STATISTICS OF K-GROUPS MODULO p FOR THE RING OF INTEGERS OF A VARYING QUADRATIC NUMBER FIELD

BRUCE W. JORDAN, ZEV KLAGSBRUN, BJORN POONEN, CHRISTOPHER SKINNER, AND YEVGENY ZAYTMAN

ABSTRACT. For each odd prime p, we conjecture the distribution of the p-torsion subgroup of $K_{2n}(\mathcal{O}_F)$ as F ranges over real quadratic fields, or over imaginary quadratic fields. We then prove that the average size of the 3-torsion subgroup of $K_{2n}(\mathcal{O}_F)$ is as predicted by this conjecture.

1. INTRODUCTION

The original Cohen–Lenstra heuristics [CL84] predicted, for each prime $p \neq 2$, the distribution of the p-primary part of $\mathrm{Cl}(F)$ as F varied over quadratic fields of a given signature. More recent work developed heuristics for other families of groups, including class groups of higher degree number fields [CM90], Picard groups of function fields [FW89], Tate–Shafarevich groups of elliptic curves [Del01, Del07, DJ14], Selmer groups of elliptic curves [PR12, BKLPR15], and Galois groups of nonabelian unramified extensions of number and function fields [BBH14].

Let F be a number field. Let $\mathcal{O}_F$ be the ring of integers of F. For $m \geq 0$, the K-group $K_m(\mathcal{O}_F)$ is a finitely generated abelian group. It is finite when m is even and positive: see [Wei05, Theorem 7]. Our goal is to study, for a fixed m and odd prime p, the p-torsion subgroup $K_m(\mathcal{O}_F)_p$ as F varies in a family of number fields, always ordered by absolute value of the discriminant. As described in Section 6, $K_m(\mathcal{O}_F)_p$ is well understood for odd m. Therefore we focus on the case $m = 2n$. Moreover, the action of $\mathrm{Gal}(F/\mathbb{Q})$ decomposes $K_{2n}(\mathcal{O}_F)_p$ into $+$ and $-$ parts, and we will see that the $+$ part is $K_{2n}(\mathbb{Z})_p$, independent of F. Therefore we focus on the variation of the $-$ part.

A Cohen–Lenstra style heuristic will lead us to the following conjecture, involving the constants

$$\alpha_{p,u,r} := \frac{\prod_{i=r+1}^{\infty}(1-p^{-i})}{p^{r(u+r)}\prod_{i=1}^{r+u}(1-p^{-i})}$$

for nonnegative integers u and r:

Conjecture 1.1. *Fix $n \geq 1$ and an odd prime p and $r \geq 0$. As F ranges over all real (resp. imaginary) quadratic fields,* $\mathrm{Prob}\left(\dim_{\mathbb{F}_p} K_{2n}(\mathcal{O}_F)_p^- = r\right)$ *is given in the following table by the entry in the row determined by n and column determined by the signature:*

Date: October 31, 2017.
2010 *Mathematics Subject Classification.* Primary 11R70; Secondary 11R29, 19D50, 19F99.
Key words and phrases. algebraic K-theory, ring of integers, class group, Cohen–Lenstra heuristics.
B.P. was supported in part by National Science Foundation grant DMS-1601946 and Simons Foundation grants #402472 (to Bjorn Poonen) and #550033. C.S. was supported in part by National Science Foundation grant DMS-1301842 and by the Simons Investigator grant #376203 from the Simons Foundation.

		real	imaginary
n even	$n \equiv 0 \pmod{p-1}$	$\frac{1}{2}(\frac{p}{p+1}\alpha_{p,2,r-1} + \frac{p+2}{p+1}\alpha_{p,1,r})$	$\frac{1}{2}(\frac{p}{p+1}\alpha_{p,1,r-1} + \frac{p+2}{p+1}\alpha_{p,0,r})$
	$n \equiv \frac{p-1}{2} \pmod{p-1}$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,2,r-1} + \frac{2p+1}{p+1}\alpha_{p,1,r})$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,1,r-1} + \frac{2p+1}{p+1}\alpha_{p,0,r})$
	all other cases	$\alpha_{p,1,r}$	$\alpha_{p,0,r}$
n odd	$n \equiv \frac{p-1}{2} \pmod{p-1}$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,1,r-1} + \frac{2p+1}{p+1}\alpha_{p,0,r})$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,2,r-1} + \frac{2p+1}{p+1}\alpha_{p,1,r})$
	all other cases	$\alpha_{p,0,r}$	$\alpha_{p,1,r}$.

To pass from the distribution of $\dim_{\mathbb{F}_p} K_{2n}(\mathcal{O}_F)_p^-$ to that of $\dim_{\mathbb{F}_p} K_{2n}(\mathcal{O}_F)_p$ itself, add the constant $\dim_{\mathbb{F}_p} K_{2n}(\mathbb{Z})_p$, which can be expressed in terms of a class group (see Section 5).

Conjecture 1.1 implies an average order for $K_{2n}(\mathcal{O}_F)_p$ as F varies over all real or imaginary fields (see Conjecture 8.7). We prove that this conjectured average order is correct for $p = 3$:

Theorem 1.2. *Fix $n \geq 1$. The average order of $K_{2n}(\mathcal{O}_F)_3$ as F ranges over real (resp. imaginary) quadratic fields is as follows:*

	real	imaginary
n even	25/12	11/4
n odd	9/4	19/12

Remark 1.3. By Theorem 5.1, $K_{2n}(\mathbb{Z})_3 = 0$ for all n since $\mathbb{Q}(\zeta_3)$ has class number 1. Thus $K_{2n}(\mathcal{O}_F)_3^- = K_{2n}(\mathcal{O}_F)_3$ for all n.

Remark 1.4. Theorem 1.2 is an analogue of the Davenport–Heilbronn theorem giving the average order of $\mathrm{Cl}(F)_3$ as F varies over all real or imaginary quadratic fields [DH71, Theorem 3].

Remark 1.5. After this article was written, the second author proved an analogue of Theorem 1.2 for $K_{2n}(\mathcal{O}_F)_2$ as K varies over cubic fields [Kla17b].

1.1. **Methods.** The p-torsion subgroup G_p of a finite abelian group G has the same $\mathbb{F}_p$-dimension as $G/p := G/pG$; therefore we study $K_{2n}(\mathcal{O}_F)/p$. The latter is isomorphic to an étale cohomology group $H^2_{\text{ét}}(\mathcal{O}_F[1/p], \mu_p^{\otimes(n+1)})$, which we relate to isotypic components of the class group and Brauer group of $\mathcal{O}_E[1/p]$, where $E := F(\zeta_p)$. The Brauer group can be computed explicitly, and we develop heuristics for the class groups; combining these gives the conjectural distribution of $K_{2n}(\mathcal{O}_F)_p$.

In the case $p = 3$, the isotypic components of $\mathrm{Cl}(\mathcal{O}_E[1/p])$ are related to $\mathrm{Cl}(\mathcal{O}_K[1/p])$ for quadratic fields K. The *average order* of the latter class groups can be computed unconditionally by using a strategy of Davenport and Heilbronn, which we refine using recent work of Bhargava, Shankar, and Tsimerman, to control averages in subfamilies with prescribed local behavior at 3. This yields unconditional results on the average order of $K_{2n}(\mathcal{O}_F)_3$.

1.2. **Prior work.** As far as we know, Cohen–Lenstra style conjectures have not been proposed for K-groups before, but some results on the distribution of $K_2(\mathcal{O}_F)$ have been proved.

Guo [Guo09] proved that 4-ranks of $K_2(\mathcal{O}_F)$ for quadratic fields F follow a Cohen–Lenstra distribution, just as Fouvry and Klüners proved for 4-ranks of $\mathrm{Cl}(\mathcal{O}_F)$ [FK07]. Studying 4-ranks is natural, since the 2-rank of $K_2(\mathcal{O}_F)$ for a quadratic field F is determined by genus theory just as the 2-rank of $\mathrm{Cl}(\mathcal{O}_F)$ is (see [BS82], for example).

