DAVENPORT-HEILBRONN THEOREMS FOR QUOTIENTS OF CLASS GROUPS

ZEV KLAGSBRUN

Abstract. We prove a generalization of the Davenport-Heilbronn theorem to quotients of ideal class groups of quadratic fields by the primes lying above a fixed set of rational primes $S$. When restricted to quadratic fields in which all primes in $S$ split completely, our results are consistent with Cohen and Lenstra’s model for such quotients.

Additionally, we obtain average sizes for the relaxed Selmer group $\text{Sel}^3_S(K)$ and for $\mathcal{O}^\times_K/(\mathcal{O}^\times_K)^3$ as $K$ varies among quadratic fields with a fixed signature ordered by discriminant.

1. Introduction

One of the few proven results concerning the distribution of class groups of number fields is the Davenport-Heilbronn theorem which states:

**Theorem 1** (Theorem 3 in [5]). When ordered by absolute discriminant,

(i) the average size of $\text{Cl}(K)[3]$ as $K$ ranges over imaginary quadratic fields is equal to 2 and

(ii) the average size of $\text{Cl}(K)[3]$ as $K$ ranges over real quadratic fields is equal to $4/3$.

We consider the case where $\text{Cl}(K)$ is replaced with its quotient by the subgroup generated by the classes of primes lying above a fixed set of rational primes $S$. Explicitly, for a quadratic field $K$, define $\text{Cl}(K)_S := \text{Cl}(K)/\langle S_K \rangle$, where $S_K$ is the set of primes of $\mathcal{O}_K$ lying above the primes in $S$ and $\langle S_K \rangle$ is the subgroup of $\text{Cl}(K)$ generated by the ideal classes of the primes in $S_K$.

One nominally expects that if each prime $p$ in $S$ splits completely as $\mathfrak{p}\overline{\mathfrak{p}}$ in $K$, then the ideal classes $[\mathfrak{p}]$ for $\mathfrak{p} \in S$ should be distributed uniformly and independently at random in $\text{Cl}(K)$.

Conditioning on the distribution for $\text{Cl}(K)$ given by the Cohen–Lenstra heuristics, this yields a prediction for the distribution of $\text{Cl}(K)_S$. Indeed, when $S$ contains a single prime, this conjecture actually appears in the original work of Cohen and Lenstra on the distribution of class groups of quadratic fields [4] — see Remark [1].

We prove that the average size of $\text{Cl}(K)_S[3]$ as $K$ ranges over imaginary (resp. real) quadratic fields where all primes in $S$ split completely in $K$ is consistent with this conjectured distribution.

**Theorem 2.** When ordered by absolute discriminant,

(i) the average size of $\text{Cl}(K)_S[3]$ as $K$ ranges over imaginary quadratic fields where all primes in $S$ split completely in $K$ is equal to $1 + 3^{-|S|}$ and

(ii) the average size of $\text{Cl}(K)_S[3]$ as $K$ ranges over real quadratic fields where all primes in $S$ split completely in $K$ is equal to $1 + 3^{-|S| - 1}$.

If we don’t condition on the splitting behavior of the primes in $S$, then we obtain the following:
Theorem 3. When ordered by absolute discriminant,
(i) the average size of \( Cl(K)_S[3] \) as \( K \) ranges over imaginary quadratic fields is equal to
\[
1 + \frac{1}{3^{|S|}} \prod_{p \in S} \left( 2 + \frac{1}{p+1} \right)
\]
and
(ii) the average size of \( Cl(K)_S[3] \) as \( K \) ranges over real quadratic fields is equal to
\[
1 + \frac{1}{3^{|S|+1}} \prod_{p \in S} \left( 2 + \frac{1}{p+1} \right).
\]

Remark 1.1. As noted above, the average sizes appearing in Theorem 2 are consistent with modeling \( Cl(K) \) as a random group subject to the Cohen-Lenstra distribution and then taking the quotient of \( Cl(K) \) by a subgroup of \( Cl(K) \) generated by \( |S| \) elements of \( Cl(K) \) chosen uniformly and independently at random. When \( |S| = 1 \) and \( K \) is an imaginary quadratic field, then Cohen and Lenstra attribute to Dick Gross the observation that the distribution obtained in the manner is identical to the Cohen-Lenstra distribution for real quadratic fields [4].

Remark 1.2. The average size in part (i) (resp. (ii)) of Theorem 2 is the same as the average size of the left-nullspace of a random \( n \times n + |S| \) (resp. \( n \times n + |S| + 1 \)) matrix with random entries in \( \mathbb{F}_3 \) as \( n \to \infty \).

