

# Pointwise Bound for $\ell$ -torsion in Class Groups: Elementary Abelian Extensions

Jiuya Wang

January 28, 2020

## Abstract

Elementary abelian groups are finite groups in the form of  $A = (\mathbb{Z}/p\mathbb{Z})^r$  for a prime number  $p$ . For every integer  $\ell > 1$  and  $r > 1$ , we prove a non-trivial upper bound on the  $\ell$ -torsion in class groups of every  $A$ -extension. Our results are pointwise and unconditional. This establishes the first case where for some Galois group  $G$ , the  $\ell$ -torsion in class groups are bounded non-trivially for every  $G$ -extension and every integer  $\ell > 1$ . When  $r$  is large enough, the unconditional pointwise bound we obtain also breaks the previously best known bound shown by Ellenberg-Venkatesh under GRH.

**Key words.**  $\ell$ -torsion conjecture, elementary abelian group, GRH

## 1 Introduction

In this paper, we study cases of the following conjecture.

**Conjecture 1** ( *$\ell$ -torsion Conjecture*). *Given an integer  $\ell > 1$  and a number field  $k$ . For any degree  $d$  extension  $F/k$ , the size of  $\ell$ -torsion in the class group of  $F$  is bounded by*

$$|\mathrm{Cl}_F[\ell]| = O_{\epsilon, k}(\mathrm{Disc}(F)^\epsilon).$$

This conjecture has been brought forward previously by [BS96, Duk98, Zha05]. Nowadays in arithmetic statistics, Conjecture 1 has been closely related to other questions. In [PTBW19], it is shown that Conjecture 1 is implied by assuming a moment version of Cohen-Lenstra heuristics. Conjecture 1 is also closely related to proving upper bounds in counting number fields [Klü05, Klü06, Klü12, Wid17, Alb20, PTBW], number of elliptic curves with a fixed conductor [BS96], number of integral points of elliptic curves, and size of Selmer groups and ranks of elliptic curves and hyperelliptic curves [BK77, BST<sup>+</sup>17, HV06].

By a theorem of Brauer-Siegel, see for example [Lan94], the class number of  $F$  with  $[F : \mathbb{Q}] = d$  is bounded by  $O_{\epsilon, d}(\mathrm{Disc}(F)^{1/2+\epsilon})$ , therefore we get the so-called *trivial bound* for  $\ell$ -torsion in class groups:

$$|\mathrm{Cl}_F[\ell]| = O_\epsilon(\mathrm{Disc}(F)^{1/2+\epsilon}). \tag{1.1}$$

As one can observe, there is a huge gap between the trivial bound and Conjecture 1. The only case where Conjecture 1 is proved to the full strength is when  $(d, \ell) = (2, 2)$  due to Gauss by genus theory. Aside from this special case, it is even wildly open to prove a result in the form of (1.1) by replacing  $1/2$  with any  $0 < 1/2 - \delta < 1/2$ . We will call such a bound a *non-trivial bound* for  $\ell$ -torsion in class groups. Notice that for a fixed degree, there are only finitely many

possible Galois groups, and fields with different Galois groups behave very differently. Therefore it is natural to split up discussions of  $(d, \ell)$  to  $(G, \ell)$  for a transitive permutation group  $G \subset S_d$  with degree  $d$ , that is, considering the bound for  $\text{Cl}_F[\ell]$  where the Galois closure  $\tilde{F}$  of  $F/k$  has  $\text{Gal}(\tilde{F}/k) = G$ , see works towards this question [PTBW, Wid17, FW18a, An18, FW18b]. Aside from special cases that can be handled by genus theory, previously people can only get non-trivial bound for  $(G, \ell)$ : when  $\ell = 2$  for all Galois groups  $G$  (i.e., for all degree  $d$ ), see [BST<sup>+</sup>17], and  $\ell = 3$  for all small degree number fields with  $d \leq 4$ , see [EV07, Pie05, HV06]. In terms of conditional results, the work of Ellenberg-Venkatesh [EV07] shows a non-trivial bound for all  $G$  and all  $\ell$  in the order of  $O_{\epsilon, k}(\text{Disc}(F)^{1/2 - \frac{1}{2\ell(d-1)} + \epsilon})$  where  $d = [F : k]$  by assuming GRH. Indeed, a critical lemma in [EV07] shows that  $|\text{Cl}_F[\ell]|$  can be non-trivially bounded as long as there exist many small split primes, which is guaranteed by GRH in general. See Lemma 5.5 for a precise statement. Recently there has been an emerging group of works, see e.g. [EPW, PTBW, Wid17, FW18a, An18, FW18b, TZ19], towards removing the GRH condition in [EV07]. All of these works only obtain results *on average* in order to remove GRH. More precisely, such average results prove that a non-trivial bound holds for number fields within a family of number fields with a possible zero-density exceptional set.

In this paper, we will focus on cases where  $G$  is an elementary abelian group with rank  $r > 1$  and  $\ell > 1$ . In particular, we obtain a genuinely pointwise bound on  $|\text{Cl}_F[\ell]|$  for arbitrary  $\ell > 1$  that is unconditional. We prove the following theorem.

**Theorem 1.1** (Theorem 6.9, Theorem 7.6 and Theorem 7.8 ). *Given  $A = (\mathbb{Z}/p\mathbb{Z})^r$  where  $r > 1$  and an integer  $\ell > 1$ . There exists  $\delta(\ell, p) > 0$  such that for any  $A$ -extension  $L/\mathbb{Q}$ , we have*

$$|\text{Cl}_L[\ell]| = O_{\epsilon}(\text{Disc}(L)^{1/2 - \delta(\ell, p) + \epsilon}).$$

**Remark 1.2.** *Analogues of Theorem 1.1 over general number field  $k$  are also proved, see Theorem 6.9 and Theorem 7.8, where different savings  $\delta_k(\ell, p)$  are obtained also depending on  $k$ . Here in order to state a uniform result in Theorem 1.1, for  $p$  odd, the saving  $\delta(\ell, p)$  is taken to be  $\delta_{\mathbb{Q}}(\ell_{(p)}, p)$  in Theorem 6.9; and for  $p = 2$ , the saving  $\delta(\ell, 2)$  is taken to be  $\delta_{\mathbb{Q}}(\ell_{(2)}, 2)$  in Theorem 7.8 and 7.1. For  $p = 2$  and  $r > 2$ , a better saving is stated in Theorem 7.6. For  $\ell = p$ , of course we have a much better bound  $|\text{Cl}_L[p]| \leq O_{\epsilon}(\text{Disc}(L)^{\epsilon})$  by genus theory, for example see Theorem 3 in [Cor83]. All results in this paper are effective.*

It is worth noticing that this is the first family of Galois groups  $G$  where  $\ell$ -torsion in class groups of  $G$ -extensions are bounded non-trivially for every integer  $\ell > 1$  unconditionally. Moreover, for every  $\ell > 3$ , this is the first case where for some Galois group  $G$  with  $\ell \nmid |G|$  (i.e. away from genus theory) a non-trivial point-wise bound is proved for every  $G$ -extension.

A very important characteristic of the savings  $\delta(\ell, p)$  in Theorem 1.1 (including its analogue  $\delta_k(\ell, p)$  over general number field  $k$ ) is that it does not depend on the rank  $r$  of  $A$ . Therefore there exists  $r_0 = r_0(\ell, p)$  such that when  $r > r_0(\ell, p)$ , we have

$$\delta(\ell, p) \geq \frac{1}{2\ell(d-1)} = \frac{1}{2\ell(p^r-1)} = \text{the saving proved in [EV07] by assuming GRH.}$$

The main strategy of this work is to take advantage of the group structure of elementary abelian groups  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $r > 1$ .

- Firstly, an elementary abelian group  $A = (\mathbb{Z}/p\mathbb{Z})^r$  has  $(p^r - 1)/(p - 1)$  index- $p$  subgroups  $A_i$  with  $A/A_i \simeq \mathbb{Z}/p\mathbb{Z}$ . Correspondingly, for any  $A$ -extension  $L/k$  with  $\text{Gal}(L/k) = A$ , we get  $(p^r - 1)/(p - 1)$  degree  $p$  sub-extensions  $K_i/k$  with Galois group  $\text{Gal}(K_i/k) = \mathbb{Z}/p\mathbb{Z}$ .

Considering  $\text{Cl}_{L/k}[\ell]$  as a Galois module with Galois group  $\text{Gal}(L/k)$ , it can be decomposed along the fixed part by  $A_i$  for all index- $p$  subgroup  $A_i$ , therefore we can obtain equalities like

$$|\text{Cl}_{L/k}[\ell]| = \prod_{K_i/k} |\text{Cl}_{K_i/k}[\ell]|, \quad \text{Disc}(L/k) = \prod_{K_i/k} \text{Disc}(K_i/k),$$

where  $K_i/k$  ranges over all degree  $p$  subfields of  $L$ . For more details on these equalities, see Lemma 3.1 and 3.3. Therefore we can reduce the question of  $L/k$  to the question of subfields  $K_i/k$ . This is essentially the key reason why the bound we obtain behave better than the GRH bound when  $r$  is sufficiently large.

- Secondly, the decomposition group of an  $A$ -extension at unramified primes must be  $\mathbb{Z}/p\mathbb{Z}$  since every cyclic subgroup of  $A$  is isomorphic to  $\mathbb{Z}/p\mathbb{Z}$ . Therefore every unramified prime  $p$  is at least split in  $(p^{r-1} - 1)/(p - 1)$  degree  $p$  subfields of  $L/k$ . This guarantees the existence of split primes.
- Thirdly, by the conductor-discriminant formula, we can give lower bound on the discriminant of subfields, see for example Lemma 3.4. Then we can apply results on upper or lower bounds of prime counting functions where the range of consideration is in the order of a polynomial in the modulus, see section 4 for a collection of some results in this direction that we use, and see Theorem 6.3 for an example how we apply them.

The organization of the paper is as follows. In section 3, we introduce the algebraic lemmas in preparation for the later proof. It includes several necessary equalities of class groups and discriminants and inequalities of discriminants. In section 4, we collect several results on upper and lower bounds of prime counting function. They all share the property that the range of primes considered is in a polynomial order of the discriminant. In section 5, we revisit the critical lemma from [EV07] on bounding  $\ell$ -torsion in the class groups conditional on the existence of small split primes. In section 6, we give the proof of Theorem 1.1, including its analogue over general number field, when  $p$  is odd. In section 7, we give the proof of Theorem 1.1, including its analogue over general number field, when  $p = 2$ . We mention that section 6 and 7 share a lot of similarities in spirit, whereas section 7 deals with some new complication when  $p = 2$ . In order to grasp the main idea, it is recommended to read section 6 first.