Similar results on the 3-ranks of $K_2(\mathcal{O}_F)$ for cyclic cubic fields are due to Cheng, Guo, and Qin [CGQ14]. In addition, Browkin showed that Cohen–Martinet heuristics suggest a conjecture on $\mathrm{Prob}(3 \mid \#K_2(\mathcal{O}_F))$ as F ranges over quadratic fields of fixed signature [Bro00].

1.3. **Notation.** If G is an abelian group and $n \geq 1$, let $G_n := \{g \in G : ng = 0\}$ and $G/n := G/nG$. For any k-representation V of a finite group G such that $\mathrm{char}\, k \nmid \#G$, and for any irreducible k-representation χ of G, let V^χ be the χ-isotypic component.

Let F be a field of characteristic 0. Let $\overline{F}$ be an algebraic closure. Let $\mu(F)$ be the group of roots of unity in F. For each prime p, let ζ_p be a primitive pth root of 1 in $\overline{F}$. If $\mathcal{O}$ is a Dedekind ring, let $\mathrm{Cl}(\mathcal{O})$ denote its class group, and let $\mathrm{Br}(\mathcal{O})$ be its Brauer group.

Let F be a number field. Then let $\mathcal{O}_F$ be its ring of integers. Also, if S is a finite set of places of F containing all the archimedean places, define the ring of S-integers $\mathcal{O}_S := \{x \in F : v(x) \geq 0 \text{ for all } v \notin S\}$. Let $d_F \in \mathbb{Z}$ be the discriminant of F.

2. From K-theory to class groups and Brauer groups

In this section, following Tate's argument for K_2 [Tat76], we relate the even K-groups to more concrete groups: class groups and Brauer groups. From now on, p is an odd prime.

Theorem 2.1 (Corollary 71 in [Wei05])**.** *For $n \geq 1$,*

$$K_{2n}(\mathcal{O}_F)/p \simeq H^2_{\text{ét}}(\mathcal{O}_F[1/p], \mu_p^{\otimes(n+1)}).$$

From now on, all cohomology is étale cohomology, and we drop the subscript ét.

Lemma 2.2. *For any number field F, there is a canonical exact sequence*

$$0 \longrightarrow \mathrm{Cl}(\mathcal{O}_F[1/p])/p \longrightarrow H^2(\mathcal{O}_F[1/p], \mu_p) \longrightarrow \mathrm{Br}(\mathcal{O}_F[1/p])_p \longrightarrow 0.$$

Proof. Consider the exact sequence

$$1 \to \mu_p \to \mathbb{G}_m \xrightarrow{p} \mathbb{G}_m \to 1$$

of sheaves on $(\mathrm{Spec}\, \mathcal{O}_F[1/p])_{\text{ét}}$. Take the associated long exact sequence of cohomology, and substitute $H^1(\mathcal{O}_F[1/p], \mathbb{G}_m) = \mathrm{Pic}(\mathcal{O}_F[1/p]) = \mathrm{Cl}(\mathcal{O}_F[1/p])$ and $H^2(\mathcal{O}_F[1/p], \mathbb{G}_m) = \mathrm{Br}(\mathcal{O}_F[1/p])$. □

Lemma 2.3. *Let E/F be a finite Galois extension of degree prime to p. Let $i \geq 0$ and $r \in \mathbb{Z}$. Then*

$$H^i(\mathcal{O}_F[1/p], \mu_p^{\otimes r}) = H^i(\mathcal{O}_E[1/p], \mu_p^{\otimes r})^{\mathrm{Gal}(E/F)}.$$

Proof. In the Hochschild–Serre spectral sequence

$$H^i(\mathrm{Gal}(E/F), H^j(\mathcal{O}_E[1/p], \mu_p^{\otimes r})) \implies H^{i+j}(\mathcal{O}_F[1/p], \mu_p^{\otimes r}),$$

the groups $H^i(\mathrm{Gal}(E/F), H^j(\mathcal{O}_E[1/p], \mu_p^{\otimes r}))$ for $i > 0$ are 0 because they are killed by both $\#\,\mathrm{Gal}(E/F)$ and p. □

In the rest of Sections 2, 3, and 4, $E = F(\zeta_p)$. The action of $\mathrm{Gal}(E/F)$ on the pth roots of 1 defines an injective homomorphism $\chi_1 \colon \mathrm{Gal}(E/F) \to (\mathbb{Z}/p\mathbb{Z})^\times$. For $m \in \mathbb{Z}$, composing χ_1 with the mth power map on $(\mathbb{Z}/p\mathbb{Z})^\times$ yields another 1-dimensional $\mathbb{F}_p$-representation of $\mathrm{Gal}(E/F)$; call it χ_m.

Lemma 2.4. *There is a split exact sequence*

$$0 \to (\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^{\chi_{-n}} \to H^2(\mathcal{O}_F[1/p], \mu_p^{\otimes(n+1)}) \to (\mathrm{Br}(\mathcal{O}_E[1/p])_p)^{\chi_{-n}} \to 0.$$

Proof. First, we have

$$\begin{aligned} H^2(\mathcal{O}_F[1/p], \mu_p^{\otimes(n+1)}) &= H^2(\mathcal{O}_E[1/p], \mu_p^{\otimes(n+1)})^{\mathrm{Gal}(E/F)} \quad \text{(Lemma 2.3)} \\ &= \left(H^2(\mathcal{O}_E[1/p], \mu_p) \otimes \mu_p^{\otimes n}\right)^{\mathrm{Gal}(E/F)} \quad \text{(since } \mu_p \subset E\text{)} \\ &= H^2(\mathcal{O}_E[1/p], \mu_p)^{\chi_{-n}} \quad \text{(since } \mu_p^{\otimes n} \simeq \chi_n\text{).} \end{aligned} \tag{1}$$

On the other hand, Lemma 2.2 for E yields a sequence of $\mathrm{Gal}(E/F)$-representations

$$0 \longrightarrow \mathrm{Cl}(\mathcal{O}_E[1/p])/p \longrightarrow H^2(\mathcal{O}_E[1/p], \mu_p) \longrightarrow \mathrm{Br}(\mathcal{O}_E[1/p])_p \longrightarrow 0,$$

which splits by Maschke's theorem. Take χ_{-n}-isotypic components, and substitute (1) in the middle. □

Substituting Theorem 2.1 into Lemma 2.4 yields the main result of this section:

Theorem 2.5. *For each $n \geq 1$,*

$$K_{2n}(\mathcal{O}_F)/p \simeq (\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^{\chi_{-n}} \oplus (\mathrm{Br}(\mathcal{O}_E[1/p])_p)^{\chi_{-n}}.$$

3. Even K-groups of the ring of integers of a quadratic field

Let $p^* = (-1)^{(p-1)/2}p$, so $\mathbb{Q}(\sqrt{p^*})$ is the degree 2 subfield of $\mathbb{Q}(\zeta_p)$. In the rest of Sections 3 and 4, F is a degree 2 extension of $\mathbb{Q}$ not equal to $\mathbb{Q}(\sqrt{p^*})$. Thus $F = \mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Q}^\times$ such that d and p^* are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Then

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \{\pm 1\}.$$

Let τ be the generator of $\mathrm{Gal}(E/\mathbb{Q}(\zeta_p)) = \{\pm 1\}$, so τ restricts to the generator of $\mathrm{Gal}(F/\mathbb{Q})$. The action of τ decomposes $K_{2n}(\mathcal{O}_F)/p$ into $+$ and $-$ eigenspaces. Let $\chi_{-n,-1}\colon G \to \mathbb{F}_p^\times$ be such that $\chi_{-n,-1}|_{\mathrm{Gal}(E/F)} = \chi_{-n}$ and $\chi_{-n,-1}(\tau) = -1$.