The core idea underlying the proof of the Davenport-Heilbronn theorem is how to use the geometry of numbers to count cubic fields. The application to class groups is almost an afterthought that arises from a bijection originally due to Hasse between the set of index 3 subgroups of \( Cl(K) \) and the set of isomorphism classes of cubic fields \( L \) with \( d_L = d_K \) [6]. We establish a similar bijection between the set of index 3 subgroups of \( Cl(K)_S \) and the set of isomorphism classes of cubic fields \( L \) with \( d_L = d_K \). Theorem 3 is then proven using recent results of Bhargava, Shankar, and Tsimerman that count the number of cubic fields with bounded discriminant satisfying a set of local conditions [1]. This counting may equivalently be accomplished by appealing to recent work of Taniguchi and Thorne [10].

1.1. Additional Results. In addition to Theorem 3, we also prove similar distribution results for a pair of objects closely connected to \( Cl(K)_S[3] \). A standard result (see Section 8.3.2 of [3], for example) shows that \( Cl(K)_S[3] \) sits in the short exact sequence
\[
0 \to \mathcal{O}^\times_{K,S}/(\mathcal{O}^\times_{K,S})^3 \to Sel_3^S(K) \to Cl(K)_S[3] \to 0,
\]
where \( \mathcal{O}^\times_{K,S} \) is the \( S_K \) units of \( \mathcal{O}_K \) and \( Sel_3^S(K) \) is the 3-Selmer group of \( K \) relaxed at \( S_K \), defined as
\[
Sel_3^S(K) := \{ \alpha \in K^\times/(K^\times)^3 : val_p(\alpha) \equiv 0 \pmod{3} \text{ for all } p \notin S_K \}.
\]
We are able to compute average sizes for both \( Sel_3^S(K) \) and \( \mathcal{O}^\times_{K,S}/(\mathcal{O}^\times_{K,S})^3 \).

Theorem 4. When ordered by absolute discriminant,
(i) the average size of \( Sel_3^S(K) \) as \( K \) ranges over real quadratic fields is equal to
\[
3^{|S|} + 3^{|S|+1} \prod_{p \in S} \left( 1 + \frac{p}{p+1} \right)
\] and
(ii) the average size of $\text{Sel}_3^S(K)$ as $K$ ranges over imaginary quadratic fields is equal to
\[3^{|S|} + 3^{|S|} \prod_{p \in S} \left(1 + \frac{p}{p+1}\right).\]

**Theorem 5.** When ordered by absolute discriminant,
(i) the average size of $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^3$ as $K$ ranges over real quadratic fields is equal to
\[3^{|S|+1} \prod_{p \in S} \left(1 + \frac{p}{p+1}\right)\]
and
(ii) the average size of $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^3$ as $K$ ranges over imaginary quadratic fields is equal to
\[3^{|S|} \prod_{p \in S} \left(1 + \frac{p}{p+1}\right).\]

**Remark 1.3.** The results of Bhargava, Shankar, and Tsimerman in [1] and Taniguchi and Thorne in [10] yield second order terms for the number of cubic fields with bounded discriminant satisfying a set of local conditions. As a result, it is possible to bounds the rate of convergence in Theorems 2, 3, 4, and 5.

**1.2. Related Work.** Recent work of Varma [11] generalized Theorem 1 to ray class groups of fixed integral conductor. While the formulas appearing in Theorem 1 in [11] are similar to those appearing in Theorem 4 above, neither result appears to directly follow from the other.

In a companion paper, the author obtains variants of Theorems 2, 3, 4, and 5 for quotients of class groups of cubic fields, considering 2-torsion in the class groups, rather than 3-torsion [9]. Those results are similar in substance to the ones appearing here, but rely on a correspondence of Heilbronn between the unramified quadratic extensions of a cubic field $K$ and the isomorphism classes of quartic fields $L$ having cubic resolvent $K$ [7].

The results in Sections 2–4 generalize results for the case $S = \{3\}$ that appear in Sections 9.1–9.4 of the author’s work with Jordan, Poonen, Skinner, and Zaytman on the distribution of $K$-groups of quadratic fields [8]. While some of the proofs included here are substantively similar to those appearing in [8], we have nonetheless included them for the benefit of the reader.

Additionally, a variant of Theorem 2 when $S$ contains a single prime was obtained independently in unpublished work of Wood and is proved using similar methods [12].

**Notation**

We will use the following notation throughout this paper:

- $S$ will be a set of rational primes.
- $K$ will be a quadratic field.
- If $F$ is a field, then $d_F$ is the discriminant of $F$.
- $\mathcal{O}_K$ will be the ring of integers of $K$.
- $S_K$ will denote the set of primes of $\mathcal{O}_K$ lying above primes in $S$.
- $\mathcal{O}_{K,S}^\times$ will denote the $S_K$-units of $K$.
- $\text{Sel}_3^S(K)$ will be the 3-Selmer group of $K$ relaxed at the primes in $S_K$.
- $\text{Cl}(K)$ will be the ideal class group of $\mathcal{O}_K$.
- $\text{Cl}(K)/S_K$ will be the quotient $\text{Cl}(K)/\langle S_K \rangle$, where $\langle S_K \rangle$ is the subgroup of $\text{Cl}(K)$ generated by primes in $S_K$. 