## 2 Notations

$k$ : a number field considered as the base field

$|\cdot|$ : the absolute norm  $\text{Nm}_{k/\mathbb{Q}}$

$\text{Gal}(F/k)$ : Galois group of  $F/k$

$\text{Disc}(F/k)$ : relative discriminant  $|\text{disc}(F/k)|$  of  $F/k$  where  $\text{disc}(F/k)$  is the relative discriminant ideal in  $k$ , when  $k = \mathbb{Q}$  it is the usual absolute discriminant

$\text{Cl}_{F/k}$ : relative class group of  $F/k$ , when  $k = \mathbb{Q}$  it is the usual class group of  $F$

$\text{Cl}_{F/k}[\ell]$ :  $\{[\alpha] \in \text{Cl}_{F/k} \mid \ell[\alpha] = 0 \in \text{Cl}_{F/k}\}$

$|\text{Cl}_{F/k}[\ell]|, |\text{Cl}_F[\ell]|$ : the size of  $\text{Cl}_{F/k}[\ell], \text{Cl}_F[\ell]$

$M^G$ : the maximal submodule of the  $G$ -module  $M$  that is invariant under  $G$

$M_G$ : the maximal quotient module  $M/I_G(M)$  of the  $G$ -module  $M$  that is invariant under  $G$

$I_G$ : the augmentation ideal  $\langle \sigma - 1 \mid \sigma \in G \rangle \subset R[G]$  in the group ring with coefficient ring  $R$

$\pi(Y; q, a)$ : the number of prime numbers  $p$  such that  $p < Y$  and  $p \equiv a \pmod q$

$\pi(Y; L/k, \mathcal{C})$ : the number of unramified prime ideals  $p$  in  $k$  with  $|p| < Y$  and  $\text{Frob}_p \in \mathcal{C}$  where  $\mathcal{C}$

is a conjugacy class of  $\text{Gal}(L/k)$

$\pi(Y; L/k, \hat{C})$ : the number of unramified prime ideals  $p$  in  $L$  with  $|p| < Y$  and  $\text{Frob}_p \notin \mathcal{C}$  where  $\mathcal{C}$  is a conjugacy class of  $\text{Gal}(L/k)$

$A \asymp B$ : there exist absolute constants  $C_1$  and  $C_2$  such that  $C_1 B \leq A \leq C_2 B$

$\Delta(\ell, d)$ : a constant number slightly smaller than  $\frac{1}{2\ell(d-1)}$ , see Remark 5.4

$\ell_{(p)}$ : the maximal factor of  $\ell$  that is relatively prime to a prime number  $p$  for an integer  $\ell > 1$

$\eta(L/k)$ : see (6.1) when  $\text{Gal}(L/k) = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  with  $p$  odd and see (7.1) when  $\text{Gal}(L/k) = (\mathbb{Z}/2\mathbb{Z})^3$

$\eta_0(\ell, p)_k$ : a cut-off for  $\eta(L/k)$  that is determined in Theorem 6.3 and 6.4 when  $\text{Gal}(L/k)$  has rank 2; we will drop  $k$  when  $k = \mathbb{Q}$

$\delta$ : through out the paper we always use  $\delta$  to denote a power saving from the trivial power  $1/2$  in the bound; we use  $\delta_c$  to denote the power saving when  $\eta(L/k)$  is small and  $\delta_{ic}$  to denote the power saving when  $\eta(L/k)$  is big. *Small* and *big* are quantified by comparing to  $\eta_0(\ell, p)_k$ .

Warning: In order to simplify the notation for the whole paper, unless specifically mentioned otherwise, the implied constants  $O_\epsilon$ ,  $O_{\epsilon, k}$ ,  $O_{\epsilon, k, \epsilon_0}$  will always depend on  $\ell, d$  aside from the dependence indicated in the symbol when we are stating results or conjectures on bounding  $\ell$ -torsion in class groups of degree  $d$  extensions.

### 3 Algebraic Theory

In this section, firstly we are going to state several standard equalities of class group and discriminants, Lemma 3.1 and 3.3 from algebraic number theory that will be of crucial use for later proof. These results and equalities are known previously, for example see [CM87]. Here we only include a proof for the convenience of the readers. Secondly, we will give a ramification analysis on  $A$ -extensions and prove critical lemmas Lemma 3.4 and 3.5 throughout the proof.

#### 3.1 Relative Class Group

In this section, we define the notion of relative class group. The relative class group  $\text{Cl}_{F/k} \subset \text{Cl}_F$  is defined to be  $\text{Ker}(\text{Nm})$  where  $\text{Nm} : \text{Cl}_F \rightarrow \text{Cl}_k$  is induced from the usual norm on fractional ideals of  $F$ .

Fix an integer  $\ell > 1$  that is relatively prime to the degree  $[F : k]$ , we will show that the following forms a short exact sequence

$$0 \rightarrow \text{Cl}_{F/k}[\ell] \rightarrow \text{Cl}_F[\ell] \rightarrow \text{Cl}_k[\ell] \rightarrow 0.$$

Indeed, denote the map  $\iota : \text{Cl}_k \rightarrow \text{Cl}_F$  which is induced from the usual embedding of fractional ideals. We know that  $\text{Nm} \circ \iota : \text{Cl}_k \rightarrow \text{Cl}_k$  is equivalent to multiplication by  $[F : k]$ , which is an isomorphism on the  $\ell$ -torsion part  $\text{Cl}_k[\ell]$ . Therefore  $\text{Nm} : \text{Cl}_F[\ell] \rightarrow \text{Cl}_k[\ell]$  is surjective and  $\iota : \text{Cl}_k[\ell] \rightarrow \text{Cl}_F[\ell]$  is injective and gives a section of the short exact sequence above.

If  $F/k$  is Galois with  $\text{Gal}(F/k) = G$ , then the class group  $\text{Cl}_F[\ell]$  can be considered as a Galois module with Galois group  $G$ . Since  $(|G|, \ell) = 1$ , the Tate cohomology  $\hat{H}^i(G, \text{Cl}_F[\ell])$  vanishes for every  $i$ . It follows from  $\hat{H}^0(G, \text{Cl}_F[\ell]) = (\text{Cl}_F[\ell])^G / \iota \circ \text{Nm}(\text{Cl}_F[\ell]) = 0$  that  $(\text{Cl}_F[\ell])^G = \iota \circ \text{Nm}(\text{Cl}_F[\ell]) = \iota(\text{Cl}_k[\ell]) \simeq \text{Cl}_k[\ell]$ . The last two equalities come from  $\text{Nm}$  being surjective and  $\iota$  being injective. Similarly, it follows from  $\hat{H}^{-1}(G, \text{Cl}_F[\ell]) = \text{Cl}_{F/k}[\ell] / I_G(\text{Cl}_F[\ell]) = 0$  that  $(\text{Cl}_F[\ell])_G = \text{Cl}_F[\ell] / I_G(\text{Cl}_F[\ell]) = \text{Cl}_F[\ell] / \text{Cl}_{F/k}[\ell] \simeq \text{Cl}_k[\ell]$ .

### 3.2 Class Group Decomposition

The main goal of the following lemma is to reduce the questions about elementary abelian extensions to those of their sub-extensions.

**Lemma 3.1.** *Given an elementary abelian group  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $r > 1$  and an integer  $\ell > 1$  with  $(\ell, p) = 1$ . For any  $A$ -extension  $L/k$ ,*

$$|\mathrm{Cl}_{L/k}[\ell]| = \prod_{K_i/k} |\mathrm{Cl}_{K_i/k}[\ell]|,$$

where  $K_i/k$  ranges over all subfields of  $L$  with  $[K_i : k] = p$ .

*Proof.* The class group  $\mathrm{Cl}_{L/k}[\ell]$  is naturally an  $\mathbb{Z}/\ell\mathbb{Z}[A]$ -module since  $\mathrm{Gal}(L/k)$  acts on it. For an elementary group  $A$  and an integer  $\ell$  with  $(|A|, \ell) = 1$ , we have that  $\mathbb{Z}/\ell\mathbb{Z}[A]$  is semi-simple by Maschke's theorem. We can decompose the augmentation ideal

$$I_A = \bigoplus_i \epsilon_i I_A,$$

where  $\epsilon_i = \frac{1}{|A_i|} \sum_{a \in A_i} a$  and  $A_i$  ranges over all index- $p$  subgroup of  $A$ . It can be easily shown that  $\epsilon_i^2 = \epsilon_i$  and  $\epsilon_i \circ \epsilon_j I_A = 0$ . Therefore any faithful  $\mathbb{Z}/\ell\mathbb{Z}[A]$ -module  $M$  (meaning  $M_A$  is trivial),  $M$  can be written as a direct sum

$$M = M \otimes (\mathbb{Z}/\ell\mathbb{Z})[A] = M \otimes I_A \oplus M \otimes (\mathbb{Z}/\ell\mathbb{Z})[A]/I_A = \bigoplus_i \epsilon_i M \oplus M_A = \bigoplus_i \epsilon_i M,$$

where the summation is over all index- $p$  subgroups  $A_i \subset A$ .

By the discussion in section 3.1, the module  $M = \mathrm{Cl}_{L/k}[\ell]$  as a submodule of  $\mathrm{Cl}_L[\ell]$  is faithful: it can be easily seen by applying  $(\cdot)_G$  to the short exact sequence in section 3.1 and noticing  $\mathrm{Cl}_F[\ell]_G \simeq \mathrm{Cl}_k[\ell]$ . Given  $\epsilon_i$  corresponding to  $A_i \subset A$  and  $K_i$  the field fixed by  $A_i$ , the sub-module  $\epsilon_i M = \mathrm{Nm}_{A_i}(M) = \mathrm{Cl}_{L/k}[\ell]/\mathrm{Cl}_{L/K_i}[\ell]$ : it can be seen by the following diagram. Therefore  $|\epsilon_i M| = |\mathrm{Cl}_{K_i/k}[\ell]|$ .

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Cl}_{L/K_i}[\ell] \cap \mathrm{Cl}_{L/k}[\ell] = \mathrm{Cl}_{L/K_i}[\ell] & \longrightarrow & \mathrm{Cl}_{L/k}[\ell] & \longrightarrow & \mathrm{Nm}_{A_i}(\mathrm{Cl}_{L/k}[\ell]) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Cl}_{L/K_i}[\ell] & \longrightarrow & \mathrm{Cl}_L[\ell] & \xrightarrow{\mathrm{Nm}_{A_i}} & \mathrm{Cl}_{K_i}[\ell] \longrightarrow 0 \end{array}$$

□

Next we apply Lemma 3.1 to degree  $p^2$  subfields of  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $r > 2$ . Notice that every  $K_i$  are contained in exactly  $(p^{r-1} - 1)/(p - 1)$  subfields  $M_j$  with  $[M_j : k] = p^2$ , so we have the following equality.

**Corollary 3.2.** *Given an elementary abelian group  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $r > 2$  and an integer  $\ell > 1$  with  $(\ell, p) = 1$ . For any  $A$ -extension  $L/k$ ,*

$$|\mathrm{Cl}_{L/k}[\ell]| = \prod_{M_j/k} |\mathrm{Cl}_{M_j/k}[\ell]|^{(p-1)/(p^{r-1}-1)} = \prod_{F_s/k} |\mathrm{Cl}_{F_s/k}[\ell]|^{(p-1)/(p^{r+1-t}-1)},$$

where  $M_j/k$  ranges over all subfields of  $L$  with  $[M_j : k] = p^2$ , and  $F_s/k$  ranges over all subfields of  $L$  with  $[F_s : k] = p^t$ .

### 3.3 Ramification Analysis

The main goal of this section is to give an analysis on the discriminants of all sub-extensions of  $L/k$  when  $\text{Gal}(L/k) = A$  and  $A$  is an elementary abelian group.

**Lemma 3.3.** *Given an elementary group  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $r > 1$ . For any  $A$ -extension  $L/k$ , we have*

$$\text{Disc}(L/k) = \prod_{K_i/k} \text{Disc}(K_i/k),$$

where  $K_i/k$  ranges over all subfield of  $L$  with  $[K_i : k] = p$ .

