Wood *Res. Number Theory* (2018) 4:41
https://doi.org/10.1007/s40993-018-0134-x

Research in Number Theory

RESEARCH

Cohen-Lenstra heuristics and local conditions

Melanie Matchett Wood*

*Correspondence:
mmwood@math.wisc.edu
Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI 53705, USA

Abstract

We prove function field theorems supporting the Cohen–Lenstra heuristics for real quadratic fields, and natural strengthenings of these analogs from the affine class group to the Picard group of the associated curve. Our function field theorems also support a conjecture of Bhargava on how local conditions on the quadratic field do not affect the distribution of class groups. Our results lead us to make further conjectures refining the Cohen–Lenstra heuristics, including on the distribution of certain elements in class groups. We prove instances of these conjectures in the number field case. Our function field theorems use a homological stability result of Ellenberg, Venkatesh, and Westerland.

Keywords: Cohen-Lenstra heuristics, Local conditions, Function fields

1 Introduction

For any odd prime p, Cohen and Lenstra [13] conjectured the distribution of the Sylow p-subgroups of class groups of imaginary and real quadratic fields. In particular, if we consider the measure on finite abelian p-groups such that

$$\mu_{CL}(A) := \frac{1}{|\operatorname{Aut}(A)|}\prod_{i\geq 1}(1-p^{-i}),$$

they conjectured that this measure gives the distribution of the Sylow p-subgroups of class groups of imaginary quadratic fields. For real quadratic fields, we make a probability measure μ^r_{CL} on finite abelian p-groups by producing a random group as follows: pick a random group B with respect to μ_{CL}, then pick a (uniform) random element $b \in B$, and then form $B/\langle b\rangle$. Then $\mu^r_{CL}(A)$ is the probability that this process produces a group isomorphic to A. They then conjectured that μ^r_{CL} gives the distribution of the Sylow p-subgroups of class groups of real quadratic fields.

One of the most compelling reasons to believe this modification for the real quadratic case is by considering the function field analog. For a finite field $\mathbb{F}_q$ and an extension $K/\mathbb{F}_q(t)$, let $\mathcal{O}_K$ be the integral closure of $\mathbb{F}_q[t]$ in K and C_K be the smooth projective curve over $\mathbb{F}_q$ associated to K. When $K/\mathbb{F}_q(t)$ is imaginary quadratic (i.e. ramified over ∞), then $\operatorname{Cl}(\mathcal{O}_K) \simeq \operatorname{Pic}^0(C_K)$. However, when $K/\mathbb{F}_q(t)$ is real quadratic (i.e. ∞ splits into ∞_1, ∞_2), then $\operatorname{Cl}(\mathcal{O}_K) \simeq \operatorname{Pic}^0(C_K)/\langle \infty_1 - \infty_2\rangle$. The most direct analogy of the Cohen–Lenstra heuristics from the number field case to the function field case asks about the distribution of $\operatorname{Cl}(\mathcal{O}_K)$. However, in the real quadratic function field case, we can ask the richer question of the distribution of the Sylow p-subgroups of $\operatorname{Pic}^0(C_K)$ and of

$\infty_1 - \infty_2 \in \mathrm{Pic}^0(C_K)$. In this paper, we prove a theorem about the actual distribution for this richer question. Before stating these results, we will explain a natural heuristic that will predict what we obtain.

A *pointed abelian p-group* is a pair (A, a) where A is an abelian p-group and $a \in A$, and two pointed abelian p-groups (A, a) and (B, b) are isomorphic if there is an isomorphism $A \to B$ taking a to b. We put a measure μ on the set of isomorphism classes of pointed abelian p-groups as follows. Pick a random group B with respect to μ_{CL}, then pick a (uniform) random element $b \in B$. Then $\mu(A, a)$ is the probability that this process produces a pointed group isomorphic to (A, a). Our heuristic is that μ gives the distribution of $(\mathrm{Pic}^0(C_K), \infty_1 - \infty_2)$.

In the progress that has been made on proving exact Cohen–Lenstra predictions for class groups (e.g. [3,14,15,17,18]), the Cohen–Lenstra measures have often been accessed through their moments—moments that determine a unique distribution. So, we now turn to the moments of μ (see [11, Sect. 3.3] for an explanation of the terminology "moments" in this situation). We let $\mathrm{Sur}((B, b), (A, a))$ denote the surjective homomorphisms from B to A that take b to a. Let $\mathcal{A}_\bullet$ be a set with one representative from each isomorphism class of pointed finite abelian p-groups.

Lemma 1.1 (Pointed moments) *For any finite abelian p-group A and $a \in A$, we have*

$$\sum_{(B,b)\in\mathcal{A}_\bullet} |\mathrm{Sur}((B, b), (A, a))|\mu(B, b) = \frac{1}{|A|}.$$

We call this average $\sum_{(B,b)\in\mathcal{A}_\bullet} |\mathrm{Sur}((B, b), (A, a))|\mu(B, b)$ the (A, a)*-moment* of μ. In fact, these moments determine the measure μ.

Lemma 1.2 (Pointed moments determine distribution) *If ν is a measure on isomorphism classes finite abelian, pointed p-groups such that for all $(A, a) \in \mathcal{A}_\bullet$ we have*

$$\sum_{(B,b)\in\mathcal{A}_\bullet} |\mathrm{Sur}((B, b), (A, a))|\nu(B, b) = \frac{1}{|A|},$$

then $\nu = \mu$.

We prove the following, which gives evidence towards the Cohen–Lenstra heuristics over function fields as well as the refined heuristic above.

Theorem 1.3 *(*Pointed $\mathrm{Pic}^0(C_K)$ distribution*) Let A be a finite odd order abelian group, let $a \in A$, and let*

$$\delta_q^+ := \limsup_{m\to\infty} \frac{\sum_{K/\mathbb{F}_q(t) \textit{real quad}, \mathrm{Nm}\,\mathrm{Disc}(K)=q^{2m}} |\mathrm{Sur}((\mathrm{Pic}^0(C_K), \infty_1 - \infty_2), (A, a))|}{\sum_{K/\mathbb{F}_q(t) \textit{ real quad}, \mathrm{Nm}\,\mathrm{Disc}(K)=q^{2m}} 1}$$

and δ_q^- the corresponding $\liminf$. *Then as $q \to \infty$ among odd prime powers such that $(q(q-1), |A|) = 1$, we have*

$$\delta_q^+, \delta_q^- \to \frac{1}{|A|}.$$

The function field analog of our refined heuristic above predicts that for each odd prime power q with $(q(q-1), |A|) = 1$ that $\delta_q^\pm = |A|^{-1}$. In the case $a = 0$ we have the usual group-indexed moments of $\mathrm{Cl}(\mathcal{O}_K)$ (Corollary 4.6) and adding over a we have the usual group-indexed moments of $\mathrm{Pic}^0(C_K)$ (Corollary 4.5).

We prove Theorem 1.3 by first converting the problem of counting pointed surjections to a problem of counting extensions of $\mathbb{F}_q(t)$, which are parametrized by a Hurwitz scheme first defined Romagny and Wewers [24], and further studied by Ellenberg et al. [16]. We use the Grothendieck-Lefschetz trace formula to count $\mathbb{F}_q$ points on these schemes. This overall approach to the Cohen–Lenstra heuristics over function fields goes back to to unpublished work of J.-K. Yu, and was also built upon by Achter [1].

Ellenberg, Venkatesh, and Westerland made a tremendous breakthrough in this approach when they proved a homological stability theorem for the complex versions of these Hurwitz schemes [17]. Also, Ellenberg, Venkatesh, and Westerland's work on Hurwitz schemes relates their components to group theoretic invariants [16]. Both of these advances will go into the proof of Theorem 1.3. Ellenberg, Venkatesh, and Westerland [17] have proven the non-pointed analog of Theorem 1.3 (i.e., the analog of Corollary 4.5) for imaginary quadratic extensions, which was the motivation for their work on Hurwitz schemes.

In [13], Cohen and Lenstra actually give a conjecture for the entire odd part of the class groups of quadratic fields. In this paper, for simplicity we restrict ourselves to Sylow p-subgroups when explaining the heuristics, but give our theorems about class groups without this restriction. Note that all results support the heuristic that p_i-parts of class group behavior are independent at finite sets of primes p_i.

We prove a similar result (Theorem 5.1) for quadratic extensions of $\mathbb{F}_q(t)$ inert over ∞ for non-pointed moments. Combining these results with those of Ellenberg, Venkatesh, and Westerland, we come to the following conclusion. *Among all quadratic $K/\mathbb{F}_q(t)$ we have proven evidence that the Sylow p-subgroups of* $\mathrm{Pic}^0(C_K)$ *are distributed by μ_{CL}, and further that this distribution is unaffected by restricting to quadratic extensions with a certain behavior at ∞*. As long as we use $\mathrm{Pic}^0(C_K)$, as opposed to $\mathrm{Cl}(\mathcal{O}_K)$, we see there is no difference between the real and imaginary distributions. Indeed, this gives evidence for the following conjecture, which was made by Bhargava for number fields at the 2011 AIM Workshop on the Cohen–Lenstra heuristics and the subject of many days of discussion at the workshop. (For a number field K, let $\mathcal{O}_K$ denote its ring of integers. For a finite abelian group A, let A_{odd} denote its odd part.)

Conjecture 1.4 (Local conditions on K, c.f. [5]) In any of the following families, ordered by discriminant, with their class groups as given:

(1) $K/\mathbb{Q}$ imaginary quadratic, $\mathrm{Cl}(\mathcal{O}_K)_{odd}$
(2) $K/\mathbb{Q}$ real quadratic, $\mathrm{Cl}(\mathcal{O}_K)_{odd}$
(3) $K/\mathbb{F}_q(t)$ quadratic, $\mathrm{Pic}^0(C_K)_{odd}$

the distribution of the respective class groups is not changed upon restricting only those K that have specific completions at a finite set of nonarchimedian places (of $\mathbb{Q}$ or $\mathbb{F}_q(t)$). In particular, in (3) the Sylow p-subgroups are distributed by μ_{CL} when $p \nmid q(q-1)$.

By the action of $\mathrm{PGL}_2(\mathbb{F}_q)$ in Theorem 1.3, we could replace ∞ by any degree 1 point of C_K, and so we have evidence for Conjecture 1.4(3), for a condition at any degree 1 place.

The prediction of Conjecture 1.4 for the average size of 3-torsion in the class groups of real or imaginary quadratic fields was proven by Bhargava and Varma [8, Corollary 4]. Evidence for a generalization of Conjecture 1.4 to cubic extensions is given by Bhargava

and Varma in [7], in which they prove the average size of 2-torsion of class groups of cubic fields is not affected by local conditions at non-archimedian places.

In Conjecture 1.4, we could lump together the two cases over $\mathbb{Q}$, so that the distribution would be the average of μ_{CL} and μ_{CL}^r and make the same statement. The work of Davenport and Heilbronn [15] shows that the distribution is indeed (provably) affected by restricting to only those $K/\mathbb{Q}$ with a specific completion at ∞. It is worth noting that the distribution of class groups of cubic fields is also provably affected by certain global conditions on the field, such as monogenicity, by work of Bhargava and Shankar [6].

Further, Theorem 1.3 leads us to conjecture the following on the distribution of special elements in class groups. For an abelian group A, let A_p denote the Sylow p-subgroup of A.