• If $p$ is a rational prime, then $\mathbb{L}_p$ will denote the unique unramified cubic extension of $\mathbb{Q}_p$.

ACKNOWLEDGEMENT

I would like to thank Bjorn Poonen and Genya Zaytman for suggesting the proof of Proposition 2.2. I would also like to thank Manjul Bhargava and Melanie Wood for valuable suggestions regarding the framing of Theorem 2 with respect to the Cohen-Lenstra heuristics.

2. CLASS FIELDS THEORY

As remarked above, Davenport and Heilbronn relied on a bijection between the set of index 3 subgroups of $\text{Cl}(K)$ and the set of isomorphism classes of cubic fields $L$ with $d_L = d_K$. We describe this correspondence, originally due to Hasse, in Proposition 2.1 before establishing a similar correspondence for $\text{Cl}(K)_S$ in Proposition 2.2.

Proposition 2.1 (Satz 7 in [6]). The following are in bijective correspondence.

(i) The set of index 3 subgroups of $\text{Cl}(K)$.
(ii) The set of unramified $\mathbb{Z}/3\mathbb{Z}$-extensions $M$ of $K$.
(iii) The set of isomorphism classes of cubic fields $L$ with $d_L = d_K$.

Proof. The correspondence (i) $\leftrightarrow$ (ii) is class field theory. The correspondence (ii) $\leftrightarrow$ (iii) will follow from Satz 3 in [6].

Suppose that $M/K$ is unramified. Since the Hilbert class field $H_K$ is Galois over $\mathbb{Q}$ and $M \subset H_K$, we get that $M/\mathbb{Q}$ is Galois. We next observe that the non-trivial element $\sigma \in \text{Gal}(K/\mathbb{Q})$ acts on $\text{Cl}(K/\mathbb{Q})$ and therefore on $\text{Gal}(H_K/\mathbb{Q})$ by inversion. As a result, $\text{Gal}(K/\mathbb{Q})$ acts non-trivially on $\text{Gal}(M/K)$, so we see that $\text{Gal}(M/\mathbb{Q}) \simeq S_3$. The map (ii) $\rightarrow$ (iii) sends $M/K$ to any of the 3 isomorphic cubic subfields $L$ of $M/\mathbb{Q}$. By Satz 3 in [6], $d_L = N_{K/\mathbb{Q}}(f)d_K$, where $f$ is the conductor of $M/K$. Since $M/K$ is unramified, we find that $d_L = d_K$.

For the opposite direction, let $M$ be the Galois closure of $L/\mathbb{Q}$. Since $L/\mathbb{Q}$ is nowhere totally ramified, $M$ must be an $S_3$ extension of $\mathbb{Q}$. As such, $M$ contains a unique quadratic field $K$ and the map (iii) $\rightarrow$ (ii) sends $L/\mathbb{Q}$ to the extension $M/K$. Once again by Satz 3 in [6], $d_L = N_{K/\mathbb{Q}}(f)d_K$. Since $d_L = d_K$, we have $f = \mathcal{O}_K$, so $M/K$ is unramified. Since the maps (ii) $\rightarrow$ (iii) and (iii) $\rightarrow$ (ii) can be seen to invert each other, the result follows.

Proposition 2.2. The following are in bijective correspondence.

(i) The set of index 3 subgroups of $\text{Cl}(K)_S$.
(ii) The set of unramified $\mathbb{Z}/3\mathbb{Z}$-extensions $M$ of $K$ in which all primes in $S_K$ split completely.
(iii) The set of isomorphism classes of cubic fields $L$ with $d_L = d_K$ such that for all $p \in S$, $d_K \in (\mathbb{Q}_p^\times)^2$, then $p$ splits completely in $L$.

Proof. By class field theory, $\text{Cl}(K)_S$ is the Galois group of the maximal unramified abelian extension $H_S$ of $K$ in which $\text{Frob}_p \in \text{Gal}(H_S/K)$ is trivial for all $p \in S_K$. As a result, the set of index 3 subgroups of $\text{Cl}(K)_S$ is in bijective correspondence with set of unramified $\mathbb{Z}/3\mathbb{Z}$-extensions $M$ of $K$ in which all primes in $S_K$ split completely.