*Proof.* Recall that  $\text{Disc}(L/k)$  is the Artin-conductor of  $L/k$  with the representation  $\rho$  of  $A$  where  $\rho$  is the regular representation of  $A$  over  $\mathbb{C}$ . Then  $\rho - 1 = \oplus_i \rho_i$  where  $\rho_i = (\rho - 1)^{A_i} = \rho^{A_i} - 1$  where 1 is denoted to be the trivial representation of  $A$ . Therefore notice that the Artin-conductor with trivial character is trivial, we get the Artin conductor  $\mathfrak{f}$  associated to  $\rho$  is decomposed as:

$$\text{Disc}(L/k) = \mathfrak{f}_{L/k}(\rho) = \prod_{[A:A_i=p]} \mathfrak{f}_{L/k}(\rho^{A_i}) = \prod_{[K_i:k]=p} \mathfrak{f}_{K_i/k}(\rho_i) = \prod_{[K_i:k]=p} \text{Disc}(K_i/k).$$

□

Similarly with Corollary 3.2, we also have

$$\text{Disc}(L/k) = \prod_{M_j/k} \text{Disc}(M_j/k)^{(p-1)/(p^{r-1}-1)} = \prod_{F_s/k} |\text{Disc}(F_s/k)|^{(p-1)/(p^{r+1-t}-1)}, \quad (3.1)$$

where  $M_j/k$  ranges over all subfields of  $L$  with  $[M_j : k] = p^2$  and  $F_s/k$  ranges over all subfields of  $L$  with  $[F_s : k] = p^t$ .

**Lemma 3.4.** *Given an elementary group  $A = (\mathbb{Z}/p\mathbb{Z})^2$ . For any  $A$ -extension  $L/k$ , denote  $K_1$  and  $K_2$  to be two arbitrary subfields of  $L/k$  with degree  $p$ . Given  $\eta = \frac{\ln \text{Disc}(K_2/k)}{\ln \text{Disc}(K_1/k)}$ . Then we have a lower bound for  $\text{Disc}(K_1/k)$  and  $\text{Disc}(K_2/k)$  as following*

$$\text{Disc}(K_1/k) \geq \text{Disc}(L/k)^{1/p(\eta+1)}, \quad \text{Disc}(K_2/k) \geq \text{Disc}(L/k)^{\eta/p(\eta+1)}.$$

*Proof.* By the conductor discriminant formula, we have that the discriminant of the compositum satisfies the following inequality, see for example [Wan17, Theorem 2.1]

$$\text{Disc}(K_1/k)^p \cdot \text{Disc}(K_2/k)^p \geq \text{Disc}(L/k).$$

By assumption, we have

$$\text{Disc}(K_1/k)^{p(\eta+1)} \geq \text{Disc}(L/k),$$

therefore

$$\text{Disc}(K_1/k) \geq \text{Disc}(L/k)^{1/p(\eta+1)}, \quad \text{Disc}(K_2/k) \geq \text{Disc}(L/k)^{\eta/p(\eta+1)}.$$

□

A similar proof yields the following lower bound for  $A = (\mathbb{Z}/2\mathbb{Z})^3$ . We will need to use the following lemma when we discuss the abelian group  $A = (\mathbb{Z}/2\mathbb{Z})^3$  in section 7.2 and 7.3.

**Lemma 3.5.** *Given the elementary abelian group  $A = (\mathbb{Z}/2\mathbb{Z})^3$ . For any  $A$ -extension  $L/k$ , denote  $M/k$  to be a quartic subfield of  $L/k$  and  $K/k$  to be a quadratic subfield of  $L/k$  that is not a quadratic subfield of  $M/k$ . Given  $\eta = \frac{\ln \text{Disc}(K/k)}{\ln \text{Disc}(M/k)}$ , we have*

$$\text{Disc}(M/k) \geq \text{Disc}(L/k)^{1/(4\eta+2)}, \quad \text{Disc}(K/k) \geq \text{Disc}(L/k)^{\eta/(4\eta+2)}.$$

## 4 Analytic Theory

As a preparation for the main proof, we are going to state Brun-Titchmarsh theorem [MV73] and a lower bound theorem in [May13], and generalizations of [May13] to general number fields [Zam17] that we can conveniently use. Results in this direction have also appeared previously in [Wei83, Deb17, TZ17, TZ18]. We apply the following statements in our proofs since the format of the statements is convenient to use in our application.

The main reason that these bounds are good for us is that they hold for  $x > f(q)$  where  $x$  is the range of consideration,  $q$  is the modulus and  $f(q)$  is some polynomial in  $q$ .

**Lemma 4.1** (Brun-Titchmarsh, [MV73]). *For  $x > q$ , we have*

$$\pi(x; q, a) \leq \frac{2}{1 - \ln q / \ln x} \cdot \frac{x}{\phi(q) \ln x}.$$

**Lemma 4.2** ([May13], Theorem 3.2). *For  $x \geq q^8$ , there exists an absolute constant  $C > 0$  and an effectively computable constant  $q_2$  such that for  $q \geq q_2$ , we have*

$$\pi(x; q, a) \geq C \frac{\ln q}{q^{1/2}} \cdot \frac{x}{\phi(q) \ln x}.$$

**Lemma 4.3** ([Zam17], Theorem 1.3.1 [TZ18], Theorem 1.2). *Given  $L/k$  a Galois extension of number fields with  $[L : \mathbb{Q}] = d$ . There exists absolute, effective constants  $\gamma = \gamma(k, G) > 2$ ,  $\beta = \beta(k, G) > 2$ ,  $D_0 = D_0(k) > 0$  and  $C = C(k) > 0$  such that if  $\text{Disc}(L/k) \geq D_0$ , then for  $x \geq \text{Disc}(L/k)^\beta$ , we have*

$$C_k \frac{1}{\text{Disc}(L/k)^\gamma} \cdot \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x} \leq \pi(x; L/k, \mathcal{C}) \leq (2 + O(dx^{-\frac{1}{166d+327}})) \cdot \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x}.$$

We will navigate where these theorems are used in this paper. For results over  $\mathbb{Q}$ , we use Lemma 4.1 in section 6 for all odd degree extensions, in section 7 for all even degree extensions with rank  $r > 2$ ; we use Lemma 4.2 in section 7.3 for  $(\mathbb{Z}/2\mathbb{Z})^2$  extensions. For results over general number field  $k$ , we did not seek after an optimal bound in this work. For simplicity, we always use the lower bound in Lemma 4.3, see both section 6 and 7. The main reason for doing this is that by using the lower bound, we can write down the power saving away from the trivial bound explicitly in terms of  $\beta(k, G)$  and  $\gamma(k, G)$ . And these numbers are determined explicitly in previous work: for example, in Theorem 1.3.1 in [Zam17], if we only consider the lower bound side, then  $\gamma(k, G)$  can be taken to be 19 and  $\beta(k, G)$  can be taken to be 35. The upper bound in Lemma 4.3 can also be used to obtain a non-trivial bound for  $(\mathbb{Z}/p\mathbb{Z})^r$ -extensions over  $k$  with  $r > 1$ , following a similar proof over  $\mathbb{Q}$  in Theorem 6.3. However we did not use them in this paper since the saving will depend on the implied constant in the error term  $O(dx^{-1/(166d+327)})$ .

## 5 Ellenberg-Venkatesh Revisited

In this section, we will revisit [EV07] and rephrase their critical lemma that we base on. By defining the notion of  $\Delta$ -good/bad in Definition 5.1, we rephrase this lemma in Lemma 5.5 in the form that we can conveniently use.

Given an element  $a \in A$  in an abelian group  $A$  (or a conjugacy class  $\mathcal{C} \subset G$  for a general finite group  $G$ ), for a Galois extension  $L/k$ , we denote  $\pi(Y; L/k, a)$  (or  $\pi(Y; L/k, \mathcal{C})$ ) to be the number of unramified prime ideals  $p$  in  $k$  with  $\text{Frob}_p = a \in A$  (or  $\text{Frob}_p \in \mathcal{C} \subset G$ ). We will always

denote  $e \in A$  (or  $e \in G$ ) to mean the identity element, and  $\text{Frob}_p = e \in A$  (or  $\text{Frob}_p = e \in G$ ) corresponds to  $p$  splitting in  $L/k$ . We will denote  $\pi(Y; L/k, \hat{a})$  to be the number of prime ideals  $p$  in  $k$  with  $\text{Frob}_p \in A \setminus \{a\}$ .

We define

$$\mathcal{B}(G, \theta, c) := \left\{ L/k \mid \text{Gal}(L/k) = G, \pi(\text{Disc}(L/k)^\theta; L/k, e) \leq c \frac{\text{Disc}(L/k)^\theta}{\ln \text{Disc}(L/k)^\theta} \right\}, \quad (5.1)$$

where  $c > 0$  is an absolute small number. In reality, the choice of  $c$  will be determined from the proof.

**Definition 5.1.** *Given  $\Delta > 0$ , we call an extension  $L/k$   $\Delta$ -bad with respect to  $c$  if  $L/k \in \mathcal{B}(A, \Delta, c)$  where  $A = \text{Gal}(L/k)$ . If  $L/k$  is not  $\Delta$ -bad with respect to  $c$ , we will say  $L/k$  is  $\Delta$ -good with respect to  $c$ . When  $c$  is clear in the set up, we will simply say  $\Delta$ -bad or  $\Delta$ -good.*

The following is the critical lemma from [EV07].

**Lemma 5.2** ([EV07]). *Given a Galois extension  $L/k$  and  $0 < \theta < \frac{1}{2\ell(d-1)}$ , denote*

$$M := \pi(\text{Disc}(L/k)^\theta; L/k, e),$$

then

$$|\text{Cl}_L[\ell]| = O_{\epsilon, k} \left( \frac{\text{Disc}(L)^{1/2+\epsilon}}{M} \right). \quad (5.2)$$

**Remark 5.3** (Transition between Absolute/Relative setting). *When  $(\ell, [L : k]) = 1$ , we have  $|\text{Cl}_L[\ell]| = |\text{Cl}_{L/k}[\ell]| \cdot |\text{Cl}_k[\ell]|$ . Notice that we always have  $\text{Disc}(L) = \text{Disc}(L/k) \cdot \text{Disc}(k)^{[L:k]}$ , we can easily adapt the original statement (5.2) to the statement about  $\text{Cl}_{L/k}$  and  $\text{Disc}(L/k)$ :*

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon, k} \left( \frac{\text{Disc}(L/k)^{1/2+\epsilon}}{M} \right). \quad (5.3)$$

More specifically, fix a number field  $k$ , an elementary abelian group  $A$  and an integer  $\ell > 1$  with  $(\ell, |A|) = 1$ . Denote  $\mathcal{F}$  to be the set of all  $L/k$  with  $\text{Gal}(L/k) = A$ , then

$$\begin{aligned} \exists \delta > 0, \forall L/k \in \mathcal{F}, \quad |\text{Cl}_{L/k}[\ell]| &= O_{k, \epsilon}(\text{Disc}(L/k)^{1/2-\delta+\epsilon}) \iff \\ \exists \delta > 0, \forall L/k \in \mathcal{F}, \quad |\text{Cl}_L[\ell]| &= O_{k, \epsilon}(\text{Disc}(L)^{1/2-\delta+\epsilon}). \end{aligned} \quad (5.4)$$

Since the two statements are equivalent, we will focus on bounding  $\text{Cl}_{L/k}[\ell]$  by  $\text{Disc}(L/k)$  for the whole paper.