Conjecture 1.5 (Distribution of elements in Cl_K) Let p be an odd rational prime and Q be $\mathbb{Q}$ or $\mathbb{F}_q(t)$ with $p \nmid q(q-1)$. For K/Q let Cl_K be $\mathrm{Cl}(\mathcal{O}_K)_p$ or $\mathrm{Pic}^0(C_K)_p$ respectively, and use $+$ to denote the group law. For a finite place v of Q, if we consider quadratic extensions K of Q that are split completely at v into v_1, v_2, ordered by discriminant, then (informally) $v_1 - v_2$ is distributed uniformly in Cl_K. More precisely, in the number field case if we restrict to K imaginary, or in the function field case, the isomorphism classes of pairs $(\mathrm{Cl}_K, v_1 - v_2)$ are distributed according to μ.

Theorem 1.3 proves evidence towards Conjecture 1.5 in function field cases. We also prove the prediction of Conjecture 1.5 on the average 3-torsion of the class groups in the number field case, building on the work of Davenport and Heilbronn [15] (which proves the original Cohen–Lenstra prediction for the average size of the 3-torsion of the class group). For example, our result in the imaginary quadratic number field case is as follows (see Theorem 6.1 for the complete result).

Theorem 1.6 (Distribution of elements in Cl_K, $\mathbb{Z}/3\mathbb{Z}$-moment) *Let $v_1, \ldots, v_n$ be finite places of $\mathbb{Q}$, and F_i be étale quadratic $\mathbb{Q}_{v_i}$-algebras, with $F_1 = \mathbb{Q}_{v_1}^{\oplus 2}$. Let S^+ be the set of imaginary quadratic extensions K of $\mathbb{Q}$ such that $K \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \simeq F_i$. Let v_1 split into w_1 and w_2 in K and let $a \in \mathbb{Z}/3\mathbb{Z}$. We have*

$$\lim_{X\to\infty} \frac{\sum_{K\in S^+, |\mathrm{Disc}(K)|<X} |\mathrm{Sur}((\mathrm{Cl}(\mathcal{O}_K), w_1 - w_2), (\mathbb{Z}/3\mathbb{Z}, a)|}{\sum_{K\in S^+, |\mathrm{Disc}(K)|<X} 1} = \frac{1}{3}.$$

Note that Theorem 1.6 also provides evidence for the philosophy of Conjecture 1.4 as the result is not changed by finitely many local conditions at finite places. Klagsbrun [21] determines the $\mathbb{Z}/3\mathbb{Z}$-moments of quotients of the class groups of random quadratic fields by primes above a fixed set of primes, which provides evidence for a generalization of Conjecture 1.5 to multiple places in the base field. Evidence for a generalization of Conjecture 1.5 to cubic extensions, as well as to multiple places in the base field, is given by Klagsbrun in [20], in which he determines the $\mathbb{Z}/2\mathbb{Z}$-moments of quotients of the class groups of cubic fields by primes above a fixed set of primes.

Our conjectures lead to some interesting predictions discussed in Sect. 7. We predict that the number of $\mathbb{F}_q$ points on a hyperelliptic curve does not affect the number of $\mathbb{F}_q$ points on the p^k-torsion of its Jacobian (even though all of the $\mathbb{F}_q$ points of the Jacobian are torsion points). We predict that among imaginary quadratic extensions $K/\mathbb{Q}$ split

completely at a rational prime ℓ into ℓ_1, ℓ_2, the distribution of $\mathrm{Cl}(\mathcal{O}_K)_p/\langle \ell_1 - \ell_2 \rangle$ is not changed if we restrict to only those K for which $\ell_1 - \ell_2$ is trivial in $\mathrm{Cl}(\mathcal{O}_K)_p$.

1.1 Outline of the paper

In Sect. 2, we describe the Cohen–Lenstra measures, their moments, and show that the moments determine the measures. In Sect. 3, we do the same for the analog for pointed groups, and in particular we prove Lemmas 1.1 and 1.2. In Sect. 4, we prove Theorem 1.3, giving evidence towards the pointed moments of real quadratic Picard groups over rational function fields. As corollaries, we obtain the non-pointed moments. In Sect. 5, we prove pointed moments of inert (at ∞) quadratic Picard groups over rational function fields. In Sect. 6, we prove instances of Conjecture 1.5 for number fields, including Theorem 1.6 (in Theorem 6.1). In Sect. 7, we discuss some interesting consequences of our conjectures.

1.2 Notation

Throughout the paper we fix an odd prime p. The letter q will always denote a prime power. Let $\mathrm{Sur}(A, B)$ denote the surjective homomorphisms from A to B. For elements g_i of an abelian group, we let $\langle g_1, \ldots, g_u \rangle$ denote the subgroup generated by the g_i. Let $\mathcal{A}$ be the set of finite abelian p-groups (or more precisely, a set with one representative from each isomorphism class of finite abelian p-groups). For a group A, we write A_p for the Sylow p-subgroup of A.

2 Cohen–Lenstra measures and moments

In this section we will explain the Cohen–Lenstra measures on $\mathcal{A}$ and the moments of these measures. Each measure will be with respect to the σ-algebra that is the full power set of $\mathcal{A}$. Let u be an integer, $u \geq 0$. We define the Cohen–Lenstra measure μ^u, following [13, Example 5.9], so that for $A \in \mathcal{A}$, we have

$$\mu^u(A) := \frac{1}{|A|^u |\operatorname{Aut}(A)|} \prod_{k=1}^{\infty} (1 - p^{-k-u}).$$

In particular, for $u = 0$ the measure (called μ_{CL} above) describes the predicted distribution of Sylow p-subgroups of imaginary quadratic class groups and for $u = 1$ the measure (called μ^r_{CL} above) describes the predicted distribution of Sylow p-subgroups of real quadratic class groups (see [13, 8.1]).

We now give the moments of these distributions.

Proposition 2.1 (Lemma 3.2 of [29]) *For any $A \in \mathcal{A}$, we have that*

$$\sum_{B \in \mathcal{A}} |\operatorname{Sur}(B, A)| \mu^u(B) = |A|^{-u}.$$

In particular, applying Proposition 2.1 when $A = 1$ shows that μ^u is a probability measure. We now give another description of μ^u (see also [22, Theorem 10.9] for this description of μ^u).

Proposition 2.2 *Take a random group G according to μ^0, and then select u elements $g_i \in G$ uniformly and independently at random. Then $G/\langle g_1, \ldots, g_u \rangle$ is distributed according to μ^u.*

Proof Let K be a finite abelian p-group of order p^b. If we apply [13, Proposition 4.3] (with their $k = \infty$), we find that for any integers $a \geq b$,

$$\sum_{\substack{B\in\mathcal{A}\\ |B|=p^a}} \mu^0(B)\frac{1}{|B|^u} \sum_{\substack{b_1,\dots,b_u\in B\\ B/\langle b_1,\dots,b_u\rangle\simeq K}} 1 = p^{-bu}\frac{1}{|\operatorname{Aut}(K)|}\prod_{k=1}^{\infty}(1-p^{-k}) \sum_{\substack{C\in\mathcal{A}\\ |C|=p^{a-b}}} \frac{|\operatorname{Sur}(\mathbb{Z}^u, C)|}{|C|^u|\operatorname{Aut}(C)|}. \tag{1}$$

By [13, Corollary 3.7] (with their $k = u$ and $s = 0$), we have

$$\sum_{a\geq b}\sum_{\substack{C\in\mathcal{A}\\ |C|=p^{a-b}}} \frac{|\operatorname{Sur}(\mathbb{Z}^u, C)|}{|C|^u|\operatorname{Aut}(C)|} = \prod_{1\leq j\leq u}(1-p^{-j})^{-1}.$$

Thus, summing Eq. (1) over all $a \geq b$, we have

$$\sum_{B\in\mathcal{A}} \mu^0(B)\frac{1}{|B|^u} \sum_{\substack{b_1,\dots,b_u\in B\\ B/\langle b_1,\dots,b_u\rangle\simeq K}} 1 = \frac{1}{|K|^u|\operatorname{Aut}(K)|}\prod_{k=1}^{\infty}(1-p^{-k}) \prod_{1\leq j\leq u}(1-p^{-j})^{-1}.$$

The left-hand side is the probability of producing K via the process described in the proposition, and the right-hand side is $\mu^u(K)$. □

In [13], it is this second description (of μ^1) that in fact comes first, and the probabilities for individual groups are later computed in [13, Example 5.9]. One can also prove that the value $\mu^u(B)$ is the limit as $n \to \infty$ of the probability that B is the cokernel of a random matrix from Haar measure in $M_{n\times(n+u)}(\mathbb{Z}_p)$, as done by Friedman and Washington [19] in the case $u = 0$ (using the same argument as Friedman and Washington). At first, it seems this could give a convenient proof of the moments in Proposition 2.1. However, since the limit in n does not a priori commute with the sum over B (though in fact this can be shown), this approach turns out to be less convenient than that above.

In fact, the moments in Proposition 2.1 determine the measure μ^u.

Proposition 2.3 *If μ is a measure on $\mathcal{A}$ such that for every $A \in \mathcal{A}$ we have*

$$\sum_{B\in\mathcal{A}} \operatorname{Sur}(B, A)\nu(B) = |A|^{-u},$$

then $\nu = \mu^u$.

The $u = 0$ case of Proposition 2.3 is Lemma 8.2 in [17]. Proposition 2.3 follows from the proof of [30, Theorem 8.3] (see [29, Theorem 3.1] for a statement). We give a much simpler proof here following [17] and in particular using the following lemma of infinite dimensional linear algebra, the argument for which is given in the proof of Lemma 8.2 in [17] (see also [10, Lemma 4.7] for a stronger statement).

Lemma 2.4 *Let $a_{i,j}$ be non-negative real numbers indexed by pairs of natural numbers i, j, such that there is an $\alpha < 2$ so that for all i, we have $a_{i,i} = 1$ and $\sum_j a_{ij} = \alpha$. Let x_j, y_j be non-negative reals indexed by natural numbers j. If for all i,*

$$\sum_j a_{i,j}x_j = \sum_j a_{i,j}y_j = 1,$$

then $x_j = y_j$ for all j.

Proof of Proposition 2.3 Enumerate the finite abelian p-groups as A_i. We apply Lemma 2.4 with

$$a_{i,j} = \frac{|A_i|^u |\operatorname{Sur}(A_j, A_i)|}{|A_j|^u |\operatorname{Aut}(A_j)|}$$

and $x_j = |A_j|^u |\operatorname{Aut}(A_j)| \nu(A_j)$ and $y_j = |A_j|^u |\operatorname{Aut}(A_j)| \mu^u(A_j)$. It remains to check that

$$\sum_j \frac{|A_i|^u |\operatorname{Sur}(A_j, A_i)|}{|A_j|^u |\operatorname{Aut}(A_j)|} < 2.$$

However, we have that

$$\begin{aligned}\sum_j \frac{|A_i|^u |\operatorname{Sur}(A_j, A_i)|}{|A_j|^u |\operatorname{Aut}(A_j)|} &= \sum_j |A_i|^u |\operatorname{Sur}(A_j, A_i)| \mu^u(A_j) \prod_{k=1}^{\infty} (1 - p^{-k-u})^{-1} \\ &= \prod_{k=1}^{\infty} (1 - p^{-k-u})^{-1}.\end{aligned}$$

So it remains to check that $\prod_{k=1}^{\infty}(1 - p^{-k-u}) > 1/2$. The expression is decreasing in p and u, so it remains to check for $p = 3$ and $u = 0$, which can be done simply. □

3 Measures and moments for pointed groups

We have the measure μ on $\mathcal{A}_\bullet$ defined in the introduction by choosing a group according to μ^0 and picking a group element uniformly at random. We will now analyze the moments of this measure analogously to the Cohen–Lenstra measures μ^u in Sect. 2.