The maps for the correspondence between (ii) and (iii) are the same as in Proposition 2.1. We only need to show that the images satisfy the properties claimed. The map (ii) $\rightarrow$ (iii) sends $M/K$ to any of the cubic subfields of the $S_3$-extension $M/\mathbb{Q}$. If $d_K \in (\mathbb{Q}_p^\times)^2$, then $p$
splits completely in $K/Q$ and each prime $p | p$ splits completely in $M/K$ by assumption. As a result, $p$ splits completely in $L/Q$.

For the reverse map $[\mathfrak{m}] \rightarrow [\mathfrak{m}]$, send $L/Q$ to the extension $M/K$ where $M$ is the Galois closure of $L/Q$ and $K \subset M$ is the unique quadratic subextension of $M$. We wish to show that all primes in $S_K$ split completely in $M/K$.

Suppose that $p \in S$. If $d_K \in (\mathbb{Q}_p^\times)^2$, then $p$ splits in $K$ and by assumption $p$ splits completely in $L$ as well. As a result, $p$ splits completely in $M/Q$ and therefore in $M/K$ as well. If $d_K \notin (\mathbb{Q}_p^\times)^2$, then $p$ has two primes lying above it in $L$. The Galois structure of $M/Q$ then forces $p$ to have three primes lying above it in $M$. Since both $K/Q$ and $M/K$ are Galois, we find that $p$ does not split in $K/Q$ and that all primes above $p$ in $K$ split completely in $M/K$.

**Corollary 2.3.** If $K$ is a quadratic field, then

$$|\text{Cl}(K)_S[3]| = 1 + 2|\{\text{cubic fields } L \text{ with } d_L = d_K \text{ such that } L \otimes \mathbb{Q}_p \neq \mathbb{L}_p \text{ for all } p \in S\}|$$

**Proof.** Since $\text{Cl}(K)_S$ is a finite abelian group, the number of index three subgroups of $\text{Cl}(K)_S$ is equal to the number of order three subgroups of $\text{Cl}(K)_S$. By Proposition 2.2 this is the same as the number of cubic fields $L$ with $d_L = d_K$ such that $L \otimes \mathbb{Q}_p \neq \mathbb{L}_p$. The result follows since each order three subgroup contains two non-trivial elements and any two distinct order three subgroups intersect in the trivial group.

## 3. Counting Fields

In order to obtain our main results, we will need the following two theorems that count the number of quadratic and cubic fields satisfying a finite set of local conditions.

**Theorem 3.1.** Let $S_1 \subset S$. Then the number of real (resp. imaginary) quadratic fields $K$ with $|d_K| < X$ such that all primes in $S_1$ split in $K/Q$ and all primes in $S \setminus S_1$ do not split in $K/Q$ is equal to

$$\frac{1}{2\zeta(2)} \left( \prod_{p \in S_1} \frac{p}{2(p+1)} \right) \left( \prod_{p \in S \setminus S_1} \frac{p+2}{2(p+1)} \right) \cdot X + o(X)$$

To prove Theorem 3.1 we will need the following lemma.

**Lemma 3.2.** Let $d$ be an odd squarefree number. Then for any class $d_0 \ (\text{mod } 16d^2)$ that occurs as a fundamental discriminant, we have

$$|\{0 < d < X : d \text{ fundamental and } d \equiv d_0 \ (\text{mod } 16d^2)\}| = \frac{1}{2\zeta(2)} \prod_{p|2d} \frac{1}{p^2-1} \cdot X + O(\sqrt{X})$$

and

$$|\{-X < d < 0 : d \text{ fundamental and } d \equiv d_0 \ (\text{mod } 16d^2)\}| = \frac{1}{2\zeta(2)} \prod_{p|2d} \frac{1}{p^2-1} \cdot X + O(\sqrt{X})$$

**Proof.** By Corollary 1 to Theorem 1 in [2], for any squarefree $d_0$, we have

$$|\{0 < d < X : d \text{ is squarefree and } d \equiv d_0 \ (\text{mod } 4d^2)\}| = \frac{1}{\zeta(2)} \prod_{p|2d} \frac{1}{p^2-1} \cdot X + O(\sqrt{X})$$

The result follows from considering each possible squarefree class modulo 4. \qed
Proof of Theorem 3.1. A prime $p$ splits in a quadratic field $K/Q$ if and only if $d_K \in (Q^*)^2$. Letting $\mathfrak{o}$ be the product of all odd primes in $S$, the splitting type in $K/Q$ of all primes in $S$ is then determined by the class of $d_K \pmod{16\mathfrak{o}^2}$.