**Remark 5.4.** *In most situations in this paper, the parameter  $\Delta$  in Definition 5.1 will be taken to be  $\Delta < \frac{1}{2\ell(d-1)}$  where  $d = [L : k]$ . We will denote  $\Delta(\ell, d)$  for such a number that is very close to  $\frac{1}{2\ell(d-1)}$  for simplicity.*

Then in our language, we will use the following format of this critical lemma throughout the proof of the theorems in section 6 and 7:

**Lemma 5.5** ([EV07]). *Given a Galois extension  $L/k$ , an integer  $\ell > 1$  with  $(\ell, [L : k]) = 1$ ,  $0 < \theta < \frac{1}{2\ell(d-1)}$ . If  $L/k$  is  $\theta$ -good with respect to  $c$ , then*

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon, k, c}(\text{Disc}(L/k)^{1/2-\theta+\epsilon}).$$

## 6 Odd $p$

In this section, we work with the elementary abelian groups  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $p$  odd and  $r > 1$ . Firstly, in section 6.1, section 6.2 and section 6.3, we will focus on the case  $r = 2$ . In section 6.4, we will apply the result we obtained for  $r = 2$  to obtain results for every  $r > 2$ .

We introduce the notation for section 6. For  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ , there are  $p + 1$  non-trivial subgroups  $A_i \simeq \mathbb{Z}/p\mathbb{Z}$  with  $A/A_i \simeq \mathbb{Z}/p\mathbb{Z}$  for  $i = 1, \dots, p + 1$ . Therefore given an arbitrary  $A$ -extension  $L/k$ , there are  $p + 1$  non-trivial sub-extensions  $K_i/k$ . For simplicity of our discussion, we will order  $K_i$  by  $\text{Disc}(K_i/k)$ , i.e., we order them so that

$$\text{Disc}(K_i/k) \leq \text{Disc}(K_j/k) \text{ iff } i \leq j.$$

We will separate the discussion depending on the size of

$$\eta = \eta(L/k) := \frac{\ln \text{Disc}(K_2/k)}{\ln \text{Disc}(K_1/k)} \geq 1. \quad (6.1)$$

We will say  $L/k$  is *comparable* if  $\eta$  is small, and *incomparable* if  $\eta$  is big. We give the proof for the two cases in section 6.1 and 6.2 respectively with two different strategies. The cut-off for the two cases is denoted  $\eta_0 = \eta_0(\ell, p)_k$ , which is determined in section 6.2 (see Theorem 6.3, 6.4 and Remark 6.7):

$$\eta_0(\ell, p)_k = \begin{cases} ((p-1) \cdot \Delta(\ell, p) \cdot (1-2/p))^{-1} & \text{if } k = \mathbb{Q}; \\ \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, p)\} / \Delta(\ell, p) & \text{if } k \neq \mathbb{Q}. \end{cases} \quad (6.2)$$

The power saving  $\delta_c$  in section 6.1 stands for comparable case and  $\delta_{ic}$  in section 6.2 stands for incomparable case.

In cases where all parameters  $\ell$ ,  $k$  and  $p$  are clear, we will write  $\eta_0$  instead of  $\eta_0(\ell, p)_k$  for simplicity. In cases where  $k = \mathbb{Q}$ , we will drop  $k$  in the notation for simplicity, i.e., we will write  $\eta_0(\ell, p)$  instead of  $\eta_0(\ell, p)_{\mathbb{Q}}$ .

### 6.1 Comparable Size

In this section, we will consider  $L/k$  with small  $\eta$ . The approach used in this section will be universally true for any bounded range of  $\eta$ . For example, we will state the theorem with  $\eta \leq \eta_0 \cdot (1 + \epsilon_0) = \eta_0(\ell, p)_k \cdot (1 + \epsilon_0)$  where  $\epsilon_0 > 0$  is a small number, and  $\eta_0(\ell, p)_k$  is listed in (6.2). We will use this strategy especially when  $\eta$  is small. When  $\eta$  is big, we refer to section 6.2. Here the introduction of  $\epsilon_0$  is only a technical treatment in order to simplify the dependence on  $c$ , the constant defined in Definition 5.1.

**Theorem 6.1.** *Given  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ , an integer  $\ell > 1$  with  $(\ell, p) = 1$  and a number field  $k$ . For any  $A$ -extension  $L/k$  with  $\eta = \eta(L/k) \leq \eta_0 \cdot (1 + \epsilon_0) = \eta_0(\ell, p)_k \cdot (1 + \epsilon_0)$ , we have the pointwise bound*

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon, k, \epsilon_0}(\text{Disc}(L/k)^{1/2 - \delta + \epsilon}).$$

where

$$\delta = \delta_c(\eta, \ell, p) = \frac{\Delta(\ell, p)}{p(\eta + 1)},$$

and  $\eta = \eta(L/k) = \frac{\ln \text{Disc}(K_2/k)}{\ln \text{Disc}(K_1/k)}$ .

*Proof.* We separate the discussion when  $K_1/k$  is  $\Delta(\ell, p)$ -bad or good with respect to  $c$  where  $c$  is a fixed absolute number satisfying  $c < \frac{1}{p+1}$ . The constant  $c$  will be fixed once and for all in the proof of the current theorem. By Lemma 3.4, we get

$$\text{Disc}(K_1/k) \geq \text{Disc}(L/k)^{1/p(\eta+1)} \geq \text{Disc}(L/k)^{1/p(\eta_0(1+\epsilon_0)+1)}.$$

Note that a fixed integer  $L_0 > 0$ , there are only finitely many  $A$ -extensions  $L/k$  where  $\text{Disc}(L/k) \leq L_0$ , thus only finitely many  $L/k$  with  $\text{Disc}(K_1/k) \leq K_0 = L_0^{1/p(\eta_0(1+\epsilon_0)+1)}$  and  $\eta(L/k) \leq \eta_0(1+\epsilon_0)$ . So we can assume both  $L/k$  and  $K_1/k$  are sufficiently large.

If  $K_1/k$  is  $\Delta(\ell, p)$ -bad, then we are going to show that at least one of  $K_i/k$  is  $\theta_i$ -good where

$$\theta_i := \Delta(\ell, p) \frac{\ln \text{Disc}(K_1/k)}{\ln \text{Disc}(K_i/k)} < \Delta(\ell, p),$$

for  $2 \leq i \leq p+1$ . Equivalently, we define  $\theta_i$  so that  $\text{Disc}(K_1)^{\Delta(\ell, p)} = \text{Disc}(K_i)^{\theta_i}$ . Consider all primes  $p$  in  $k$  with  $|p| < Y$  where  $Y = \text{Disc}(K_1/k)^{\Delta(\ell, p)}$ . Since  $K_1/k$  is  $\Delta(\ell, p)$ -bad, there are at most  $cY/\ln Y$  primes in  $k$  splitting in  $K_1/k$ . The number of primes in  $k$  that are ramified in  $L/k$  is bounded by

$$O_{\epsilon, k}(\text{Disc}(L/k)^\epsilon) \leq O_{\epsilon, k, \epsilon_0}(Y^\epsilon),$$

since  $Y \geq \text{Disc}(L/k)^{\Delta(\ell, p)/p(\eta_0(1+\epsilon_0)+1)}$ . Therefore when  $L/k$  is sufficiently large,

$$\pi(Y; K_1/k, \hat{e}) = \pi(Y) - \pi(Y; K_1/k, e) - O_{\epsilon, k, \epsilon_0}(Y^\epsilon) \geq (1 - c - \epsilon) \cdot \frac{Y}{\ln Y}, \quad (6.3)$$

where the last inequality holds whenever  $Y \geq Y_0 = Y_0(\epsilon, \epsilon_0)$  with  $Y_0$  depending at most on  $\epsilon$  and  $\epsilon_0$ . Since the decomposition group of  $A$  at an unramified prime is cyclic, a prime  $p$  in  $k$  that is inert in  $K_1/k$  and must be split in some  $K_i$  for  $2 \leq i \leq p+1$ . By pigeon hole principle, there exists at least one  $K_i/k$  satisfying

$$\pi(Y; K_i/k, e) \geq \frac{1 - c - \epsilon}{p} \cdot \frac{Y}{\ln Y} \geq c \frac{Y}{\ln Y},$$

then  $K_i/k$  is  $\theta_i$ -good. Let's say  $K_j/k$  with  $j > 1$  is  $\theta_j$ -good, then by Lemma 5.5, we get

$$|\text{Cl}_{K_j/k}[\ell]| = O_{\epsilon, k}(\text{Disc}(K_j/k)^{1/2-\theta_j+\epsilon}),$$

where we drop the dependence on  $c$  since we fix the absolute number  $c < \frac{1}{p+1}$  from the beginning. Therefore by Lemma 3.1 and 3.3 and 3.4, when  $\text{Disc}(L/k) \geq L_0(\epsilon, \epsilon_0) = Y_0(\epsilon, \epsilon_0)^{p(\eta_0(1+\epsilon_0)+1)/\Delta(\ell, p)}$ , we get

$$\begin{aligned} |\text{Cl}_{L/k}[\ell]| &= \prod_i |\text{Cl}_{K_i/k}[\ell]| = O_{\epsilon, k}(\text{Disc}(K_j/k)^{1/2-\theta_j+\epsilon}) \prod_{i \neq j} \text{Disc}(K_i/k)^{1/2+\epsilon} \\ &= O_{\epsilon, k} \left( \frac{\text{Disc}(L/k)^{1/2+\epsilon}}{\text{Disc}(K_j/k)^{\theta_j}} \right) = O_{\epsilon, k}(\text{Disc}(L/k)^{1/2-\Delta(\ell, p)/p(\eta+1)+\epsilon}). \end{aligned} \quad (6.4)$$

If  $K_1$  is  $\Delta(\ell, p)$ -good, then we get from Lemma 5.5 that

$$|\text{Cl}_{K_1/k}[\ell]| = O_{\epsilon, k}(\text{Disc}(K_1/k)^{1/2-\Delta(\ell, p)+\epsilon}).$$

Then similarly, by Lemma 3.1 and 3.3 and 3.4, we get

$$\begin{aligned} |\text{Cl}_{L/k}[\ell]| &= \prod_i |\text{Cl}_{K_i/k}[\ell]| = O_{\epsilon, k} \left( \text{Disc}(K_1/k)^{1/2-\Delta(\ell, p)+\epsilon} \right) \prod_{i \neq 1} \text{Disc}(K_i/k)^{1/2+\epsilon} \\ &= O_{\epsilon, k} \left( \frac{\text{Disc}(L/k)^{1/2+\epsilon}}{\text{Disc}(K_1/k)^{\Delta(\ell, p)}} \right) = O_{\epsilon, k}(\text{Disc}(L/k)^{1/2-\Delta(\ell, p)/p(\eta+1)+\epsilon}). \end{aligned} \quad (6.5)$$

Since we assume  $L/k$  sufficiently large for later discussion, i.e.,  $\text{Disc}(L/k) \geq L_0(\epsilon, \epsilon_0)$ , in summary, we show that for any  $A$ -extension  $L/k$

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon, k, \epsilon_0}(\text{Disc}(L/k)^{1/2-\delta+\epsilon}),$$

with  $\delta = \delta_c(\eta, \ell, p) = \frac{\Delta(\ell, p)}{p(\eta+1)}$ . □

This gives a power saving on the pointwise bound of  $\text{Cl}_{L/k}[\ell]$  in terms of  $\eta(L/k)$ .