Theorem 3.1. *For each $n \geq 1$,*

$$\begin{aligned} (K_{2n}(\mathcal{O}_F)/p)^+ &\simeq K_{2n}(\mathbb{Z})/p \\ (K_{2n}(\mathcal{O}_F)/p)^- &\simeq (\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^{\chi_{-n,-1}} \oplus (\mathrm{Br}(\mathcal{O}_E[1/p])_p)^{\chi_{-n,-1}}. \end{aligned}$$

Proof. To obtain the first statement, use Theorem 2.1 to rewrite each term as an étale cohomology group and apply Lemma 2.3 with E/F there being $F/\mathbb{Q}$. To obtain the second, take minus parts in Theorem 2.5. □

4. Brauer groups

The goal of this section is to determine the rightmost term in Theorem 3.1 when $F = \mathbb{Q}(\sqrt{d})$ with d and p^* independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

Lemma 4.1 (Equation (5.6) in [Wei05])**.** *Let F and $\mathcal{O}_S$ be as in Section 1.3. Let r_1 be the number of real places of F. Then there is an exact sequence*

$$0 \longrightarrow \mathrm{Br}\,\mathcal{O}_S \longrightarrow \left(\tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\right)^{r_1} \oplus \bigoplus_{\text{finite } v \in S} \mathbb{Q}/\mathbb{Z} \xrightarrow{\text{sum}} \mathbb{Q}/\mathbb{Z}.$$

Corollary 4.2. *Let $\mathcal{O}_S$ be as in Section 1.3. Then $\mathrm{Br}(\mathcal{O}_S)_p \simeq (\mathbb{Z}/p\mathbb{Z})^{\{\text{finite } v \in S\}}_{\text{sum } 0}$, where the "sum 0" subscript denotes the subgroup of elements whose sum is 0.*

Corollary 4.3. *We have $\mathrm{Br}(\mathbb{Z}[\zeta_p, 1/p])_p = 0$.*

Proof. There is only one prime above p in $\mathbb{Z}[\zeta_p]$. □

Proposition 4.4. *Suppose that $F = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Q}^\times$ is such that d and p^* are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Then*

$$(\mathrm{Br}(\mathcal{O}_E[1/p])_p)^{\chi^{-n,-1}} = \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{if } n \equiv 0 \pmod{p-1} \text{ and } d \in \mathbb{Q}_p^{\times 2}; \\ \mathbb{Z}/p\mathbb{Z}, & \text{if } n \equiv \dfrac{p-1}{2} \pmod{p-1} \text{ and } p^*d \in \mathbb{Q}_p^{\times 2}; \\ 0, & \text{in all other cases.} \end{cases}$$

Proof. The hypothesis implies that F is not the quadratic subfield $\mathbb{Q}(\sqrt{p^*})$ of $\mathbb{Q}(\zeta_p)$. Thus E is the compositum of linearly disjoint extensions $\mathbb{Q}(\zeta_p)$ and F over $\mathbb{Q}$, and $\mathrm{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \{\pm 1\}$. Let $\mathfrak{p}$ be a prime of E lying above p. Let $D \leq \mathrm{Gal}(E/\mathbb{Q})$ be the decomposition group of $\mathfrak{p}$. Since p totally ramifies in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, we have $p-1 \mid \#D$. Let S_p be the set of primes of E lying above p, so $S_p \simeq \mathrm{Gal}(E/\mathbb{Q})/D$, which by the previous sentence is of size 1 or 2; it is 2 if and only if p splits in one of the quadratic subfields of E. These quadratic subfields are $\mathbb{Q}(\sqrt{p^*})$, F, and the field $F' = \mathbb{Q}(\sqrt{p^*d})$, but p is ramified in $\mathbb{Q}(\sqrt{p^*})$. Thus by Corollary 4.2,

$$\mathrm{Br}(\mathcal{O}_E[1/p])_p = (\mathbb{Z}/p\mathbb{Z})^{S_p}_{\text{sum } 0} = \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{if } p \text{ splits in } F \text{ or } F'; \\ 0, & \text{otherwise} \end{cases}$$

as an abelian group, and it remains to determine in the first case which character it is isomorphic to. We will compute the action of $\mathrm{Gal}(E/F) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\mathrm{Gal}(E/\mathbb{Q}(\zeta_p)) \simeq \{\pm 1\}$ separately.

If p splits in F (that is, $d \in \mathbb{Q}_p^{\times 2}$), then $D = \mathrm{Gal}(E/F)$, which acts trivially on $S_p \simeq \mathrm{Gal}(E/\mathbb{Q})/D$, so $\mathrm{Gal}(E/F)$ acts on $\mathrm{Br}(\mathcal{O}_E[1/p])_p$ as the trivial character χ_0. If instead p splits in F' (that is, $p^*d \in \mathbb{Q}_p^{\times 2}$), then $D \neq \mathrm{Gal}(E/F)$, so $\mathrm{Gal}(E/F)$ acts nontrivially on the two-element set $S_p \simeq \mathrm{Gal}(E/\mathbb{Q})/D$, so $\mathrm{Gal}(E/F)$ acts on $\mathrm{Br}(\mathcal{O}_E[1/p])_p$ as the character $\mathrm{Gal}(E/F) \twoheadrightarrow \{\pm 1\}$, which is $\chi_{(p-1)/2}$.

Finally, consider the action of the generator τ of $\mathrm{Gal}(E/\mathbb{Q}(\zeta_p)) \simeq \{\pm 1\}$ on $\mathrm{Br}(\mathcal{O}_E[1/p])_p$. Lemma 2.3 shows that the $+$ eigenspace is $\mathrm{Br}(\mathbb{Z}[\zeta_p, 1/p])_p$, which is 0 by Corollary 4.3. Thus $\mathrm{Br}(\mathcal{O}_E[1/p])_p$ equals its $-$ eigenspace. □

Remark 4.5. Let d be a fundamental discriminant. Then $d \in \mathbb{Q}_p^{\times 2}$ if and only if $\left(\frac{d}{p}\right) = 1$, and $p^*d \in \mathbb{Q}_p^{\times 2}$ if and only if $p|d$ and $\left(\frac{-d/p}{p}\right) = 1$.

5. Even K-groups of $\mathbb{Z}$

Theorem 5.1. *For each $n \geq 1$,*

$$K_{2n}(\mathbb{Z})/p \simeq (\mathrm{Cl}(\mathbb{Z}[\zeta_p])/p)^{\chi^{-n}}.$$

Proof. In Theorem 2.5 for $F = \mathbb{Q}$, the Brauer term is 0 by Corollary 4.3, and $\mathrm{Cl}(\mathbb{Z}[\zeta_p, 1/p]) = \mathrm{Cl}(\mathbb{Z}[\zeta_p])$ since the unique prime ideal above p in $\mathbb{Z}[\zeta_p]$ is principal. □

For $n \geq 1$, let

$$\kappa_{2n,p} := \dim_{\mathbb{F}_p} K_{2n}(\mathbb{Z})/p = \dim_{\mathbb{F}_p} (\mathrm{Cl}(\mathbb{Z}[\zeta_p])/p)^{\chi^{-n}}.$$

Remark 5.2. Assuming Vandiver's conjecture that $p \nmid \#\mathrm{Cl}(\mathbb{Z}[\zeta_p + \zeta_p^{-1}])$ for every prime p, the K-groups of $\mathbb{Z}$ are known; see [Wei05, Section 5.9]. To state the results for even K-groups, let $B_k \in \mathbb{Q}$ be the kth Bernoulli number, and let c_k be the numerator of $B_k/(4k)$. Then

- Vandiver's conjecture implies that $K_{4k}(\mathbb{Z}) = 0$ for all $k \geq 1$.
- For $k \geq 1$, the order of $K_{4k-2}(\mathbb{Z})$ is c_k if k is odd, and $2c_k$ if k is even; moreover, Vandiver's conjecture implies that $K_{4k-2}(\mathbb{Z})$ is cyclic.

In fact, for each prime p, Vandiver's conjecture for p implies the conclusions above for the p-primary part of the K-groups. Thus Vandiver's conjecture for an odd prime p implies that for any $n \geq 1$,

$$\kappa_{2n,p} = \begin{cases} 1 & \text{if } n = 2k-1 \text{ and } p|c_k; \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, Vandiver's conjecture is known for $p < 163577856$ [BH11].