Recall from the introduction, we have the following.

Lemma 1.1. (Pointed moments) For any finite abelian p-group A and $a \in A$, we have

$$\sum_{(B,b)\in\mathcal{A}_\bullet} |\operatorname{Sur}((B, b), (A, a))| \mu(B, b) = \frac{1}{|A|}.$$

Proof We have

$$\begin{aligned}\sum_{(B,b)\in\mathcal{A}_\bullet} |\operatorname{Sur}((B, b), (A, a))| \mu(B, b) &= \sum_{B\in\mathcal{A}} \frac{1}{|B|} \sum_{b\in B} |\operatorname{Sur}((B, b), (A, a))| \mu^0(B) \\ &= \sum_{B\in\mathcal{A}} \frac{\mu^0(B)}{|B|} \sum_{\phi\in\operatorname{Sur}(B,A)} |\ker(\phi)| \\ &= \sum_{B\in\mathcal{A}} \frac{\mu^0(B)}{|A|} |\operatorname{Sur}(B, A)| = \frac{1}{|A|},\end{aligned}$$

where the last equality is by Proposition 2.1. □

Lemma 3.1 *We have*

$$\mu(B, b) = \frac{1}{|B||\operatorname{Aut}(B, b)|} \prod_{k=1}^{\infty} (1 - p^{-k}).$$

Proof As $\operatorname{Aut}(B)$ acts on the elements of B, we have $|\operatorname{Aut}(B)| = |\operatorname{Aut}(B, b)| \cdot \#\{h \in B \mid (B, h) \simeq (B, b)\}$, and the lemma follows. □

In fact, the moments of Lemma 1.1 determine the distribution μ.

Lemma 1.2. If ν is a measure on $\mathcal{A}_\bullet$ such that for every $(A, a) \in \mathcal{A}_\bullet$ we have

$$\sum_{(B,b)\in\mathcal{A}_\bullet} |\operatorname{Sur}((B, b), (A, a))|\nu(B, b) = \frac{1}{|A|},$$

then $\nu = \mu$.

Proof Enumerate the finite abelian pointed p-groups as (A_i, a_i). We apply Lemma 2.4 with

$$a_{i,j} = \frac{|A_i||\operatorname{Sur}((A_j, a_j), (A_i, a_i))|}{|A_j||\operatorname{Aut}(A_j, a_j)|}$$

and $x_j = |A_j||\operatorname{Aut}(A_j, a_j)|\nu(A_j, a_j)$ and $y_j = |A_j||\operatorname{Aut}(A_j, a_j)|\mu(A_j, a_j)$. It remains to check that

$$\sum_j \frac{|A_i||\operatorname{Sur}((A_j, a_j), (A_i, a_i))|}{|A_j||\operatorname{Aut}(A_j, a_j)|} < 2.$$

However, we have that

$$\begin{aligned}\sum_j \frac{|A_i||\operatorname{Sur}((A_j, a_j), (A_i, a_i))|}{|A_j||\operatorname{Aut}(A_j, a_j)|} &= \sum_j |A_i||\operatorname{Sur}((A_j, a_j), (A_i, a_i))|\mu(A_j, a_j)\prod_{k=1}^{\infty}(1 - p^{-k})^{-1} \\ &= \prod_{k=1}^{\infty}(1 - p^{-k})^{-1}.\end{aligned}$$

So it remains to check that $\prod_{k=1}^{\infty}(1 - p^{-k}) > 1/2$, as in Proposition 2.3. □

4 Theorems for real quadratic function fields

In this section we prove Theorem 1.3. The overall strategy is the same as in [10, Sects. 5 and 6] and [31, Sect. 3], which both prove function field results about non-abelian analogs of class groups. However, many of the details are different and the argument below is self-contained. We first translate the problem of interest into one of counting certain extensions of $\mathbb{F}_q(t)$. We then will use the existence of a Hurwitz scheme parametrizing such extensions (as they are equivalently curves with a map to the line), which comes from work of Ellenberg, Venkatesh, and Westerland [16], building on work of Romagny and Wewers [24]. Unlike in [10] and [31], in this paper we also use the homological stability results of Ellenberg, Venkatesh, and Westerland [17] to have a bound on the ith cohomology groups of the Hurwitz schemes that is exponential in i.

4.1 Notation

Let $Q = \mathbb{F}_q(t)$ for this section and the next. Let SCQ be the set of all quadratic extensions of Q split completely at ∞. For $K \in SCQ$, let ∞_1, ∞_2 be the two places of K over ∞. We define $\operatorname{Pic}(C_K)$ to be the Picard group of the unique smooth, proper curve C_K over $\mathbb{F}_q$ associated to K. Let M_K be the set of places of K, which are in bijection with the closed points of C_K. We have

$$\operatorname{Pic}(C_K) = \left(\bigoplus_{v\in M_K} \mathbb{Z}v\right)/\{div(f)\ |f \in K\}.$$

There is a natural map $\mathrm{Pic}(C_K) \to \mathbb{Z}$ sending a place v corresponding to a closed point of degree d to d, with kernel $\mathrm{Pic}^0(C_K)$. Let $K^{un,ab}$ be the maximal unramified abelian extension of K. By class field theory, we have that the profinite completion $\widehat{\mathrm{Pic}(C_K)}$ is isomorphic to $\mathrm{Gal}(K^{un,ab}/K)$.

Note that $\delta_K := \infty_1 - \infty_2$ is not a well defined element in $\mathrm{Pic}^0(C_K)$ because it depends on the ordering of ∞_1, ∞_2, but it is well defined up to $\pm$, and thus the isomorphism class of the pointed group $(\mathrm{Pic}^0(C_K), \delta_K)$ is well-defined. The remainder of this section is devoted to the proof of the pointed moments of Picard groups of real quadratic function fields.

4.2 Counting pointed surjections

In order to prove Theorem 1.3, we will first translate the problem from one of counting pointed surjections to one of counting certain extensions of K. If $K/\mathbb{F}_q(t)$ is a quadratic extension corresponding to $\phi : C_K \to \mathbb{P}^1_{\mathbb{F}_q}$, we have $\phi^*(\infty) \in \mathrm{Pic}(C_K)$, where if ∞ splits into $\prod_i \infty_i^{e_i}$, we have $\phi^*(\infty) = \sum_i e_i \infty_i$.

Proposition 4.1 *Let $K/\mathbb{F}_q(t)$ be a quadratic extension corresponding to the map $\phi : C_K \to \mathbb{P}^1_{\mathbb{F}_q}$ of curves over $\mathbb{F}_q$, and let d be the greatest common divisor of the degrees of the points of C_K. Let L be a subfield $K \subset L \subset K^{un,ab}$ and let $P \subset \widehat{\mathrm{Pic}(C_K)}$ be the corresponding subgroup via Galois theory. Then $d\phi^*(\infty) \in P$ if and only if*

(1) *L/Q is Galois, and*
(2) *$\mathrm{Gal}(K/Q)$, by conjugation in $\mathrm{Gal}(L/Q)$, acts as inversion on $\mathrm{Gal}(L/K)$.*

Also, since $d|2$, if P is odd index, then $d\phi^*(\infty) \in P$ if and only if $\phi^*(\infty) \in P$.

Proof Let σ be the generator of $\mathrm{Gal}(K/Q)$. First, suppose that $d\phi^*(\infty) \in P$. If x is a point of C_K, then in $\widehat{\mathrm{Pic}(C_K)}$ we have $\sigma(x) + x = \deg(x)\phi^*(\infty)$. Thus for $D \in P$, we have $\sigma(D) = \deg(D)(\infty_1 + \infty_2) - D \in P$. Thus L/Q is Galois. For any $D \in \mathrm{Pic}(C_K)$, we have $\sigma(D) + D = \deg(D)(\infty_1 + \infty_2) \in P$, so σ acts as inversion on $\mathrm{Gal}(L/K)$.

Second, suppose that L/Q is Galois, and σ acts as inversion on $\mathrm{Gal}(L/K)$. Let D be a divisor of degree d. Since $d\phi^*(\infty) = D + \sigma(D)$, it must be in the kernel of the map to $\mathrm{Gal}(L/K)$, i.e. P. □

Let Q be a global field with a place ∞. Let H be a finite group, and c a conjugacy class of H. We fix a separable closure $\bar{Q}_\infty$ of the completion Q_∞. Then, inside $\bar{Q}_\infty$ we have the separable closure $\bar{Q}$ of Q. This gives a map $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to \mathrm{Gal}(\bar{Q}/Q)$, and in particular distinguished decomposition and inertia groups in $\mathrm{Gal}(\bar{Q}/Q)$ at ∞. We define (as in [16, Sect. 10.2]) a *marked* (H, c) *extension* of Q to be (L, π, m) such that L/Q is a Galois extension of fields, π is an isomorphism $\pi : \mathrm{Gal}(L/Q) \simeq H$ such that all inertia groups in $\mathrm{Gal}(L/Q)$ (except for possibly the one at ∞) have image in $\{1\} \cup c$, and m, the *marking*, is a homomorphism $L_\infty := L \otimes_Q Q_\infty \to \bar{Q}_\infty$. Note that restriction to L gives a bijection between homomorphisms $L_\infty \to \bar{Q}_\infty$ and homomorphisms $L \to \bar{Q}$. Two marked (H, c) extensions (L_1, π_1, m_1) and (L_2, π_2, m_2) are isomorphic when there is an isomorphism $L_1 \to L_2$ taking π_1 to π_2 and m_1 to m_2. The marking m in a marked (G', c) extension (L, π, m) gives a map $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to \mathrm{Gal}(L/Q)$. Composing with π we get an *infinity type* $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to G'$.

Proposition 4.2 *Let A be a finite abelian group of odd order, $H := A \rtimes_{-1} S_2$ with the action of S_2 by inversion, and c the conjugacy class of order 2 elements of H. When K/Q is a quadratic extension, we have a $|A|$-to-1 map*

$$\{\textit{isom. classes of marked}(H,c)\textit{-extns}L/Q | L^A \simeq K\} \to \mathrm{Sur}\left(\mathrm{Pic}^0(C_K), A\right)$$

When $K \in SCQ$ and $a \in A$, the surjections that send $\delta_K \to a$ correspond to those L for which $2\,\mathrm{Frob}_{\infty_1} \mapsto a \in \mathrm{Gal}(L/Q)$. In particular, we have for $a \in A$:

$$\left|\mathrm{Sur}((\mathrm{Pic}^0(C_K), \delta_K), (A, a))\right| = \frac{\#\{\textit{isom. classes of marked}(H,c)\textit{-extns}L/Q | 2\,\mathrm{Frob}_{\infty_1} \mapsto a, L^A \simeq K\}}{|A|}.$$

Moreover, for the L above we have $\mathrm{Nm}\,\mathrm{Disc}(L) = \mathrm{Nm}\,\mathrm{Disc}(K)^{|A|}$.

