} \times \widetilde{G}_{n_2}} \mathbb{P}_{(\mathbf{k})}(Y) \mathcal{N}_2(|\mathbf{k}|_1 - \dim(Y))$$

and where $\mathbf{v} \cdot \mathbf{k}$ denotes the inner product.

We begin the proof of Theorem 5.7 by showing that the distribution μ is characterized by the moment equations given above. Indeed we show more, namely assume x is a map $\mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}} \rightarrow [0, 1]$ satisfying for any $\mathbf{k} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ the moment relations

$$\sum_{\mathbf{v} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}} 2^{\mathbf{v} \cdot \mathbf{k}} x(\mathbf{v}) = C_{\mathbf{k}}. \quad (7.1)$$

Observe that one has the trivial bound $C_{\mathbf{k}} \ll 2^{|\mathbf{k}|_1} \mathcal{N}_2(|\mathbf{k}|_1)$, which leads to $C_{\mathbf{k}} \ll 2^{\frac{|\mathbf{k}|_1^2 + 4|\mathbf{k}|_1}{4}}$.

Letting $F(t) := \prod_{n=0}^{\infty} (1 - t2^{-n})$, we therefore see that for any $\mathbf{k} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$, the following series is absolutely convergent,

$$\sum_{\mathbf{n} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}} a_{\mathbf{n}} C_{\mathbf{n}} 2^{-\mathbf{n} \cdot \mathbf{k}}, \quad (7.2)$$

where $a_{\mathbf{n}}$ is the \mathbf{n} -coefficient of the Taylor expansion of

$$\widetilde{F}(\mathbf{z}) := \prod_{\chi \in \widehat{G}_{n_1} \times \widetilde{G}_{n_2}} F(z_{\chi}).$$

Injecting (7.1) into (7.2), expanding in terms of x and exchanging the order of summation, we obtain

$$\sum_{\mathbf{n} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}} a_{\mathbf{n}} C_{\mathbf{n}} 2^{-\mathbf{n} \cdot \mathbf{k}} = \sum_{\mathbf{m} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}} \widetilde{F}((2^{\mathbf{m}_\chi - \mathbf{k}_\chi})) x(\mathbf{m}).$$

If for all χ we have $\mathbf{m}_\chi < \mathbf{k}_\chi$ then $\widetilde{F}((2^{\mathbf{m}_\chi - \mathbf{k}_\chi})) \neq 0$, otherwise we have $\widetilde{F}((2^{\mathbf{m}_\chi - \mathbf{k}_\chi})) = 0$. Therefore, the right side is a finite sum supported in the region $\mathbf{m}_\chi < \mathbf{k}_\chi$ for every χ . Hence, using the triangular system of relations above one can successively reconstruct the function $x(\mathbf{m})$ from the moments $C_{\mathbf{k}}$. Therefore, we necessarily have $x(\mathbf{m}) = \mu(\mathbf{m})$ described above.

Let a, q be integers as in Theorem 5.7 and for any $\mathbf{j} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ and $X \in \mathbb{R}_{\geq 1}$, define the quantity $d_{\mathbf{j}}(X)$ as the proportion of all positive square-free integers $D \leq X$ satisfying $D \equiv a \pmod{q}$ and $\mathbf{m}_\chi(D) = 2^{\mathbf{j}_\chi}$ for all χ . Therefore, Theorem 5.6 shows that for any $\mathbf{k} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ we have $\sum_{\mathbf{r}} d_{\mathbf{r}}(X) 2^{\mathbf{r} \cdot \mathbf{k}} = C_{\mathbf{k}} + o(1)$, as $X \rightarrow +\infty$, where the sum is taken

over $\mathbf{r} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$. The argument concludes as follows: fix any vector $\mathbf{v} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$; by compactness of the interval $[0, 1]$ and a standard diagonal argument, one can choose a sequence $\{Y_n\}_{n \in \mathbb{N}}$ tending to infinity, such that $d_{\mathbf{v}}(Y_n)$ converges to any of the limit points of $\{d_{\mathbf{v}}(X) : X \in \mathbb{R}_{\geq 1}\}$, call it $d'_{\mathbf{v}}$, while for every other \mathbf{w} the sequence $d_{\mathbf{w}}(Y_n)$ is also converging to some limit point $d'_{\mathbf{w}}$. Next, we fix $\mathbf{h} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$, and we use the previous moment relation for $\mathbf{k} = 2\mathbf{h}$, trivially bounding each term with the total sum, providing $d_{\mathbf{r}}(Y_n) \ll_{\mathbf{h}} 2^{-\mathbf{r} \cdot \mathbf{h}}$. This enables us to apply the dominated convergence theorem to exchange the sum and the limit in the expression of the \mathbf{h} -th moment, from which we deduce that $d'_{\mathbf{w}}$ satisfies the following moment equations as well:

$$\sum_{\mathbf{w} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}} 2^{\mathbf{w} \cdot \mathbf{h}} d'_{\mathbf{w}} = C_{\mathbf{h}}.$$