For odd $p$, the number of non-trivial square classes modulo $p^2$ is equal to $\frac{p^2 - p}{2}$ and the number of non-trivial square classes modulo $16$ is $2$. Therefore, the number of admissible classes $d \pmod{16\mathfrak{o}^2}$ such that if $d_K \equiv d \pmod{16\mathfrak{o}^2}$, then all primes of $S_1$ split in $K/Q$ and all primes in $S \setminus S_1$ do not split in $K/Q$ is given by

$$
\left(2\right) \quad c_2 \prod_{p \in S_1} \frac{p^2 - p}{2} \prod_{p \in S \setminus S_1} \frac{p^2 + p - 2}{2},
$$

where $c_2 = \begin{cases} 2 & \text{if } 2 \in S \text{ and } \\ 6 & \text{if } 2 \not\in S. \end{cases}$

By Lemma 3.2, the number of fundamental discriminants in each class is given by

$$
\left(3\right) \quad \frac{1}{2\zeta(2)} \prod_{p \mid 2\mathfrak{o}} \frac{1}{p^2 - 1} \cdot X + O(\sqrt{X}).
$$

Multiplying (2) by (3) and accounting for whether or not $2 \in S$ gives the result. □

Remark 3.3. By taking $S = \emptyset$, we recover the standard asymptotic for the number of quadratic fields with bounded discriminant.

In order to count cubic fields, we will use the following specialization of a theorem of Bhargava, Shankar, and Tsimerman.

Theorem 3.4 (Theorem 8 in \cite{1}). Let $S$ be a finite set of primes. For each prime $p \in S$, let $\Sigma_p$ be a set of maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified. Then the number of totally real (resp. complex) cubic fields $L$ with $|d_L| < X$ that are nowhere totally ramified and have $\mathcal{O}_L \otimes \mathbb{Z}_p \in \Sigma_p$ for all $p$ is given by

$$
\left(4\right) \quad N(X) = c_\infty \left( \prod_{p \in S} \frac{p}{p + 1} \sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)} \right) \cdot X + o(X),
$$

where $c_\infty = \frac{1}{12}$ (resp. $c_\infty = \frac{1}{4}$) and $\text{Disc}_p(R)$ is the $p$-part of the discriminant of $R$.

Proof. Following the convention in \cite{1}, for all primes $p \not\in S$, set $\Sigma_p$ to be the set of all maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified.

By Theorem 8 in \cite{1}, the number of totally real (resp. complex) cubic fields $L$ with $|d_L| < X$ and $\mathcal{O}_L \otimes \mathbb{Z}_p \in \Sigma_p$ for all $p$ is given by

$$
\left(5\right) \quad N(X) = c_\infty \left( \prod_{p} \frac{p - 1}{p} \sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)} \right) \cdot X + o(X),
$$

where $c_\infty$ is as above. The choice of $\Sigma_p$ for $p \not\in S$ ensures that we count exactly those fields that are nowhere totally ramified.
Letting $\Gamma_p$ be the set of all maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified, it is an easy exercise to see that
\[
\sum_{R \in \Gamma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)} = \frac{p+1}{p}.
\]
As a result, for all $p \not\in S$, we have
\[
\sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)} = \frac{p+1}{p}.
\]
Letting $S_\Sigma = \prod_p \left(1 - \frac{1}{p^2}\right) \prod_{p \in S} \sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)}$, we have
\[
S_\Sigma = \prod_p \left(1 - \frac{1}{p^2}\right) \prod_{p \in S} \frac{p+1}{p+1} \sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)} = \frac{1}{\zeta(2)} \prod_{p \in S} \frac{p+1}{p+1} \sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)}
\]
Combined with (3), this gives (4). \hfill \Box

4. Average Sizes of Quotients of Class Groups

By Corollary 2.3, in order to count elements of $\text{Cl}(K)_S[3]$, we want to count cubic fields $L$ such that $O_L \otimes \mathbb{Z}_p \neq O_{L_p}$ for all $p \in S$. We are able to do this using Theorem 3.4

**Theorem 4.1.** The number of nowhere totally ramified totally real (resp. complex) cubic fields $L$ with $|d_L| < X$ and $O_L \otimes \mathbb{Z}_p \neq O_{L_p}$ for all $p \in S$ is
\[
\frac{c_\infty}{3^{|S|} \zeta(2)} \prod_{p \in S} \left(2 + \frac{1}{p+1}\right) + o(X),
\]
where $c_\infty = \frac{1}{12}$ (resp. $c_\infty = \frac{1}{4}$).

**Proof.** For each prime $p \in S$, let $\Gamma_p$ be the set of all maximal cubic orders over $\mathbb{Z}_p$ that are not totally ramified and set $\Sigma_p = \Gamma_p \setminus \{O_{L_p}\}$.