Proof We have a natural identification of $\mathrm{Sur}(\mathrm{Pic}^0(C_K), A)$ and

$$\mathrm{Sur}(\mathrm{Pic}(C_K)/\langle \phi^*(\infty)\rangle, A),$$

since we have the exact sequence

$$1 \to \mathrm{Pic}^0(C_K) \to \mathrm{Pic}(C_K)/\langle \phi^*(\infty)\rangle \to \mathbb{Z}/2\mathbb{Z}.$$

We will now construct the map. Note that in each isomorphism class of marked (H, c) extensions of Q, there is a distinguished element such that $L \subset \bar{Q}$ and $m|_L$ is the inclusion map. We start with a distinguished

$$L \in \left\{\text{isom. classes of marked}(H,c)\text{-extns}L/Q | L^A \simeq K, 2\,\mathrm{Frob}_\infty \mapsto \pm a\right\}.$$

The H structure gives an isomorphism $\mathrm{Gal}(L/K) \simeq A$. Since L/Q is an (H, c)-extension, this implies that L/K is abelian and unramified, so we have $L \subset K^{un,ab}$. This gives us a surjection $\widehat{\mathrm{Pic}(C_K)} \to A$. We can see that the surjection sends $\phi^*(\infty)$ to 0 by Proposition 4.1, and also when $K \in SCQ$, we can trace the image of Frob_∞ by the argument above.

We have that $\mathrm{Gal}(K^{un,ab}/K) \simeq \widehat{\mathrm{Pic}(C_K)}$. From Proposition 4.1, we see that a surjection $\mathrm{Pic}(C_K)/\langle \phi^*(\infty)\rangle \to A$ corresponds exactly to an L with $K \subset L \subset K^{un,ab}$ and an isomorphism $\mathrm{Gal}(L/K) \simeq A$ such that L/Q is Galois and $\mathrm{Gal}(K/Q) = \langle \sigma \rangle$ acts as inversion on $\mathrm{Gal}(L/K)$. In particular when $K \in SCQ$, in $\mathrm{Gal}(L/Q)$, we have that $\delta_K = \mathrm{Frob}_{\infty_1} - \mathrm{Frob}_{\infty_2} = \mathrm{Frob}_{\infty_1} - \sigma(\mathrm{Frob}_{\infty_1}) = 2\,\mathrm{Frob}_{\infty_1}$.

Since L/Q is Galois and σ acts as -1 on $\mathrm{Gal}(L/K)$, we have $\mathrm{Gal}(L/Q) \simeq A \rtimes_{-1} S_2$. Moreover, there are $|A|$ choices of an isomorphism $\mathrm{Gal}(L/Q) \simeq A \rtimes_{-1} S_2$ that restrict to the given choice of $\mathrm{Gal}(L/K) \simeq A$, each determined by which element of $H \setminus A$ goes to $(1, \tau)$, where τ is the generator of S_2. The fact that L/K is unramified implies that we obtain, for each of these $|A|$ choices, a marked (H, c)-extension, where the marking is by the inclusion into $\bar{Q}$.

Since L/K is unramified, we have the statement on their discriminants.

We can check that the constructions given above are inverse to each other, which completes the proof of the proposition. □

4.3 Group theory definitions

In this section, we will give necessary group theory definitions for using the results from [16]. In this section, we will work with a finite group H.

Given a finite group H and a conjugacy class c of H, we will define the *universal marked central extension* $\widetilde{H}$ of H (with respect to c), following [16, Sect. 7]. *In this section, we suppose that if* $[g] \in c$ *and* d *is relatively prime to the order of* g, *then* $[g^d] \in c$. (If this is not the case, more complicated definitions are required.) Let C be a Schur cover of H so we have an exact sequence

$$1 \to H_2(H, \mathbb{Z}) \to C \to H \to 1$$

by the Schur covering map. For $x, y \in H$ that commute, let $\hat{x}$ and $\hat{y}$ be arbitrary lifts to C, and let $\langle x, y \rangle$ be the commutator $[\hat{x}, \hat{y}] \in C$, which actually lies in $H_2(H, \mathbb{Z})$ since x and y commute. It we take the quotient of the above exact sequence by all $\langle x, y \rangle$ for $x \in c$ and y commuting with x, we obtain an exact sequence

$$1 \to H_2(H, c) \to \widetilde{H}_c \to H \to 1, \tag{2}$$

which is still a central extension, defining $H_2(H, c)$ and $\widetilde{H}_c$. Let $(H)^{ab}$ denote the abelianization of H. The universal marked central extension is $\widetilde{H} := \widetilde{H}_c \times_{(H)^{ab}} \mathbb{Z}$ and the map $\mathbb{Z} \to (H)^{ab}$ sends 1 to an image of an element of c. We have a map $\widetilde{H} \to H$, given through projecting to the first factor. (See [16, Sect. 7] for why this is called a universal marked central extension.)

Let $\hat{\mathbb{Z}}$ be the inverse limit $\varprojlim \mathbb{Z}/n\mathbb{Z}$ taken over n relatively prime to q (we follow the notation of [16] instead of the more customary $\hat{\mathbb{Z}}'$). We are now going to define an action of $\hat{\mathbb{Z}}^\times$ on $\widetilde{H}$, called the *discrete action* [16, Sect. 8.1.7, Eq. 9.4.1]. There is an action of $\hat{\mathbb{Z}}^\times$ on H given by powering. We pick one element $g \in c$ and one lift $\hat{g} \in \widetilde{H}_c$ of g. Next we will extend this to a map $\widehat{\ }: c \to \widetilde{H}_c$ such that for all $g \in c$, we have $\hat{g}$ has image g in H. We define $\widehat{hgh^{-1}} = \tilde{h}\hat{g}\tilde{h}^{-1}$ for any choice of lift $\tilde{h} \in \widetilde{H}_c$ of h, and since $\widetilde{H}_c \to H$ is central, the definition does not depend on our choice of lift. For $\alpha \in \hat{\mathbb{Z}}^\times$

$$z(\alpha) = \hat{g}^{-\alpha}\widehat{g^\alpha}.$$

First, we note that $z(\alpha)$ is defined by a product in $\widetilde{H}_c$, but actually lies in $H_2(H, c)$ since its image in H is trivial. Second, one can work out that $z(\alpha)$ does not depend on the choice of $g \in c$ (see [31, Sect. 3.1]).

The discrete action of $\hat{\mathbb{Z}}^\times$ on $\widetilde{H}$ is given by

$$\alpha * (g, m) = (g^\alpha z(\alpha)^m, m).$$

4.4 Properties of the Hurwitz scheme

In this theorem, we recall the properties of the Hurwitz scheme constructed by Ellenberg, Venkatesh, and Westerland, building on work on Romagny and Wewers [24], as well as results on its homological stability from [17] and components [16]. An extension $L/\mathbb{F}_q(t)$ is *regular* if it does not contain a non-trivial base field extension $\mathbb{F}_{q^r}(t)/\mathbb{F}_q(t)$.

Theorem 4.3 (Ellenberg, Venkatesh, and Westerland)[1] *Let H be a finite group with trivial center and let c be a conjugacy class of order 2 elements of H, such that the elements of c generate H. Let $\mathbb{F}_q$ be a finite field with q relatively prime to $|H|$. There is a Hurwitz scheme* $\mathsf{CHur}_{H,n}$ *over $\mathbb{Z}[|H|^{-1}]$ constructed in [16, Sect. 8.6.2] with the following properties:*

[1] The paper [16] has been temporarily withdrawn by the authors because of a gap which affects Sects. 6, 12 and some theorems of the introduction of [16]. That gap does not affect any of the results from [16] that we use in this paper.

(1) *We have* $\mathsf{CHur}_{H,n}$ *is a finite étale cover of the relatively smooth n-dimensional configuration space* Conf^n *of n distinct unlabeled points in* $\mathbb{A}^1$ *over* $\operatorname{Spec}\mathbb{Z}[|H|^{-1}]$.

(2) *There is an action of H on* $\mathsf{CHur}_{H,n}$.

(3) *The scheme* $\mathsf{CHur}_{H,n}$ *has an open and closed subscheme* $\mathsf{CHur}^{c,1}_{H,n}$ *such that for* $h \in H$ *there is a bijection between*

   (a) *isomorphism classes of regular marked* (H, c)*-extensions* M *of* $\mathbb{F}_q(t)$ *with unramified infinity type* ϕ *such that* $\phi(F_\Delta) = h$ *and such that the total degree of ramified non-infinite places of* $\mathbb{F}_q(t)$ *is n (where* F_Δ *is a lift of Frobenius to* $\mathrm{Gal}(\overline{\mathbb{F}_q(t)_\infty}/\mathbb{F}_q(t)_\infty)$ *that acts trivially on* $\mathbb{F}_q((t^{-1/\infty}))$*).*

   (b) *points of* $s \in \mathsf{CHur}^{c,1}_{H,n}(\bar{\mathbb{F}}_q)$ *such that* $h^{-1}\operatorname{Frob}(s) = s$ *[16, Sect. 10.4].*

(4) *We have* $\mathsf{CHur}_{H,n}(\mathbb{C})$ *is homotopy equivalent to a topological space* $\mathrm{CHur}_{H,n}$ *[16, Section 8.6.2], such that for any field k of characteristic relatively prime to* $|H|$*, there is a constant C such that for all* $i \geq 1$ *and for all n we have* $\dim H^i(\mathrm{CHur}_{H,n}, k) \leq C^i$ *[17, Proposition 2.5 and Theorem 6.1].*

(5) *Given H, for all n sufficiently large and all q with* $(q, |H|) = 1$*, for* $h \in H$ *the* $h^{-1}\operatorname{Frob}$ *fixed components of* $\mathsf{CHur}^{c,1}_{H,n} \otimes_{\mathbb{Z}[|H|^{-1}]} \bar{\mathbb{F}}_q$ *are in bijection with elements* $(x, n) \in \widetilde{H}$ *such that* $q^{-1} * (x, n) = \hat{h}^{-1}(x, n)\hat{h}$ *(where* $\hat{h}$ *is any lift of h to* $\widetilde{H}$*) and x has trivial image in H [16, Theorem 8.7.3] (see Sect. 4.3 for definitions).*

Remark 4.4 The scheme $\mathsf{CHur}^{c,1}_{H,n}$ comes from restricting to the parametrization of covers of $\mathbb{P}^1$ all of whose local inertia groups have image in $c \cup \{1\}$ and that are unramified at ∞. The argument that $\mathsf{CHur}^{c,1}_{H,n}$ is an open and closed subscheme is as in [17, Sect. 7.3].

Our description of the components requires a bit of translation from that in [16, Theorem 8.7.3]. They biject the components with $\hat{\mathbb{Z}}^\times$ equivariant functions from topological generators of $\varprojlim \mu_n$ (taken over n relatively prime to q) to the preimage of 1 in $\widetilde{H}$ that are fixed by the action of $h^{-1}\operatorname{Frob}$ on $\varprojlim \mu_n$. By choosing any topological generator of $\varprojlim \mu_n$, its image under a function to $\widetilde{H}$ gives us a corresponding element of $\widetilde{H}$, and the action of Frob corresponds to the above discrete action of q^{-1} on $\widetilde{H}$.