Assuming that $K_{4k}(\mathbb{Z}) = 0$ for all $k \geq 1$, the smallest n such that $\#K_{2n}(\mathbb{Z})$ is divisible by an odd prime is $n = 11$: we have $K_{22}(\mathbb{Z}) \simeq \mathbb{Z}/691\mathbb{Z}$. The smallest odd prime p for which there exists n such that $p|\#K_{2n}(\mathbb{Z})$ is 37, which divides $\#K_{2n}(\mathbb{Z})$ if and only if $n \equiv 31 \pmod{36}$; thus $\kappa_{2n,37}$ is 1 if $n \equiv 31 \pmod{36}$, and 0 otherwise. See [Wei05, Example 96] for these and other examples.

6. Odd K-groups

Proposition 6.1. *For any number field F, positive integer i, and prime p, we have*

$$K_{2i-1}(\mathcal{O}_F)_p = \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{if } [F(\zeta_p) : F] \text{ divides } i; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Define the group

$$\mu^{(i)}(F) := \{\zeta \in \mu(\overline{F}) : \sigma^i \zeta = \zeta \text{ for all } \sigma \in \mathrm{Gal}(\overline{F}/F)\}.$$

For $n \geq 1$, let $\zeta_n \in \overline{F}$ be a primitive nth root of 1, and let H_n be the image of the restriction homomorphism $\mathrm{Gal}(F(\zeta_n)/F) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, so $\#H_n = [F(\zeta_n) : F]$. Then the following are equivalent:

- $\zeta_n \in \mu^{(i)}(F)$;
- $\sigma^i \zeta_n \equiv \zeta_n$ for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$;
- $a^i = 1$ for all $a \in H_n$.

Now suppose that n is a prime power p^e. Then H_n contains a cyclic subgroup of index at most 2. The last condition above implies $\#H_n|2i$, which after multiplication by $[F : \mathbb{Q}]$ becomes the statement that $[F(\zeta_n) : \mathbb{Q}]$ divides $2i[F : \mathbb{Q}]$, which implies that the integer $\phi(n) := [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ divides $2i[F : \mathbb{Q}]$, which bounds $\phi(n)$ and hence n. Thus $\mu^{(i)}(F)$ contains p^eth roots of 1 for only finitely many prime powers p^e, so it is finite. Define $w^{(i)}(F) := \#\mu^{(i)}(F)$.

By Theorem 70 in [Wei05], $K_{2i-1}(\mathcal{O}_F)_p$ is $\mathbb{Z}/p\mathbb{Z}$ or 0, according to whether p divides $w^{(i)}(F)$ or not. The previous paragraph shows that the latter condition is equivalent to H_p being killed by i, and to $\#H_p|i$ since H_p is cyclic (a subgroup of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$). Finally, $\#H_p = [F(\zeta_p) : F]$. □

7. Heuristics for class groups

Let E be an abelian extension of $\mathbb{Q}$. Suppose that the Galois group $G := \mathrm{Gal}(E/\mathbb{Q})$ is of exponent dividing $p-1$. Let I_E^p be the group of fractional ideals of $\mathcal{O}_E[1/p]$, that is, the free abelian group on the set of finite primes of E not lying above p. We have the standard exact sequence of $\mathbb{Z}G$-modules

$$1 \to \mathcal{O}_E[1/p]^\times \to E^\times \to I_E^p \to \mathrm{Cl}(\mathcal{O}_E[1/p]) \to 0. \tag{2}$$

Let S be a finite set of places of $\mathbb{Q}$ including p and ∞. Let S_E be the set of places of E above S. We approximate (2) by using only S_E-units and ideals supported on S_E. Let S_E^p be the set of places of E above $S - \{p\}$. Let $\mathcal{O}_{E,S}$ be the ring of S_E-integers in E. Let $I_{E,S}^p$ be the free abelian group on the nonarchimedean places in S_E^p. If S is large enough that the finite primes in S_E^p generate $\mathrm{Cl}(\mathcal{O}_E[1/p])$, then we have an exact sequence of $\mathbb{Z}G$-modules

$$1 \to \mathcal{O}_E[1/p]^\times \to \mathcal{O}_{E,S}^\times \to I_{E,S}^p \to \mathrm{Cl}(\mathcal{O}_E[1/p]) \to 0. \tag{3}$$

Dropping the first term and tensoring with $\mathbb{F}_p$ yields an exact sequence of $\mathbb{F}_pG$-modules

$$\mathcal{O}_{E,S}^\times/p \to I_{E,S}^p/p \to \mathrm{Cl}(\mathcal{O}_E[1/p])/p \to 0.$$

Let χ be an irreducible $\mathbb{F}_p$-representation of G such that $\mu_p(E)^\chi = 0$; our assumption on G guarantees that χ is 1-dimensional. Taking χ-isotypic components yields

$$\left(\mathcal{O}_{E,S}^\times/p\right)^\chi \to \left(I_{E,S}^p/p\right)^\chi \to (\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi \to 0. \tag{4}$$

Let $u := \dim_{\mathbb{F}_p} (\mathcal{O}_E[1/p]^\times/p)^\chi$.

Lemma 7.1.

(a) *Let S_∞ (resp. S_p) be the set of places of E lying above ∞ (resp. p). Then*

$$u = \dim_{\mathbb{F}_p}(\mathbb{F}_p^{S_\infty})^\chi + \dim_{\mathbb{F}_p}(\mathbb{F}_p^{S_p})^\chi - \begin{cases} 1, & \text{if } \chi = 1; \\ 0, & \text{otherwise.} \end{cases}$$

(b) *We have*

$$\dim_{\mathbb{F}_p} \left(\mathcal{O}_{E,S}^\times/p\right)^\chi = \dim_{\mathbb{F}_p} \left(I_{E,S}^p/p\right)^\chi + u$$

(c) *The quantity $\dim_{\mathbb{F}_p} \left(I_{E,S}^p/p\right)^\chi$ can be made arbitrarily large by choosing S appropriately.*

Proof.

(a) The Dirichlet S-unit theorem implies that the abelian group $\mathcal{O}_E[1/p]^\times$ is finitely generated with torsion subgroup $\mu(E)$. Let M be the $\mathbb{Z}G$-module $\mathcal{O}_E[1/p]^\times/\mu(E)$. Tensoring the exact sequence

$$\mu(E) \longrightarrow \mathcal{O}_E[1/p]^\times \longrightarrow M \longrightarrow 0$$

with $\mathbb{F}_p$ and taking χ-isotypic components yields

$$0 \longrightarrow \left(\mathcal{O}_E[1/p]^\times/p\right)^\chi \longrightarrow (M/p)^\chi \longrightarrow 0,$$

so $u = \dim_{\mathbb{F}_p}(M/p)^\chi$.

On the other hand, the proof of the Dirichlet S-unit theorem yields

$$M \otimes \mathbb{R} \simeq \mathcal{O}_E[1/p]^\times \otimes \mathbb{R} \simeq \left(\mathbb{R}^{S_\infty \cup S_p}\right)_{\text{sum } 0}$$

as $\mathbb{R}G$-modules. A $\mathbb{Z}_{(p)}G$-module that is free of finite rank over $\mathbb{Z}_{(p)}$ is determined by its character, so

$$M \otimes \mathbb{Z}_{(p)} \simeq \left(\mathbb{Z}_{(p)}^{S_\infty \cup S_p}\right)_{\text{sum } 0}$$

as $\mathbb{Z}_{(p)}G$-modules. Both sides are free over $\mathbb{Z}_{(p)}$, so we may tensor with $\mathbb{F}_p$ to obtain

$$M/p \simeq \left(\mathbb{F}_p^{S_\infty \cup S_p}\right)_{\text{sum } 0}$$

as $\mathbb{F}_pG$-modules. In other words, there is an exact sequence

$$0 \longrightarrow M/p \longrightarrow \mathbb{F}_p^{S_\infty} \oplus \mathbb{F}_p^{S_p} \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Taking dimensions of the χ-components yields the formula for u.