For each $p \in S$, we then have
\[
\frac{p}{p+1} \sum_{R \in \Sigma_p} \frac{1}{|\text{Aut}(R)|} \cdot \frac{1}{\text{Disc}_p(R)} = \frac{p}{p+1} \left(\frac{p+1}{p} - \frac{1}{3}\right) = 1 - \frac{p}{3(p+1)} = \frac{1}{3} \left(2 + \frac{1}{p+1}\right)
\]
The result then follows from Theorem 3.4. \hfill \Box

**Proof of Theorem 4.1.** Combining Theorem 4.1 with Corollary 2.3, the total number of non-trivial elements of $\text{Cl}(K)_S[3]$ for all real (resp. imaginary) quadratic fields $K$ with $|d_K| < X$ is given by
\[
\frac{c_\infty}{3^{|S|} \zeta(2)} \prod_{p \in S} \left(2 + \frac{1}{p+1}\right) \cdot X + o(X),
\]
where $c_\infty = \frac{1}{6}$ (resp. $c_\infty = \frac{1}{2}$). As noted in Remark 3.3, the total number of real (resp. imaginary) quadratic fields $K$ with $|d_K| < X$ is equal to $\frac{c_\infty'}{3^{|S|} \zeta(2)} \cdot X + o(X)$. We therefore get that the average number of non-trivial elements of $\text{Cl}(K)_S[3]$ for all real (resp. imaginary) quadratic fields $K$ with $|d_K| < X$ is equal to
\[
\frac{c_\infty'}{3^{|S|}} \cdot \prod_{p \in S} \left(2 + \frac{1}{p+1}\right),
\]
where $c_\infty' = 1/3$ (resp. $c_\infty' = 1$). \hfill \Box
5. Averages for S-Unit Groups

We now want to consider the average size of $\mathcal{O}_{K,S}^x / (\mathcal{O}_{K,S}^x)^3$ as $K$ varies over real (resp. imaginary) quadratic fields. For uniformity, we will assume that $K \neq \mathbb{Q}(\sqrt{-3})$ and note that this does not affect the averages.

**Lemma 5.1.** Let $K$ be a quadratic field and let $S_1 \subset S$ be the set of primes in $S$ that split in $K/\mathbb{Q}$. Then $|\mathcal{O}_{K,S}^x / (\mathcal{O}_{K,S}^x)^3| = 3^{r_\infty + |S| + |S_1|}$, where $r_\infty = \begin{cases} 1 & \text{if } K \text{ is real} \\ 0 & \text{if } K \text{ is imaginary} \end{cases}$.

**Proof.** This follows directly from Dirichlet’s unit theorem. □

**Lemma 5.2.** For each quadratic field $K$, let $S_1 = S_1(K)$ be the set of primes in $S$ that split in $K/\mathbb{Q}$. Then as $K$ varies over real (resp. imaginary) quadratic fields ordered by discriminant, we have

$$\text{Avg} \left(3^{|S_1|}\right) = \prod_{p \in S} \left(1 + \frac{p}{p + 1}\right).$$

**Proof.** We proceed by induction. Suppose that $S = \{p\}$. Then $p$ splits in $K$ exactly when $d_K \in (\mathbb{Q}_p^x)^2$. As $d_K$ ranges over fundamental discriminants, the proportion of $d_K$ such that $d_K \in (\mathbb{Q}_p^x)^2$ is equal to $\frac{p}{2(p+1)}$. We therefore have

$$\text{Avg} \left(3^{|S_1|}\right) = 1 \cdot \frac{p+2}{2(p+1)} + 3 \cdot \frac{p}{2(p+1)} = \frac{4p+2}{2(p+1)} = 1 + \frac{p}{p+1}.$$

Now suppose that (6) holds for a set $S$ and let $S' = S \cup \{q\}$ for some prime $q \notin S$. We then have

$$\text{Avg} \left(3^{|S_1|}\right) = \rho \cdot \text{Avg} \left(3^{|S_1|}\big| q \in S_1 \right) + (1 - \rho) \cdot \text{Avg} \left(3^{|S_1|}\big| q \notin S_1 \right),$$

where $\rho$ is the probability that $q \in S_1$. By the inductive hypothesis, we have

$$\text{Avg} \left(3^{|S_1|}\big| q \in S_1 \right) = 3 \prod_{p \in S} \left(1 + \frac{p}{p+1}\right)$$

and

$$\text{Avg} \left(3^{|S_1|}\big| q \notin S_1 \right) = \prod_{p \in S} \left(1 + \frac{p}{p+1}\right).$$

Since the probability that $q \in S_1$ is given by $\frac{q}{2(q+1)}$, we have

$$\text{Avg} \left(3^{|S_1|}\right) = 1 \cdot \frac{q+2}{2(q+1)} + 3 \cdot \frac{q}{2(q+1)} \prod_{p \in S} \left(1 + \frac{p}{p+1}\right) = \prod_{p \in S'} \left(1 + \frac{p}{p+1}\right).$$