4.5 Proof of Theorem 1.3

We continue the notation from Sect. 4.1. Let $H := A \rtimes_{-1} S_2$ and $Q = \mathbb{F}_q(t)$. In Proposition 4.2, given K, we have

$$\begin{aligned}&\#\left\{\text{isom. classes of marked}(H, c)\text{-extns}L/Q|2 \operatorname{Frob}_{\infty_1} \mapsto a, L^A \simeq K\right\}\\ =&\#\left\{\text{isom. classes of marked}(H, c)\text{-extns}L/Q|2 \operatorname{Frob}_{\infty_2} \mapsto a, L^A \simeq K\right\}.\end{aligned}$$

The F_Δ in Theorem 4.3 is a Frobenius element in $\mathrm{Gal}(L/Q)$ and since K/Q is split completely, we have $F_\Delta = \operatorname{Frob}_{\infty_1}$ or $\operatorname{Frob}_{\infty_2}$. So we can sum Proposition 4.2 over $K \in SCQ$ to obtain

$$\begin{aligned}&\sum_{K \in SCQ, \mathrm{Nm}\operatorname{Disc}(K/Q) = q^{2m}} \left|\operatorname{Sur}((\mathrm{Pic}^0(C_K), \delta_K), (A, a))\right|\\ =&\frac{\#\{\text{isom. classes of marked}(H, c)\text{-extns}L/Q|L^A \in SCQ, 2F_\Delta \mapsto a\}}{|A|}.\end{aligned}$$

We will now see that all of the L that appear above are regular. If L/Q contains an extension of $\mathbb{F}_q(t)$, then it corresponds to some cyclic quotient of H. However, the abelianization of H is S_2, so this can only happen when L^A is $\mathbb{F}_{q^2}(t)$. However, $\mathbb{F}_{q^2}(t)$ is not split completely over ∞.

By Theorem 4.3 (3) with $h = a/2$ and $n = 2m$, we then have

$$\sum_{K\in SCQ,\mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} \left|\mathrm{Sur}((\mathrm{Pic}^0(C_K),\delta_K),(A,a))\right| = \frac{\#\{s\in \mathsf{CHur}^{c,1}_{H,2m}(\bar{\mathbb{F}}_q)\mid h^{-1}\,\mathrm{Frob}(s)=s\}}{|A|}.$$

Let $X := \mathsf{CHur}^{c,1}_{H,2m}\otimes_{\mathbb{Z}[|H|^{-1}]}\mathbb{F}_q$. If $h=1$, we would need to then count $\mathbb{F}_q$ points of X. However, for general h, we need to count $\mathbb{F}_q$ points of a different variety Y over $\mathbb{F}_q$ such that $Y\otimes_{\mathbb{F}_q}\bar{\mathbb{F}}_q \simeq X\otimes_{\mathbb{F}_q}\bar{\mathbb{F}}_q$. We can descend $X' := X\otimes_{\mathbb{F}_q}\bar{\mathbb{F}}_q$ to Y over $\mathbb{F}_q$ using the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ on X' in which the Frobenius in the Galois group acts as h^{-1} Frob on X', where Frob is the action of Frobenius using X as the $\mathbb{F}_q$ structure of X' (see, e.g. [23, Corollary 16.25]). So the Frobenius action on $Y(\bar{\mathbb{F}}_q)$ corresponds to the action of h^{-1} Frob on $X(\bar{\mathbb{F}}_q)$. Thus, we have

$$\sum_{K\in SCQ,\mathrm{Nm}\,Disc(K/Q)=q^{2m}} \left|\mathrm{Sur}((\mathrm{Pic}^0(C_K),\delta_K),(A,a))\right| = \frac{\#\,Y(\mathbb{F}_q)}{|A|}.$$

We will apply the Grothendieck-Lefschetz trace formula to $X'\simeq Y\otimes_{\mathbb{F}_q}\bar{\mathbb{F}}_q$. By Theorem 4.3 (1), we have that X' is smooth of dimension $2m$. We have that $\dim H^i_{c,\text{ét}}(X',\mathbb{Q}_\ell) = \dim H^{4m-i}_{\text{ét}}(X',\mathbb{Q}_\ell)$ by Poincaré Duality.

Next, we will relate $\dim H^j_{\text{ét}}(X',\mathbb{Q}_\ell)$ to $\dim H^j(\mathsf{CHur}^{c,1}_{H,2m}(\mathbb{C}),\mathbb{Q}_\ell)$ for some $\ell > 2m$. To compare étale cohomology in characteristic 0 and positive characteristic, we will use [17, Proposition 7.7]. The result [17, Proposition 7.7] gives an isomorphism of étale cohomology between characteristic 0 and positive characteristic in the case of a finite cover of a complement of a reduced normal crossing divisor in a smooth proper scheme. Though [17, Proposition 7.7] is only stated for étale cohomology with coefficients in $\mathbb{Z}/\ell\mathbb{Z}$, the argument goes through identically for coefficients in $\mathbb{Z}/\ell^k\mathbb{Z}$, and then we can take the inverse limit and tensor with $\mathbb{Q}_\ell$ to obtain the result of [17, Proposition 7.7] with $\mathbb{Z}/\ell\mathbb{Z}$ coefficients replaced by $\mathbb{Q}_\ell$ coefficients. So we apply this strengthened version to conclude that $\dim H^j_{\text{ét}}(X',\mathbb{Q}_\ell) = \dim H^j_{\text{ét}}((\mathsf{CHur}^{c,1}_{H,2m})_{\mathbb{C}}),\mathbb{Q}_\ell)$. (As in [17, Proof of Proposition 7.8], we apply comparison to $\mathsf{CHur}^{c,1}_{H,2m}\times_{\mathrm{Conf}^{2m}}\mathrm{PConf}_{2m}$, where PConf_{2m} is the moduli space of $2m$ labelled points on $\mathbb{A}^1$, and is the complement of a relative normal crossings divisor in a smooth proper scheme [17, Lemma 7.6]. Then we take S_{2m} invariants to compare the étale cohomology of $\mathsf{CHur}^{c,1}_{H,2m}$ across characteristics.) By the comparison of étale and analytic cohomology [2, Exposé XI, Theorem 4.4] $\dim H^j(\mathsf{CHur}^{c,1}_{H,2m}(\mathbb{C}),\mathbb{Q}_\ell) = \dim H^j_{\text{ét}}((\mathsf{CHur}^{c,1}_{H,2m})_{\mathbb{C}}),\mathbb{Q}_\ell)$.

By Theorem 4.3 (4), there is a constant C such that for all $j\geq 1$ and for all m, we have $\dim H^j(\mathsf{CHur}^{c,1}_{H,2m}(\mathbb{C}),\mathbb{Q}_\ell)\leq C^j$. Thus $\dim H^j_{\text{ét}}(X',\mathbb{Q}_\ell)\leq C^j$ for all $j\geq 1$. Thus using Poincaré duality, $\dim H^i_{c,\text{ét}}(X',\mathbb{Q}_\ell)\leq C^{4m-i}$ for all $i<4m$.

We will apply Grothendieck-Lefschetz for the Frobenius map from Y on X', which is h^{-1} Frob (where Frob is the Frobenius map from X). By Theorem 4.3 (5), we have that the number of components of X' fixed by h^{-1} Frob for $2m\geq n_H$ for some fixed n_H is

equal to the number of $(x, 2m) \in \tilde{H}$ with $x \in H_2(H, c)$ and $q^{-1} * (x, 2m) = \hat{h}^{-1}(x, 2m)\hat{h}$. Since x is central in $\tilde{H}_c$, this is the same as the number of $(x, 2m) \in \tilde{H}$ with $x \in H_2(H, c)$ and $q^{-1} * (x, 2m) = (x, 2m)$, which is $\#H_2(H, c)[q-1]$ by [31, Proposition 3.1]. By [16, Example 9.3.2], we have that $\#H_2(H, c)$ is a quotient of $\#H_2(A, \mathbb{Z})$ so if $(q-1, |A|) = 1$ then $\#H_2(H, c)[q-1] = 1$.

So we have

$$\#Y(\mathbb{F}_q) = \sum_{j\geq 0}(-1)^j \operatorname{Tr}\left(h^{-1}\operatorname{Frob}|_{H^j_{c,\text{ét}}(X',\mathbb{Q}_\ell)}\right)$$

and also we know $\operatorname{Tr}(h^{-1}\operatorname{Frob}|_{H^{4m}_{c,\text{ét}}((X',\mathbb{Q}_\ell)})$ is q^{2m} times the number of components of X' fixed by h^{-1} Frob. Since X is smooth, we have that the absolute value of any eigenvalue of Frob on $H^j_{c,\text{ét}}(X', \mathbb{Q}_\ell)$ is at most $q^{j/2}$ in absolute value, and since h^{-1} is finite order and commutes with Frob the same is true for eigenvalues of h^{-1} Frob. Thus, for $2m \geq n_A$,

$$\begin{aligned}\left|\#Y(\mathbb{F}_q) - q^{2m}\right| &= \left|\sum_{0\leq j<2\dim X}(-1)^j \operatorname{Tr}(\operatorname{Frob}|_{H^j_{c,\text{ét}}(X_{\mathbb{F}_q},\mathbb{Q}_\ell)})\right| \\ &\leq \sum_{0\leq j<2\dim X} q^{j/2}C^{4m-j} \\ &\leq q^{2m}\sum_{1\leq i}(\sqrt{q}/C)^{-i}.\end{aligned}$$

Thus, for fixed $q > C^2$,

$$\begin{aligned}&\limsup_{m\to\infty} \frac{\sum_{K\in SCQ,\operatorname{Nm}\operatorname{Disc}(K/Q)=q^{2m}} |\operatorname{Sur}((\operatorname{Pic}^0(C_K), \delta_K), (A, a))|}{\sum_{K\in SCQ,\operatorname{Nm}\operatorname{Disc}(K/Q)=q^{2m}} 1} \\ =&\limsup_{m\to\infty} \frac{\sum_{K\in SCQ,\operatorname{Nm}\operatorname{Disc}(K/Q)=q^{2m}} |\operatorname{Sur}((\operatorname{Pic}^0(C_K), \delta_K), (A, a))|}{q^{2m} - q^{2m-1}} \\ =&\limsup_{m\to\infty} \frac{q^{2m} + O(\frac{q^{2m}}{\sqrt{q}/C-1})}{(q^{2m} - q^{2m-1})|A|} \\ =&\limsup_{m\to\infty} \frac{1 + O(\frac{1}{\sqrt{q}/C-1})}{(1 - q^{-1})|A|}.\end{aligned}$$

The implied constant in the big O notation is 1. A similar argument works for the lim inf and the theorem follows.

4.6 Corollaries

Note that by adding Theorem 1.3 over all elements $a \in A$, we have the following corollary, which gives evidence that among real quadratic $K/\mathbb{F}_q(t)$, the Sylow p-subgroups $\operatorname{Pic}^0(C_K)_p$ are distributed according the measure μ^0 defined in Sect. 2.

Corollary 4.5 *For a finite odd order abelian group A, let*

$$\delta_q^+ := \limsup_{m\to\infty} \frac{\sum_{K/\mathbb{F}_q(t)\ \text{real quad},\ \operatorname{Nm}\operatorname{Disc}(K)=q^{2m}} |\operatorname{Sur}(\operatorname{Pic}^0(C_K), A)|}{\sum_{K/\mathbb{F}_q(t)\ \text{real quad},\ \operatorname{Nm}\operatorname{Disc}(K)=q^{2m}} 1}$$

and δ_q^- *the corresponding* lim inf. *Then as* $q \to \infty$ *among odd prime powers such that* $(q(q-1), |A|) = 1$, *we have*

$$\delta_q^+, \delta_q^- \to 1.$$

By restricting Theorem 1.3 to the case $a = 0$ and using the fact that $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathrm{Pic}^0(C_K)/\langle \infty_1 - \infty_2 \rangle$, we obtain the following corollary, which gives evidence that among real quadratic $K/\mathbb{F}_q(t)$, the groups $\mathrm{Cl}(\mathcal{O}_K)_p$ are distributed according the measure μ^1 defined in Sect. 2.