**Remark 6.2.** Notice that here in Theorem 6.1 we only take the bound  $\eta_0(\ell, p)_k \cdot (1 + \epsilon_0)$  for  $\eta$  for simplicity. The same non-trivial saving  $\delta = \delta_c(\eta, \ell, p)$  can be obtained with  $\eta \leq M$  for arbitrary number  $M$ . In this scenario, the implied constant depends on  $M$  instead of  $\epsilon_0$ .

## 6.2 Incomparable Size

In this section, we will give another strategy when  $\eta$  is very large, equivalently when  $K_2$  is much larger than  $K_1$ . We will also see the cut-off  $\eta_0(\ell, p)_k$  from the following theorem. We will first prove the result over  $\mathbb{Q}$  in Theorem 6.3 and then prove the result over a general number field  $k$  in Theorem 6.4.

**Theorem 6.3.** Given  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  with odd  $p$ , an integer  $\ell > 1$  with  $(\ell, p) = 1$ . Denote  $\eta_0 = \eta_0(\ell, p) = ((p-1) \cdot \Delta(\ell, p) \cdot (1-2/p))^{-1}$ . For any  $A$ -extension  $L/\mathbb{Q}$  with  $\eta = \eta(L/\mathbb{Q}) > \eta_0(1 + \epsilon_0)$ , we have the pointwise bound

$$|\text{Cl}_L[\ell]| = O_{\epsilon, \epsilon_0}(\text{Disc}(L)^{1/2-\delta+\epsilon})$$

for some

$$\delta = \delta_{ic}(\eta, \ell, p) = \frac{\Delta(\ell, p)\eta}{p(\eta+1)}$$

where  $\eta = \frac{\ln \text{Disc}(K_2)}{\ln \text{Disc}(K_1)}$ .

*Proof.* By Lemma 3.4, we have  $\text{Disc}(K_2) \geq \text{Disc}(L)^{\eta/p(\eta+1)} \geq \text{Disc}(L)^{\eta_0(1+\epsilon_0)/p(\eta_0(1+\epsilon_0)+1)}$ . Note that for a fixed integer  $L_0 > 0$ , there are only finitely many  $L$  with  $\text{Disc}(L) \leq L_0$ , thus only finitely many  $L$  with  $\text{Disc}(K_2) \leq K_0 = L_0^{\eta_0(1+\epsilon_0)/p(\eta_0(1+\epsilon_0)+1)}$  and  $\eta > \eta_0(1 + \epsilon_0)$ . So we can assume that both  $L$  and  $K_2$  are sufficiently large.

We will show that at least one of  $K_i$  for  $2 \leq i \leq p+1$  is  $\theta_i$ -good for some  $\theta_i > 0$  with respect to  $c$  where  $c$  is a fixed small number satisfying  $c < \frac{(p-2)\epsilon_0}{2+p\epsilon_0}$ . The constant  $c = c(\epsilon_0)$  will be fixed once and for all for the current theorem.

If  $\eta(L/\mathbb{Q}) > \eta_0(1 + \epsilon_0)$ , then we can apply Lemma 4.1 with

$$x = \text{Disc}(K_2)^{\Delta(\ell, p)}, \quad q = \text{Cond}(K_1) \asymp \text{Disc}(K_1)^{1/(p-1)},$$

to count the number of primes in  $\mathbb{Q}$  splitting in  $K_1/\mathbb{Q}$ . By class field theory, this is equivalent to taking  $\frac{\phi(q)}{p}$  residue classes  $a \pmod q$  and then adding up  $\pi(x; q, a)$  over  $a$ . Therefore we have positive density of primes up to  $x$  in  $\mathbb{Q}$  that are inert in  $K_1/\mathbb{Q}$ ,

$$\begin{aligned} \pi(x; K_1/\mathbb{Q}, \hat{e}) &= \pi(x) - \pi(x; K_1/\mathbb{Q}, e) - O_\epsilon(\text{Disc}(L)^\epsilon) \\ &\geq \pi(x) - \frac{2}{1 - 1/\Delta(\ell, p)(p-1)\eta} \cdot \frac{x}{p \ln x} - O_{\epsilon, \epsilon_0}(x^\epsilon), \\ &\geq C \frac{x}{\ln x}. \end{aligned} \tag{6.6}$$

The first inequality comes from Lemma 4.1 and  $\text{Disc}(K_2) \geq \text{Disc}(L)^{\eta_0(1+\epsilon_0)/p(\eta_0(1+\epsilon_0)+1)}$ . The second inequality holds when we take  $C = 1 - \frac{2}{p} \frac{1}{1-1/\Delta(\ell,p)(p-1)\eta_0(1+\epsilon_0)} - \epsilon$  and  $x \geq x_0 = x_0(\epsilon)$  with  $x_0$  depending at most on  $\epsilon$ . Primes that are inert in  $K_1$  must be split in  $K_i$  for some  $i > 1$ . Therefore by pigeon hole principle, there exists at least one  $K_j$  for  $2 \leq j \leq p+1$  satisfying

$$\pi(x; K_j, e) \geq \frac{C}{p} \cdot \frac{x}{\ln x} \geq c \frac{x}{\ln x}, \quad (6.7)$$

where the last inequality comes from the assumption  $c < \frac{(p-2)\epsilon_0}{2+\epsilon_0}$ . This  $K_j$  is  $\theta_j$ -good for

$$\theta_j := \Delta(\ell, p) \cdot \frac{\ln \text{Disc}(K_2)}{\ln \text{Disc}(K_j)} \leq \Delta(\ell, p). \quad (6.8)$$

Then by Lemma 5.5, we get

$$|\text{Cl}_{K_j}[\ell]| = O_{\epsilon,c}(\text{Disc}(K_j)^{1/2-\theta_j+\epsilon}) = O_{\epsilon,\epsilon_0}(\text{Disc}(K_j)^{1/2-\theta_j+\epsilon}),$$

since our constant  $c$  is a small number depending at most on  $\epsilon_0$ . By Lemma 3.3 and 3.1 and 3.4, we have for every  $L$  that

$$|\text{Cl}_L[\ell]| = O_{\epsilon,\epsilon_0}(\text{Disc}(L)^{1/2-\Delta(\ell,p)\eta/p(\eta+1)+\epsilon}). \quad (6.9)$$

So we prove this theorem with

$$\delta_{ic}(\eta, \ell, p) = \frac{\Delta(\ell, p)\eta}{p(\eta+1)}.$$

□

Then we give the version over a general number field. The only distinction is that we will apply Lemma 4.3 instead of Lemma 4.1.

**Theorem 6.4.** *Given  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ , an integer  $\ell > 1$  with  $(\ell, p) = 1$ . Denote  $\eta_0 = \eta_0(\ell, p)_k = \max\{\beta, \gamma + \Delta(\ell, p)\}/\Delta(\ell, p)$  where  $\beta = \beta(k, \mathbb{Z}/p\mathbb{Z})$  and  $\gamma = \gamma(k, \mathbb{Z}/p\mathbb{Z})$ . For any  $A$ -extension  $L/k$  with  $\eta(L/k) > \eta_0$ , we have the pointwise bound*

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon,k}(\text{Disc}(L/k)^{1/2-\delta+\epsilon}),$$

where

$$\delta = \delta_{ic,k}(\eta, \ell, p) = \frac{(\Delta(\ell, p) - \gamma/\eta)\eta}{p(\eta+1)}.$$

*Proof.* Notice that by Lemma 3.4, we have

$$\text{Disc}(K_2/k) \geq \text{Disc}(L/k)^{\eta/p(\eta+1)} \geq \text{Disc}(L/k)^{\eta_0/p(\eta_0+1)}.$$

Note that for a fixed integer  $L_0 > 0$ , there are only finitely many  $L/k$  with  $\text{Disc}(L/k) \leq L_0$ , thus only finitely many  $L/k$  with  $\text{Disc}(K_2/k) \leq K_0 = L_0^{\eta_0/p(\eta_0+1)}$  and  $\eta > \eta_0$ . So we can assume that both  $K_2/k$  and  $L/k$  are sufficient large.

Firstly, we will show that there exist a lot of primes inert in  $K_1/k$  with the range of consideration  $x = \text{Disc}(K_2/k)^{\Delta(\ell,p)}$  when  $L/k$  is sufficiently large. We will apply Lemma 4.3 to  $K_1/k$  with  $x = \text{Disc}(K_2/k)^{\Delta(\ell,p)}$ . Recall the absolute constant  $D_0 = D_0(k)$  depending at most on  $k$  in Lemma 4.3.

If  $\text{Disc}(K_1/k) < D_0$ , then it follows from the standard Chebotarev density theorem that for  $C' = \frac{p-1}{p} - \epsilon$ , we have

$$\pi(x; K_1/k, \hat{e}) \geq C' \frac{x}{\ln x} = \frac{C'}{\Delta(\ell, p)} \cdot \frac{\text{Disc}(K_2/k)^{\Delta(\ell, p)}}{\ln \text{Disc}(K_2/k)},$$

when  $x$  is sufficiently large comparing to  $D_0$ , say  $x \geq x_0 = x_0(D_0, \epsilon) = x_0(k, \epsilon)$  where  $x_0$  depends at most on  $D_0$  and  $\epsilon$ , thus depends at most on  $k$  and  $\epsilon$ . If we take  $K_0^{\Delta(\ell, p)} = x_0(k, \epsilon)$ , then when  $\text{Disc}(L/k) \geq L_0(k, \epsilon) = K_0(k, \epsilon)^{p(\eta_0+1)/\eta_0}$  is sufficiently large, we know that if  $\text{Disc}(K_1/k) < D_0$  then  $\pi(x; K_1/k, \hat{e}) \geq \frac{C'}{\Delta(\ell, p)} \cdot \frac{\text{Disc}(K_2/k)^{\Delta(\ell, p)}}{\ln \text{Disc}(K_2/k)}$ .

If  $\text{Disc}(K_1/k) \geq D_0(k)$ , then we apply Lemma 4.3. When  $\eta > \eta_0$ , we have  $\text{Disc}(K_2/k)^{\Delta(\ell, p)} \geq \max\{\text{Disc}(K_1/k)^\beta, \text{Disc}(K_1/k)^\gamma\}$  for  $\beta = \beta(k, \mathbb{Z}/p\mathbb{Z})$  and  $\gamma = \gamma(k, \mathbb{Z}/p\mathbb{Z})$  in Lemma 4.3. By Lemma 4.3 there exists some  $C_k > 0$  such that

$$\pi(x; K_1/k, \hat{e}) \geq C_k \frac{1}{\text{Disc}(K_1/k)^\gamma} \cdot \frac{x}{\ln x} \geq \frac{C_k}{\Delta(\ell, p)} \cdot \frac{\text{Disc}(K_2/k)^{\Delta(\ell, p) - \gamma/\eta}}{\ln \text{Disc}(K_2/k)}, \quad (6.10)$$

where  $C_k$  is some constant only depending on  $k$ . So in summary, as  $L/k$  is sufficiently large (i.e.,  $\text{Disc}(L/k) \geq L_0(k, \epsilon) = K_0(k, \epsilon)^{p(\eta_0+1)/\eta_0}$ ), we show

$$\pi(x; K_1/k, \hat{e}) \geq \frac{C_k''}{\Delta(\ell, p)} \cdot \frac{\text{Disc}(K_2/k)^{\Delta(\ell, p) - \gamma/\eta}}{\ln \text{Disc}(K_2/k)},$$

where  $C_k'' = \min\{C', C_k'\}$  depends only on  $k$ .