□

**Proof of Theorem 5.** By Lemma 5.1, we have

$$\text{Avg} \left|\mathcal{O}_{K,S}^x / (\mathcal{O}_{K,S}^x)^3\right| = \text{Avg} \left(3^{r_\infty + |S| + |S_1|}\right) = 3^{r_\infty + |S|} \cdot \text{Avg} \left(3^{|S_1|}\right)$$

The result then follows from Lemma 5.2. □

6. Average Sizes of Selmer Groups

**Lemma 6.1.** Let $K$ be a quadratic field and let $S_1 \subset S$ be the set of primes that split in $K/\mathbb{Q}$. Then $|\text{Sel}_3^S(K)| = 3^{r_\infty + |S| + |S_1|} \cdot |\text{Cl}(K)_S[3]|$ where $r_\infty$ is as in Lemma 5.1.

**Proof.** This follows from Lemma 5.1 combined with (1). □
**Remark 6.3.** It is worth noting that the average size of fields (ordered by absolute discriminant) such that all primes in \( S \) and all primes in \( p \in S \setminus S \) do not split in \( K/\mathbb{Q} \), we have \( \text{Avg} (|\text{Cl}(K)_S[3]|) = 1 + \frac{c'_\infty}{3|S_1|} \), where

\[
\begin{aligned}
c'_\infty &= \begin{cases} 
1/3 & \text{if } K \text{ is real and } \\
1 & \text{if } K \text{ is imaginary}. 
\end{cases}
\end{aligned}
\]

**Proof.** This will be a consequence of Theorem 3.4. For \( p \in S_1 \), set \( \Sigma_p = \{ \mathbb{Z}_p \} \) and for \( p \in S \setminus S_1 \), set \( \Sigma_p = \{ \mathbb{Z}_p \times O_{K_p} : K_p/\mathbb{Q} \text{ quadratic} \} \). Observe that if \( L \) is a nowhere totally ramified cubic field such that \( O_L \otimes \mathbb{Z}_p \in \Sigma_p \) for all \( p \in S \), then the set of primes in \( S \) for which \( (d_L \in \mathbb{Q}_p^\times)^2 \) is equal to \( S_1 \).

We then have

\[
\frac{p}{p + 1} \sum_{R \in \Gamma_p} \frac{1}{|\text{Aut}(R)|} \frac{1}{\text{Disc}_p(R)} = \begin{cases} 
p \in S_1 \\frac{p}{6(p+1)} & p \in S_1 \\
p \in S \setminus S_1 \\frac{p + 2}{2(p+1)} & p \in S \setminus S_1.
\end{cases}
\]

As a result, by Theorem 3.4 the number of nowhere totally ramified totally real (resp. complex) cubic fields \( L \) with \( |d_L| < X \) such that \( O_L \otimes \mathbb{Z}_p \in \Sigma_p \) for all \( p \in S \) is given by

\[
\frac{c_{\infty}}{\zeta(2)} \prod_{p \in S_1} \frac{p}{6(p+1)} \prod_{p \in S \setminus S_1} \frac{p + 2}{2(p+1)} \cdot X + o(X),
\]

where \( c_{\infty} = \frac{1}{12} \) (resp. \( c_{\infty} = \frac{1}{4} \)).

By Corollary 2.3 we therefore get that the total number of non-trivial elements of \( \text{Cl}(K)_S \) as \( K \) varies over all real (resp. imaginary) quadratic fields such that all primes in \( S_1 \) split in \( K/\mathbb{Q} \) and all primes in \( S \setminus S_1 \) do not split in \( K/\mathbb{Q} \) is equal to

\[
\frac{2c_{\infty}}{\zeta(2)} \prod_{p \in S_1} \frac{p}{6(p+1)} \prod_{p \in S \setminus S_1} \frac{p + 2}{2(p+1)} \cdot X + o(X),
\]

By Theorem 3.4 the number of such real (resp. imaginary) quadratic fields is equal to

\[
\frac{1}{2\zeta(2)} \prod_{p \in S_1} \frac{p}{2(p+1)} \prod_{p \in S \setminus S_1} \frac{p + 2}{2(p+1)} \cdot X + o(X)
\]

and as a result, the average number of non-trivial elements in \( \text{Cl}(K)_S[3] \) for as \( K \) ranges over real (resp. imaginary) quadratic fields such that all primes in \( S_1 \) split in \( K/\mathbb{Q} \) and all primes in \( S \setminus S_1 \) do not split in \( K/\mathbb{Q} \) is given by

\[
4 \cdot c_{\infty} \prod_{p \in S_1} \frac{1}{3} = \frac{c'_\infty}{3|S_1|}.
\]

**Remark 6.3.** It is worth noting that the average size of \( |\text{Cl}(K)_S[3]| \) in Lemma 6.2 depends only on \( |S_1| \) and not on the actual primes contained in \( S \) or \( S_1 \).