(b) The composition $G \xrightarrow{\chi} (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_p^\times$ lets us identify χ with a $\mathbb{Z}_p$-representation of G. Tensor (3) with $\mathbb{Z}_p$, and take χ-isotypic components:

$$0 \to \left(\mathcal{O}_E[1/p]^\times \otimes \mathbb{Z}_p\right)^\chi \to \left(\mathcal{O}_{E,S}^\times \otimes \mathbb{Z}_p\right)^\chi \to \left(I_{E,S}^p \otimes \mathbb{Z}_p\right)^\chi \to (\mathrm{Cl}(\mathcal{O}_E[1/p]) \otimes \mathbb{Z}_p)^\chi \to 0.$$

Since $\mu_p(E)^\chi = 0$, the first three $\mathbb{Z}_p$-modules are free; on the other hand, the last is finite as a set. Take $\mathbb{Z}_p$-ranks. If V is a $\mathbb{Z}_pG$-module such that V^χ is a free $\mathbb{Z}_p$-module of finite rank, then $\dim_{\mathbb{F}_p}(V/p)^\chi = \mathrm{rank}_{\mathbb{Z}_p} V^\chi$. This proves the formula.

(c) If S contains m rational primes that split completely in E, then $I_{E,S}^p$ contains $(\mathbb{Z}G)^m$, so $\dim_{\mathbb{F}_p}\left(I_{E,S}^p/p\right)^\chi \geq m$, and m can be chosen arbitrarily large. □

Sequence (4) and Lemma 7.1(b,c) imply that $(\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi$ is naturally the cokernel of a linear map $\mathbb{F}_p^{m+u} \to \mathbb{F}_p^m$ for arbitrarily large m. Our heuristic will be that the distribution of this cokernel is the limiting distribution of a *random* linear map $\mathbb{F}_p^{m+u} \to \mathbb{F}_p^m$ as $m \to \infty$. This limiting distribution and the limiting expected size of the cokernel are known:

Proposition 7.2. *Fix a prime p and an integer $u \geq 0$. For $m \geq 0$, let A be a linear map $\mathbb{F}_p^{m+u} \to \mathbb{F}_p^m$ chosen uniformly at random, and let $\mathcal{A}_{p,u,m}$ be the random variable* $\dim_{\mathbb{F}_p} \mathrm{coker}(A)$. *Then*

(a) *For each $r \geq 0$,*

$$\lim_{m\to\infty} \mathrm{Prob}(\mathcal{A}_{p,u,m} = r) \;=\; \alpha_{p,u,r} := \frac{\prod_{i=r+1}^{\infty}(1-p^{-i})}{p^{r(u+r)}\prod_{i=1}^{r+u}(1-p^{-i})}.$$

(b) *We have $\sum_{r=0}^{\infty} \alpha_{p,u,r} = 1$.*

(c) *We have $\sum_{r=0}^{\infty} p^r \alpha_{p,u,r} = 1 + p^{-u}$.*

Proof.

(a) This is [KL75, Theorem 1].

(b) This is the $q = 1/p$ and $\alpha = 0$ case of [CL84, Corollary 6.7].

(c) This is the $q = 1/p$ and $\alpha = 1$ case of [CL84, Corollary 6.7]. □

Remark 7.3. The constant $\alpha_{p,u,r}$ appeared also in [CL84, Theorem 6.3], as the u-probability that a random finite abelian p-group has p-rank r. The connection between u-probabilities and coranks of random matrices was made in [FW89].

8. Heuristics for class groups and even K-groups associated to quadratic fields

8.1. **Distribution.** We now specialize Section 7 to the setting of Section 3. For the rest of this paper, F is $\mathbb{Q}(\sqrt{d})$ for a fundamental discriminant $d = d_F$ such that d and p^* are independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, and $E = F(\zeta_p)$, and $\chi = \chi_{-n,-1}$.

Proposition 8.1. *The value of u for $(\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi$ is given by the following table:*

		$d>0$	$d<0$
n even	$n \equiv 0 \pmod{p-1}$, $d \in \mathbb{Q}_p^{\times 2}$	2	1
	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	2	1
	all other cases	1	0
n odd	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	1	2
	all other cases	0	1

Proof. Apply Lemma 7.1(a) with $\chi = \chi_{-n,-1}$. The complex conjugation in $\mathrm{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \{\pm 1\}$ is $c := (-1, \pm 1)$, where the ± 1 is $+1$ if F is real, and -1 if F is imaginary. The G-set S_∞ is isomorphic to $G/\langle c\rangle$, so $\mathbb{F}_p^{S_\infty}$ is the c-invariant subrepresentation of the regular representation $\mathbb{F}_pG$. The multiplicity of χ in $\mathbb{F}_pG$ is 1, so the multiplicity of χ in $\mathbb{F}_p^{S_\infty}$ is 1 or 0, according to whether $\chi(c)$ is 1 or -1. By definition of $\chi_{-n,-1}$, we have $\chi(c) = (-1)^{-n}\operatorname{sgn}(d)$, so

$$\dim_{\mathbb{F}_p}\left(\mathbb{F}_p^{S_\infty}\right)^\chi = \begin{cases} 1, & \text{if } (-1)^n d > 0; \\ 0, & \text{if } (-1)^n d < 0. \end{cases}$$

Next, Corollary 4.2 implies

$$\dim_{\mathbb{F}_p}\left(\mathbb{F}_p^{S_p}\right)^\chi = \dim_{\mathbb{F}_p}(\mathrm{Br}(\mathcal{O}_E[1/p])_p)^\chi,$$

which is given by Proposition 4.4. The third term in Lemma 7.1(a) is 0 since $\chi \neq 1$. □

Suppose that $\mathscr{F}$ is a family of quadratic fields ordered by discriminant. For a function $\gamma\colon \mathscr{F} \to \mathbb{Z}_{\geq 0}$ and a $\mathbb{Z}_{\geq 0}$-valued random variable X, we say that the distribution of $\gamma(F)$ for $F \in \mathscr{F}$ is X if the distribution of $\gamma(F)$ for the $F \in \mathscr{F}$ with $|d| \leq b$ tends as $b \to \infty$ to the distribution of values of X. Define the average value of $\gamma(F)$ for $F \in \mathscr{F}$ similarly.

Proposition 8.1 combined with the reasoning of Section 7 (Proposition 7.2(a), in particular) suggests the following statement:

Conjecture 8.2 (Distribution of class group components)**.** *Fix one of the ten boxes (below and right of the double lines) in the following table, and fix a corresponding $n \geq 1$. Also fix an odd prime p and $r \geq 0$. As F ranges over the quadratic fields $\mathbb{Q}(\sqrt{d})$ with d satisfying the conditions defining that box,* $\mathrm{Prob}\left(\dim_{\mathbb{F}_p}(\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi = r\right)$ *is as follows:*

		$d>0$	$d<0$
n even	$n \equiv 0 \pmod{p-1}$, $d \in \mathbb{Q}_p^{\times 2}$	$\alpha_{p,2,r}$	$\alpha_{p,1,r}$
	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	$\alpha_{p,2,r}$	$\alpha_{p,1,r}$
	all other cases	$\alpha_{p,1,r}$	$\alpha_{p,0,r}$
n odd	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	$\alpha_{p,1,r}$	$\alpha_{p,2,r}$
	all other cases	$\alpha_{p,0,r}$	$\alpha_{p,1,r}$

If Conjecture 8.2 holds, then substituting it and Proposition 4.4 (with Remark 4.5) into Theorem 3.1 yields the following:

Conjecture 8.3 (Distribution of K-groups modulo p in residue classes)**.** *Fix $n \geq 1$ and an odd prime p and $r \geq 0$. As F ranges over the quadratic fields $\mathbb{Q}(\sqrt{d})$ with d satisfying the conditions defining a box below,* $\mathrm{Prob}\left(\dim_{\mathbb{F}_p}(K_{2n}(\mathcal{O}_F)/p)^- = r\right)$ *is as follows:*