Corollary 4.6 *For a finite odd order abelian group A, let*

$$\delta_q^+ := \limsup_{m\to\infty} \frac{\sum_{K/\mathbb{F}_q(t) \text{ real quad}, \mathrm{Nm}\,\mathrm{Disc}(K)=q^{2m}} |\mathrm{Sur}(\mathrm{Cl}(\mathcal{O}_K), A)|}{\sum_{K/\mathbb{F}_q(t) \text{ real quad}, \mathrm{Nm}\,\mathrm{Disc}(K)=q^{2m}} 1}$$

and δ_q^- *the corresponding* lim inf. *Then as* $q \to \infty$ *among odd prime powers such that* $(q(q-1), |A|) = 1$, *we have*

$$\delta_q^+, \delta_q^- \to \frac{1}{|A|}.$$

Note that it is not clear whether the groups $\mathrm{Cl}(\mathcal{O}_K)_p$ (or $\mathrm{Pic}^0(C_K)_p$) are "distributed according to a measure," i.e. whether there is a measure ν such that for all non-negative functions f, we have

$$\lim_{m\to\infty} \frac{\sum_{K\in SCQ, \mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} f(\mathrm{Cl}(\mathcal{O}_K)_p)}{\sum_{K\in SCQ, \mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} 1} = \sum_{H \text{ fin ab } p\text{-group}} f(H)\nu(H).$$

So even if we knew $\delta_q^\pm = 1$, we could not use Proposition 2.3 to conclude that the averages of an arbitrary f are predicted as by the Cohen–Lenstra heuristics. Informally, the moments determine the measure, but we don't know whether the class groups are distributed according to a measure! (Though for f an indicator function, see [17, Corollary 8.2].)

5 Inert quadratic function fields

We continue with the notation given in Sect. 4.1. Let INQ be the set of quadratic extensions of Q inert at ∞. We then have the following theorem giving evidence that over $K \in INQ$, the Sylow p-subgroups $\mathrm{Pic}^0(C_K)_p$ are distributed according to μ^0.

Theorem 5.1 *For a finite odd order abelian group A, let*

$$\delta_q^+ := \limsup_{m\to\infty} \frac{\sum_{K\in INQ} \mathrm{Nm}\,\mathrm{Disc}(K)=q^{2m}} |\mathrm{Sur}(\mathrm{Pic}^0(C_K), A)|}{\sum_{K\in INQ} \mathrm{Nm}\,\mathrm{Disc}(K)=q^{2m}} 1}$$

and δ_q^- *the corresponding* lim inf. *Then as* $q \to \infty$ *among odd prime powers such that* $(q(q-1), |A|) = 1$, *we have*

$$\delta_q^+, \delta_q^- \to 1.$$

The proof below is analogous to, but easier than, the proof of Theorem 1.3.

Proof Let $H := A \rtimes_{-1} S_2$ and $Q = \mathbb{F}_q(t)$. We sum Proposition 4.2 over $K \in INQ$ to obtain

$$\sum_{K \in INQ, \mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} |\mathrm{Sur}(\mathrm{Pic}^0(C_K), A)|$$
$$= \#\{\text{isom. classes of marked}(H, c)\text{-extns} L/Q | L^A \in INQ\}.$$

Note that $L^A \in INQ$ if and only if in the marked extension $\pi(F_\Delta) \in H \setminus A$ and π is unramified at ∞.

Almost all of the L that appear above are regular. If L/Q contains an extension of $\mathbb{F}_q(t)$, then it corresponds to some cyclic quotient of H. However, the abelianization of H is S_2, so this can only happen when $L^A = K$ is $\mathbb{F}_{q^2}(t)$. Since $\mathrm{Pic}^0(C_{\mathbb{F}_{q^2}(t)})$ is trivial, it does not contribute to the sum unless A is trivial (in which case the theorem is immediate).

Thus, when A is non-trivial, by Theorem 4.3 (3), we then have

$$\sum_{K \in INQ, \mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} |\mathrm{Sur}(\mathrm{Pic}^0(C_K), A)|$$
$$= \sum_{h \in H \setminus A} \frac{\#\{s \in \mathsf{CHur}^{c,1}_{H,n}(\bar{\mathbb{F}}_q) \mid h^{-1}\,\mathrm{Frob}(s) = s\}}{|A|}.$$

We let $n = 2m$. Let $X' := X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q$. As in the proof of Theorem 1.3, we construct Y_h so that

$$\#\{s \in \mathsf{CHur}^{c,1}_{H,n}(\bar{\mathbb{F}}_q) \mid h^{-1}\,\mathrm{Frob}(s) = s\} = \#Y_h(\mathbb{F}_q)$$

and $Y_h \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q \simeq X'$. As in the proof of Theorem 1.3, for some prime ℓ we have $\dim H^i_{c,\text{ét}}(X', \mathbb{Q}_\ell) \le C^{2n-i}$ for all $i < 2n$.

We will apply Grothendieck-Lefschetz for the Frobenius map from Y_h on X', which is $h^{-1}\,\mathrm{Frob}$ (where Frob is the Frobenius map from X). As in the proof of Theorem 1.3, we apply Theorem 4.3 (5) to conclude that the number of components of X' fixed by $h^{-1}\,\mathrm{Frob}$ for even $n \ge n_H$ for some fixed n_H is 1.

So we have, as in the proof of Theorem 1.3, for even $n \ge n_A$,

$$|\#Y_h(\mathbb{F}_q) - q^n| \le q^n \sum_{1 \le i} (\sqrt{q}/C)^{-i}.$$

Thus, for fixed $q > C^2$,

$$\limsup_{m\to\infty} \frac{\sum_{K \in INQ, \mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} |\mathrm{Sur}(\mathrm{Pic}^0(C_K), A)|}{\sum_{K \in INQ, \mathrm{Nm}\,\mathrm{Disc}(K/Q)=q^{2m}} 1}$$
$$= \limsup_{m\to\infty} \sum_{h \in H \setminus A} \frac{q^{2m} + O(\frac{q^{2m}}{\sqrt{q}/C-1})}{(q^{2m} - q^{2m-1})|A|}$$
$$= \limsup_{m\to\infty} \frac{1 + O(\frac{1}{\sqrt{q}/C-1})}{(1 - q^{-1})}.$$

The implied constant in the big O notation is 1. A similar argument works for the lim inf and the theorem follows. □

6 Number field results on distribution of $\wp_1 - \wp_2$

In this section, we see that the $(\mathbb{Z}/3\mathbb{Z}, g)$-moments predicted by Conjecture 1.5 hold in the number field case, and moreover are not affected by finitely many local conditions on the quadratic field, in the spirit of Conjecture 1.4. We reduce the problem to counting cubic and quadratic extensions with certain local conditions, and then use the work of Davenport and Heilbronn [15] to count cubic extensions. This strategy and the computation of local masses follows along similar lines to the proof of [8, Corollary 4]. For a number field K, let $\mathcal{O}_K$ denote its ring of integers.

Theorem 6.1 (Distribution of elements in Cl_K, $\mathbb{Z}/3\mathbb{Z}$-moment) *Let $v_1, \ldots, v_n$ be finite places of $\mathbb{Q}$, and F_i be étale quadratic $\mathbb{Q}_{v_i}$-algebras, with $F_1 = \mathbb{Q}_{v_1}^{\oplus 2}$. Let S be the set of quadratic extensions K of $\mathbb{Q}$ such that $K \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \simeq F_i$. Let S^+ and S^- denote the imaginary and real extensions in S, respectively. Let v_1 split into w_1 and w_2 in K and let $g \in \mathbb{Z}/3\mathbb{Z}$. We have*

$$\lim_{X\to\infty} \frac{\sum_{K\in S^+,|\operatorname{Disc}(K)|<X} |\operatorname{Sur}((\mathrm{Cl}(\mathcal{O}_K), w_1 - w_2), (\mathbb{Z}/3\mathbb{Z}, g)|}{\sum_{K\in S^+,|\operatorname{Disc}(K)|<X} 1} = \frac{1}{3},$$

and

$$\lim_{X\to\infty} \frac{\sum_{K\in S^-,|\operatorname{Disc}(K)|<X} |\operatorname{Sur}((\mathrm{Cl}(\mathcal{O}_K), w_1 - w_2), (\mathbb{Z}/3\mathbb{Z}, g)|}{\sum_{K\in S^-,|\operatorname{Disc}(K)|<X} 1} = \frac{1}{9}.$$

We can of course add these pointed moments up over the three choices of $g \in \mathbb{Z}/3\mathbb{Z}$ and recover the theorem of Davenport and Heilbronn [15, Theorem 3] in the case $n = 0$ or the theorem of Bhargava and Varma [8, Corollary 4] when there are local conditions. (Note that $|\operatorname{Sur}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Z}/3\mathbb{Z})| + 1$ is the size of the 3-torsion of $\mathrm{Cl}(\mathcal{O}_K)$.)

The proof of the following proposition is similar to that of Proposition 4.2. This number field version is easier than the function field version, because for any $K/\mathbb{Q}$ quadratic with σ generating $\mathrm{Gal}(K/\mathbb{Q})$ and L/K unramified abelian we have that $L/\mathbb{Q}$ is Galois and σ acts by inversion of $\mathrm{Gal}(L/\mathbb{Q})$, and so an analog of Proposition 4.1 is not required. We say a cubic extension L is *nowhere overramified* if no rational prime ramifies to degree 3.

Proposition 6.2 *Let c the conjugacy class of order 2 elements of S_3. When $K/\mathbb{Q}$ is quadratic, we have a 2-1 map*

$$\operatorname{Sur}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Z}/3\mathbb{Z}) \to \{\textit{isom. classes of nowhere overram. non-cyclic cubic } L/Q | \tilde{L}^{A_3} \simeq K\},$$

given by letting $\tilde{L}$ be the unramified extension of K associated to the surjection, and L a cubic subfield of $\tilde{L}$ so that $\tilde{L}$ is the Galois closure of L over $\mathbb{Q}$. Moreover, if v_1 is split into w_1 and w_2 in K, then under the above bijection, the image of $w_1 - w_2$ is trivial in $\mathbb{Z}/3\mathbb{Z}$ if and only if L is split completely over v_1.

Asking that $K \in S$ in Theorem 6.1 translates directly into conditions on the allowable restrictions on the isomorphism type of $L \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i}$. Thus in order to count the objects on the right hand side in Proposition 6.2, we will count isomorphism classes of cubic number fields $L/\mathbb{Q}$ with restrictions on the isomorphism type of $L \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i}$. To ask that L is nowhere overramified and non-cyclic we need 1) that $L/\mathbb{Q}$ is not Galois and 2) in the associated map $\phi_3 : G_{\mathbb{Q}} \to S_3$ to L no inertia group has image including a 3-cycle. The second requirement is a condition on the isomorphism type of $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$ at every finite place v.

The following theorem on counting cubic extensions with local restrictions will be essential. For a prime p of $\mathbb{Q}$ let $|\cdot|_p$ be the p-adic absolute value so that $|p|_p = p^{-1}$, and let $|\cdot|_\infty \equiv 1$ be the trivial absolute value.