We must therefore have $d'_{\mathbf{w}} = \mu(\mathbf{w})$ for all $\mathbf{w} \in \mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$. Note that $d'_{\mathbf{v}}$ was an arbitrary limit point of $d_{\mathbf{v}}(X)$, hence we deduce that

$$\lim_{X \rightarrow \infty} d_{\mathbf{v}}(X) = \mu(\mathbf{v}).$$

Since \mathbf{v} was chosen arbitrarily in $\mathbb{Z}_{\geq 0}^{\widehat{G}_{n_1} \times \widetilde{G}_{n_2}}$ we have thus shown that Theorem 5.7 holds, thereby concluding the proof of Theorem 5.7.

REFERENCES

- [1] B. Alberts and J. Klys, The distribution of H_8 -extensions of quadratic fields. [arXiv:1611.05595](#), (2017).
- [2] M. Bhargava, A. Shankar and J. Tsimerman, On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.* **193** (2013), 439–499.
- [3] M. Bhargava and I. 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** (2015), 1911–1933.
- [4] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields. *Number theory, Noordwijkerhout 1983*, Lecture Notes in Math., Springer, Berlin, (1984), 33–62.
- [5] D. Dummit and J. Voight (with appendix of R. Foote), The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units. [arXiv:1702.00092](#), (2017).
- [6] J. Ellenberg, A. Venkatesh and C. Westerland, Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. *Ann. of Math.* **183** (2016), 729–786.
- [7] É. Fouvry and J. Klüners, Cohen-Lenstra heuristics of quadratic number fields. *Algorithmic number theory*, Lecture Notes in Comput. Sci., Springer, Berlin, (2006), 40–55.
- [8] ———, On the 4-rank of class groups of quadratic number fields. *Invent. Math.* **167** (2007), 455–513.
- [9] F. Gerth, Extension of conjectures of Cohen and Lenstra. *Exposition. Math.* **5** (1987), 181–184.
- [10] R. Heath-Brown, The size of Selmer groups for the congruent number problem. II. *Invent. Math.* **118** (1994), 331–370.
- [11] ———, A mean value estimate for real character sums. *Acta Arith.* **72** (1995), 235–275.
- [12] H. Iwaniec and E. Kowalski, *Analytic number theory*. American Math. Soc. Providence, RI, (2004).
- [13] B. W. Jordan, Z. Klagsbrun, B. Poonen, C. Skinner and Y. Zaytman, Statistics of K -groups modulo p for the ring of integers of a varying quadratic number field. [arXiv:1703.00108](#), (2017).
- [14] J. Klys, The distribution of p -torsion in degree p cyclic fields. [arXiv:1610.00226](#), (2016).
- [15] J. Neukirch, *Algebraic number theory*. Springer-Verlag, Berlin, (1999).
- [16] A. Smith, 2^∞ -Selmer groups, 2^∞ -class groups, and Goldfeld’s conjecture. [arXiv:1702.02325v2](#), (2017).
- [17] R. P. Stanley, *Enumerative combinatorics. Volume 1*. Cambridge University Press, Cambridge, (2012)
- [18] I. Varma, The mean number of 3-torsion elements in ray class groups of quadratic fields. [arXiv:1609.02292](#), (2016).

- [19] C. A. Weibel, *An introduction to homological algebra*. Cambridge University Press, Cambridge, (1994).
- [20] M. M. Wood, Cohen–Lenstra and local conditions. *Preprint*, (2017).
- [21] ———, Non-abelian Cohen–Lenstra moments. [arXiv:1702.04644](https://arxiv.org/abs/1702.04644), (2017).
- [22] ———, Random integral matrices and the Cohen–Lenstra Heuristics. arxiv.org/abs/1504.04391, (2015).

MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN, LEIDEN, 2333 CA, NETHERLANDS
E-mail address: c.pagano@math.leidenuniv.nl

MAX PLANCK INSTITUTE FOR MATHEMATICS, VIVATSGASSE 7, BONN, 53111, GERMANY
E-mail address: sofos@mpim-bonn.mpg.de