By pigeon hole principle, there exists at least one  $K_j/k$  for  $2 \leq j \leq p+1$  where

$$\pi(x; K_j/k, e) \geq \frac{C_k''}{p\Delta(\ell, p)} \cdot \frac{\text{Disc}(K_2/k)^{\Delta(\ell, p) - \gamma/\eta}}{\ln \text{Disc}(K_2/k)}. \quad (6.11)$$

Finally by Lemma 5.5 and Lemma 3.4, we have for any  $L/k$  that

$$|\text{Cl}_{L/k}[\ell]| \leq O_{\epsilon, k}(\text{Disc}(L/k)^{1/2 - \delta + \epsilon}), \quad (6.12)$$

where

$$\delta = \delta_{ic, k}(\eta, \ell, p) = \frac{(\Delta(\ell, p) - \gamma/\eta)\eta}{p(\eta + 1)}.$$

□

**Remark 6.5.** Here when  $k = \mathbb{Q}$  and  $p = 2$ , we can apply Lemma 4.2 as a sub-case of Lemma 4.3 with  $\gamma(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 1/2 - \epsilon$ ,  $\beta(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 8$  and  $D_0 = q_2$ .

### 6.3 Savings for Odd $A$ with Rank 2

So combining Theorem 6.1 and 6.3 and (5.4) in Remark 5.3, we get the following theorem.

**Theorem 6.6** (Odd Exponent, Rank 2, Over  $\mathbb{Q}$ ). *Given  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  with odd  $p$  and an integer  $\ell > 1$  with  $(\ell, p) = 1$ . For any  $A$ -extension  $L/\mathbb{Q}$ , we have*

$$|\text{Cl}_L[\ell]| = O_\epsilon(\text{Disc}(L)^{1/2 - \delta(\ell, p) + \epsilon}),$$

with

$$\delta(\ell, p) = \delta_c(\eta_0, \ell, p) = \frac{\Delta(\ell, p)}{p(1 + \eta_0)},$$

where  $\eta_0 = \frac{1}{(p-1)\Delta(\ell, p)(1-2/p)}$ .

*Proof.* Combining Theorem 6.1 and Theorem 6.3, for every fixed small  $\epsilon_0$ , we show that for every  $A$ -extension  $L/\mathbb{Q}$

$$|\mathrm{Cl}_L[\ell]| = O_\epsilon(\mathrm{Disc}(L)^{1/2-\delta(\ell,p,\epsilon_0)+\epsilon}),$$

where  $\delta(\ell,p,\epsilon_0) = \delta_c(\eta_0(1+\epsilon_0), \ell, p) = \frac{\Delta(\ell,p)}{p(1+\eta_0(1+\epsilon_0))}$ . Since we can take arbitrarily small  $\epsilon_0$  and we also state the theorem with arbitrarily small  $\epsilon$ , we can get

$$|\mathrm{Cl}_L[\ell]| = O_\epsilon(\mathrm{Disc}(L)^{1/2-\delta(\ell,p)+\epsilon}),$$

for  $\delta(\ell,p) = \delta_c(\eta_0, \ell, p)$ . □

For general number field  $k$ , similarly notice that since  $\delta_{ic,k}(\eta, \ell, p)$  always increases as  $\eta$  increases and  $\delta_c(\eta, \ell, p)$  always decreases as  $\eta$  increases. By comparing  $\delta_c(\eta_0, \ell, p)$  and  $\delta_{ic,k}(\eta_0, \ell, p)$  at  $\eta_0 = \eta_0(\ell, p)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, p)\}/\Delta(\ell, p)$ , we see that the smallest saving always happens at  $\delta_c(\eta_0, \ell, p)_k$ . So we are guaranteed to find the universal saving  $\delta > 0$  for all ranges of  $\eta$  at the cut-off  $\eta_0$ .

**Remark 6.7.** *In the proof of Theorem 6.4, we can see that it suffices to take  $\eta_0(\ell, p)_k$  to be  $\max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z})\}/\Delta(\ell, p)$ . The reason that instead we take*

$$\eta_0(\ell, p)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, p)\}/\Delta(\ell, p),$$

*is that it guarantees  $\delta_{ic,k}(\eta_0, \ell, p) > \delta_c(\eta_0, \ell, p)$  and simplifies the final expression of the saving. However, notice that usually  $\beta$  is larger than  $\gamma$  in reality, see [Zam17] for example, so in such situations it will not change the actual value of  $\eta_0(\ell, p)_k$  after plugging in  $\beta$  and  $\gamma$ .*

**Theorem 6.8** (Odd Exponent, Rank 2, Over  $k$ ). *Given  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  with odd  $p$  and an integer  $\ell > 1$  with  $(\ell, p) = 1$ . For any  $A$ -extension  $L/k$ , we have*

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon,k}(\mathrm{Disc}(L)^{1/2-\delta_k(\ell,p)+\epsilon}),$$

where  $\delta_k(\ell, p) = \delta_c(\eta_0, \ell, p) = \frac{\Delta(\ell,p)}{p(1+\eta_0)}$  and  $\eta_0 = \eta_0(\ell, p)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, p)\}/\Delta(\ell, p)$ .

## 6.4 Induction

In this section, we will derive the  $\ell$ -torsion bound for every  $A = (\mathbb{Z}/p\mathbb{Z})^r$  when  $r > 2$  from the case  $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

**Theorem 6.9** (Odd Exponent, Over  $k$ ). *Given  $A = (\mathbb{Z}/p\mathbb{Z})^r$  with  $r \geq 2$  and  $p$  odd. Given an arbitrary integer  $\ell = \ell_{(p)} \cdot \ell_p$  where  $\ell_{(p)}$  is the maximal factor of  $\ell$  relatively prime to  $p$ . For any  $A$ -extension  $L/k$ , we have*

$$|\mathrm{Cl}_L[\ell]| = O_{k,\epsilon}(\mathrm{Disc}(L)^{1/2-\delta_k(\ell_{(p)},p)+\epsilon}),$$

where  $\delta_{\mathbb{Q}}(\ell, p) = \delta(\ell, p)$  in Theorem 6.6 when  $k = \mathbb{Q}$ , and  $\delta_k(\ell, p)$  in Theorem 6.8 for general  $k$ .

*Proof.* Firstly we assume  $(\ell, p) = 1$ . The result for  $r = 2$  and  $(\ell, p)$  is stated in Theorem 6.6 and 6.8. For  $r > 2$  and  $(\ell, p) = 1$ , notice that

$$\begin{aligned} |\mathrm{Cl}_{L/k}[\ell]| &= \prod_i |\mathrm{Cl}_{K_i/k}[\ell]| = \left( \prod_j |\mathrm{Cl}_{M_j/k}[\ell]| \right)^{1/(p+1)} = O_{\epsilon,k} \left( \prod_j \mathrm{Disc}(M_j/k)^{1/2-\delta(\ell,p)+\epsilon} \right)^{1/(p+1)} \\ &= O_{\epsilon,k} \left( \prod_j \mathrm{Disc}(M_j/k)^{1/(p+1)} \right)^{1/2-\delta(\ell,p)+\epsilon} = O_{\epsilon,k}(\mathrm{Disc}(L/k)^{1/2-\delta(\ell,p)+\epsilon}). \end{aligned} \tag{6.13}$$

where  $M_j$  ranges over all degree  $p^2$  sub-extensions in  $L$  over  $\mathbb{Q}$ . The first equality comes from Lemma 3.1. The second equality comes from Corollary 3.2. The first inequality comes from Theorem 6.6. The last equality comes from (3.1). Finally it follows from (5.4) in Remark 5.3.

For general  $\ell = \ell_{(p)}\ell_p$ , notice that  $|\text{Cl}_L[\ell]| = |\text{Cl}_L[\ell_{(p)}]| \cdot |\text{Cl}_L[\ell_p]|$  and  $|\text{Cl}_L[\ell_p]| = O_\epsilon(\text{Disc}(L)^\epsilon)$ , we get  $|\text{Cl}_L[\ell]| = O_{k,\epsilon}(\text{Disc}(L)^{1/2-\delta_k(\ell_{(p)},p)+\epsilon})$ .  $\square$

**Remark 6.10** (Odd Exponent,  $\ell = 2$ , Over  $k$ ). *When  $\ell = 2$ , we can obtain better results because of the pointwise result on 2-torsion from [BST<sup>+</sup>17]. It is proved that  $|\text{Cl}_F[2]| \leq O(\text{Disc}(F)^{1/2-1/2d+\epsilon})$  where  $d = [F : \mathbb{Q}]$  by [BST<sup>+</sup>17]. By (5.4) in Remark 5.3, we get for  $K$  with  $\text{Gal}(K/k) = \mathbb{Z}/p\mathbb{Z}$ , the 2-torsion is bounded*

$$|\text{Cl}_{K/k}[2]| = O_{\epsilon,k}(\text{Disc}(L/k)^{1/2-1/2p+\epsilon}).$$

Then the statement follows from a straight forward use of Lemma 3.1.

## 7 Even $p$

In this section, we will discuss the cases when  $A$  is an elementary abelian group with even exponent, i.e., when  $A = (\mathbb{Z}/2\mathbb{Z})^r$  and  $r > 1$ . In section 7.1, we first give the result for  $r = 2$ . Then in order to get a better saving than that obtained in section 7.1, we focus on  $r = 3$  in section 7.2, 7.3 and 7.4, and use an induction to get an overall better saving for  $r > 3$  in section 7.5.

The main reason that we separate the discussion for  $p$  being odd and even is that in Theorem 6.3 we ask the constant  $c$  to be smaller than  $\frac{(p-2)\epsilon_0}{2+\epsilon_0}$ , which is only positive when  $p$  is odd. So when  $p = 2$ , we need to replace Theorem 6.3, and, more importantly, consequences of Theorem 6.3. The strategy for doing this is treat  $r = 3$  as the initial case for  $p = 2$ , i.e., we replace Theorem 6.3 with Theorem 7.3 in this section.

### 7.1 Even Exponent with Rank 2

In this section, we work with  $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . We will follow the notation introduced at the beginning of section 6. Recall that we have  $K_i$  for  $i = 1, 2, 3$  where  $\text{Disc}(K_1/k) \leq \text{Disc}(K_2/k) \leq \text{Disc}(K_3/k)$ , and  $\eta(L/k) := \frac{\ln \text{Disc}(K_2/k)}{\ln \text{Disc}(K_1/k)}$ . Again we split the discussion to  $\eta$  being small (the comparable case) and  $\eta$  being big (the incomparable case). We take

$$\eta_0 = \eta_0(\ell, 2)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, 2)\} / \Delta(\ell, 2)$$

in this section.

For the comparable case, we recall Theorem 6.1 (which is stated for all  $A$ , not just odd  $A$ ), which states that

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon,k,\epsilon_0}(\text{Disc}(L/k)^{1/2-\delta+\epsilon}),$$

where  $\delta = \delta_c(\eta, \ell, 2) = \frac{\Delta(\ell, 2)}{2(\eta+1)}$  and  $\eta = \eta(L/k) = \frac{\ln \text{Disc}(K_2/k)}{\ln \text{Disc}(K_1/k)} \leq \eta_0(\ell, 2)_k(1 + \epsilon_0)$ .

For the incomparable case, we recall Theorem 6.4 (which is stated for all  $A$ , not just odd  $A$ ), which states that

$$|\text{Cl}_{L/k}[\ell]| = O_{\epsilon,k}(\text{Disc}(L/k)^{1/2-\delta+\epsilon}),$$

where  $\delta = \delta_{ic,k}(\eta, \ell, 2) = \frac{(\Delta(\ell, 2) - 1/\eta)\eta}{2(\eta+1)}$  when  $\eta > \eta_0(\ell, 2)_k$ . Combining the two cases, we get the following theorem.