		$d>0$	$d<0$
n even	$n \equiv 0 \pmod{p-1}$, $d \in \mathbb{Q}_p^{\times 2}$	$\alpha_{p,2,r-1}$	$\alpha_{p,1,r-1}$
	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	$\alpha_{p,2,r-1}$	$\alpha_{p,1,r-1}$
	all other cases	$\alpha_{p,1,r}$	$\alpha_{p,0,r}$
n odd	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	$\alpha_{p,1,r-1}$	$\alpha_{p,2,r-1}$
	all other cases	$\alpha_{p,0,r}$	$\alpha_{p,1,r}$

To pass from the distribution of $\dim_{\mathbb{F}_p}(K_{2n}(\mathcal{O}_F)/p)^-$ *to that of* $\dim_{\mathbb{F}_p} K_{2n}(\mathcal{O}_F)/p$ *itself, add the constant* $\kappa_{2n,p} = \dim_{\mathbb{F}_p} K_{2n}(\mathbb{Z})_p$ *of Section 5.*

Finally, combining the various congruence conditions yields

Conjecture 8.4 (Distribution of K-groups modulo p; cf. Conjecture 1.1)**.** *Fix $n \geq 1$ and an odd prime p and $r \geq 0$. As F ranges over all real (resp. imaginary) quadratic fields,* $\mathrm{Prob}\left(\dim_{\mathbb{F}_p}(K_{2n}(\mathcal{O}_F)/p)^- = r\right)$ *is given in the following table by the entry in the row determined by n and column determined by the signature:*

		real	imaginary
n even	$n \equiv 0 \pmod{p-1}$	$\frac{1}{2}(\frac{p}{p+1}\alpha_{p,2,r-1} + \frac{p+2}{p+1}\alpha_{p,1,r})$	$\frac{1}{2}(\frac{p}{p+1}\alpha_{p,1,r-1} + \frac{p+2}{p+1}\alpha_{p,0,r})$
	$n \equiv \frac{p-1}{2} \pmod{p-1}$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,2,r-1} + \frac{2p+1}{p+1}\alpha_{p,1,r})$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,1,r-1} + \frac{2p+1}{p+1}\alpha_{p,0,r})$
	all other cases	$\alpha_{p,1,r}$	$\alpha_{p,0,r}$
n odd	$n \equiv \frac{p-1}{2} \pmod{p-1}$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,1,r-1} + \frac{2p+1}{p+1}\alpha_{p,0,r})$	$\frac{1}{2}(\frac{1}{p+1}\alpha_{p,2,r-1} + \frac{2p+1}{p+1}\alpha_{p,1,r})$
	all other cases	$\alpha_{p,0,r}$	$\alpha_{p,1,r}$.

To pass from the distribution of $\dim_{\mathbb{F}_p}(K_{2n}(\mathcal{O}_F)/p)^-$ *to that of* $\dim_{\mathbb{F}_p} K_{2n}(\mathcal{O}_F)/p$*, add* $\kappa_{2n,p}$*.*

8.2. **Average order.** Proposition 8.1 combined with the reasoning of Section 7 (Proposition 7.2(c), in particular) suggests the following statement:

Conjecture 8.5 (Average order of class group components in residue classes)**.** *Fix an odd prime p. The average order of* $(\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi$ *for F ranging over the quadratic fields $\mathbb{Q}(\sqrt{d})$ satisfying the conditions defining a box below is as follows:*

		$d>0$	$d<0$
n even	$n \equiv 0 \pmod{p-1}$, $d \in \mathbb{Q}_p^{\times 2}$	$1+p^{-2}$	$1+p^{-1}$
	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	$1+p^{-2}$	$1+p^{-1}$
	all other cases	$1+p^{-1}$	2
n odd	$n \equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d \in \mathbb{Q}_p^{\times 2}$	$1+p^{-1}$	$1+p^{-2}$
	all other cases	2	$1+p^{-1}$

Conjecture 8.5, in turn, would imply the following:

Conjecture 8.6 (Average order of K-groups modulo p in residue classes)**.** *Fix $n \geq 1$ and an odd prime p. The average order of* $(K_{2n}(\mathcal{O}_F)/p)^-$ *for F ranging over the quadratic fields $\mathbb{Q}(\sqrt{d})$ satisfying the conditions defining a box below is as follows:*

		$d>0$	$d<0$
n even	$n\equiv 0 \pmod{p-1}$, $d\in\mathbb{Q}_p^{\times 2}$	$p+p^{-1}$	$p+1$
	$n\equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d\in\mathbb{Q}_p^{\times 2}$	$p+p^{-1}$	$p+1$
	all other cases	$1+p^{-1}$	2
n odd	$n\equiv \frac{p-1}{2} \pmod{p-1}$, $p^*d\in\mathbb{Q}_p^{\times 2}$	$p+1$	$p+p^{-1}$
	all other cases	2	$1+p^{-1}$

To get the average order of $K_{2n}(\mathcal{O}_F)/p$ itself, multiply each entry by $p^{\kappa_{2n,p}}$.

If instead we average over all fundamental discriminants d of a fixed sign, we obtain the following:

Conjecture 8.7 (Average order of K-groups modulo p)**.** *Fix $n\geq 1$ and an odd prime p. The average order of $(K_{2n}(\mathcal{O}_F)/p)^-$ for F ranging over all real (resp. imaginary) quadratic fields is given in the following table by the entry in the row determined by n and column determined by the signature:*

		real	imaginary
n even	$n\equiv 0 \pmod{p-1}$	$\frac{p^3+p^2+4p+2}{2p^2+2p}$	$\frac{p^2+3p+4}{2p+2}$
	$n\equiv \frac{p-1}{2} \pmod{p-1}$	$\frac{3p^2+3p+2}{2p^2+2p}$	$\frac{5p+3}{2p+2}$
	all other cases	$\frac{p+1}{p}$	2
n odd	$n\equiv \frac{p-1}{2} \pmod{p-1}$	$\frac{5p+3}{2p+2}$	$\frac{3p^2+3p+2}{2p^2+2p}$
	all other cases	2	$\frac{p+1}{p}$

To get the distribution of the order of $K_{2n}(\mathcal{O}_F)/p$ itself, multiply each entry by $p^{\kappa_{2n,p}}$.

To deduce Conjecture 8.7 from Conjecture 8.6, we take a weighted average of averages. For instance, the first box in Conjecture 8.7 is obtained from the first and third boxes in the $d>0$ column of Conjecture 8.6. A fundamental discriminant d is equally likely to be in any of the p^2-1 congruence classes modulo p^2. Among these, we have $d\in\mathbb{Q}_p^{\times 2}$ if d mod p is one of the $(p-1)/2$ quadratic residues; this amounts to $p(p-1)/2$ congruence classes modulo p^2, so the proportion is $\frac{p(p-1)/2}{p^2-1}=\frac{p}{2p+2}$. This gives the weights, so the first box in Conjecture 8.7 is

$$\frac{p}{2p+2}(p+p^{-1})+\frac{p+2}{2p+2}(1+p^{-1})=\frac{p^3+p^2+4p+2}{2p^2+2p}.$$

Remark 8.8. It is not quite clear that Conjectures 8.2, 8.3, and 8.4, imply Conjectures 8.5, 8.6, and 8.7, respectively. For such implications, one would need to know that the contribution to each average from the rare cases of very large class groups or K-groups is negligible.