Theorem 6.3 (Theorem 4.1 of [14], see also Theorem 1 and Section 5 of [15]) *Let $v_0 = \infty, v_1, \dots v_n$ be distinct places of $\mathbb{Q}$ and R_i (for $i = 0, \dots, n$) be a set of isomorphism classes of degree 3 étale $\mathbb{Q}_{v_i}$-algebras. For a place v of $\mathbb{Q}$ and an étale $\mathbb{Q}_v$-algebra M_v, let $c(M_v) = |\operatorname{Aut}(M_v/Q_v)|^{-1} |\operatorname{Disc}(M_v/Q_v)|_v$, and $c(R_i) = \sum_{M \in R_i} c(M)$. Let $c_3(v) = \sum_{M/\mathbb{Q}_v \text{ deg. 3 étale}} c(M)$. Then*

$$\lim_{X\to\infty} \frac{\#\{L/\mathbb{Q} \text{ cubic, up to isom.} \mid |\operatorname{Disc} L| < X; L \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \in R_i \ i = 0, \dots, n\}}{X} = \frac{1}{3\zeta(3)} \prod_{i=0}^{n} \frac{c(R_i)}{c_3(v_i)}.$$

We will need a similar theorem for quadratic extensions.

Theorem 6.4 (follows from Theorem 1.1 of [28], see also Lemma 6.1 of [27]) *Let $v_0 = \infty, v_1, \dots v_n$ be distinct places of $\mathbb{Q}$ and R_i (for $i = 0, \dots, n$) be a set of isomorphism classes of degree 2 étale $\mathbb{Q}_{v_i}$-algebras. For a place v of $\mathbb{Q}$ and an étale $\mathbb{Q}_v$-algebra M_v, let $c(M_v) = |\operatorname{Aut}(M_v/Q_v)|^{-1} |\operatorname{Disc}(M_v/Q_v)|_v$, and $c(R_i) = \sum_{M \in R_i} c(M)$. Let $c_2(v) = \sum_{M/\mathbb{Q}_v \text{ deg. 2 étale}} c(M)$. Then*

$$\lim_{X\to\infty} \frac{\#\{K/\mathbb{Q} \text{ quad., up to isom.} \mid |\operatorname{Disc} K| < X; K \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \in R_i \ i = 0, \dots, n\}}{X} = \frac{1}{\zeta(2)} \prod_{i=0}^{n} \frac{c(R_i)}{c_2(v_i)}.$$

Proof of Theorem 6.1 For $i = 2, \dots, n$, let R_i be the set of cubic étale extensions of $\mathbb{Q}_{v_i}$ such that the associated $\phi_3 : G_{\mathbb{Q}_{v_i}} \to S_3$ has sign map $\phi_2 : G_{\mathbb{Q}_{v_i}} \to S_2$ corresponding to F_i, *and* such that the image of inertia under ϕ_3 does not include a 3-cycle. For $i = 1$, we let $R_1 = \{\mathbb{Q}_{v_1}^{\oplus 3}\}$, and for $i = 0$ we let R_0 be $\{\mathbb{C} \oplus \mathbb{R}\}$ or $\{\mathbb{R}^{\oplus 3}\}$ depending on whether we are in the S^+ or S^- case, respectively. Label the places $v \notin \{v_0, \dots, v_n\}$ by $v_{n+1}, v_{n+2}, \dots$, and for $i \geq n+1$, let R_i be the set of cubic étale extensions of $\mathbb{Q}_{v_i}$ such that the associated $\phi_3 : G_{\mathbb{Q}_{v_i}} \to S_3$ does not have a 3-cycle in its image of inertia. Let F_0 be $\{\mathbb{C}\}$ or $\{\mathbb{R}^{\oplus 2}\}$ depending on whether we are in the S^+ or S^- case, respectively.

We have, from Proposition 6.2,

$$\lim_{X\to\infty} \frac{\sum_{K \in S^+, |\operatorname{Disc}(K)| < X} |\operatorname{Sur}((\operatorname{Cl}(\mathcal{O}_K), w_1 - w_2), (\mathbb{Z}/3\mathbb{Z}, 0)|}{\sum_{K \in S^+, |\operatorname{Disc}(K)| < X} 1} = \lim_{X\to\infty} \frac{2\#\{\text{isom. classes of non-cyclic cubic} L/\mathbb{Q} || \operatorname{Disc}(L_1)| < X, L \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \in R_i, \ i \geq 0\}}{\#\{\text{isom. classes of quad.} K/\mathbb{Q} || \operatorname{Disc}(K)| < X, K \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \simeq F_i, \ i = 0, \dots, n\}}.$$

Let

$$N_Y(X) := \#\{\text{isom. classes of cubic} L/\mathbb{Q} || \operatorname{Disc}(L)| < X, L \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \in R_i, \ i = 0, \dots, Y\}.$$

By Theorem 6.3, for finite $Y \geq n$, we have

$$\lim_{X\to\infty} \frac{N_Y(X)}{X} = \frac{1}{3\zeta(3)} \prod_{i=0}^{Y} \frac{c(R_i)}{c_3(v_i)}.$$

We have $N_\infty(X) \le N_Y(X)$, so

$$\limsup_{X\to\infty} \frac{N_\infty(X)}{X} \le \frac{1}{3\zeta(3)} \prod_{i=0}^{\infty} \frac{c(R_i)}{c_3(v_i)}.$$

Also, we have

$$N_\infty(X) \ge N_Y(X) - \sum_{i>Y} \#\{\text{isom. classes of cubic} L/\mathbb{Q} || \operatorname{Disc}(L)| < X, v_i \text{ ram. deg.3in} L.\}$$

By [14, Lemma 5.1], there is a constant C such that for all $i \ge 1$, and associated prime v_i, we have

$$\frac{\#\{\text{isom. classes of cubic} L/\mathbb{Q} || \operatorname{Disc}(L)| < X, v_i \text{ ram. deg.3in} L\}}{X} \le \frac{C}{v_i^2}.$$

So,

$$\frac{N_\infty(X)}{X} \ge \frac{N_Y(X)}{X} - \sum_{i>Y} \frac{C}{v_i^2},$$

and thus

$$\liminf_{X\to\infty} \frac{N_\infty(X)}{X} \ge \frac{1}{3\zeta(3)} \prod_{i=0}^{\infty} \frac{c(R_i)}{c_3(v_i)}$$

and we conclude

$$\lim_{X\to\infty} \frac{N_\infty(X)}{X} = \frac{1}{3\zeta(3)} \prod_{i=0}^{\infty} \frac{c(R_i)}{c_3(v_i)}.$$

Since

$$\lim_{X\to\infty} \frac{\#\{\text{isom. classes of cyclic cubic} L/\mathbb{Q} || \operatorname{Disc}(L)| < X\}}{X} = 0$$

by [12, Eq. (1)], if we define

$$\begin{aligned} N'_Y(X) \ &:= \#\{\text{isom. classes of non-cyclic cubic} L/\mathbb{Q} || \operatorname{Disc}(L)| \\ &\quad < X, L \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \in R_i,\ i = 0, \dots, Y\}, \end{aligned}$$

we have

$$\lim_{X\to\infty} \frac{N'_\infty(X)}{X} = \frac{1}{3\zeta(3)} \prod_{i=0}^{\infty} \frac{c(R_i)}{c_3(v_i)}.$$

By Theorem 6.4, we have that

$$\begin{aligned} &\lim_{X\to\infty} \frac{\#\{\text{isom. classes of quad.} K/\mathbb{Q} || \operatorname{Disc}(K)| < X, K \otimes_{\mathbb{Q}} \mathbb{Q}_{v_i} \simeq F_i,\ i = 0, \dots, n\}}{X} \\ &= \frac{1}{\zeta(2)} \prod_{i=0}^{n} \frac{c(F_i)}{c_2(v_i)}. \end{aligned}$$

Thus,

$$\begin{aligned} &\lim_{X\to\infty} \frac{\sum_{K\in S^+, |\operatorname{Disc}(K)|<X} |\operatorname{Sur}((\operatorname{Cl}(\mathcal{O}_K), w_1 - w_2), (\mathbb{Z}/3\mathbb{Z}, 0)|}{\sum_{K\in S^+, |\operatorname{Disc}(K)|<X} 1} \\ &= \frac{2\zeta(2)}{3\zeta(3)} \prod_{i=0}^{\infty} \frac{c(R_i)}{c_3(v_i)} \prod_{i=0}^{n} \frac{c_2(v_i)}{c(F_i)}. \end{aligned}$$

It remains to compute the local factors.

We have that for a finite place v that $c_3(v) = 1 + v^{-1} + v^{-2}$ and $c_2(v) = 1 + v^{-1}$ and for $i > n$ that $c(R_i) = 1 + v^{-1}$. (For tame v this is a simple computation with the absolute tame Galois group, and for wild v these are the $n = 2, 3$ cases of Bhargava's mass formula for local fields [4, Theorem 1.1], and follow from Serre's mass formula [25, Théorème 2], as well.) Also, $c_3(\infty) = 2/3$ and $c_2(\infty) = 1$.

When $2 \le i \le n$, we will see that $c(R_i) = c(F_i)$. Given $\phi : G_{\mathbb{Q}_v} \to S_3$ such that the inertia group does not have image containing a 3-cycle, since the inertia group is a normal subgroup, either $|\operatorname{im}(\phi)| = 2$ or ϕ is unramified. If F_i is unramified, then every element of R_i must be unramified. If $F_i = \mathbb{Q}_{v_i}^{\oplus 2}$, then $R_i = \{\mathbb{Q}_{v_i}^{\oplus 3}, K_{v_i}\}$, where $K_{v_i}/\mathbb{Q}_{v_i}$ is the unramified extension of degree 3, and $c(F_i) = 1/2$ and $c(R_i) = 1/6 + 1/3 = 1/2$. If $F_i/\mathbb{Q}_{v_i}$ is an unramified field extension of degree 2, then $R_i = \{F_i\}$, and $c(F_i) = c(R_i)$. If F_i is ramified, then since $|\operatorname{im}(\phi)| = 2$, we have $R_i = \{F_i \oplus Q_{v_i}\}$ and $c(F_i) = c(R_i)$. Now in the case $i = 1$, we have $c(R_1) = 1/6$ and $c(F_1) = 1/2$. So,

$$\lim_{X\to\infty} \frac{\sum_{K\in S^+, |\operatorname{Disc}(K)|<X} |\operatorname{Sur}((\operatorname{Cl}(\mathcal{O}_K), w_1 - w_2), (\mathbb{Z}/3\mathbb{Z}, 0)|}{\sum_{K\in S^+, |\operatorname{Disc}(K)|<X} 1}$$
$$= \frac{\zeta(2)}{3\zeta(3)} \frac{c(R_0)}{c(F_0)} \prod_p^{\infty} \frac{1 + p^{-1}}{1 + p^{-1} + p^{-2}} = \frac{c(R_0)}{3c(F_0)}.$$

Since $c(\{\mathbb{C}\}) = 1/2$ and $c(\{\mathbb{R} \oplus \mathbb{C}\}) = 1/2$, we conclude the first case of the theorem when $g = 1$. Since $c(\{\mathbb{R}^{\oplus 2}\}) = 1/2$ and $c(\mathbb{R}^{\oplus 3}) = 1/6$, we conclude the second case of the theorem when $g = 1$.