**Theorem 7.1** (Even Exponent, Rank 2, Over  $k$ ). *Given  $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and  $\ell > 1$  an odd integer. For any  $A$ -extension  $L/k$ , we have*

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon, k}(\mathrm{Disc}(L)^{1/2 - \delta_k(\ell, 2) + \epsilon}),$$

with

$$\delta_k(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)},$$

where  $\eta_0 = \max\{\beta(k, \mathbb{Z}/2\mathbb{Z}), \gamma(k, \mathbb{Z}/2\mathbb{Z}) + \Delta(\ell, 2)\}/\Delta(\ell, 2)$ . In particular, when  $k = \mathbb{Q}$ , we have

$$\delta_{\mathbb{Q}}(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)} = \frac{1}{64\ell^2 + 4\ell}.$$

*Proof.* If  $k = \mathbb{Q}$ , by Lemma 4.2, we can take  $\beta(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 8$  and  $\gamma(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 1/2 - \epsilon$ . Then  $\eta_0(\ell, 2)_{\mathbb{Q}} = \frac{8}{\Delta(\ell, 2)}$ . By comparing  $\frac{\Delta(\ell, 2)}{p(\eta_0 + 1)}$  and  $\frac{(\Delta(\ell, 2) - \gamma(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})/\eta_0)\eta_0}{p(\eta_0 + 1)}$ , we see that a universal saving is

$$\delta_{\mathbb{Q}}(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)} = \frac{1}{64\ell^2 + 4\ell}.$$

Similarly, we have

$$\delta_k(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)},$$

where  $\eta_0 = \max\{\beta(k, \mathbb{Z}/2\mathbb{Z}), \gamma(k, \mathbb{Z}/2\mathbb{Z}) + \Delta(\ell, 2)\}/\Delta(\ell, 2)$ . □

## 7.2 Comparable Size for Rank 3

In this section, we work with  $A = (\mathbb{Z}/2\mathbb{Z})^r$  with  $r > 2$ . In section 7.2, 7.3 and 7.4, we focus on the case  $r = 3$  over  $\mathbb{Q}$ . In section 7.5, we apply the result we obtained for  $r = 3$  to obtain results for  $r > 3$ . The main reason that we can get a better saving here for  $r = 3$  over  $\mathbb{Q}$  than  $r = 2$  is that we can apply the Lemma 4.1 for the incomparable case of  $A = (\mathbb{Z}/2\mathbb{Z})^3$  instead of Lemma 4.2.

We introduce the notation for the current section and section 7.3. For  $A = (\mathbb{Z}/2\mathbb{Z})^3$ , there are 7 index-2 subgroups and 7 index-4 subgroups. For an  $A$ -extension  $L/\mathbb{Q}$ , we denote  $M_1$  to be the quartic subfield with smallest discriminant, and  $K_m$  to be the smallest quadratic field outside  $M_1$ . Denote  $K_i$  for  $i = 1, 2, 3$  to be subfields of  $M_1$  ordered by  $\mathrm{Disc}(K_i)$ . Denote  $K'_i$  to be the other quadratic subfield of the compositum  $K_m K_i$ . So we always have  $\mathrm{Disc}(K'_i) \geq \mathrm{Disc}(K_m)$ . In this section and section 7.3 and 7.4, we will denote

$$\eta = \eta(L/k) := \frac{\ln \mathrm{Disc}(K_m)}{\ln \mathrm{Disc}(M_1)}, \quad \eta_0 = \frac{1}{\Delta(\ell, 2)}. \quad (7.1)$$

See Theorem 7.3 for the reason on the choice of  $\eta_0$ . We will use  $\delta'_c(\eta, \ell)$  and  $\delta'_{ic}(\eta, \ell)$  to denote the savings in section 7.2 and 7.3 to distinguish from  $\delta_c(\eta, \ell, 2)$  and  $\delta_{ic}(\eta, \ell, 2)$  used in section 7.1.

**Theorem 7.2.** *Given  $A = (\mathbb{Z}/2\mathbb{Z})^3$  and an odd integer  $\ell > 1$ . For any  $A$ -extension  $L/\mathbb{Q}$  with  $\eta(L/\mathbb{Q}) \leq \eta_0(1 + \epsilon_0) = \frac{1 + \epsilon_0}{\Delta(\ell, 2)}$ , we have*

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon, \epsilon_0}(\mathrm{Disc}(L)^{1/2 - \delta + \epsilon}),$$

for

$$\delta = \delta'_c(\eta, \ell) = \frac{\Delta(\ell, 4)}{4\eta + 2} > 0,$$

where  $\eta = \frac{\ln \mathrm{Disc}(K_m)}{\ln \mathrm{Disc}(M_1)}$ .

*Proof.* The proof is similar with that of Theorem 6.1. We separate the discussion for  $M_1$  being  $\Delta(\ell, 4)$ -bad or not with respect to  $c$  where  $c$  is a fixed small number satisfying  $c < 1/7$ . We fix  $c$  once and for all for the current theorem. By Lemma 3.5, we have  $\text{Disc}(M_1) \geq \text{Disc}(L)^{1/(4\eta+2)} \geq \text{Disc}(L)^{1/(4\eta_0(1+\epsilon_0)+2)}$ . Note that for a fixed  $L_0 > 0$ , there are only finitely many  $L/Q$  with  $\text{Disc}(L) \geq L_0$ , thus only finitely many  $\text{Disc}(M_1) \geq M_0 = L_0^{1/(4\eta_0(1+\epsilon_0)+2)}$  with  $\eta(L/Q) \leq \eta_0(1+\epsilon_0)$ . So we can assume both  $M_1$  and  $L$  are sufficiently large.

If  $M_1$  is  $\Delta(\ell, 4)$ -good, then by Lemme 3.1 and Lemma 3.5, we have

$$|\text{Cl}_L[\ell]| = |\text{Cl}_{M_1}[\ell]| \prod_{K_i \not\subset M_1} |\text{Cl}_{K_i}[\ell]| = O_\epsilon(\text{Disc}(L)^{1/2 - \Delta(\ell, 4)/(4\eta+2) + \epsilon}). \quad (7.2)$$

If  $M_1$  is  $\Delta(\ell, 4)$ -bad, then we have for  $x = \text{Disc}(M_1)^{\Delta(\ell, 4)}$  that

$$\pi(x; M_1, \hat{e}) \geq (1 - c - \epsilon) \cdot \frac{x}{\ln x},$$

when  $x \geq x_0(\epsilon, \epsilon_0)$  is sufficiently large with  $x_0$  depending at most on  $\epsilon$  and  $\epsilon_0$ . These primes are inert in  $M_1/k$ , so will always split at exactly 2 of  $\{K_m, K'_1, K'_2, K'_3\}$  not contained in  $M_1$ . Denote

$$\theta_i = \frac{\Delta(\ell, 4) \ln \text{Disc}(M_1)}{\ln \text{Disc}(K'_i)}, \quad i = 1, 2, 3, \quad \theta_m = \frac{\Delta(\ell, 4) \ln \text{Disc}(M_1)}{\ln \text{Disc}(K_m)},$$

for  $K'_i$  ( $i = 1, 2, 3$ ) and  $K_m$  respectively. By pigeon hole principle, we get at least  $\frac{1-c}{\binom{4}{2}} \frac{x}{\ln x}$  many primes that are all split in two of  $S$ . Since  $c < 1/7$ , we get at least two of  $K_i$  of  $S$  that are  $\theta_i$ -good. Denote them by  $K_j$  for  $j \in J$ . Therefore when  $\text{Disc}(L/k) \geq L_0(\epsilon, \epsilon_0) = x_0(\epsilon, \epsilon_0)^{(4\eta_0(1+\epsilon_0)+2)/\Delta(\ell, 2)}$ , we always get for two  $K_j$  that

$$|\text{Cl}_{K_j}[\ell]| = O_\epsilon(\text{Disc}(K_j)^{1/2 - \theta_j + \epsilon}),$$

and it follows that for every  $L$  we get

$$|\text{Cl}_L[\ell]| = \prod_{i \notin J} |\text{Cl}_{K_i}[\ell]| \prod_{j \in J} |\text{Cl}_{K_j}[\ell]| = O_{\epsilon, \epsilon_0}(\text{Disc}(L)^{1/2 - 2\Delta(\ell, 4)/(4\eta+2) + \epsilon}), \quad (7.3)$$

where the last inequality follows from Lemma 3.5. Therefore we can always get a saving with

$$\delta'_c(\eta, \ell) = \frac{\Delta(\ell, 4)}{4\eta + 2}.$$

□

### 7.3 Incomparable Size for Rank 3

In this section, we will treat the case when  $A = (\mathbb{Z}/2\mathbb{Z})^3$  and the base field is  $\mathbb{Q}$ , and  $\eta(L/\mathbb{Q})$  is large.

**Theorem 7.3.** *Given  $A = (\mathbb{Z}/2\mathbb{Z})^3$  and an odd integer  $\ell > 1$ . For any  $A$ -extension  $L/k$ , if  $\eta > \eta_0(1 + \epsilon_0) = \frac{1+\epsilon_0}{\Delta(\ell, 2)}$ , then*

$$|\text{Cl}_L[\ell]| = O_{\epsilon, \epsilon_0}(\text{Disc}(L)^{1/2 - \delta + \epsilon}),$$

for

$$\delta = \delta'_{ic}(\eta, \ell) = \frac{\Delta(\ell, 2)\eta}{2\eta + 1} > 0.$$

*Proof.* Similarly with the proof of Theorem 6.3, by Lemma 3.5, we can assume both  $L$  and  $K_m$  are sufficiently large.

We will show that at least 2 of quadratic fields  $K_i$  in  $\{K_m, K'_1, K'_2, K'_3\}$  are  $\theta_i$  good for

$$\theta_i = \frac{\Delta(\ell, 2) \ln \text{Disc}(K_m)}{\ln \text{Disc}(K'_i)}, \quad i = 1, 2, 3, \quad \theta_m = \Delta(\ell, 2),$$

with respect to  $c$  where  $c$  is a small number satisfying  $c < \frac{\epsilon_0}{6(1+2\epsilon_0)}$ . We will fix  $c = c(\epsilon_0)$  once and for all for the current theorem.