9. The average order of even K-groups modulo 3

In this section, we prove Conjecture 8.5 for $p=3$; then Conjectures 8.6 and 8.7 for $p=3$ follow too; the latter becomes Theorem 1.2. For $p=3$, the table in Conjecture 8.5 to be verified simplifies to

		$d>0$	$d<0$
n even	$d \in \mathbb{Q}_3^{\times 2}$	10/9	4/3
	$d \notin \mathbb{Q}_3^{\times 2}$	4/3	2
n odd	$-3d \in \mathbb{Q}_3^{\times 2}$	4/3	10/9
	$-3d \notin \mathbb{Q}_3^{\times 2}$	2	4/3

We have $G = \mathrm{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times \{\pm 1\}$. Let $H := \ker \chi$, which is generated by $(-1, (-1)^n)$. Let $K := E^H$, which is F if n is even, and F' if n is odd. For any $\mathbb{F}_p$-representation V of G, we have $V^H = V^G \oplus V^\chi$. Apply this to $V = \mathrm{Cl}(\mathcal{O}_E[1/p])/p$, and use Lemma 2.3 twice to obtain

$$\mathrm{Cl}(\mathcal{O}_K[1/p])/p \simeq \mathrm{Cl}(\mathbb{Z}[1/p])/p \oplus (\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi \simeq (\mathrm{Cl}(\mathcal{O}_E[1/p])/p)^\chi,$$

since $\mathrm{Cl}(\mathbb{Z}[1/p])$ is a quotient of $\mathrm{Cl}(\mathbb{Z}) = 0$. It remains to show that for each box, the average order of $\mathrm{Cl}(\mathcal{O}_K[1/p])/p$ is as given in the table above.

For fixed n, as d ranges over fundamental discriminants of fixed sign in a fixed coset of $\mathbb{Q}_p^{\times 2}$ up to some bound, the field K ranges over quadratic fields with fundamental discriminant of fixed sign in a fixed coset of $\mathbb{Q}_p^{\times 2}$ up to some bound (the same sign and coset if n is even, or sign and coset multiplied by -3 if n is odd). Thus it suffices to prove that the average order of $\mathrm{Cl}(\mathcal{O}_K[1/p])/p$ for such K is given by the table

	$d_K>0$	$d_K<0$
$d_K \in \mathbb{Q}_3^{\times 2}$	10/9	4/3
$d_K \notin \mathbb{Q}_3^{\times 2}$	4/3	2.

Remark 9.1. There are four cosets of $\mathbb{Q}_3^{\times 2}$ in $\mathbb{Q}_3^\times$. Which coset contains a given fundamental discriminant d_K is determined by whether d_K is 1 mod 3, 2 mod 3, 3 mod 9, or 6 mod 9. In particular, $d_K \in \mathbb{Q}_3^{\times 2}$ if and only if $d_K \equiv 1 \pmod 3$.

Remark 9.2. The results in Sections 9.1 to 9.3 have been generalized by the second author to compute the average size of $\mathrm{Cl}(\mathcal{O}_K[1/S])/3$ for an arbitrary finite set of primes S using essentially identical methods [Kla17a]. There is also unpublished work of Wood using similar methods to compute the average size of $\mathrm{Cl}(O_K[1/p])/3$ when p splits in K [Woo16].

9.1. **From class groups to cubic fields.** To compute the average order of $\mathrm{Cl}(\mathcal{O}_K[1/p])/p$, we adapt the strategy of Davenport and Heilbronn [DH71], which relies on the following:

Theorem 9.3 (cf. [Has30, Satz 7])**.** *Fix a quadratic field K. Then the following are naturally in bijection:*

(i) *The set of index 3 subgroups of $\mathrm{Cl}(\mathcal{O}_K)$.*
(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. Class field theory gives (i)↔(ii). The nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts as -1 on $\mathrm{Cl}(\mathcal{O}_K)$, so each M in (ii) is an S_3-extension of $\mathbb{Q}$. The map (ii)→(iii) sends M to one of its cubic subfields L. The map (iii)→(ii) sends L to its Galois closure M. To see that these are inverse bijections it suffices to show that M is unramified over K if and only if $d_L = d_K$. This follows from [Has30, Satz 3], which states that $d_L = N_{K/\mathbb{Q}}(\mathfrak{f}) d_K$, where $\mathfrak{f}$ is the conductor of M/K. □

We are interested in $\mathrm{Cl}(\mathcal{O}_K[1/3])$ instead of $\mathrm{Cl}(\mathcal{O}_K)$, so we need the following variant.

Corollary 9.4. *Fix a quadratic field K. Then the following are naturally in bijection:*

(i) *The set of index 3 subgroups of* $\mathrm{Cl}(\mathcal{O}_K)[1/3]$.

(ii) *The set of unramified $\mathbb{Z}/3\mathbb{Z}$-extensions M of K in which the primes above 3 in K split completely in M/K.*

(iii) *The set of isomorphism classes of cubic fields L with $d_L = d_K$ such that if $d_K \in \mathbb{Q}_3^{\times 2}$, then 3 splits completely in $L/\mathbb{Q}$.*

Proof. The group $\mathrm{Cl}(\mathcal{O}_K)[1/3]$ is the quotient of $\mathrm{Cl}(\mathcal{O}_K)$ by the group generated by the classes of the primes $\mathfrak{p}|3$ in K. Thus we need to restrict the bijections in Theorem 9.3 to the index 3 subgroups H containing these classes. Because the class field theory isomorphism $\mathrm{Cl}(\mathcal{O}_K)/H \simeq \mathrm{Gal}(M/K)$ sends $[\mathfrak{p}]$ to $\mathrm{Frob}_\mathfrak{p}$, which is trivial if and only if $\mathfrak{p}$ splits in M/K, we obtain (i)$\leftrightarrow$(ii). If 3 is inert or ramified in $K/\mathbb{Q}$, then the prime above 3 is of order dividing 2 in $\mathrm{Cl}(\mathcal{O}_K)$, so to require it to be in the index 3 subgroup is no condition. If 3 splits in $K/\mathbb{Q}$ (that is, $d_K \in \mathbb{Q}_3^{\times 2}$), then the primes above 3 in K split in M/K if and only if they split completely in $M/\mathbb{Q}$, which is if and only if they split in $L/\mathbb{Q}$. □

Corollary 9.5. *Let K be a quadratic field.*

(a) *If $d_K \in \mathbb{Q}_3^{\times 2}$, then*

$$\#\,\mathrm{Cl}(\mathcal{O}_K[1/3])/3 = 2\,\#\{\text{cubic fields } L \text{ with } d_L = d_K \text{ in which 3 splits}\} + 1.$$

(b) *If $d_K \notin \mathbb{Q}_3^{\times 2}$, then*

$$\#\,\mathrm{Cl}(\mathcal{O}_K[1/3])/3 = 2\,\#\{\text{cubic fields } L \text{ with } d_L = d_K\} + 1.$$

Proof. For an elementary abelian 3-group V,

$$\#V = 2\,\#\{\text{index 3 subgroups of } V\} + 1.$$

Take $V = \mathrm{Cl}(\mathcal{O}_K[1/3])/3$, and apply Corollary 9.4(i)$\leftrightarrow$(iii). □

9.2. **Counting quadratic fields.** To compute the average of each left hand side in Corollary 9.5, we compute the average number of cubic fields appearing in each right hand side. That is, we need the limit of

$$\frac{\#\{\text{cubic fields of bounded discriminant satisfying the conditions}\}}{\#\{\text{quadratic fields of bounded discriminant satisfying the conditions}\}}. \tag{5}$$

for each box in the table before Remark 9.1. We first compute the denominator.

Proposition 9.6. *The number of quadratic fields K satisfying $|d_K| < X$ and prescribed sign and 3-adic congruence conditions is $\alpha_2 X/\zeta(2) + o(X)$, where α_2 is given by the following table:*

	$d_K > 0$	$d_K < 0$
$d_K \equiv 1 \pmod 3$	3/16	3/16
$d_K \equiv 2 \pmod 3$	3/16	3/16
$d_K \equiv 3 \pmod 9$	1/16	1/16
$d_K \equiv 6 \pmod 9$	1/16	1/16

Proof. Use an elementary squarefree sieve. □

Remark 9.7. Even though many entries in the table of Proposition 9.6 coincide, it is stronger to give the asymptotics for the individual field families without merging them, and we need the stronger results.