For non-trivial g, we can either subtract the pointed moments we have just proven from the known (non-pointed) moments, or make the argument as above but with R_1 replaced the set of the unramified cubic field extension of $\mathbb{Q}_{v_1}$. Either approach tells us the average number of surjections in which $w_1 - w_2$ has non-trivial image. We note that by the automorphism of $\mathbb{Z}/3\mathbb{Z}$ there must be an equal number of surjections with each non-trivial image, and we conclude the theorem. □

In fact, if finitely many places v_i are required to split completely into v_i' and v_i'' in the quadratic extension, using the argument in the proof of Theorem 6.1, one can count surjections where $\pm(v_i' - v_i'')$ have any given possible list of images in $\mathbb{Z}/3\mathbb{Z}$. However, note that $(\operatorname{Cl}(\mathcal{O}_K), v_1' - v_1'', v_2' - v_2'')$ is not a well-defined "double-pointed group," and so one necessarily must keep track of the images of plus or minus certain elements if tracking more than one. Klagsbrun [21] avoids this technical issue by studying the quotients of $\operatorname{Cl}(\mathcal{O}_K)$ by the elements of $v_i' - v_i''$ instead of moments of pointed groups.

7 Predictions of conjectures

In this section, we will discuss some of the predictions of Conjectures 1.4 and 1.5. In the function field analog, the question of the size of Pic^0 can be rephrased more geometrically. We consider hyperelliptic curves over $\mathbb{F}_q$, and ask how many $\mathbb{F}_q$ points there are on their Jacobians (as $\operatorname{Pic}^0(C_K) = \operatorname{Jac}(C_K)(\mathbb{F}_q)$). Since the differences of $\mathbb{F}_q$ points of a curve give $\mathbb{F}_q$ points of its Jacobian, one might first guess that curves with more points would have more points in the p-torsion of their Jacobians. Conjecture 1.4 has the counter-intuitive prediction that the number of $\mathbb{F}_q$ points on the curve, $\#C_K(\mathbb{F}_q)$, does not affect the number of $\mathbb{F}_q$ points on the p^k-torsion of the Jacobian, $\#\operatorname{Jac}(C_K)[p^k](\mathbb{F}_q)$ (even though all of the points in $\operatorname{Jac}(C_K)(\mathbb{F}_q)$ are torsion points). This is because the number of $\mathbb{F}_q$ points on

C_K is determined by the completions of K at the $q+1$ degree 1 places of $\mathbb{F}_q(t)$. So even if we restrict to hyperelliptic curves with the maximum number of $\mathbb{F}_q$ points, $2q+2$, Conjecture 1.4 predicts that $\#\operatorname{Jac}(C_K)[p^k](\mathbb{F}_q)$ is distributed just as it is for hyperelliptic curves with no points, or for all hyperelliptic curves. In particular, the predicted average of $\#\operatorname{Jac}(C_K)[p^k](\mathbb{F}_q)$ is $k+1$

It is worth noting that restricting to hyperelliptic curves C_K with the maximal number of $\mathbb{F}_q$ points does indeed provably make the asymptotics of the average of $\#\operatorname{Jac}(C_K)(\mathbb{F}_q)$ larger, which can be deduced from work of Taniguchi [26, Theorem 6.7]. There are at least two important caveats, which are that 1) the average size of $\#\operatorname{Jac}(C_K)(\mathbb{F}_q)$ is infinite and 2) $\operatorname{Jac}(C_K)(\mathbb{F}_q)$ includes 2-torsion which does not follow the heuristics discussed in this paper.

Suppose we consider imaginary quadratic extensions K of $\mathbb{Q}$ split completely at a rational prime ℓ into ℓ_1, ℓ_2. Conjecture 1.5 then predicts that the probability that $\ell_1 - \ell_2$ is trivial in $\operatorname{Cl}(\mathcal{O}_K)_p$ is $1-p^{-1}$. We can see this since $\sum_{A\in\mathcal{A}} |\operatorname{Aut}(G)|^{-1}|G|^{-1}\prod_{k\geq 1}(1-p^{-k}) = 1-p^{-1}$. Further, for a random group G from μ_{CL} and a uniform random element $g\in G$ we have that

$$\begin{aligned}\operatorname{Prob}(G\simeq A|g=1) &= (1-p^{-1})^{-1}\operatorname{Prob}(G\simeq A \text{ and } g=1)\\ &= |\operatorname{Aut}(A)|^{-1}|A|^{-1}\prod_{k\geq 2}(1-p^{-k}).\end{aligned}$$

Thus, if we restrict to those K such that $\ell_1-\ell_2$ is trivial in $\operatorname{Cl}(\mathcal{O}_K)_p$, Conjecture 1.5 predicts that $\operatorname{Cl}(\mathcal{O}_K)_p$ is then distributed according to μ_{CL}^r, like the Sylow p-subgroups of class groups of real quadratic fields. Said another way, if among imaginary quadratic extensions K of $\mathbb{Q}$ split completely at a rational prime ℓ we consider the group $\operatorname{Cl}(\mathcal{O}_K)_p/\langle\ell_1-\ell_2\rangle$, the distribution is predicted to be μ_{CL}^r, and is predicted to not change even if we restrict to only those K for which $\ell_1-\ell_2$ is trivial in $\operatorname{Cl}(\mathcal{O}_K)_p$.

We now see somewhat of a contrast to the first paragraph of this section. We restrict to imaginary quadratic extensions K of $\mathbb{Q}$ split completely at a rational prime ℓ such that $\ell_1-\ell_2$ is non-trivial in $\operatorname{Cl}(\mathcal{O}_K)_p$ (forcing, in particular, $\operatorname{Cl}(\mathcal{O}_K)_p$ to be non-trivial). In this case, Conjecture 1.5 predicts, for example, that the p-torsion $\operatorname{Cl}(\mathcal{O}_K)[p]$ has average size $p+p^{-1}$ (as opposed to average size 2 among all imaginary quadratics).

Acknowledgements

The author would like to thank Jordan Ellenberg, Akshay Venkatesh, Nigel Boston, Silas Johnson, Manjul Bhargava, Takashi Taniguchi, and Jürgen Klüners for useful conversations and comments on this paper. The author would also like to thank the anonymous referee for detailed comments that improved the exposition of the paper. This work was done with the support of an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, and National Science Foundation Grants DMS-1147782 and DMS-1301690 and CAREER Grant DMS-1652116, and a Vilas Early Career Investigator Award.

Received: 19 October 2017 Accepted: 10 September 2018 Published online: 25 September 2018

References

1. Achter, J.D.: The distribution of class groups of function fields. J. Pure Appl. Algebra **204**(2), 316–333 (2006)
2. Artin, M., Grothendieck, A., Verdier, J.-L.: Théorie Des Topos et Cohomologie Étale Des Schémas. Tome 3. Lecture Notes in Mathematics, Vol. 305. Springer, Berlin (1973). Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat
3. Bhargava, M.: The density of discriminants of quartic rings and fields. Ann. Math. (2) **162**(2), 1031–1063 (2005)
4. Bhargava, M.: Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. Int. Math. Res. Not. IMRN **2007**(9), rnm052 (2007)
5. Bhargava, M.: Variations on the Cohen-Lenstra heuristics. The Cohen-Lenstra heuristics for class groups. Talk at AIM Workshop (2011)

6. Bhargava, M., Shankar, A.: Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. arXiv:1006.1002v2. (reference is to arxiv version 2, not published version) (2010)
7. Bhargava, M., Varma, I.: On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. Duke Math. J. **164**(10), 1911–1933 (2015)
8. Bhargava, M., Varma, I.: The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. Proc. Lond. Math. Soc. (3) **112**(2), 235–266 (2016)
9. Bhargava, M., Shankar, A., Tsimerman, J.: On the Davenport-Heilbronn theorems and second order terms. Invent. Math. **193**(2), 439–499 (2013)
10. Boston, N., Matchett Wood, M.: Non-abelian Cohen-Lenstra heuristics over function fields. Compos. Math. **153**(7), 1372–1390 (2017)
11. Clancy, J., Kaplan, N., Leake, T., Payne, S., Melanie, M.M.: On a Cohen–Lenstra heuristic for Jacobians of random graphs. J. Algebr. Comb. **42**(3), 701–723 (2015)
12. Cohn, H.: The density of abelian cubic fields. Proc. Am. Math. Soc. **5**, 476–477 (1954)
13. Cohen, H., Jr Lenstra, H.W.: Heuristics on Class Groups of Number Fields. In Number Theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Mathematics, vol. 1068, pp. 33–62. Springer, Berlin (1984)
14. Datskovsky, B., Wright, D.J.: Density of discriminants of cubic extensions. J. Reine Angew. Math. **386**, 116–138 (1988)
15. Davenport, H., Heilbronn, H.: On the density of discriminants of cubic fields. II. Proc. R. Soc. London Ser. A **322**(1551), 405–420 (1971)
16. Ellenberg, J.S., Venkatesh, A., Westerland, C.: Homological Stability for Hurwitz Spaces and the Cohen-Lenstra Conjecture over Function Fields, II. arXiv:1212.0923 [math] (December 2012)
17. Ellenberg, J.S., Venkatesh, A., Westerland, C.: Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. Ann. Math. Second Ser. **183**(3), 729–786 (2016)
18. Fouvry, É., Klüners, J.: On the 4-rank of class groups of quadratic number fields. Invent. Math. **167**(3), 455–513 (2007)
19. Friedman, E., Washington, L.C.: On the Distribution of Divisor Class Groups of Curves Over a Finite Field. Théorie des nombres (Quebec. PQ, 1987). de Gruyter, Berlin (1989)
20. Klagsbrun, Z.: The Average Sizes of Two-Torsion Subgroups in Quotients of Class Groups of Cubic Fields. arXiv:1701.02838 [math] (Jan 2017)
21. Klagsbrun, Z: Davenport-Heilbronn Theorems for Quotients of Class Groups. arXiv:1701.02834 [math] (Jan 2017)
22. Lengler, J.: The Cohen-Lenstra heuristic: methodology and results. J. Algebra **323**(10), 2960–2976 (2010)
23. Milne, J.S.: Descent Theory. In Algebraic Geometry, http://www.jmilne.org/math/CourseNotes/ag.html. (2015)
24. Romagny, M., Wewers, S.: Hurwitz spaces. In: Bertrand, D. (ed.), Groupes de Galois Arithmétiques et Différentiels, Séminar Congress, vol. 13, pp. 313–341. Mathematical Society of France, Paris (2006)
25. Serre, J.-P.: Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local. C. R. Acad. Sci. Paris Sér. A-B **286**(22), A1031–A1036 (1978)
26. Taniguchi, T.: A mean value theorem for orders of degree zero divisor class groups of quadratic extensions over a function field. J. Number Theory **109**(2), 197–239 (2004)
27. Taniguchi, T., Thorne, F.: Secondary terms in counting functions for cubic fields. Duke Math. J. **162**(13), 2451–2508 (2013)
28. Wood, M.M.: On the probabilities of local behaviors in abelian field extensions. Compos. Math. **146**(1), 102–128 (2010)
29. Wood, M.M.: Random integral matrices and the Cohen Lenstra heuristics. Am. J. Math. arXiv:1504.04391 [math] (April 2015)
30. Wood, M.M.: The distribution of sandpile groups of random graphs. J. Am. Math. Soc. **30**(4), 915–958 (2017)
31. Wood, M.M.: Nonabelian Cohen-Lenstra moments. Duke Math. J. arXiv:1702.04644 [math] (Feb 2017)