We apply Lemma 4.1 with

$$x = \text{Disc}(K_m)^{\Delta(\ell, 2)}, \quad q = \text{Cond}(M_1) \asymp \text{Disc}(M_1)^{1/2},$$

to count the number of primes in  $\mathbb{Q}$  that split in  $M_1/\mathbb{Q}$ . By class field theory, this is equivalent to take  $\frac{\phi(q)}{p}$  residue classes  $a \pmod{q}$  and then add up over  $a$ , and we get

$$\pi(x; M_1/\mathbb{Q}, e) \leq \frac{2}{1 - \ln q / \ln x} \cdot \frac{x}{4 \ln x} = \frac{2}{1 - 1/2\Delta(\ell, 2)\eta} \cdot \frac{x}{4 \ln x}.$$

So we get a positive density  $C$  of primes that are inert in  $M_1/\mathbb{Q}$

$$\pi(x; M_1/\mathbb{Q}, \hat{e}) \geq \left(1 - \frac{1}{2 - 1/\Delta(\ell, 2)\eta} - \epsilon\right) \frac{x}{\ln x} = C \frac{x}{\ln x}, \quad (7.4)$$

when  $x \geq x_0(\epsilon, \epsilon_0)$  is sufficiently large. Primes that are inertia in  $M_1$  must be split in exactly two of  $K_j$  in  $\{K_m, K'_1, K'_2, K'_3\}$ . Therefore by pigeon hole principle, there exist at least two such  $K_j$  satisfy

$$\pi(x; K_j, e) \geq \frac{C}{\binom{4}{2}} \cdot \frac{x}{\ln x} \geq c \frac{x}{\ln x}, \quad (7.5)$$

which implies that  $K_j$  is  $\theta_j$ -good. The second inequality comes from  $\eta > \eta_0(1 + \epsilon_0)$  and the assumption on  $c$ . Then by Lemma 5.5, we get

$$|\text{Cl}_{K_j}[\ell]| = O_{\epsilon, \epsilon_0}(\text{Disc}(K_j)^{1/2 - \theta_j + \epsilon}).$$

By Lemma 3.3 and 3.1 and Lemma 3.5, we have for every  $L$  that

$$|\text{Cl}_L[\ell]| \leq O_{\epsilon, \epsilon_0}(\text{Disc}(L)^{1/2 - 2\Delta(\ell, 2)\eta/(4\eta + 2) + \epsilon}). \quad (7.6)$$

So we prove this theorem with

$$\delta'_{ic}(\eta, \ell) = \frac{\Delta(\ell, 2)\eta}{(2\eta + 1)}.$$

□

## 7.4 Savings for Even $A$ with Rank 3

Finally combining Theorem 7.2 and 7.3, we get the following theorem.

**Theorem 7.4.** *Given  $A = (\mathbb{Z}/2\mathbb{Z})^3$  and an odd prime integer  $\ell$ . For any  $A$ -extension  $L/\mathbb{Q}$ , we have*

$$|\text{Cl}_L[\ell]| = O_\epsilon(\text{Disc}(L)^{1/2 - \delta + \epsilon})$$

for some

$$\delta = \delta'_c(\eta_0, \ell) = \frac{\Delta(\ell, 4)}{4\eta_0 + 2},$$

where  $\eta_0 = \frac{1}{\Delta(\ell, 2)}$ .

*Proof.* Similarly with Theorem 6.6 we can take  $\epsilon_0$  arbitrarily small. Notice that  $\delta'_c(\eta, \ell)$  decreases as  $\eta$  increases and  $\delta'_{ic}(\eta, \ell)$  increases as  $\eta$  increases. We compare

$$\delta'_c(\eta_0, \ell) = \frac{1}{48\ell^2 + 12\ell}, \quad \delta'_{ic}(\eta_0, \ell) = \frac{1}{4\ell + 1}.$$

So the worst point in all range of  $\eta$  is the exactly at  $\eta = \eta_0$ . We can pick  $\delta = \frac{\Delta(\ell, 4)}{4\eta_0 + 2} = \frac{1}{48\ell^2 + 12\ell}$ .  $\square$

**Remark 7.5.** Comparing the saving we get in Theorem 7.1 and 7.4, here we get an improvement over  $\mathbb{Q}$ , i.e.,

$$\frac{1}{48\ell^2 + 12\ell} > \frac{1}{64\ell^2 + 4\ell}$$

for arbitrary  $\ell > 1$ .

## 7.5 Induction

In this section, we will derive  $\ell$ -torsion bound for every  $A = (\mathbb{Z}/2\mathbb{Z})^r$  with  $r > 2$ . Following the Remark 7.5, we will use Theorem 7.4 to prove a point-wise saving for elementary 2-abelian group with rank greater than 3.

**Theorem 7.6** (Even Exponent, Over  $\mathbb{Q}$ ). *Given  $A = (\mathbb{Z}/2\mathbb{Z})^r$  with  $r > 2$  and an arbitrary integer  $\ell = \ell_{(2)}\ell_2 > 1$ . For any  $A$ -extension  $L/\mathbb{Q}$ , we have the pointwise bound*

$$|\text{Cl}_L[\ell]| = O_\epsilon(\text{Disc}(L/k)^{1/2 - \delta(\ell_{(2)}) + \epsilon}),$$

for  $\delta(\ell) = \frac{1}{48\ell^2 + 12\ell}$ .

*Proof.* By a similar proof of Theorem 6.9,

$$|\text{Cl}_L[\ell]| = \prod_s |\text{Cl}_{F_s}[\ell]|^{1/7} = O_\epsilon\left(\prod_s \text{Disc}(F_s)^{1/2 - \delta + \epsilon}\right)^{1/7} = O_\epsilon(\text{Disc}(L)^{1/2 - \delta + \epsilon}). \quad (7.7)$$

where  $F_s$  ranges over all degree 8 subfields of  $L$ . It follows directly from Corollary 3.2 and (3.1). Similarly with Theorem 6.9, we derive the results for general  $\ell$  by  $|\text{Cl}_L[\ell]| = |\text{Cl}_L[\ell_{(2)}]| \cdot |\text{Cl}_L[\ell_2]|$ .  $\square$

**Remark 7.7** (Even Exponent,  $\ell = 3$ , Over  $\mathbb{Q}$ ). *When  $\ell = 3$ , we can do induction over an even better result from [EV07] that  $|\text{Cl}_F[3]| = O(\text{Disc}(F)^{1/3 + \epsilon})$  for any quadratic extension  $F/\mathbb{Q}$ . From a direct use of Corollary 3.2 and (3.1), we can take  $\delta(3) = 1/3$ .*

When  $k \neq \mathbb{Q}$ , we use the induction from  $r = 2$ . It follows from a similar proof with Theorem 6.9 directly:

**Theorem 7.8** (Even Exponent, Over  $k$ ). *Given  $A = (\mathbb{Z}/2\mathbb{Z})^r$  with  $r \geq 2$  and an integer  $\ell > 1$ . For any  $A$ -extension  $L/k$ , we have the pointwise bound*

$$|\text{Cl}_L[\ell]| = O_{\epsilon, k}(\text{Disc}(L/k)^{1/2 - \delta_k(\ell_{(2)}) + \epsilon}),$$

for  $\delta_k(\ell) = \delta_k(\ell, 2)$  in Theorem 7.1.

## 8 Acknowledgement

The author is supported by Foerster-Bernstein Fellowship at Duke University. I would like to thank Jürgen Klüners, Weitong Wang and Asif Zaman for providing helpful references. I would like to thank Dimitris Koukoulopoulos, Robert J. Lemke Oliver, Melanie Matchett Wood, Asif Zaman and Ruixiang Zhang for helpful conversations. I would like to thank Jordan Ellenberg, Melanie Matchett Wood and Yongqiang Zhao for suggestions on an earlier draft.

## References

- [Alb20] B. Alberts. The weak form of Malle’s conjecture and solvable groups. *Research in Number Theory*, 6(10), 2020.
- [An18] C. An.  $\ell$ -torsion in class group of certain  $D_4$ -quartic fields. *arXiv:1808.02148v1*, 2018.
- [BK77] A. Brumer and K. Kramer. The rank of elliptic curves. *Duke Math. J.*, 1977.
- [BS96] A. Brumer and J. Silverman. The number of elliptic curves over  $\mathbb{Q}$  with conductor  $n$ . *Manuscripta Mathematica*, 1996.
- [BST<sup>+</sup>17] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *arXiv: 1701. 02458*, 2017.
- [CM87] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Mathematics of Computation*, 48(177):123–137, 1987.
- [Cor83] Gary Cornell. Relative genus theory and the class group of  $l$ -extensions. *Trans. Amer. Math. Soc.*, 277(1):421–429, 1983.
- [Deb17] K. Debaene. Explicit counting of ideals and a Brun-Titchmarsh inequality for the Chebotarev Density Theorem. *arXiv: 1611.10103*, 2017.
- [Duk98] W. Duke. Bounds for arithmetic multiplicities. *Proc. Intern. Congr. Math.*, II:163–172, 1998.
- [EPW] J. Ellenberg, L. B. Pierce, and M. M. Wood. On  $\ell$ -torsion in class groups of number fields. *arXiv: 1606.06103*.
- [EV07] J. S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. *Internat. Math. Res. Notices*, 2007.
- [FW18a] Christopher Frei and Martin Widmer. Average bounds for the  $\ell$ -torsion in class groups of cyclic extensions. *Res. Number Theory*, 4(3):Art. 34, 25, 2018.
- [FW18b] Christopher Frei and Martin Widmer. Averages and higher moments for the  $\ell$ -torsion in class groups. *arXiv:1810.04732*, 2018.
- [HV06] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527 – 550, 2006.
- [Klü05] J. Klüners. A counter example to Malle’s conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.
- [Klü06] J. Klüners. Asymptotics of number fields and the Cohen-Lenstra heuristics. *J. Théor. Nombres Bordeaux*, pages 607–615, 2006.
- [Klü12] J. Klüners. The distribution of number fields with wreath products as Galois groups. *Int. J. Number Theory*, (8):845–858, 2012.
- [Lan94] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1994.

- [May13] J. Maynard. On the Brun-Titchmarsh theorem. *Acta Arithmetica*, 157, 2013.
- [MV73] H.L. Montgomery and R.C. Vaughan. The large sieve. *Mathematika*, 20:119–134, 1973.
- [Pie05] L. B. Pierce. The 3-part of class numbers of quadratic fields. *J. London Math. Soc.*, 71:579–598, 2005.
- [PTBW] L. B. Pierce, C. Turnage-Butterbaugh, and M. M. Wood. An effective Chebotarev density theorem for families of number fields, with an application to  $\ell$ -torsion in class groups. *arXiv: 1709.09637*.
- [PTBW19] L. B. Pierce, C. Turnage-Butterbaugh, and M. M. Wood. On a conjecture for  $\ell$ -torsion in class groups of number fields: from the perspective of moments. *arXiv: 1902.02008*, 2019.
- [TZ17] J. Thorner and A. Zaman. An explicit bound for the least prime ideal in the chebotarev density theorem. *Algebra & Number Theory*, 11(5):1135–1197, 2017.
- [TZ18] J. Thorner and A. Zaman. A Chebotarev variant of the Brun-Titchmarsh theorem and bounds for the lang-trotter conjectures. *Int. Math. Res. Not.*, 11(4991-5027), 2018.
- [TZ19] J. Thorner and A. Zaman. A zero density estimate for Dedekind zeta functions. *arXiv:1909.01338v1*, 2019.
- [Wan17] J. Wang. Malle’s conjecture for  $S_n \times A$  for  $n = 3, 4, 5$ . *arXiv: 1705.00044*, 2017.
- [Wei83] A. Weiss. The least prime ideal. *J. Reine Angew. Math*, 1983.
- [Wid17] M. Widmer. Bounds for the  $\ell$ -torsion in class groups. *preprint*, 2017.
- [Zam17] A. Zaman. Analytic estimates for the Chebotarev density theorem and their applications. *Ph.D. thesis, University of Toronto*, 2017.
- [Zha05] S.-W. Zhang. Equidistribution of CM-points on quaternion Shimura varieties. *Int. Math. Res. Not.*, 59:3657–3689, 2005.

Jiuya Wang, DEPARTMENT OF MATHEMATICS, DUKE UNIVERSITY, 120 SCIENCE DRIVE 117 PHYSICS BUILDING DURHAM, NC 27708, USA

*E-mail address:* wangjiuy@math.duke.edu