9.3. **Counting cubic fields.** To compute the numerator in (5), we follow the Davenport–Heilbronn approach, in the form of a refinement due to Bhargava, Shankar, and Tsimerman [BST13].

For every prime p, let $\widehat{\Sigma}_p$ be the set of maximal cubic $\mathbb{Z}_p$-orders that are not totally ramified, up to isomorphism. For $R \in \widehat{\Sigma}_p$, let $\mathrm{Disc}_p(R)$ be the power of p generating the discriminant ideal of R.

Theorem 9.8. *For each prime p, let $\Sigma_p \subseteq \widehat{\Sigma}_p$. Suppose that $\Sigma_p = \widehat{\Sigma}_p$ for all p outside a finite set $\mathcal{P}$. Define*

$$c_p := \frac{p}{p+1} \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)\ |\mathrm{Aut}\, R|}.$$

(a) *The number of nowhere totally ramified totally real cubic fields L (up to isomorphism) such that $|d_L| < X$ and $\mathcal{O}_L \otimes \mathbb{Z}_p \in \Sigma_p$ for all $p \in \mathcal{P}$ is $\frac{1}{12\zeta(2)} \left(\prod_{p \in \mathcal{P}} c_p \right) X + o(X)$.*

(b) *The number of nowhere totally ramified complex cubic fields L (up to isomorphism) such that $|d_L| < X$ and $\mathcal{O}_L \otimes \mathbb{Z}_p \in \Sigma_p$ for all $p \in \mathcal{P}$ is $\frac{1}{4\zeta(2)} \left(\prod_{p \in \mathcal{P}} c_p \right) X + o(X)$.*

Proof. The definition of c_p yields

$$\frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\mathrm{Disc}_p(R)\ |\mathrm{Aut}\, R|} = \left(1 - \frac{1}{p^2}\right) c_p.$$

For each $p \notin \mathcal{P}$, enumerating $\widehat{\Sigma}_p$ explicitly shows that $c_p = 1$. Substituting this into [BST13, Theorem 8] yields the result. □

Corollary 9.9. *The number of nowhere totally ramified cubic fields L with $|d_L| < X$ satisfying prescribed sign and 3-adic congruence conditions below such that 3 splits completely in L if $d_L \equiv 1 \pmod 3$, is $\alpha_3 X/\zeta(2) + o(X)$, where α_3 is given by the following table:*

	$d_L > 0$	$d_L < 0$
$d_L \equiv 1 \pmod 3$	1/96	1/32
$d_L \equiv 2 \pmod 3$	1/32	3/32
$d_L \equiv 3 \pmod 9$	1/96	1/32
$d_L \equiv 6 \pmod 9$	1/96	1/32

Proof. We apply Theorem 9.8 with $\mathcal{P} = \{3\}$ and with Σ_3 tailored to the row. For the first row, let $\Sigma_3 := \{\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3\}$, so

$$c_3 = \frac{3}{4} \cdot \frac{1}{\mathrm{Disc}_p(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)\ |\mathrm{Aut}\,(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)|} = \frac{3}{4} \cdot \frac{1}{6} = \frac{1}{8}.$$

For each other row, let $\Sigma_3 := \{\mathbb{Z}_3 \times \mathbb{Z}_3(\sqrt{d_L})\}$, and calculate c_3 similarly. □

9.4. **End of proof.** Divide each entry in Corollary 9.9 by the corresponding entry in Proposition 9.6 to get the average number of cubic fields for the situation, α_3/α_2. Following Corollary 9.5, we multiply by 2 and add 1 to obtain the average order of $\mathrm{Cl}(\mathcal{O}_K[1/3])/3$. The results are as claimed in the table before Remark 9.1. This completes the proof of Conjecture 8.5 for $p = 3$, and hence also Conjectures 8.6 and 8.7 for $p = 3$ and Theorem 1.2.

References

[BKLPR15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra Jr., Bjorn Poonen, and Eric Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3** (2015), no. 3, 275–321. MR3393023

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499, DOI 10.1007/s00222-012-0433-0. MR3090184

[BBH14] Nigel Boston, Michael Bush, and Farshid Hajir, *Heuristics for p-class towers of imaginary quadratic functions fields*, December 10, 2014. With an appendix by Jonathan Blackhurst. Preprint, `arXiv:1111.4679v2`.

[Bro00] Jerzy Browkin, *Tame kernels of quadratic number fields: numerical heuristics*, Funct. Approx. Comment. Math. **28** (2000), 35–43. Dedicated to Włodzimierz Staś on the occasion of his 75th birthday. MR1823991

[BS82] J. Browkin and A. Schinzel, *On Sylow 2-subgroups of K_2O_F for quadratic number fields F*, J. Reine Angew. Math. **331** (1982), 104–113, DOI 10.1515/crll.1982.331.104. MR647375

[BH11] J. P. Buhler and D. Harvey, *Irregular primes to 163 million*, Math. Comp. **80** (2011), no. 276, 2435–2444. MR2813369

[CGQ14] XiaoYun Cheng, XueJun Guo, and HouRong Qin, *The densities for 3-ranks of tame kernels of cyclic cubic number fields*, Sci. China Math. **57** (2014), no. 1, 43–47, DOI 10.1007/s11425-013-4622-0. MR3146514

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082 (85j:11144)

[CM90] Henri Cohen and Jacques Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76 (French). MR1037430 (91k:11097)

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420. MR0491593 (58 #10816)

[Del01] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$*, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670 (2003a:11065)

[Del07] Christophe Delaunay, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340. MR2322355 (2008i:11089)

[DJ14] Christophe Delaunay and Frédéric Jouhet, *p^ℓ-torsion points in finite abelian groups and combinatorial identities*, Adv. Math. **258** (2014), 13–45, DOI 10.1016/j.aim.2014.02.033. MR3190422

[FK07] Étienne Fouvry and Jürgen Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), no. 3, 455–513, DOI 10.1007/s00222-006-0021-2. MR2276261 (2007k:11187)

[FW89] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239. MR1024565 (91e:11138)

[Guo09] Xuejun Guo, *On the 4-rank of tame kernels of quadratic number fields*, Acta Arith. **136** (2009), no. 2, 135–149, DOI 10.4064/aa136-2-3. MR2475682

[Has30] Helmut Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. **31** (1930), no. 1, 565–582, DOI 10.1007/BF01246435 (German). MR1545136

[Kla17a] Zev Klagsbrun, *Davenport–Heilbronn theorems for quotients of class groups*, June 26, 2017. Preprint, `arXiv:1701.02834v2` .

[Kla17b] Zev Klagsbrun, *The average sizes of two-torsion subgroups in quotients of class groups of cubic fields*, September 19, 2017. Preprint, `arXiv:1701.02838v3` .

[KL75] I. N. Kovalenko and A. A. Levitskaja, *Limiting behavior of the number of solutions of a system of random linear equations over a finite field and a finite ring*, Dokl. Akad. Nauk SSSR **221** (1975), no. 4, 778–781 (Russian). MR0380957

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483

[Tat76] John Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274. MR0429837 (55 #2847)

[Wei05] Charles Weibel, *Algebraic K-theory of rings of integers in local and global fields*, Handbook of K-theory. Vol. 1, 2, Springer, Berlin, 2005, pp. 139–190, DOI 10.1007/3-540-27855-9_5. MR2181823

[Woo16] Melanie Matchett Wood, *Cohen–Lenstra heuristics and local conditions*, June 24, 2016. Preprint, available at `https://www.math.wisc.edu/~mmwood/Publications/` .

Department of Mathematics, Baruch College, The City University of New York, One Bernard Baruch Way, New York, NY 10010-5526, USA
E-mail address: `bruce.jordan@baruch.cuny.edu`

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1969
E-mail address: `zevklagsbrun@gmail.com`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: `poonen@math.mit.edu`
URL: `http://math.mit.edu/~poonen/`

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA
E-mail address: `cmcls@princeton.edu`

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540-1966, USA
E-mail address: `ykzaytm@idaccr.org`