**Proof of Theorem 2.** This is Lemma 6.2 with \( S = S_1 \). 

**Theorem 6.4.** Let \( S_1 \subset S \). Then as \( K \) varies through all real (resp. imaginary) quadratic fields (ordered by absolute discriminant) such that all primes in \( S_1 \) split in \( K/\mathbb{Q} \) and all primes in \( S \setminus S_1 \) do not split in \( K/\mathbb{Q} \), we have

\[
\text{Avg} (|\text{Sel}^S_3(K)|) = 3^{r_\infty + |S_1| + |S|} + 3^{|S|},
\]

where \( r_\infty \) is as in Lemma 5.4.
Proof. By Lemma 6.1 we have

\[ \text{Avg} \left( |\text{Sel}_3^S(K)| \right) = \text{Avg} \left( 3^{r \infty + |S| + |S_1|} \cdot |\text{Cl}(K)_S[3]| \right) = 3^{r \infty + |S| + |S_1|} \cdot \text{Avg} \left( |\text{Cl}(K)_S[3]| \right), \]

where the second equality follows from the fact that \( S_1 \) is fixed. The result then follows from applying Lemma 6.2 and observing that with \( c'_{\infty} \) as in Lemma 6.2, we have \( 3^{r \infty} \cdot c'_{\infty} = 1. \)

Proof of Theorem 4. By Theorem 6.4, for each \( S_1 \subset S \), \( \text{Avg} \left( |\text{Sel}_3^S(K)| \right) = 3^{r \infty + |S_1| + |S| + 3|S_1|} \) when we vary over real (resp. imaginary) quadratic fields \( K \) such that all primes in \( S_1 \) split in \( K/\mathbb{Q} \) and all primes in \( S \setminus S_1 \) do not split in \( K/\mathbb{Q} \). Therefore, if we vary over all real (resp. imaginary) quadratic fields \( K \), we have

\[ \text{Avg} \left( |\text{Sel}_3^S(K)| \right) = \sum_{S_1 \subset S} \rho(S_1) \left( 3^{r \infty + |S_1| + |S|} + 3^{|S_1|} \right), \]

where \( \rho(S_1) \) is the probability that all of the primes in \( S_1 \) split in \( K/\mathbb{Q} \) and all primes in \( S \setminus S_1 \) do not split in \( K/\mathbb{Q} \) as \( K \) varies. However,

\[ \sum_{S_1 \subset S} \rho(S_1) \left( 3^{r \infty + |S_1| + |S|} + 3^{|S_1|} \right) = 3^{r \infty + |S|} \sum_{S_1 \subset S} \rho(S_1) 3^{|S_1|} + 3^{|S_1|} \sum_{S_1 \subset S} \rho(S_1) = 3^{r \infty + |S|} \text{Avg} \left( 3^{|S_1|} \right) + 3^{|S|}, \]

so by Lemma 5.2 we get that \( \text{Avg} \left( |\text{Sel}_3^S(K)| \right) = 3^{r \infty + |S|} \prod_{p \in S} \left( 1 + \frac{p}{p + 1} \right) + 3^{|S|}. \)

References

[1] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. Inventiones mathematicae. 193 (2013): 439–499.
[2] E. Cohen and R. Robinson. On the distribution of the k- free integers in residue classes. Acta Arithmetica. 3 (1963): 283–93.
[3] H. Cohen. Number theory: Volume I: Tools and diophantine equations. 239 Springer Verlag, 2009.
[4] H. Cohen and H. Lenstra Jr. Heuristics on class groups of number fields. Number Theory Noordwijkerhout 1983 : 33–62.
[5] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields II. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1971): 405–420.
[6] H. Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Mathematische Zeitschrift 31 (1930): 565–582.
[7] H. Heilbronn. On the 2-classgroup of cubic fields. Studies in Pure Mathematics. (1971): 117-119.
[8] B. 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 fields. arXiv preprint 1703.00108 (2017).
[9] Z. Klagsbrun. The average sizes of two-torsion subgroups in quotients of class groups of cubic fields. arXiv preprint 1701.02838.
[10] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. Duke Mathematical Journal 162 (2013): 2451–2508.
[11] I. Varma. The mean number of 3-torsion elements in ray class groups of quadratic fields. https://arxiv.org/abs/1609.02292.
[12] M. Wood. Cohen-Lenstra heuristics and local conditions. Preprint available at https://www.math.wisc.edu/ mmwood/Publications.